Erste Stellungnahme der ISOC.DE zu den Vorschlägen der EU-Kommission für eine Harmonisierung des europäischen Datenschutzrechts

Die Internet Society German Chapter e.V. (ISOC.DE e.V.) ist ein unter diesem Namen seit 1995 bestehender Verein, der die Verbreitung des Internets in Deutschland fördert und dessen Entwicklung sowohl in technischer, als auch in gesellschaftlicher Hinsicht begleitet. ISOC.DE ist dabei eigenständiger Teil der vor 20 Jahren von einer Gruppe um den Internet-Erfinder Vint Cerf gegründeten Internet Society (ISOC), die heute mit insgesamt über 50.000 Mitgliedern in 72 Ländern in einer zunehmend von Markt und Wettbewerb geprägten Umgebung die Voraussetzungen für den Fortbestand und Zusammenhalt des Internet schafft. In den ihr verbundenen Organisationen wie der Internet Engineering Task Force (IETF), dem Internet Architecture Board (IAB), der Internet Engineering Steering Group (IESG) und der Internet Research Task Force (IRTF) versammelt die ISOC unter einem Dach zentrale Institutionen der Standardisierung und Forschung von und für die Internet Community. Getragen werden sie von der gemeinsamen Überzeugung, dass offene und transparente „Internet Governance" unter Beteiligung aller Anspruchsgruppen eine wesentliche Bedingung für den Erfolg und die Weiterentwicklung eines freien Internets sind.

I. Hintergrund

Die EU-Kommission legte Ende Januar 2012 den bereits seit langem angekündigten Vorschlag für eine europäische Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr 2012/0011 (COD) vor. Die Datenschutz-Grundverordnung (DSVO) soll (zusammen mit einer weiteren neuen Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, (2012/0010 (COD)), die bisher geltende europäische Datenschutzrichtline ersetzen. Sie soll als Rechtsakt in der Europäischen Union allgemeine Geltung erlangen.

Der Vorschlag der Kommission dient dazu, ein dichtes Kontrollnetz für den Datenschutz in Europa mit starken Aufsichtsbehörden und empfindlichen Bußgeldkatalogen vorzugeben. Die Kommission setzt auf umfassende staatliche Kontrollen der Datenverarbeitung und damit auch auf eine strikte Überwachung der Kommunikation im Internet. Die geplanten Änderungen des materiellen Datenschutzrechts sind demgegenüber als eher marginal zu bewerten. Es bleibt bei einem umfassenden Verbot der Datenverarbeitung (mit Erlaubnisvorbehalt). Zugleich soll die freiwillige Einwilligungsmöglichkeit des Nutzers in die Verarbeitung der auf die eigene Person bezogenen Daten beschränkt werden. Der Personenbezug soll weiterhin das ausschlaggebende Kriterium für die Anwendbarkeit des Datenschutzrechts und aller seiner Restriktionen sein – jedoch erfolgt keine Konkretisierung des in der Vergangenheit zu vielen Rechtsunsicherheiten geführten Begriffs. Schließlich soll dem Verbraucher

gestattet werden, seinen (unter Umständen selbst) verbreiteten Datenbestand möglichst komplett rückabzuwickeln. Hinzu kommen Vorschriften zur Datenportabilität in der „Cloud“.

Ein zentrales Ziel bei diesem Vorhaben ist eine Harmonisierung des Datenschutzrechts in Europa auf einem hohen Schutzniveau. Zudem sollen viele gemeinhin als veraltet geltenden datenschutzrechtlichen Regelungen modernisiert werden, um den Bedingungen der allgegenwärtig digitalisierten und vernetzten Welt besser gerecht zu werden. Das europäische Parlament und der Rat werden sich nunmehr in Ausschusssitzungen und Anhörung mit dem vorliegenden Entwurf der Kommission befassen. Der endgültige Erlass der Verordnung im ersten Halbjahr 2013 avisiert.

Die vorgelegten Vorschläge zur Harmonisierung der europäischen Regelungen zum Datenschutz sind vor dem Hintergrund des kürzlich ergangenen Urteils des Europäische Gerichtshofs vom 24. November 2011 (Az. C-468/10 und C-469/10) zu betrachten, wonach nationale Abweichungen vom Normenbestand der bislang schon geltenden Richtlinie künftig kaum noch zu rechtfertigen sein dürften. Dies dürfte bereits kurzfristig und schon vor Inkrafttreten der Verordnung zu der Konsequenz führen, dass sich deutsche "Sonderwege" im Datenschutz für die Zukunft faktisch erledigt haben und damit auch die teilweise in Deutschland existenten Auffassung, dass insbesondere in Zeiten eines grenzüberschreitenden, globalen Internets ein national bestimmtes Datenschutzrecht lokal durchsetzbar sei und als Behörde oder Bundesverfassungsgericht wesentlich mitbestimmt werden könnte.

