Die Reform des EU-Datenschutzes: Vorwärts zu einem effektiveren und kohärenteren Datenschutz in der EU[1]

Peter Hustinx
Europäischer Datenschutzbeauftragter

Ich möchte Ihnen heute in großen Zügen die begonnene Reform des EU-Datenschutz-Regelwerks schildern. Nach einer kurzen Einführung werde ich auf die Hauptgründe für die Überarbeitung, die Kernelemente des im Januar 2012 vorgelegten Kommissionsvorschlags und die vermutlichen nächsten Schritte des Reformprozesses eingehen.

Im Mittelpunkt meiner Ausführungen steht das Bestreben, einen „effektiveren und kohärenteren" Datenschutz in der EU zu gewährleisten. Der Datenschutz kann seinen Zweck *nur dann* erfüllen, wenn er *in der Praxis* auch tatsächlich angewandt wird, und sein Wert in der Praxis hängt davon ab, welchen *Schutz* er bieten kann. In unserer zunehmend von Technologie bestimmten und globalisierten Welt bleibt uns hier noch einiges zu tun. Das Erfordernis eines effektiveren und kohärenteren Schutzes wird daher in den verschiedenen Abschnitten meiner Ausführungen immer wieder zur Sprache kommen.

Funktion des EDSB

Zunächst einige Worte zur Funktion des Europäischen Datenschutzbeauftragten (EDSB). Der EDSB ist eine unabhängige Behörde, die nichts mit der Europäischen Kommission zu tun hat, gegenüber der Kommission und anderen EU-Organen aber eine Reihe besonderer Aufgaben wahrnimmt. Der EDSB ist eine eigenständige Einrichtung der EU. Seine erste Aufgabe besteht darin, die Kommission und andere EU-Organe zu beaufsichtigen und dafür zu sorgen, dass sich diese bei der Verarbeitung personenbezogener Daten an das EU-Datenschutzrecht halten. Zu

[1] Überarbeitete Fassung eines Vortrags auf dem 5. Schweizer Datenschutzrechtstag am 15. Juni 2012 an der Universität Freiburg (Schweiz). Veröffentlicht in: Astrid Epiney /Tobias Fasnacht (Hrsg./ed.), „Die Entwicklung der europarechtlichen Vorgaben im Bereich des Datenschutzes und Implikationen für die Schweiz" / „Le développement du droit européen en matière de protection des données et ses implications pour la Suisse", Zürich 2012, S. 15-21.

diesem Zweck ist er mit weitreichenden Aufsichts- und Durchführungsbefugnissen ausgestattet.

Als Zweites hat er die Aufgabe, Kommission, Rat und Parlament zu neuen Rechtsvorschriften mit Auswirkungen auf den Datenschutz zu beraten. In manchen Fällen kann er auch beim Gerichtshof beantragen, Verfahren beizutreten und so seine Ansichten zu einer bestimmten Sache vorzutragen, die interessante Datenschutzaspekte aufweist. Auf unserer Website finden Sie zahlreiche Beispiele für solche Fälle. Hier kann sich der EDSB nur auf überzeugende Argumente verlassen.

Dritte Aufgabe ist die Zusammenarbeit mit anderen Datenschutzbehörden, im Wesentlichen auf nationaler Ebene, um den Datenschutz in der EU kohärenter zu gestalten. Auch hier muss der EDSB allein mit Autorität und Diplomatie vorgehen, da alle nationalen Datenschutzbehörden unabhängig sind und der EDSB nur auf EU-Ebene über Zuständigkeiten verfügt. Grundlage für diese Aufgaben ist die Verordnung (EG) Nr. 45/2001, die im Wesentlichen die Datenschutzrichtlinie 95/46/EG auf EU-Ebene umsetzt.

