EUROPÄISCHES PARLAMENT 2009 - 2014

Ausschuss für bürgerliche Freiheiten, Justiz und Inneres

8.10.2012

ARBEITSDOKUMENT 2

über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und den freien Datenverkehr (Datenschutz-Grundverordnung)

Ausschuss für bürgerliche Freiheiten, Justiz und Inneres

Berichterstatter: Jan Philipp Albrecht

1. Stärkung des europäischen Datenschutzsystems: Ergriffene Maßnahmen und Ausblick

Die Debatte über die von der Kommission im Januar 2012 vorgeschlagene neue Datenschutzregelung hat bei den Organen der EU in den Mitgliedstaaten Fortschritte gemacht. Wie die beiden Berichterstatter für die Verordnung bzw. die Richtlinie in ihrem ersten Arbeitsdokument[1] deutlich gemacht haben, werden in dem Reformpaket die Empfehlungen des Parlaments weitgehend übernommen, und zwar a) die Entscheidung für ein Gesamtkonzept, b) die Stärkung der Rechte des Einzelnen, c) die weitere Stärkung der Binnenmarktdimension und d) die Stärkung der weltweiten Dimension. Zu betonen ist, dass der Datenschutz inzwischen ein bindendes Grundrecht aufgrund von Artikel 8 der Charta der Grundrechte ist und in Artikel 16 AEUV eine besondere Rechtsgrundlage hat. Deshalb sollten wir den Schutz von Verbrauchern und Bürgern („betroffenen Personen") im Zeitalter der Digitalisierung und der Globalisierung stärken.

Debatten über Themen wie delegierte Rechtsakte und Durchführungsrechtsakte, Verwaltungsaufwand und das „Kohärenzverfahren" sind bei allen Organen noch im Gang. Der Ratsvorsitz hat den Mechanismus „Freunde des Vorsitzes" zwecks Erörterung solcher horizontaler Themen eingeleitet, und das Parlament wird in der jährlichen Sitzung des Ausschusses für bürgerlichte Freiheiten, Justiz und Inneres (LIBE) am 9./10. Oktober 2012 Sachverständige anhören und mit Interessenträgern diskutieren. Die Vorlage des Entwurfs eines Berichts über die Verordnung wird für Ende 2012 vorgesehen, und im Anschluss daran wird eine großzügige Frist gesetzt, durch die die Mitglieder ihre Änderungsanträge rechtzeitig einreichen können (Ende Februar 2013), und eine orientierende Abstimmung ist für April 2013 vorgesehen, sodass die Verhandlungen in der Zeit des irischen Ratsvorsitzes beginnen können. Die mitberatenden Ausschüsse planen ihre Arbeit entsprechend. Wegen der dringenden Notwendigkeit eines kohärenten Rechtsrahmens in diesem sich rasch fortentwickelnden Umfeld sind der Berichterstatter und die Schattenberichterstatter bestrebt, in dieser Wahlperiode Einigung mit dem Rat über das Paket zu erzielen.

Nach viermaligem Meinungsaustausch im Ausschuss, bei einem Workshop des Ausschusses mit Interessenträgern sowie in umfangreichen Beratungen mit den Schattenberichterstattern, den mitberatenden Ausschüssen, der Kommission, dem Ratsvorsitz und Interessenträgern legt der Berichterstatter hiermit gezieltere Textvorschläge und Bewertungen vor. In diesem Stadium ist es nicht möglich, eine endgültige Antwort auf alle relevanten Fragen zu geben. In Bezug auf den Berichtsentwurf lassen sich allerdings Grundsätze darlegen, die als Anleitung dienen können. Sie beruhen auf der bisherigen Datenschutzrichtlinie[2] und werden aus der Entschließung des Parlaments vom 6. Juli 2011 (Bericht Voss)[3] deutlich. Dem Berichterstatter wäre an einem Konsens bezüglich der nachstehend genannten Eckpfeiler des Berichtsentwurfs gelegen. In diesem Arbeitsdokument werden inhaltliche Aspekte dargelegt, und die institutionellen Aspekte werden im Arbeitsdokument 3 behandelt.

2. Stärkung wesentlicher Grundsätze und Klärung von Definitionen

[1] PE491.322v01-00, 6. Juli 2012.
[2] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, S. 31 bis 50.
[3] Angenommene Texte, P7_TA(2011)0323, 6 . Juli 2011.

