Manfred Weber

Mitglied des Europäischen Parlaments

Stellvertretender Vorsitzender der EVP-Fraktion

Niederbayerns Stimme in Europa

Thema	**Europäischer Datenschutz unter Lissabon - Europäisches Parlament als Wächter** **Vortrag anlässlich des 5. Europäischen Datenschutztages am 28. Januar 2011 in Berlin**

Neue Voraussetzungen für den europäischen Datenschutz

Mit Inkrafttreten des Vertrags von Lissabon wurde eine neue Epoche europäischer Politik eingeleitet. Vielfach wurde in der Vergangenheit kritisiert, dass das einzige direkt vom Volk legitimierte Organ auf europäischer Ebene nicht ausreichend Einflussmöglichkeiten habe. Die mit dem Vertrag von Lissabon einhergehende Kompetenzerweiterung des Europäischen Parlaments wirkt sich nun maßgeblich auf die Bewältigung neuer Herausforderungen aus. Das neue Vertragswerk hat auch Auswirkungen auf die rechtlichen Rahmenbedingungen für den Datenschutz in der Europäischen Union. Artikel 16 des Vertrages über die Arbeitsweise der Europäischen Union bildet das Fundament für einheitliche datenschutzrechtliche Regelungen. Die Charta der Grundrechte ist zwar kein Bestandteil der EU-Verträge, erhält jedoch dieselbe Rechtsverbindlichkeit. Neben klassischen Bürgerrechten wie Meinungs-, Rede- und Versammlungsfreiheit beinhaltet sie auch "modernere" Rechte, beispielsweise Rechte von Kindern, das Recht auf sichere und würdige Arbeitsbedingungen und eben auch den Schutz personenbezogener Daten. In Artikel 8 der Charta werden einschlägige Datenschutzprinzipien wie Recht auf Auskunft und Berichtigung sowie die Zweckgebundenheit bei der Datenverarbeitung genannt. Bürger, die sich durch EU-Rechtsvorschriften in ihrem Grundrecht auf Datenschutz verletzt sehen, können sich auf die Charta berufen. Das Europäische Parlament unterstrich seine Funktion als Bürgerkammer und die Bedeutung der Charta, indem es durchsetzte, dass diese während der Plenartagung im Dezember 2007 von den Präsidenten des Parlaments, des Rates und der Kommission feierlich proklamiert wurde. Dieses Bürgerrecht eines umfassenden Datenschutzes in Kombination mit effektivem Datenaustausch ist und wird auch künftig eine große Herausforderung sein.

Der internationale Terrorismus, die organisierte Kriminalität sowie modernste Kommunikationsmittel erfordern im Bereich des Datenaustauschs eine immer engere internationale Kooperation. Es wird deutlich, dass angesichts dieser weltweiten Dimension die Nationalstaaten nur bedingt in der Lage sind, für ihre Bürger effiziente und praktikable Lösungen zu fin-

den. Die Koordinierung innerhalb Europas hat für entsprechende internationale Verhandlungen daher zum Teil die Europäische Union übernommen. Im Folgenden soll dargelegt werden, mit welchen Lösungsansätzen die Europäische Union an verschiedene Interessenskonflikte herangeht.

Transatlantischer Datenaustausch

SWIFT

Datenschutz gerät besonders dann ins Zentrum der öffentlichen Aufmerksamkeit, wenn Datenmaterial mit Drittstaaten ausgetauscht wird. An erster Stelle sind hier die transatlantischen Beziehungen, insbesondere mit den Vereinigten Staaten zu nennen. Die Nutzung personenbezogener Daten europäischer Bürger durch US-amerikanische Strafverfolgungsbehörden ist insofern problematisch, da das amerikanische Verständnis von Privatsphäre und Datenschutz auf vollkommen anderen Stützen steht als das europäische und beide Systeme nicht direkt miteinander zu vergleichen sind. Die Forderung "Europäische Datenschutzstandards für europäische Bürger!" war immer die zentrale Forderung des Europäischen Parlaments, lässt sich jedoch nur schwer umsetzen, z.B. auch vor dem Hintergrund, dass derzeit EU-Bürgern nicht dieselben Klagemöglichkeiten vor US-Gerichten zur Verfügung stehen wie vor europäischen Gerichten.