Die ISOC.DE begrüßt daher den längst überfälligen Ansatz, das bestehende Datenschutzrecht europaweit zu modernisieren und insbesondere auch stärker zu harmonisieren, als es die bislang bestehende Datenschutzrichtlinie vermochte. Gerade aus Sicht der in der ISOC versammelten Anspruchsgruppen, die das Internet auch von seiner technischen Seite her und international betrachten, kann dies zu einer Vereinfachung des rechtskonformen Umgangs mit den datenschutzrechtlichen Vorgaben führen und damit Rechtssicherheit für die Entwicklung zukünftiger Innovationen und die Gestaltung technisch-organisatorischer Abläufe bringen.

Daher sieht die ISOC.DE gleichzeitig noch erheblichen Nachbesserungsbedarf bei den bestehenden Vorschlägen für die europäische Datenschutzgrundverordnung. Dies bezieht sich einerseits auf den generellen regulatorischen Ansatz (II.), bei dem sich die Frage der notwendigen Anpassung an einen auch den Bedingungen des Internet angepassten Datenschutz stellt, als auch die Ausgestaltung einzelner, konkreter Vorschriften im Hinblick auf ihre tatsächliche Durchführbarkeit und ihre Auswirkungen (III.).

II. Generelle Kritik: Anknüpfung an das Verbot mit Erlaubnisvorbehalt

Die ISOC.DE hält es für dringend geboten, aus Anlass der Neufassung der europäischen Normen, auch einmal ganz grundsätzlich zu hinterfragen, weshalb der Entwurf der Verordnung mit Art. 6 DSVO eine Perpetuierung des Verbotes mit Erlaubnisvorbehalt vorsieht und ob dieses Prinzip aus analogen Zeiten ins Internetzeitalter übertragen werden sollte. In diesem Zusammenhang sollten auch Vorschläge wie das Recht auf Vergessen (Art. 17 DSVO), die Regelungen zur Portabilität von Daten (Art. 18 DSVO) nachgebessert werden, da die Fragen des Datenschutzrechts deutlich komplexer und weitreichender sind, als dass sie auf Problemfelder der sozialen Netzwerke oder Suchmaschinen reduziert werden dürften. Im Gegenteil führt die verengte und augenscheinlich undifferenzierte Sichtweise auf

Facebook & Co. in den Rechtsfolgen zu Ergebnissen, die in anderen Bereichen des vielfältigen Geschehens im Internet nicht gewollt sein können.

Insbesondere eine Perpetuierung des Verbots mit Erlaubnisvorbehalts bei gleichzeitiger Ausdehnung des „Personenbezugs“ eines Datums auf alles, was auch nur im entferntesten „personenbeziehbar“ ist, führt heute schon zu (aus Sicht von ISOC.DE insoweit auch vielfach berechtigten) Kritik am heutigen System des institutionellen Datenschutzes in der Praxis – insbesondere im Hinblick auf die Einordnung von IP-Adressen als grundsätzlich stets personenbezogenes Datum. Dabei ist insbesondere problematisch, dass sich die Mitgliedstaaten einerseits vorbehalten, selbst jederzeit auf alle Arten von Daten ihrer Bürger zuzugreifen, sogar Zwang auszuüben um sie zu erheben (Beispiel: Fingerabdrücke für den elektronischen Pass), ohne dass es einer Einwilligung des Bürgers bedürfen würde oder die staatlichen Datenschutzbeauftragten dagegen einschreiten (könnten), andererseits ihre Aktivitäten zum Datenschutz nunmehr auf das Geschehen zwischen Privaten fokussieren wollen und dabei sogar zum Teil so weit gehen möchten, ihren Bürgern die Möglichkeit zu einer freiwilligen Einwilligung einer Nutzung ihrer Daten gänzlich zu nehmen.

Bereits heute zeichnet sich in der Praxis der Trend ab, dass Verbraucher einerseits aufgrund der Omnipräsenz von Einwilligungsprozessen in ihrer Sensibilität abstumpfen, andererseits jedoch auch häufig nicht erkennen können, in welchen Situationen ein gesetzlicher Erlaubnistatbestand die Erforderlichkeit einer Einwilligung eigentlich entbehrlich macht. ISOC.DE regt daher dringend an, das Verbotsprinzip noch einmal kritisch zu beleuchten und mit anderen Prinzipien, wie einem grundsätzlichen Erlaubnisprinzip, zu vergleichen. Selbst wenn sich der europäische Gesetzgeber letztlich für eine Fortführung der bestehenden Dogmatik entscheiden sollte, müsste im Rahmen des aktuellen Gesetzgebungsverfahrens die Chance genutzt werden, auch einmal andere, innovativere Ansätze auf ihre Tauglichkeit hin zu prüfen.