Die Definitionen der Begriffe „personenbezogene Daten“ und „betroffene Person“ sind von entscheidender Bedeutung, weil sie den Geltungsbereich und die konkrete Anwendung der in der Verordnung vorgesehenen Garantien für die verschiedenen Arten der Verarbeitung personenbezogener Daten festlegen. In diesem Sinn sollte der materielle Geltungsbereich der Verordnung der gleiche sein wie bei der geltenden Richtlinie 95/46/EG. Weil im Rechtsrahmen für den Datenschutz ein Grundrecht zum Ausdruck kommt, liegt eine Beschränkung des materiellen Geltungsbereichs nicht in der Hand des Gesetzgebers. Allerdings können berechtigte Anliegen, die einzelne Geschäftsmodelle betreffen, an anderen Stellen im Verordnungstext angemessen zur Geltung gebracht werden.

Um das optimale Datenschutzniveau zu erreichen und neue Geschäftsmodelle zu ermöglichen, müssen wir die Nutzung von Dienstleistungen mit pseudonymisierten und anonymisierten Daten fördern. Die deutliche Definition des Begriffs „Anonymität“ dürfte den für Verarbeitung Verantwortlichen auch helfen zu wissen, wann sie vom Geltungsbereich der Verordnung ausgenommen sind. Was die Verwendung pseudonymisierter Daten – in dem Sinn, dass der für die Verarbeitung Verantwortliche einzelne Personen mittels eines Pseudonyms von anderen trennen kann – betrifft, könnte es Erleichterungen geben, die sich auf die Pflichten des Verantwortlichen beziehen.

Die Einwilligung sollte ein Eckstein des EU-Ansatzes zur Regelung des Datenschutzes sein. Weil die Einwilligung eine wichtige Rechtsgrundlage ist, die allgemein genutzt wird, um Datenverarbeitung zu legitimieren, muss sie im Verordnungstext eindeutig definiert sein. Das Wissen der betroffenen Personen darüber, was mit ihrer „digitalen Identität“ geschieht, erweitert sich durch ihre unmittelbare Mitwirkung und ihre freie Entscheidung. Wir sollten klarstellen, dass technische Normen, in denen die Wünsche einer betroffenen Person zum Ausdruck kommen, eine brauchbare Art der ausdrücklichen Einwilligung bieten[1] . Die Information der betroffenen Personen sollte leicht verständlich formuliert werden, etwa durch abgestufte Strategien zum Schutz der Privatsphäre („layered privacy policies”) und standardisierte Logos oder Icons[2] . Um Anreize für die für die Verarbeitung Verantwortlichen zu schaffen, können wir auch deren Belastung verringern, indem wir ein einfaches Mittel, um Einwilligung nachzusuchen, schaffen, sofern eine Abschätzung der Folgen für die Privatsphäre vorgenommen wurde und das System als mit den Grundsätzen des Datenschutzes durch Technik und dem Gebot datenschutzfreundlicher Voreinstellungen konform zertifiziert ist. Der Begriff des „erheblichen Ungleichgewichts“ muss geklärt werden. Insbesondere sollte klar definiert sein, durch welche Fälle von Marktverzerrungen, wie Monopole oder Oligopole, das Ungleichgewicht entsteht. Besonders wichtig sind die Mittel zur Erlangung der Einwilligung zur Verarbeitung der personenbezogenen Daten von Kindern zu nehmen.
Klar zu definieren sind auch andere Rechtsgrundlagen für die Verarbeitung als die Einwilligung. Die Vorschrift über die Datenverarbeitung in Fällen, in denen sie zur Ausführung eines Vertrags notwendig ist, sollte auf die Erbringung einer von der betroffenen Person angeforderten Dienstleistung ausgedehnt werden. Die Definition des Begriffs der „berechtigten Interessen“ sollte keine Angelegenheit für einen delegierten Rechtsakt sein.

[1] Beispielsweise kann das Verbot des Aufspürens („Do Not Track“), das derzeit beim World Wide Web Consortium (W3C) entwickelt wird, zu einer solchen Norm werden, wenn der richtige Rechtsrahmen dafür geschaffen wird.
[2] Artikel 29 der Arbeitsgruppe, 11987/04/EN, WP 100: Stellungnahme 10/2004 zum Thema Vorschriften über stärker harmonisierte Informationen, 25. November 2004.

Die Zweckbindung ist ein Kernelement des Datenschutzes, denn sie schützt die betroffenen Personen vor einer unvorhersehbaren Ausdehnung der Datenverarbeitung durch Behörden oder Unternehmen. Eine Änderung des Zwecks personengebundener Daten nach ihrer Erfassung sollte nur auf der Basis eines berechtigten Interesses des für die Verarbeitung Verantwortlichen möglich sein.