Aufmerksamkeit erregte das Europäische Parlament im Februar 2010, als es das zur Abstimmung stehende SWIFT-Übergangsabkommen zwischen der EU und den USA aufgrund gravierender datenschutzrechtlicher Lücken und unzureichender inhaltlicher Qualität ablehnte. Die Kommission war daraufhin gezwungen, ein besseres Abkommen auszuhandeln, in dem sich eindeutige europäische Datenschutzstandards wiederfinden. In seiner Resolution zum neuen Verhandlungsmandat hat das europäische Parlament seine Erwartungen und Bedingungen zu einer Zustimmung klar definiert. Das neu verhandelte Abkommen stellt ein insgesamt zufriedenstellendes Ergebnis dar. Deutliche Fortschritte konnten bei der Einschränkung des Umfangs der übermittelten Datenpakete, bei der Weitergabe von Informationen aus der Datenanalyse an Drittstaaten, bei Rechtsbehelfsmöglichkeiten für EU-Bürger sowie bei der Kontrolle der Datenextraktion auf US-Territorium durch EUROPOL erreicht werden. Die Europäische Kommission hat während der Verhandlungen zahlreiche Bedenken des Europäischen Parlaments aufgegriffen und dadurch Verbesserungen erreicht. Auch der Rat ist dem Parlament bei abschließenden Gesprächen weit entgegen gekommen.

Was wir noch verbessern müssen ist das Reporting für die Anwendung des Abkommens. Wie das Abkommen in der Praxis tatsächlich angewandt wird und worin sein praktischer Mehrgewinn in der Terrorismusbekämpfung für die EU besteht, sind entsprechende Fragen. Erwähnenswert ist, dass die Vereinigten Staaten und Europol besondere Arbeitsmodalitäten

vereinbart haben, die die Bearbeitung der Anfragen durch das US-Finanzministerium regeln: Zum Zwecke der Überwachung der Datenextraktion wird Europol eine eigene Abteilung einrichten, die der Überwachung des Datenschutzbeauftragen der Agentur untersteht. Dieser soll die Vereinbarkeit mit den anzuwendenden rechtlichen Rahmenbedingungen zum Datenschutz gewährleisten, wann immer sich Anfragen des US-Finanzministeriums auf identifizierte Individuen beziehen. Für April 2011 ist eine erste gemeinsame Evaluierung der Anwendung des Abkommens vorgesehen, die genauere Auskünfte darüber geben wird, ob alle Bestimmungen erfüllt werden. Vorbereitungen zum Aufbau eines eigenen EU-TFTP wurden bereits eingeleitet. Vor dem Hintergrund einer Folgenabschätzung konnten bereits Konzeptideen mit verschiedenen Stakeholdern ausgetauscht werden.

PNR-Abkommen EU-USA

Die Verhandlungen zu einem Abkommen zum Austausch von Fluggastdaten zwischen dem US-Heimatschutzministerium und der Europäischen Kommission sind seit Dezember 2010 in Gange. Während der ersten Verhandlungsrunde stellte sich heraus, dass die USA beabsichtigen, das Abkommen auch auf die Bereiche "Einwanderung" und "Zoll" auszudehnen sowie die Datenabfrage auf Basis eines Pull-Systems zu gestalten. Die Erwartungen der EU, dass die PNR-Daten der Überwachung einer unabhängigen Datenschutz-Behörde unterstehen, wurden bisher dahingehend enttäuscht, dass die USA die Unabhängigkeit dieser Behörde nur bis zu einem gewissen Grad garantieren möchten. Auch hinsichtlich einer Reduzierung der zu übermittelnden Datenkategorien zeigen sich die USA bisher nur wenig verhandlungsbereit. Auch bei den verschiedenen Rechtsbehelfsmöglichkeiten sowie der Speicherdauer (derzeit 15 Jahre) gibt es noch Gesprächsbedarf. Dem Ehrgeiz der EU wird dies nicht gerecht. Bei der Aushandlung des Abkommens müssen unbedingt bessere Datenschutzvorschriften, verkürzte Speicherdauern und bessere Klagemöglichkeiten für EU-Bürger erreicht werden.

