Deutscher Bundestag
Enquete-Kommission
Internet und digitale Gesellschaft

Ausschussdrucksache
17(24)035

TOP 1c am 4.7.2011

1.7.2011

Projektgruppe Datenschutz

Ergänzende Textvorschläge der Fraktionen SPD, DIE LINKE., BÜNDNIS 90/DIE GRÜNEN zu den konsensualen Handlungsempfehlungen aller Fraktionen

Jeweils einzufügen am Ende der angegebenen Kapitel

II. Vorgaben für nationalen, europäischen und internationalen Datenschutz

Gemeinsamer Textvorschlag der Fraktionen von SPD, B90/die Grünen, die Linke:

Über die gemeinsam mit allen Fraktionen beschlossenen Handlungsempfehlungen wird dem Deutschen Bundestag empfohlen,

Die fortschreitende grenzüberschreitende Vernetzung und Globalisierung von Kommunikations-Infrastrukturen macht eine Abstimmung und Modernisierung auch auf supra- wie internationaler Ebene notwendig. Zusätzlichen Anlass auf EU-Ebene bieten die Änderungen des Lissabon-Vertrages und die Inkorporation der Grundrechtecharta, darunter das Grundrecht auf Datenschutz. Vor diesem Hintergrund ist der Reformansatz der EU- Kommission zu begrüßen.

Die Enquete-Kommission empfiehlt dem Deutschen Bundestag:

> die Bundesregierung aufzufordern, sich für eine umfassende Novellierung der EG-Datenschutzrichtlinie einzusetzen. Dabei begrüßt er die Absicht, auch den öffentlichen Sektor einschließlich der Sicherheitsbehörden in die Harmonisierung einzubeziehen. Er fordert dazu auf, Regelungen insbesondere zu privacy by design, zum Profiling sowie zum Daten- und Personenbezugsbegriff zu schaffen bzw. vorhandene Regelungen grundlegend zu überarbeiten. Die Revision der Richtlinie muss dabei insbesondere den Herausforderungen der digitalen Gesellschaft, wie z. B. Cloud Computing Rechnung tragen.

IV. Einwilligung

Gemeinsamer Textvorschlag der Fraktionen von SPD, B90/die Grünen, die Linke:

Über die gemeinsam mit allen Fraktionen beschlossenen Handlungsempfehlungen wird darüber hinaus dem Deutschen Bundestag empfohlen,

in Rechtsbeziehungen, in denen von einer wirklich freien Einwilligungsentscheidung nicht ausgegangen werden kann, weil die betroffene Person nicht dieselbe Machtposition hat wie sein Gegenüber (also z. b. die öffentliche Stelle bzw. der privatwirtschaftliche Vertragspartner gegenüber dem einfachen Nutzer) eine Einwilligung nur dort zuzulassen, wo ihre Erteilung ebenso wie ihre Ablehnung im freien Ermessen der betroffenen Person steht.

VI. Privacy by design / by default

Gemeinsamer Textvorschlag der Fraktionen von SPD, B90/die Grünen, die Linke:

Über die gemeinsam mit allen Fraktionen beschlossenen Handlungsempfehlungen wird darüber hinaus dem Deutschen Bundestag empfohlen,

die Anbieter von Diensten und Anwendungen, die auf der Erhebung, Verarbeitung und Speicherung personenbezogener Daten basieren bzw. zu ihrer Funktionserfüllung personenbezogene Daten erheben, verarbeiten und speichern, zu verpflichten, die grundsätzlich höchstmöglichen Datenschutzeinstellungen voreinzustellen (privacy by default).

IX. Soziale Netzwerke

Gemeinsamer Textvorschlag der Fraktionen von SPD, B90/die Grünen, die Linke:

Die Enquete-Kommission hat in ihrem Bericht herausgearbeitet, dass es in sozialen Netzwerken zahlreiche Besonderheiten und Probleme im Umgang mit Daten und Informationen durch die Betreiber der Plattformen gibt.

Über die gemeinsam mit allen Fraktionen beschlossenen Handlungsempfehlungen empfiehlt die Enquete-Kommission dem Deutschen Bundestag deshalb,

1. die Betreiber sozialer Netzwerke zu verpflichten, höchst mögliche Sicherheitsvorkehrungen zu treffen, um Datendiebstähle und Systemeinbrüche zu vermeiden. Regelmäßige Kontrollen, die Nutzung aktueller und effektiver Technologien sowie der Vorrang des Schutzes der Daten der Nutzer vor dem des Komforts sind dabei zu gewährleisten. Technische Neuerungen müssen vor ihrer Einführung auf ihre Auswirkungen für den Schutz der Daten und Inhalte der Mitglieder von den Plattformbetreibern umfassend geprüft werden.