Das Profiling, d. h. der Zugriff auf Daten über die Vorlieben, das Verhalten und die Einstellungen von Einzelpersonen zu dem Zweck, Entscheidungen über sie zu treffen, ist weit verbreitete Praxis geworden. Profiling-Aktivitäten müssen definiert und geregelt werden, damit für eine Einwilligung in Kenntnis der Sachlage gesorgt ist. Hier bieten die Empfehlungen des Europarates Anleitung[1] . Als Ergebnis des Profilings können betroffene Personen höhere Zinsen oder Versicherungsbeiträge zu zahlen haben, nur weil sie bestimmten Kriterien und Vorhersagemodellen entsprechen, über die sie selbst nicht einmal Klarheit haben. Es ist wichtig, dass es für jede nachteilige Auswirkung des Profilings durchweg eine Möglichkeit der Kontrolle durch Menschen gibt.

Der räumliche Geltungsbereich der Verordnung ist ein Thema, das für die konsequente Anwendung des EU-Datenschutzrechts wichtig ist. Der Berichterstatter und die Schattenberichterstatter treten dafür ein, dass die geplante Verordnung immer Anwendung findet, wenn Daten über Unionsbürger und Personen mit Aufenthalt in der Union verarbeitet werden, unabhängig davon, wo der für die Verarbeitung Verantwortliche seinen Sitz hat. In Bezug auf sonstige Datenübermittlungen in Drittstaaten müssen möglicherweise die Kriterien für einen Angemessenheitsbeschluss verschärft werden. Bei Übermittlungen, die nicht auf einem Angemessenheitsbeschluss beruhen, fragt es sich, wie private Vereinbarungen, etwa Vertragsklauseln und verbindliche unternehmensinterne Vorschriften, in Staaten durchgesetzt werden sollen, die keine Datenschutzgesetze haben oder in denen die Rechtsordnung die Durchsetzung verhindert. Anträgen von Behörden oder Gerichten in Drittstaaten auf Zugang zu in der EU gespeicherten und verarbeiteten personenbezogenen Daten sollte nur dann stattgegeben werden, wenn sie auch im Unionsrecht eine Rechtsgrundlage haben[2]. Dieses Thema wird durch die Zunahme des Cloud Computing sogar noch wichtiger.

3. Stärkung der Rechte des Einzelnen und Vertrauen der Verbraucher

Seit jeher sind spezielle Rechte der Einzelperson gegenüber den für die Verarbeitung Verantwortlichen Grundlage des Datenschutzes. Diese Rechte müssen garantiert aber auch gestärkt und verdeutlicht werden, um die Herausforderungen des digitalen Zeitalters zu bewältigen und Rechtssicherheit für Verbraucher und Unternehmen zu schaffen. Andererseits lässt sich die vorgeschlagene Verordnung vereinfachen, indem Rechte, die sehr ähnlich gelagert, sozusagen zwei Seiten einer Medaille, sind, zusammengeführt werden. Dadurch verringert sich der Verwaltungsaufwand der für die Verarbeitung Verantwortlichen, und für einzelne Personen wird es leichter, ihre Rechte zu verstehen und auszuüben.

[1] Empfehlung CM/Rec(2010)13 des Ministerkomitees des Europarats an die Mitgliedstaaten betreffend den Schutz von Personen vor der automatischen Verarbeitung personenbezogener Daten im Rahmen des Profiling, 23. November 2010.

[2] In allen Fraktionen bestehen erhebliche Bedenken gegen den Zugang ausländischer Behörden zu europäischen Bank-, Gesundheits- und Kommunikationsdaten – vgl. mündliche Anfragen und die diesbezügliche Aussprache mit dem für Justiz zuständigen Kommissionsmitglied, Vizepräsidentin Viviane Reding, 15. Februar 2012, Ausführliche Sitzungsberichte von diesem Datum, Punkt 19.

Informationen für betroffene Personen können grundsätzlich identisch mit interner Dokumentation sein, wenn der Ansatz eines abgestuften Datenschutzhinweises verfolgt wird, bei dem dem Verbraucher zunächst eine Standard- oder Kurzfassung der Datenschutzstrategie angeboten wird und er auf Verlangen die vollständigen Unterlagen erhalten kann. Das Recht, sich verständliche Informationen über die Datenschutzlogik geben zu lassen, das bereits in der Richtlinie 95/46/EG vorgesehen war und in der Entschließung des Parlaments vom 6. Juli 2010 hervorgehoben wurde, sollte erhalten bleiben. Die betroffenen Personen müssen sich darüber kundig machen können, was mit ihren Daten geschieht, während die Geschäftsgeheimnisse im einzelnen zu schützen sind.