Datenschutzrahmenabkommen EU-US

Zur großen Enttäuschung der EU sind die USA nicht bereit, die Verhandlungen für ein allgemeines Datenschutzrahmenabkommen zu eröffnen, das den transatlantischen Beziehungen langfristig Rechtssicherheit, Stabilität und hohe Datenschutzstandards bei der Rechtsdurchsetzung gewähren würde. Bei einem Treffen vergangenen Dezember wurden von US-Seite lediglich Sondierungsgespräche angeboten, die den Mehrwert eines solchen Abkommens hinterfragten. Angesichts der umfassenden Vorbereitungsarbeit durch die hochrangige EU-US-Kontaktgruppe für das Datenschutzrahmenabkommen und das durch den Ministerrat im Dezember 2010 erteilte Verhandlungsmandat für die Europäische Kommission stünde den Verhandlungseröffnungen eigentlich nichts im Wege.

EU-interne Dimension des Datenschutzes

Aber auch in ihrer inneren Dimension muss die EU einen Weg finden, wie sie ihre Datenschutzprinzipien weiterhin aufrechterhalten kann. Die Datenschutzrichtlinie von 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr verlieh zwei grundlegenden Zielen des europäischen Integrationsprozesses Ausdruck: dem Grundrecht auf Datenschutz sowie dem freien Verkehr personenbezogener Daten, was zur Vollendung des Binnenmarkts beitrug. Diese Prinzipien sowie die Grundsätze der Richtlinie haben weiterhin Bestand, allerdings muss der Datenschutz den sich stetig ändernden Rahmenbedingungen angepasst werden. Im Folgenden möchte ich auf einige Punkte eingehen, die Gegenstand einer Überarbeitung werden könnten.

Rechte des Einzelnen

Beispielsweise sind die Vorschriften über die Informationen, die dem von der Verarbeitung Betroffenen mitgeteilt werden müssen, nicht mehr ausreichend. Transparenz ist jedoch eine Basis dafür, um Kontrolle über die eigenen personenbezogenen Daten zu bewahren. Gerade in der Online-Umgebung ist es von Bedeutung, dass Informationen auf einfachem Wege zugänglich und verständlich formuliert sind. Die Europäische Kommission zieht daher die Einführung eines allgemeinen Transparenztheorems für die Verarbeitung personenbezogener Daten in Erwägung. Hinzu kommt die Festlegung von Pflichten bezüglich Art und Bereitstellung von Informationen, die von den Verantwortlichen berücksichtigt werden müssen. Hierbei muss auch eine benutzerangemessene Lösung für Kinder gefunden werden, die sich der Konsequenzen der Verarbeitung ihrer Daten weniger bewusst sind. Auch hinsichtlich Datenschutzverstöße prüft die Kommission die Einführung einer allgemeinen Anzeigepflicht.

Im Zeitalter der sozialen Netzwerke im Internet wird sichtbar, dass bestehende Rechte in der Praxis nicht einheitlich geregelt sind oder die Gewährleistung von Rechten sich als immer komplizierter darstellt. Beispielsweise werden Daten häufig ohne Kenntnis und Genehmigung des Nutzers gespeichert oder die Betroffenen können von ihrem Recht auf Zugang zu ihren Daten, auf deren Korrektur oder Löschung nicht Gebrauch machen. Die Kommission plant daher, das Prinzip der Datensparsamkeit - also die Verarbeitung von Daten nur zu ganz bestimmten Zwecken - zu stärken und Modalitäten für die Wahrnehmung der Rechte auf Zugang zu Daten sowie auf deren Korrektur und Löschung zu verbessern. Auch das "Recht auf Vergessen", d.h. die Löschung der Daten, wenn sie nicht mehr für einen rechtmäßigen Zweck gebraucht werden, sollte aus sicht der EVP klarer umrissen werden. Hierbei ist allerdings fraglich, wie diese Anforderung überhaupt technisch zu erfüllen ist. Auch für Fälle, in denen ein solches Recht auf Vergessen mit anderen legitimen Interessen, z.B. bei

der Strafverfolgung oder bei der Aufzeichnung geschäftlicher Transaktionen kollidiert, muss noch eine Lösung gefunden werden. Weiterhin wird erwogen, die Rechte des Einzelnen auszudehnen, was die Datenübertragbarkeit anbetrifft. Hierunter versteht man das Zurückholen und anschließende Übertragen derselben Daten auf eine andere Anwendung oder einen anderen Dienst. Allerdings muss hier geprüft werden, ob dieses Ziel tatsächlich ausschließlich durch neue legislative Maßnahmen erreicht werden kann oder ob nicht eher selbstregulierende Anstrengungen verfolgt werden könnten.