2. eine Verpflichtung der Anbieter, die Nutzungsmöglichkeit von sozialen Netzwerken nicht an eine Einwilligung in die über die Erfüllung des Vertragszwecks hinausgehende Datennutzung zu koppeln.

3. einen gesetzlichen Anspruch für die Nutzer sozialer Netzwerke auf Löschung des Accounts inklusive aller gespeicherter Nutzerdaten zu schaffen. Dies entspricht den datenschutzrechtlichen Vorgaben. Eine bloße Deaktivierung des Accounts als einzige Option der Abmeldung ist nicht ausreichend, da hierbei alle Daten weiterhin gespeichert bleiben und das Account samt der vorhandenen Daten jederzeit wieder aktiviert werden kann. Die Löschung des Accounts muss für den/die Nutzer/in ohne Hürden möglich sein. Die Löschungspflicht der Daten sollte gesetzlich verankert werden.

4. die Anbieter sozialer Netzwerke dazu anzuhalten, in einer verständlichen Formulierung der Nutzungs- und Datenschutzbestimmungen sowie zur Aufklärung über die möglichen Risiken der Nutzung sozialer Netzwerke verpflichtet werden.

5. Bei der Neuanmeldung in einem sozialen Netzwerk sollen die Betreiber der Netzwerke die Datenerhebung auf ein Minimum der für die Anmeldung erforderlichen Daten beschränken. Ein Recht auf pseudonyme Nutzung sollte ebenfalls gewährleistet sein.

6. die Anbieter sozialer Netzwerke zu verpflichten, die Voreinstellungen der Nutzerprofile auf den Mindestzugriff der für die Nutzung des Netzwerks notwendigen Daten zu beschränken, so dass Nutzer und Nutzerinnen sich aktiv für die Freigabe ihrer Daten entscheiden können. Da sich gezeigt hat, dass Datenschutzinformationen bei der Anmeldung bei einem sozialen Netzwerk selten gelesen werden, empfiehlt es sich, dass während der Nutzung des Dienstes, bspw. bei Änderungen der Datenschutzeinstellungen, die der/die Nutzer/in vornimmt, eingebaute, kontext-sensitive Funktionen dazu dienen, den User über die möglichen Konsequenzen seines Handelns zu informieren.

7. die Anbieter sozialer Netzwerke zu verpflichten, bei der Umsetzung von Programmierschnittstellen für externe Anwendungen, die sogenannten „Apps“, dafür Sorge zu tragen, dass Dritte nur mit einer aktiven und informierten Einwilligung der NutzerInnen auf Daten zugreifen können. Die Betreiber der sozialen Netzwerke tragen ebenfalls dafür Sorge, dass die Schnittstelle von Netzwerk und externer Anwendung nicht zum Missbrauch genutzt werden kann. Auch die Daten anderer Nutzer und Nutzerinnen, wie von „Freunden“ der die externe Anwendung nutzenden Person dürfen über die Schnittstelle nicht ohne explizite Einwilligung der betroffenen Person dieser „Freunde“ preisgegeben werden.

X. Datenschutzaufsicht

Gemeinsamer Textvorschlag der Fraktionen von SPD, B90/die Grünen, die Linke:

Über die gemeinsam mit allen Fraktionen beschlossenen Handlungsempfehlungen hinaus empfiehlt die Enquete-Kommission, die auch von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder geforderten nachfolgenden gesetzgeberischen Maßnahmen und appelliert an Bund und Länder,

1. dass eine wirksame Kontrolle die Voraussetzung eines erfolgreichen Datenschutzes ist. Wenn man Datenschutz zudem zunehmend als Querschnittsaufgabe begreifen will, muss dies auch institutionelle Folgen haben. Um die – auch von der EU-Datenschutzrichtlinie 95/46 geforderte und vom EuGH bestätigte – vollständige Unabhängigkeit der Datenschutzinstanzen zu stärken und um Interessenkonflikte zu vermeiden, sollte der Bundesbeauftragte für Datenschutz und Informationsfreiheit weder dem Innenministerium noch einer anderen Bundesbehörde zugeordnet sein. Er sollte frei von Rechts- oder Fachaufsicht seiner Aufsichtstätigkeit nachgehen können. Eine Dienstaufsicht ist allenfalls in eingeschränkter Form zulässig.

2. das Urteil des EuGH zu berücksichtigen und die gesetzlichen Grundlagen für die Unabhängigkeit der Kontrollstellen im Sinne der 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 umzusetzen.