Insbesondere bewertet die ISOC.DE die Regelung in Art. 7 Abs. 4 DSVO als kritisch, wonach die Einwilligung dann keine Rechtsgrundlage für die Verarbeitung personenbezogene Daten sein kann, wenn zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen ein „erhebliches Ungleichgewicht“ vorliegt. Dies soll nach dem Erwägungsgrund 34 „vor allem“, aber eben nicht ausschließlich, der Fall sein, wenn der Betroffene sich gegenüber der verantwortlichen Stelle in einem Abhängigkeitsverhältnis befindet. Diese Norm führt zu erheblichen Rechtsunsicherheiten und bedroht nicht nur große und von einer Vielzahl von Menschen genutzte Geschäftsmodelle im Internet, sondern könnte insgesamt eine besondere Innovationsfeindlichkeit entfalten. Zudem beschneidet sie den Einzelnen in seiner selbstbestimmten Dispositionsbefugnis über seine höchstpersönlichen Daten.

Klarzustellen ist dabei, dass es an dieser Stelle nicht um die Frage der Freiwilligkeit geht oder vom Betroffenen eine Einwilligung in Datenverarbeitungen verlangt wird, die nicht aus der jeweiligen Vertragsbeziehung zu rechtfertigen ist. Aus Sicht der ISOC sollte Freiwilligkeit und ein „Opt-In“ der Grundsatz einer jeglichen Verarbeitung personenbezogenen (sensibler) Daten sein.

Daher ist es als kritisch anzusehen, wenn es dem Betroffenen - in der Folge einer Beurteilung Dritter - überhaupt nicht mehr erlaubt sein sollte, in die Datenverarbeitung von beispielsweise Gesundheitsdaten, Arbeitnehmerdaten oder auch sozialen Netzwerken, wie Facebook oder Xing, rechtswirksam einzuwilligen, wenn z.B. eine Datenschutzbehörde hierin ein „Ungleichgewicht“ erkennen will – selbst wenn der Betroffene damit völlig einverstanden sein sollte und die Einwilligung informiert,

freiwillig und bewusst vornehmen möchte. Nach der vorgeschlagenen Regelung wäre es in der Konsequenz letztlich dann nur noch einem entsprechenden Kollektiv (Betriebsrat, Datenschutzbehörden, Gesetzgeber etc.) überlassen, zu bestimmen, ob die individuellen Daten des Betroffenen verarbeitet werden dürften oder nicht. Besonders problematisch wäre dann aber, dass eine solche Kollektiventscheidung andererseits zu allen möglichen Arten der Verarbeitung seiner Daten verurteilen würde und es auf seine persönliche Einwilligung dann gar nicht mehr ankäme.

Nach Auffassung der ISOC.DE ist jedoch die zentrale Idee und zugleich Rechtfertigung des Datenschutzes gerade die **Dispositionsbefugnis** des Betroffenen zum Schutz der informationellen Selbstbestimmung des Bürgers als Ausprägung seiner Persönlichkeitsrechte und Menschenwürde. Einen Anspruch auf entsprechende Daten und ihre Verarbeitung sollte in der Folge dem Staat nur dann zustehen, wenn dafür eine gesetzliche Rechtfertigung existiert, während der Betroffene gegenüber Gleichgeordneten selbst entscheiden können soll, was er Dritten offenbaren will, oder nicht.

Soweit nunmehr die vorgesehenen Regelungen dazu führen sollten, dass nur noch der Staat, eine Behörde oder ein anderes Kollektiv über die Einwilligungsmöglichkeit des Betroffenen bestimmen kann, wendet sich das Argument des Datenschutzes jedoch in sein Gegenteil: Die Idee des Schutzes der Daten eines Bürgers zur Sicherung seiner individuellen Freiheit und Persönlichkeit durch den Staat, wendet sich in ein staatliches Verbot und Beschränkung seiner Dispositionsfreiheit unter kollektivistischer (behördlicher) Aufsicht. Diesen Vorwurf kann auch das Argument des „unmündigen" Bürgers, welcher die Folgen seiner Einwilligung gar nicht übersehen könne, nicht entkräften. Denn es begründet bereits das „Ungleichgewicht" und ist zudem vielmehr als Aufgabe an den Staat zu verstehen, den Betroffenen besser vor Missbräuchen zu schützen und ihm dagegen zu helfen, nicht aber jeden theoretisch möglichen Missbrauch der Daten dadurch abstellen, dass dem Bürger die freie Weitergabe und Nutzung der eigenen Daten einfach untersagt wird.