Die Überarbeitung des EU-Datenschutzregelwerks ist ein Thema, das natürlich mit der zweiten und der dritten Aufgabe zu tun hat. Wir sind daher zu den Kommissionsvorschlägen konsultiert worden und haben zusammen mit den Kollegen aus den Mitgliedstaaten immer wieder Kommentare und Feedback an die Kommission gesandt. Auf der Website des EDSB finden Sie nähere Informationen zu diesen Aktivitäten.

EU-Datenschutz

Als Zweites gestatten Sie mir den Hinweis, dass der „Schutz personenbezogener Daten“ ein anderes Konzept als das der „Achtung des Privatlebens“ ist, wie es in Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) verankert ist. Die Kerngrundsätze des Datenschutzes wurden im Datenschutzübereinkommen des Europarates niedergelegt, besser bekannt als Übereinkommen Nr. 108, das von mehr als 40 europäischen Staaten einschließlich der Schweiz ratifiziert wurde. Mit diesem Übereinkommen wurde ein eher proaktiver und systematischer Schutz personenbezogener Daten möglich, denn es gilt grundsätzlich für alle

personenbezogenen Daten, und zwar unabhängig davon, ob auch das Recht auf Schutz der Privatsphäre berührt ist.

Die Grundsätze des Übereinkommens Nr. 108 fanden Eingang in einzelstaatliche Gesetze. Das sich abzeichnende Risiko voneinander abweichender einzelstaatlicher Rechtsvorschriften war für die EU Anlass, sich einzuschalten. Dies führte zur Annahme der Richtlinie 95/46/EG sowie einer Reihe spezifischerer Rechtsinstrumente wie der Richtlinie 2002/58/EG, auch als Datenschutzrichtlinie für elektronische Kommunikation bekannt. 2008 folgte dann als weiterer Schritt die Annahme allgemeiner Vorschriften für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen. Mit anderen Worten: Das EU-Datenschutzregelwerk umfasst mehr Instrumente als nur die Richtlinie 95/46/EG.

Grundrechtecharta und Vertrag von Lissabon

Es sollten zwei weitere Elemente erwähnt werden: erstens die Annahme der Europäischen Charta der Grundrechte im Jahr 2000, die ursprünglich nur als politisches Dokument gedacht war. Sie stützte sich zwar auf die Europäische Menschenrechtskonvention, enthielt aber auch neuartige Elemente wie die Anerkennung eines Rechts auf den Schutz personenbezogener Daten (Artikel 8) neben einem Recht auf Achtung des Privat- und Familienlebens (Artikel 7).

Zweitens Ende 2009 das Inkrafttreten einer Reihe neuer Verträge für die EU (Vertrag von Lissabon), mit dem die Charta ein rechtsverbindliches Dokument wurde, und auch eine horizontale Rechtsgrundlage für den Datenschutz eingeführt wurde, die nicht länger auf die Bedürfnisses des Binnenmarkts Rücksicht nahm, sondern in vollem Umfang dem Charakter des Datenschutzes als einem Grundrecht Rechnung trug, das in einer modernen Informationsgesellschaft ganz besondere Merkmale aufweist (Artikel 16 AEUV). Damit wurde eine sich über fast vier Jahrzehnte erstreckende rechtliche Entwicklung abgeschlossen.

Gründe für die Überarbeitung

Lassen Sie mich nun aber zur derzeitigen Überarbeitung des EU-Datenschutzregelwerks zurückkommen. Warum findet diese Überprüfung überhaupt statt? Hierfür gibt es im Wesentlichen drei Gründe. Der erste ist, dass das aktuelle

Regelwerk – genauer gesagt sein Kernbestandteil, die Richtlinie 95/46/EG – 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 es 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 einzelstaatliches Recht umgesetzt werden muss – so ist es nun einmal bei Richtlinien – und wir nun 27 Fassungen der gleichen Grundprinzipien haben. Das ist schlicht und einfach zu viel und führt zu zusätzlichen Kosten, aber auch zu einem Verlust an Effektivität.