3. Diese Unabhängigkeit muss rechtlich, organisatorisch und finanziell abgesichert werden.

4. § 38 BDSG sollte dahingehend überarbeitet werden, dass

- das Anordnungsrecht gem. § 38 Abs. 5 BDSG effektiver ausgestaltet und den üblichen Grundsätzen des Verwaltungsvollzugs angepasst wird.

- eine gesetzliche Mitwirkungspflicht der kontrollierten Stelle gegenüber Kontrollen der Aufsichtsbehörde geschaffen wird, ähnlich der Mitwirkungspflicht i. S. d. § 24 Abs. 4 BDSG oder des § 5 des Gesetzes zur Bekämpfung der Schwarzarbeit und illegalen Beschäftigung.

5. Der Bundesbeauftragte benötigt die den Länderbehörden entsprechenden Anordnungsbefugnisse ebenfalls für alle Bereiche, in denen er die Aufsicht führt, also auch für die Aufsicht über die nicht-öffentlichen Stellen nach dem Telekommunikationsgesetz sowie dem Postgesetz.

6. die Ausdehnung der Zeugnisverweigerungsrechte und Beschlagnahmeschutzvorschriften auf Informationen und Unterlagen, die die Aufsichtsbehörden bei Berufsgeheimnisträgerinnen und -trägern erlangt haben, wird vorgeschlagen

7. Eine Strafantragsbefugnis für die Datenschutzaufsichtsbehörden sollte in § 205 StGB festgelegt werden

XI. Vorbildwirkung öffentlicher IT-Projekte

Gemeinsamer Textvorschlag der Fraktionen von SPD, B90/die Grünen, die Linke:

Über die gemeinsam mit allen Fraktionen beschlossenen Handlungsempfehlungen wird darüber hinaus dem Deutschen Bundestag empfohlen,

1. dass öffentliche IT-Projekte der Vorbildwirkung gerecht werden und auf besonders hohem Schutzniveau basieren. Dabei ist auf weitere Datensammelprojekte großen Umfangs zu verzichten, die Kritik der Datenschützer ernst zu nehmen und in eine breite gesellschaftliche Debatte mit staatlichen und nicht-staatlichen Akteuren zu treten.

2. die genannten Projekte sind einer erneuten Prüfung zu unterwerfen, die insbesondere die technischen Grundlagen einer ergebnisoffenen datenschutzrechtlichen Evaluation zugänglich macht. eGovernment-Angebote im Bereich der Dienstleistungen für Bürgerinnen und Bürger müssen den aktuellsten technischen und organisatorischen Anforderungen an einen wirksamen Datenschutz genügen.

3. eine stärkere aktive Einbeziehung datenschutzrechtlicher Aspekte in alle Planungsetappen im Bereich des verwaltungsübergreifenden Arbeitens, weil dies eine besondere Herausforderung in datenschutzrechtlicher Hinsicht darstellt. Dies insbesondere vor dem Hintergrund, national wie international, bei Offshoring und Outsourcing einen unsensiblen Umgang mit Datenschutzbelangen frühzeitig zu verhindern.

4. bei zentralen IT-Projekten, auch jener, die von der EU eingeleitet werden, den Datenschutz bereits von Beginn an in der Konzeption zu berücksichtigen.

5. beim Einkauf komplexer Standardprodukte wie Zeiterfassungs- oder Zugangskontrollsystemen für öffentliche Einrichtungen sicher zu stellen, dass die erfassten Daten tatsächlich nur im Rahmen ihrer Zweckbestimmung verwertet werden. Wenn Aufträge für die Entwicklung solcher Projekte vergeben werden, sollten sie stets die Programmierung entsprechende technischer Begrenzungen beinhalten. Im Interesse der Verwirklichung möglichst vorbildlichen Datenschutzes sollte dies bereits bei der finanziellen Planung berücksichtigt werden.

6. in Ämtern und Behördern wegen des erhöhten Einsatzes von Software und des Zugriffs hierauf durch verschiedene Mitarbeiter Vorkehrungen zu treffen, die eine Verletzung insbesondere des Sozialdatenschutzes ebenso ausschließen wie des Steuergeheimnisses.

7. dafür Sorge zu tragen, dass in den kommenden fünf Jahren mindestens 10% der Forschungsgelder aus dem Bereich IT in Bereichen der Datenschutztechnologien gebunden werden. Über die Verwendung der Gelder sollte nach Beratung mit dem Bundesbeauftragten für Datenschutz, der geplanten Stiftung Datenschutz und Interessenvertretern der betroffenen Akteure entschieden werden.