Anstatt dem Bürger das Recht zur Einwilligung zu nehmen, wäre es daher im Interesse des Datenschutzes geboten, die Transparenz und damit Freiwilligkeit der Einwilligung des Betroffenen zu stärken. Das könnte durch administrative Instrumente wie etwa einen „Datenbrief" geschehen, aber auch die Förderung technischer Lösungen wie die der W3C-Arbeitsgruppe „Do not Track" http://www.w3.org/QA/2011/09/do_not_track_standards_for_the.html oder auch durch die Etablierung regulierter und überprüfter Standard-Einwilligungsbestimmungen nach dem Vorbild von Standard-Lizenzbedingungen wie „Creative Commons" http://de.creativecommons.org/was-ist-cc/, bei denen der Nutzer schon anhand der verwendeten Symbole hinreichend klar erkennen könnte, welche seiner Daten wie und von wem und zu welchem Zweck verarbeitet werden, falls er eine Einwilligung erteilen will. Die wirksame Stärkung der Dispositionsbefugnis des Einzelnen ist einer weiteren bloß symbolisch und ansonsten unter Umständen sogar schädlich wirkenden Verbotsnorm vorzuziehen.

Kritisch bewertet die ISOC.DE in diesem Zusammenhang auch das sog. „Recht auf Vergessenwerden" gemäß Art. 17 DSVO. Dieses begründet Ansprüche des Betroffenen auf die Löschung von personenbezogenen Daten. Im Rahmen der in Deutschland bereits geführten Diskussionen über die Möglichkeiten der Datenlöschung im Internet (Stichwort: „Digitaler Radiergummi") ist insbesondere die Formulierung des „Vergessens" problematisch. Denn es handelt sich nicht etwa um eine andere Form der Ideen, wie sie beispielsweise für einen „Datenbrief" formuliert werden, die dem Betroffenen ein Mehr an Transparenz hinsichtlich der über ihn gespeicherten Daten verschaffen sollen. Die Verpflich-

tung nach Art. 17 Abs. 2 DSVO wonach die verantwortliche Stelle alle vertretbaren Schritte einzuleiten hat, um Querverweise, Replikationen oder Kopien zu löschen, ist nicht praxisgerecht.

Gerade infolge von dem häufigen Fall der Verlinkung einer im Internet vorgehaltenen Information, welche sich kaum verhindern lässt, können im Internet vorhandene Daten von Cachingdiensten und Suchmaschinen zwischengespeichert, auf lokalen Rechnern abgelegt, ausgedruckt, per Screenshot gesichert, etc. werden. Gerade unter Berücksichtigung der dezentralen Struktur des Internets ist das „Vergessen“ nicht realisierbar und widerspricht technischen Gegebenheiten. Im Gegenteil, wendet sich die gute Absicht hier schnell in das Gegenteil: Datenbanktechnisch bedingt das Recht auf Vergessen, das selbst ansonsten in „Datensilos“ vergessene Daten (beispielsweise in Backupsystemen) künftig im „aktiven“ Datenbestand gehalten und indiziert bleiben müssen. Sprich: Eine datenverarbeitende Stelle könnte durch das „Recht auf Vergessen“ geradezu dazu gezwungen werden, den Umfang seiner Verarbeitung personenbezogener Daten dramatisch zu erweitern, um auch ansonsten längst „verschwundene“ Altdaten auffindbar, also suchfähig indiziert zu halten. Dieses aber erwiese sich für die Betroffenen (Beispiel: Bonitätsdaten) als erheblich schädlicher und weniger zielführend, als der heute bereits bestehende Auskunfts- und Löschungsansprüche. Diesbezüglich fehlen jedoch konkrete Vorschläge, wie die Betroffenen künftig einfacher und wirksamer Transparenz über den sie betreffenden (aktiven) Datenbestand herstellen könnten.

Eine Vermischung von Fragen des Persönlichkeitsrechts mit denen des Datenschutzes, wie sie sich aus dem vorgeschlagenen „Recht auf Vergessen“ ergibt, ist dagegen abzulehnen. Denn auch wenn die konkrete Reichweite des „Vergessens“ an konkurrierenden europäischen Grundwerten Dritter zu messen sein wird, würden damit jedoch (Datenschutz-) Behörden zu einem Einschreiten ermächtigt, die nicht dazu berufen sein sollten, beispielsweise konkret über die die Reichweite der Presse- und Meinungsfreiheit zu befinden.