Mit anderen Worten: Wir brauchen mehr Harmonisierung und müssen das System nicht nur stärken und in der Praxis wirksamer machen, sondern auch kohärenter. Dies wird zu einem Abbau von *nicht hilfreicher* Vielfalt und Komplexität führen.

Der dritte Grund hat mit dem neuen Rechtsrahmen der EU zu tun. Im Vertrag von Lissabon haben die Grundrechte großes Gewicht. So enthält unter anderem Artikel 8 der Grundrechtecharta eine Datenschutzbestimmung, und Artikel 16 AEUV enthält eine neue horizontale Rechtsgrundlage für einen umfassenden Schutz in allen Politikbereichen der EU, unabhängig davon, ob es um den Binnenmarkt, Strafverfolgung oder irgendeinen anderen Bereich im öffentlichen Sektor geht.

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

Wenn wir uns nun ansehen, was auf dem Tisch liegt, sehen wir ein Paket aus mindestens zwei Hauptvorschlägen: einer Richtlinie für, kurz gesagt, den Strafverfolgungsbereich und einer unmittelbar anwendbaren Verordnung als Ersatz für die derzeitige Richtlinie 95/46/EG, die für die Privatwirtschaft und den öffentlichen Sektor mit Ausnahme der Strafverfolgung gilt.

Schon diese Architektur deutet darauf hin, dass das Paket nicht wirklich umfassend ist. Betrachtet man es nämlich aus der Nähe, weist das Paket genau hier die größten Schwachstellen auf. Das Schutzniveau in der vorgeschlagenen Richtlinie liegt deutlich unter dem in der vorgeschlagenen Verordnung.

Dies kann für sich allein untersucht werden, doch nimmt der Datenaustausch zwischen öffentlichen und privaten Stellen, etwa zwischen Strafverfolgungsbehörden auf der einen und Banken, Telefon- und Reiseanbietern auf der anderen Seite, ständig zu, und ein Mangel an Ausgewogenheit wird praktische Folgen in einem größeren Bereich haben.

Kontinuität und Wandel

Wenn wir uns jetzt näher mit der Verordnung befassen, sind ein paar wichtige Faktoren zu berücksichtigen.

Erstens: Trotz aller Innovation herrscht weitgehend Kontinuität. Alle Grundkonzepte und Prinzipien, die wir derzeit haben, werden auch weiterhin Bestand haben, wenn auch teilweise klargestellt und weiterentwickelt. Ein Beispiel für Innovation wäre, dass heute mehr Gewicht auf Datenminimierung gelegt wird, d. h., es werden nicht mehr Daten als unbedingt erforderlich verarbeitet. Ein weiteres Beispiel ist die Anerkennung des „eingebauten Datenschutzes“ als allgemeiner Grundsatz.

Bei Innovation geht es in der Hauptsache darum, „den Datenschutz in der Praxis effektiver zu gestalten“. Wie wir noch sehen werden, beinhaltet dies eine starke Betonung der Umsetzung von Grundsätzen und der Durchsetzung von Rechten und Pflichten, um sicherzustellen, dass Schutz in der Praxis besteht.

Die Verordnung strebt aber auch Vereinfachung und Kostensenkung an. Ein deutliches Beispiel hierfür ist, dass die Meldepflicht für Datenverarbeitungen abgeschafft wurde. Sie wird nur noch in Situationen verlangt, die besondere Risiken beinhalten. Ferner sieht die Verordnung eine zentrale Anlaufstelle für Unternehmen mit Niederlassungen in verschiedenen Mitgliedstaaten vor. Dies bringt die Einführung einer federführenden Datenschutzbehörde mit sich.

Eine unmittelbar verbindliche Verordnung bedeutet natürlich auch viel stärkere Harmonisierung (im Prinzip ein einziger, in allen Mitgliedstaaten anwendbarer Rechtsakt) und mehr Kohärenz. Auch dies hat für in mehreren Mitgliedstaaten tätige Unternehmen erhebliche Vereinfachungen und Kostensenkungen zur Folge.