Nachbesserungsbedarf gibt es zudem beim Schutz sensiblen Datenmaterials. Daten, die beispielsweise Rückschlüsse auf rassische Herkunft, politische Meinungen sowie über den Gesundheitszustand zulassen, dürfen mit wenigen Ausnahmen im Allgemeinen nicht verarbeitet werden. Kontrolliert werden muss aber, ob diese Schutzbestimmungen nun auf andere Datenkategorien übertragen werden müssen, beispielsweise auch auf Gendaten. Darüber hinaus muss erwogen werden, ob die Bedingungen für die Zulassung und Verarbeitung bestimmter Kategorien sensibler Daten präzisiert und vereinheitlicht werden sollte.

Zur Durchsetzung der Datenschutzvorschriften sind wirksame Bestimmungen über Rechtsbehelfe und Sanktionen nötig. Die Kommission prüft, inwiefern derzeit existierende Sanktionsbestimmungen verschärft werden sollen. Ebenso untersucht sie, ob auch Datenschutzbehörden, Verbänden der Zivilgesellschaft sowie Verbänden, die die Interessen der Betroffenen vertreten, vor nationalen Gerichten zur Klage befugt sind. Was ein solches Klagerecht für Dritte anbetrifft, sollte aber erst der Beweis erbracht werden, dass bestehende Klagemöglichkeiten tatsächlich unzureichend sind. Auch stellt man in der EVP die Frage, warum Dritte klagen dürfen, wo es sich doch beim Datenschutz um ein individuelles Recht handelt. Auch das Einschreiten der Datenschutzbehörden als "Anwälte der Öffentlichkeit" bei Fragen öffentlicher oder privater Datenkontrolle ist zu hinterfragen.

Die Kommission ist der Ansicht, dass die Pflichten der für die Verarbeitung Verantwortlichen stärker rechtlich verankert werden müssen. Hierbei sind auch Bestimmungen über interne Kontrollverfahren, die die Kooperation mit Datenschutzbehörden sowie die Benennung von Datenschutzbeauftragten in Unternehmen vorsehen. Von Datenschutzbehörden wird in diesem Zusammenhang immer öfter der Begriff der "accountability" vorgebracht, den auch die Kommission aufgreift. Hierbei bedarf es aus Sicht der EVP allerdings noch begrifflicher und konzeptueller Präzisierung, um Missinterpretationen zu vermeiden. Sollte dieser Rechenschaftsgrundsatz in der Praxis wie eine Beweislastumkehr funktionieren - z.B. dass ein Unternehmen beweisen muss, dass es nicht gegen Datenschutzbestimmungen verstößt - ist zu beachten, dass der Verwaltungsaufwand für Unternehmen und insbesondere für KMU so gering wie möglich gehalten wird. Bei der Einsetzung von Technologien zum Schutz der Privatsphäre könnte in Zukunft das Konzept des "Privacy by Design", also Technologien mit eingebautem Datenschutz zur Anwendung kommen. Auch dieses Konzept muss aber noch

klarer umrissen werden und darf nicht Gefahr laufen, der technologischen Neutralität entgegenzustehen.