Hinsichtlich der Regelung nach Art. 18 DSVO über die Möglichkeit der Portabilität von Daten geht die ISOC.DE davon aus, dass sich diese Vorgaben insbesondere auf soziale Netzwerke beziehen sollen. Nach Auffassung der ISOC.DE stellt die Portabilität von Daten jedoch keine Maßnahme zum Datenschutz dar, sondern hat vielmehr den Charakter einer Marktregulierung, da sie den Betroffenen einen Wechsel zu anderen Unternehmen mit allen Daten ermöglichen soll. Damit kann sich die Vorgabe jedoch auch zur Gefahr für den Datenschutz entwickeln: zur Gewährleistung der Datenportabilität ist es häufig erforderlich, Schnittstellen zwischen eigentlich getrennten Datensystemen „in the cloud“ zu etablieren, die diese zusammenzuführen und/oder in einer Weise verknüpfen können, die dem Separierungsgebot entgegensteht. Soweit eine solche Marktregulierung gewünscht ist, sollte sie jedoch nicht im Kontext von Datenschutz, sondern an anderer Stelle diskutiert werden. Egal ob und wie sie am Ende ausgestaltet sein würde, sind die Schnittstellen selbstverständlich anschließend datenschutzkonform zu gestalten.

III. Ausgestaltung einzelner Vorschriften

Zur Gewährleistung von Planungssicherheit sowie der tatsächlichen und rechtlichen Umsetzbarkeit der DSVO möchte die ISOC.DE dringend um weitere Konkretisierung der Vorgaben bereits im Rahmen des gegenständlichen Verordnungsentwurfs bitten, damit die Ausgestaltung der Vielzahl „unbestimmter Rechtsbegriffe“ nicht allein (Datenschutz-) Behörden und Gerichten überlassen bleibt und der politischen Verantwortung für die Rechtsfolgen entzogen sind.

Dies gilt umso mehr vor dem Hintergrund, dass bereits unter dem gegenwärtigen Rechtsrahmen erhebliche Rechtsunsicherheiten in Deutschland und Europa und damit einhergehend erhebliche Auslegungsbedürfnisse existieren, welche sich etwa auch im Ergebnis in der oben genannten Entscheidung des EuGH wiederspiegeln. Zudem ist das in Deutschland heute bestehende Datenschutzrecht in weiten Teilen nicht „internetkompatibel“. Der Verordnungsentwurf ändert daran leider in wesentlichen Punkten aber nichts.

Die ISOC.DE begrüßt hier den Ansatz der möglichst weitgehenden Harmonisierung des Datenschutzrechts, bezweifelt in diesem Zusammenhang jedoch die Möglichkeiten einer praxisgerechten (globalen) Rechtsdurchsetzung, wie sie durch die Verordnung skizziert wird, allein mit den vorgestellten rechtlichen Instrumenten. Um globale Rechtsdurchsetzung zu gewährleisten, bedürfte es aus Sicht der ISOC.DE neben einer (wie dargestellt veränderter) EU-Regulierung noch ergänzend technischer Regulierung und völkerrechtlicher Vereinbarungen unter Beteiligung von Institutionen wir eben der ISOC, um zugunsten des Datenschutzes Regeln zu etablieren und durchzusetzen, die sowohl größtmögliche Akzeptanz bei allen Anspruchsgruppen finden, als auch möglichst international durchsetzbar sind.

Neben den grundsätzlichen und im Detail gemachten Vorschlägen zur Änderung des Entwurfs der Verordnung, wünschen wir uns daher dringend, auch andere Aspekte in die Diskussion um die Gestaltung eines wirksamen europäischen Datenschutzes mit einzubeziehen – insbesondere nicht allein auf rechtliche Instrumente zu setzen, sondern auch die technischen und regulatorischen Standards in die Überlegungen mit einzubeziehen und hier einen wirksamen Datenschutz zu befördern. Die Internet Society und ISOC.DE sind hier gern bereit, Unterstützung zu leisten.

Berlin, den 20.03.2012

Für den Vorstand der ISOC.DE

Jan Mönikes, Rechtsanwalt
Kontakt: jan@moenikes.de

###

ISOC.DE e.V. Büro
c/o ict-Media GmbH
Zedernweg 85
53757 Sankt Augustin
Telefon: +49 (0) 2241 396415
Telefax: +49 (0)2241 396414
E-Mail: sek@isoc.de
Web: https://www.isoc.de/