Allgemeine Anwendbarkeit

Lassen Sie mich unterstreichen, dass die vorgeschlagene Verordnung einen weit gefassten Anwendungsbereich hat: Sie findet sowohl auf den privaten als auch auf den öffentlichen Sektor Anwendung. Dies entspricht völlig der Situation, wie wir sie im Zusammenhang mit der Richtlinie 95/46/EG kennen. Die Möglichkeit einer systematischen Unterscheidung in dieser Richtlinie zwischen öffentlichem und privatem Sektor wurde seinerzeit ausdrücklich erwogen, dann aber verworfen.

Der umfassende Ansatz der derzeitigen Richtlinie war machbar, weil einige ihrer Bestimmungen über öffentliche Aufgaben eher für öffentliche Einrichtungen von Bedeutung sind, während andere Bestimmungen, in denen es um Verträge oder berechtigte Interessen geht, eher für private Akteure von Belang sind.

In seinem Urteil in der Rechtssache *Rechnungshof* (Mai 2003) hat der EuGH deutlich erklärt, dass die Richtlinie auch auf den öffentlichen Sektor eines Mitgliedstaats anwendbar ist. Er unterstrich aber auch, dass einzelstaatliches Recht nur dann als Rechtsgrundlage für eine Verarbeitung dienen kann, wenn es im Einklang mit den Grundrechten steht.

Verstärkt wird dies noch durch die Tatsache, dass Artikel 8 der EU-Charta nunmehr auch das Recht auf den Schutz personenbezogener Daten ausdrücklich anerkennt und dass Artikel 16 AEUV eine ausdrückliche horizontale Rechtsgrundlage für die

Annahme von Vorschriften über den Schutz personenbezogener Daten sowohl auf EU-Ebene als auch in den Mitgliedstaaten im Rahmen von Tätigkeiten vorsieht, die in den Anwendungsbereich des Unionsrechts fallen.

Zur gleichen Zeit ist aber auch eine sehr viel gründlichere Analyse des Verhältnisses zwischen EU-Recht und einzelstaatlichem Recht auf der Grundlage der vorgeschlagenen Verordnung erforderlich. Es trügt der Eindruck, die Verordnung werde einfach an die Stelle der einschlägigen nationalen Rechtsvorschriften treten. Es gibt mindestens vier unterschiedliche Wege, auf denen einzelstaatliches und Unionsrecht nebeneinander existieren und in Wechselwirkung miteinander stehen werden. Dazu gehört auch die Tatsache, dass sich die Verordnung genauso auf einzelstaatliches Recht stützen wird, wie es in der Rechtssache *Rechnungshof* der Fall war. Es könnte durchaus sein, dass noch mehr Raum für eine noch bessere Interaktion zwischen EU-Recht und einzelstaatlichem Recht benötigt wird.

Inhaltlich stärkt die Verordnung die Rollen der wichtigsten Akteure, also der betroffenen Person, der verantwortlichen Organisation und der Aufsichtsbehörden.

Nutzerkontrolle

Als Erstes könnte man von einer Stärkung der Nutzerkontrolle sprechen. Die bestehenden Rechte der betroffenen Person wurden insgesamt bestätigt und sogar noch gestärkt und ausgeweitet.

Das Erfordernis der Einwilligung wurde klargestellt. *Wenn* eine Einwilligung erforderlich ist, muss sie echt und belastbar sein. Auch das Recht auf Einspruch wurde gestärkt. Es stehen bessere Mittel zur Verfügung, mit denen sich die Wahrung der Rechte der betroffenen Person in der Praxis gewährleisten lässt. Der Transparenz wurde größeres Gewicht beigemessen. Es gibt eine Bestimmung, die kollektive Rechtsbehelfe einführt, nicht im Sinne einer Sammelklage nach US-Art, aber doch für Organisationen, die im Namen ihrer Mitglieder oder ihrer Klientel tätig werden.