Das Recht auf Datenübertragbarkeit – das Recht, Daten von einer Plattform zu einer anderen zu verlagern – ist nur eine geeignete Form des seit langem bestehenden Zugriffsrechts. Im digitalen Zeitalter haben die Bürger, auch als Verbraucher, die berechtigte Erwartung, ihre personenbezogenen Daten in einem allgemein üblichen elektronischen Format zu erhalten. Dadurch entsteht mehr Wettbewerb in einem Bereich, in dem es regelmäßig zu natürlichen Monopolen durch Netzeffekte kommt, und es wird ein vom Markt ausgehender Anreiz geschaffen, datenschutzkompatible Dienstleistungen zu erbringen.

Das Recht auf Datenlöschung und das Recht auf Datenkorrektur bleiben wichtig für die betroffenen Personen in einer Zeit, in der immer mehr Informationen offengelegt werden, die sich erheblich auswirken können. Das Recht auf Vergessenwerden ist vor diesem Hintergrund zu sehen, denn es klärt die genannten Rechte gegenüber dem digitalen Umfeld, ohne etwas an der allgemein in Bezug auf das Recht auf freie Meinungsäußerung geltenden Ausnahme zu ändern. Das sollte in den Formulierungen deutlich zum Ausdruck kommen.

Das Recht auf Widerspruch gegen weitere Datenverarbeitung sollte durchweg kostenlos ausgeübt werden können. Zudem muss es bessere Möglichkeiten zu wirkungsvollem Rechtsbehelf geben, auch für Verbrauchervereinigungen.

4. Stärkung des Grundsatzes der Rechenschaftspflicht und Verringerung des Verwaltungsaufwands

Aus der Verarbeitung gruppierter personenbezogener Daten ergeben sich viele Geschäftschancen für die für die Verarbeitung Verantwortlichen und die Personen, die Daten verarbeiten. Weil aber der Schutz personenbezogener Daten ein Grundrecht ist, bringt die Verarbeitung auch Verantwortlichkeiten mit sich. Die entsprechenden Verpflichtungen sollten klar und verständlich formuliert sein, damit keine Rechtsunsicherheit für Unternehmen und Behörden sowie für die betroffenen Personen entsteht. Aus diesen Gründen bedarf es einer weitaus klareren Aufteilung der Pflichten und Verantwortlichkeiten auf die für die Verarbeitung Verantwortlichen und die Personen, die Daten verarbeiten. Der Begriff der „gemeinsam für die Verarbeitung Verantwortlichen“ muss weiter erörtert werden. Zudem brauchen wir eine Klärung der Grenzen dessen, was Daten verarbeitende Personen dürfen, ohne von dem für die Verarbeitung Verantwortlichen angewiesen zu sein, auch in den Fällen, in denen ein Verantwortlicher einen Subunternehmer zur Datenverarbeitung heranzieht.

Die Datenschutzbeauftragten von Unternehmen und Behörden sind wesentlicher Bestandteil der heutigen Datenschutzpraxis, und es wird allgemein befürwortet, dass sie verbindlich in der gesamten Union eingeführt werden, ebenso wie die Rechtsstellung und die Aufgaben, die sie haben sollen. Einzelheiten über ihre Unabhängigkeit, ihre Befugnisse und Pflichten sind

möglicherweise noch zu klären. Es besteht allgemein Einigung darüber, dass die Schwellenwerte für die vorgeschriebene Ernennung eines Datenschutzbeauftragten nicht nur nach der Unternehmensgröße zu bemessen wäre, sondern hauptsächlich nach der Relevanz der Datenverarbeitungsvorgänge. Ein geeigneter Maßstab kann in der Zahl der Personen bestehen, deren Daten verarbeitet werden sollen.

Meldungen über Datenschutzverletzungen und Datenschutzvorschriften müssen mit den Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation[1] und der anstehenden Richtlinie über Angriffe auf Informationssysteme abgestimmt werden.

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen werden als wesentliches neues Element der Reform begrüßt. Dieses Element würde beispielsweise bewirken, dass die Anwendung eines Smartphones nur auf diejenigen auf dem Telefon vorhandenen Daten zugreift, die für die Erbringung eines bestimmten Dienstes wirklich notwendig sind, wie Routing-Daten oder Wetterinformationen. Allerdings brauchen Hersteller und Dienstleister weitaus deutlichere Anleitungen und stärkere Anreize zur Umsetzung dieser Prinzipien. Abschätzung der Folgen für die Privatsphäre machen ebenfalls Klärung und deutlichere Anleitungen nötig. Beide Ansätze erfordern zudem eine starke Rolle für Datenschutzbeauftragte.

Verhaltenskodizes und Zertifizierung und Datenschutzsiegel werden grundsätzlich befürwortet, aber auch hier sind Anreize und deutlichere Vorschriften über die Konsequenzen nötig, was die Rechtmäßigkeit der Verarbeitung, die Haftung und verwandte Themen angeht.

[1] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.7.2002, S. 37 bis 47;