Polizeiliche und justizielle Zusammenarbeit

Der Schutz personenbezogener Daten muss in sämtlichen Politikbereichen gewahrt werden, auch bei Strafverfolgung und Kriminalitätsprävention, auf deren Besonderheiten Rücksicht genommen werden muss. Die Kommission wird erwägen, diesen Bereich in den Anwendungsbereich der allgemeinen Datenschutzbestimmungen einzubeziehen, auch wenn die Daten ausschließlich innerhalb eines Mitgliedstaates verarbeitet werden sollten. Parallel könnten aber gewisse Datenschutzprinzipien von Individuen beschnitten werden, beispielsweise das Zugriffsrecht oder das Transparenzprinzip. Denkbar ist auch, dass die Novellierung Sonderbestimmungen zur Verarbeitungen von Gendaten zu strafrechtlichen Zwecken beinhalten wird, ebenso wie spezifische Vorschriften für bestimmte Gruppen von Betroffenen wie Zeugen oder Verdächtige. Um eine effektive und kohärente Datenschutzkontrolle in Institutionen, Behörden und Agenturen der EU zu garantieren, werden involvierte Kreise im Rahmen einer Konsultation gebeten, ihre Sicht zur Änderung des gegenwärtigen Kontrollsystems im Bereich der polizeilichen und justiziellen Zusammenarbeit darzulegen. Ebenfalls steht zur Debatte, ob die für diesen Bereich sektorspezifischen EU-Vorschriften an die überarbeiteten Datenschutzbestimmungen angepasst werden sollten.

Globale Dimension

Die Übermittlung personenbezogener Daten in Drittstaaten ist nach einer Angemessenheitsprüfung generell möglich. Jedoch sind die Bedingungen für die Anerkennung eines angemessenen Datenschutzniveaus eines Drittlandes oder einer internationalen Organisation in der bisherigen Richtlinie nicht ausreichend geregelt. Für eine hinreichende Bewertung muss daher die Angemessenheitsprüfung noch präzisiert werden. Zudem werden in internationalen Abkommen häufig bestimmte Datenschutzbestimmungen festgelegt, was u.U. zu einer Inkohärenz für die Rechte der Betroffenen führen kann. Die Kommission hält aus diesem Grund die Erarbeitung genereller Datenschutzprinzipien für den internationalen Datenaustausch für unerlässlich. Zur Aufhebung der ermittelten Probleme wird folglich untersucht, inwieweit die gegenwärtigen Verfahren einschließlich rechtsverbindlicher Instrumente und konzerninterner Vorschriften für den internationalen Datenaustausch besser abgestimmt werden können und worin wesentliche Elemente des Datenschutzes bestehen, die auf sämtliche Übereinkommen übertragen werden können.

Fazit

Die Europäische Volkspartei im Europäischen Parlament unterstützt eine Überarbeitung der Datenschutzprinzipien, woraus sich einschlägige Folgen für unsere moderne, informationsbetriebene Gesellschaft ergeben werden. Während sich das alte Regelwerk auf die Prinzipien des Binnenmarkts konzentrierte, müssen nun die Grundrechte im Fokus stehen. Der Gesetzgeber wird mit der Überarbeitung der Datenschutzrichtlinie vor die komplizierte Aufgabe gestellt, einen Rechtsakt zu schaffen, der trotz der verschiedensten Veränderungen der Datenübermittlung und -verwendung zumindest mittelfristig Bestand haben muss. Neben der Herausforderung, unterschiedlichste, oft sogar konkurrierende Interessen und auch Grundrechte in einem unfassenden und allgemeinen Regelwerk zu berücksichtigen, muss Rechtssicherheit darüber bestehen, welches Recht und welche Standards nationale Behörden durchsetzen müssen und wonach die Entwicklung neuer und neutraler Technologien auszurichten ist. Das Ergebnis muss ein flexibler Mechanismus sein, der nicht zu sektorspezifisch ausgerichtet ist und der den Mitgliedstaaten Freiräume bei der Umsetzung gewährt. Bei der geplanten Einführung neuer Maßnahmen, etwa von Datenschutzzertifikaten ist genau zu bewerten, ob hierfür wirklich eine Nachfrage besteht. Künftig wird auch zu prüfen sein, inwiefern andere Gesetze und sektorspezifische Regelungen an die überarbeiteten generellen Datenschutzprinzipien angepasst werden müssen. Was die künftige Rolle der Datenschutzbehörden anbelangt, so ist entscheidend, dass sie untereinander kooperieren und sich abstimmen, besonders dann, wenn mehr als eine Rechtssprechung involviert ist. Auch sollten Anpassungskosten und Verwaltungsaufwand für grenzüberschreitend tätige Bürger und Unternehmen zudem verringert werden oder so gering wie möglich ausfallen.

Gelingt es der EU, in ihrer internen Dimension wirksame und harmonisierte Datenschutzstandards zu etablieren, so ist dies der erste Schritt, dem europäischen Datenschutzniveau auch global zu seiner Durchsetzung zu verhelfen.