Es wird viel über das „Recht, vergessen zu werden“ geredet, doch wird bei näherer Betrachtung klar, dass hier nur betont wird, dass Daten zu löschen sind, sobald kein hinreichender Grund mehr für ihre Aufbewahrung besteht. Das Recht auf

Datenübertragbarkeit ist im Grunde auch nur eine genauere Fassung des bestehenden Rechts, eine Kopie der über eine Person gespeicherten Daten verlangen zu können, und zwar in einem bestimmten Format.

Verantwortlichkeit

Das größte Augenmerk liegt jedoch auf einer echten Übernahme von Verantwortung durch verantwortliche Organisationen. Verantwortlichkeit ist kein Konzept, das erst greift, wenn es zu spät ist, wenn also etwas schiefgelaufen ist. Stattdessen ist es eine Verpflichtung, in der Praxis ein gutes Datenmanagement zu entwickeln. Dies zeigt sich an Formulierungen wie etwa die, dass *durch geeignete Maßnahmen sichergestellt wird, dass die Bestimmungen der Verordnung eingehalten werden* und *dass die Wirksamkeit dieser Maßnahmen zu überprüfen und der Nachweis dafür zu erbringen ist*.

Hier haben sich die Akzente deutlich verschoben. Daran wird auch deutlich, dass die Beweislast in vielen Fällen bei der verantwortlichen Organisation liegt, die zeigen können muss, dass es eine angemessene Rechtsgrundlage gibt, dass Einwilligungen wirksam erteilt wurden und dass ergriffene Maßnahmen auch weiterhin effektiv sind.

Die Verordnung beinhaltet ferner einige spezifische Anforderungen, etwa für Datenschutzfolgenabschätzungen, die Dokumentation der Datenverarbeitung und die Ernennung eines behördlichen oder betrieblichen Datenschutzbeauftragten. Einige dieser Anforderungen, insbesondere zur Dokumentation, sind meiner Ansicht nach zu detailliert und müssten geändert werden, um sie angemessener zu gestalten. Einige der in den Bestimmungen aufgeführten Ausnahmen sind möglicherweise nicht ganz gerechtfertigt. Mehr Ausgewogenheit in diesem Teil des Vorschlags könnte beide Probleme auf einen Schlag lösen.

Darüber hinaus wurde eine allgemeine Bestimmung zur Meldung von Sicherheitsverletzungen eingeführt. Im Moment gibt es eine solche Verpflichtung im EU-Recht nur für Telekommunikationsanbieter.

Aufsicht und Durchsetzung

Ein dritter Schwerpunkt der Verordnung ist der Bedarf an effektiverer Aufsicht und Durchsetzung. Die Garantien für die völlige Unabhängigkeit von Datenschutzbehörden wurden in voller Übereinstimmung mit dem Urteil des EuGH in der Rechtssache *Kommission gegen Deutschland* gestärkt.

Die Verordnung sieht auch in allen Mitgliedstaaten Aufsichtsbehörden mit starken Durchsetzungsbefugnissen vor. Bußgelder in Millionenhöhe – von der gleichen Größenordnung wie im Wettbewerbsrecht – ziehen viel Aufmerksamkeit auf sich, aber die Botschaft, die damit vermittelt werden soll, ist folgende: Wenn das hier wichtig ist, soll entsprechend damit umgegangen werden. Dies wird dazu führen, dass der „Datenschutz" in den Chefetagen auf der Tagesordnung nach oben rückt, was zu begrüßen wäre.

Aus der Nähe betrachtet verfügt die Durchsetzung über schärfere Waffen, wie Abhilfemaßnahmen, Bußgelder und in einigen Fällen verstärkte zivilrechtliche Haftung.

Auch die internationale Zusammenarbeit zwischen Datenschutzbehörden wird deutlich gefördert und erleichtert. Die Einführung einer „federführenden Behörde" für Unternehmen mit mehreren Niederlassungen ist eine gute Idee, aber diese Behörde wird nicht alleine handeln, sondern *de facto* Teil eines eng zusammenarbeitenden Netzwerks mit anderen zuständigen Behörden sein.

Von großer Bedeutung ist die Einführung eines Kohärenzverfahrens im Rahmen des Europäischen Datenschutzausschusses, der auf der derzeitigen Gruppe von Datenschutzbehörden („Artikel 29-Datenschutzgruppe") aufbauen wird. Dieses Verfahren soll kohärente Ergebnisse der Aufsichts- und Durchführungsaktivitäten in den Mitgliedstaaten gewährleisten. Seine Sekretariatsgeschäfte werden vom EDSB wahrgenommen.

Datenschutz weltweit

Ein letztes Element ist die internationale Dimension der Verordnung im weiteren Sinn, und das in zweierlei Hinsicht. Der Anwendungsbereich der Verordnung wurde

klargestellt und ausgeweitet. Diese Bestimmungen werden nunmehr nicht nur auf alle Datenverarbeitungen einer Niederlassung in der EU anwendbar sein, sondern auch, wenn Waren oder Dienstleistungen von einem Drittland auf den europäischen Markt geliefert oder dort erbracht werden oder wenn das Verhalten von Europäern online überwacht wird.

Das ist heutzutage im Internet Realität. Gleichzeitig ist es ein realistischer Ansatz, der auf einer wachsenden Konvergenz bei den Ansichten über Datenschutz weltweit aufbaut.

Bezüglich anderer internationaler Aspekte wurden die Bestimmungen über grenzüberschreitende Datenströme erweitert und in gewisser Weise gestrafft und vereinfacht. Es gibt nun eine spezifische Bestimmung zu verbindlichen unternehmensinternen Vorschriften, die ebenfalls eine Reihe von Vereinfachungen mit sich bringt.

Lassen Sie mich an dieser Stelle noch erwähnen, dass sich die internationale Zusammenarbeit zwischen Datenschutzbehörden – z. B. zwischen der Federal Trade Commission in den USA und Datenschutzbehörden in der EU – mit einem weltweiten Netz (GPEN) auch in einem breiteren Kontext weiterentwickelt. Damit wird es möglich sein, besser mit globalen Akteuren im Internet umzugehen. Grundlage ist weiter eine weltweit wachsende Übereinstimmung von Datenschutzgrundsätzen und -praxis.

Schlussbemerkungen

Zusammenfassend kann ich sagen, dass es sich meiner Auffassung nach – vorbehaltlich gewisser Änderungen bei einigen wichtigen Elementen – um einen durchaus begrüßenswerten Vorschlag handelt.

Abgesehen vom derzeit bestehenden Mangel an Ausgewogenheit zwischen der Verordnung und der Richtlinie für die Strafverfolgung gilt dies auch für den möglichen Bedarf an mehr Raum für mehr Interaktion zwischen EU-Recht und nationalem Recht sowie für ein eventuelles Überdenken einiger der derzeitigen Ausnahmen, einschließlich der für kleine und mittelständische Unternehmen. In

meinen Augen ist es *essenziell*, dass allgemeine Bestimmungen grundsätzlich *skalierbar* sind. Unangemessene Detailbestimmungen können hingegen zu unnötigen Ausnahmen führen.

Abschließend noch eine Anmerkung zum Verfahren: Im Moment finden die Erörterungen in Rat und Parlament statt. Sie werden nicht nur ein paar Monate dauern. Ich vermute, dass erste Schlussfolgerungen im Laufe des nächsten Jahres vorliegen werden, möglicherweise unter irischem Vorsitz.

Ich würde sagen: Die Chancen stehen gut, dass der Hauptvorschlag auf jeden Fall bis 2014 angenommen wird. Und ich gehe auch davon aus, dass die Verordnung, natürlich mit einigen notwendigen Änderungen, angenommen werden wird.