**Enquete-Kommission Internet und digitale Gesellschaft**

Deu

**Deutscher Bundestag**
Enquete-Kommission
Internet und digitale Gesellschaft
Ausschussdrucksache
17(24)029
TOP 1c am 7.4.2011
30.6.2011

**Projektgruppe Datenschutz, Persönlichkeitsrechte**

**Handlungsempfehlungen - <u>konsensuale</u> Vorschläge (Stand: 30. Juni 2011)**

## 3. Kapitel: Handlungsempfehlungen

### I. Einleitung

Die anhaltenden Veränderungen der IT-Technologien ziehen notwendig Veränderungen in nahezu allen Lebensbereichen und damit auch bei den dafür geschaffenen Datenschutzbestimmungen nach sich. Seit ihren Anfängen haben sich die Anforderungen an den Schutz personenbezogener Daten laufend stark verändert. Nicht nur, aber besonders auch aufgrund des Erfolges des Internets (z. B. schnell steigende Rechner- und Leitungskapazitäten, Ausweitung und fortlaufende Verbesserung von Software sowie von mobilen Anwendungen) und der zunehmenden Vernetzung in den Diensten und Anwendungen des Web 2.0 bis hin zu einer praktisch allgegenwärtigen rechnergestützten Informationsverarbeitung ("ubiquitous computing") haben sich die Herausforderungen an den Datenschutz in den letzten Jahren potenziert.

Sowohl der nationale als auch der europäische Gesetzgeber sind diesem rasanten technischen und kulturellen Wandel in Teilen gefolgt. Seit den 1970er Jahren wurden daher die datenschutzrechtlichen Bestimmungen immer wieder angepasst und fortgeschrieben. Dies hat dazu geführt, dass in Deutschland mittlerweile vergleichsweise sehr differenzierte Aussagen sowohl zu den Inhalten als auch zu den Grenzen des Datenschutzes existieren. Obwohl bereits mehrere Anläufe zu einer grundsätzlichen Modernisierung auf nationaler und auf europäischer Ebene unternommen wurden, konnten sie bisher allerdings noch nicht erfolgreich abgeschlossen werden. Aufgrund des technologischen Fortschritts steht der Gesetzgeber jedoch weiterhin unter einem ständigen Veränderungs- und Nachbesserungsdruck, um ein Leerlaufen bestehender Regelungen aufgrund des technologischen Fortschritts zu vermeiden. Hinzu kommt, dass auch die zu schützenden Werte in einer digitalen Gesellschaft in dem Maße weiter an Wert und Bedeutung zunehmen werden, in dem diese durch den technologischen Wandel unter Druck geraten. Viele datenschutzrechtliche Grundprinzipien beruhen noch immer auf dem Schutzmodell der 1970er Jahre. Ihr Fortbestand und ihre Anwendbarkeit auf die digitale Gesellschaft werden daher vor dem Hintergrund der großen Anzahl neu aufgeworfener Fragen und Probleme kritisch diskutiert.

Auch wenn der Datenschutz einem gesellschaftlichen Wandel und somit auch unterschiedlichen „Strömungen“ unterliegt, sind sich die Mitglieder der Enquete-Kommission einig, dass das Grundrecht auf informationelle Selbstbestimmung nach wie vor Geltung beansprucht und dieser Anspruch auch nicht aufgegeben werden darf. Es ist ein Grundelement ei-

ner freien und demokratischen Kommunikationsverfassung und damit elementare Funktionsbedingung eines freiheitlich-demokratischen Gemeinwesens, das auf die Handlungs- und Mitwirkungsfähigkeit seiner Bürger angewiesen ist. Es vermag über die mittelbare Drittwirkung auf das Privatrecht einzuwirken und kann den Gesetzgeber in seinem objektiv-schutzrechtlichen Gehalt zu effektiven Schutzmaßnahmen verpflichten. In der digitalen Gesellschaft ist ihm und seiner adäquaten Ausgestaltung ein noch höherer Wert beizumessen.

Gesellschaftliche Veränderungen hinsichtlich der Wahrnehmung des Umgangs mit (personenbezogenen) Daten im Internet sind in Deutschland spätestens seit der breiten, öffentlichen Diskussion über Anbieter von Geodatendiensten im Jahr 2010 erkennbar. Auch wenn sich diese öffentliche Diskussion aus datenschutzrechtlicher Sicht an einem wenig geeigneten Thema entzündete, weil es sich zumindest bei den bildmäßig erfassten Hausfassaden um überwiegend öffentlich wahrnehmbare Objekte handelt, bei denen bereits der Personenbezug streitig ist, so kommt darin doch eine zunehmende Besorgnis gegenüber den möglichen Folgen des technologischen Fortschritts im Internet zum Ausdruck.

Die gesellschaftliche Reaktion auf die genannten Veränderungen sind in Deutschland deutlich. In Umfragen[1] wünscht sich regelmäßig eine deutliche Mehrheit der Bundesbürger einen verbesserten Schutz ihrer Daten. Denn viele Bürger fürchten sich vor dem Missbrauch ihrer personenbezogenen Daten, besonders bei der Nutzung des Internet.

Beispiele wie Google Street View oder der vergleichbare Dienst Microsoft Streetside, aber auch z. B. die Möglichkeiten, in sozialen Netzwerken Fotos und Adressbücher (und damit Daten Dritter) einzustellen, führen dazu, dass es zunehmend schwerer wird, sich einer ungewollten Erhebung und –weiterverarbeitung der personenbezogenen Daten im Internet gänzlich zu entziehen. Hierdurch kann auch eine Verschiebung der „Handlungslast“ auf die Betroffenen eintreten. Dies gilt insbesondere für den Fall, dass er nicht mit einer Veröffentlichung seiner personenbezogenen Daten einverstanden war. Häufig muss er nun von sich aus aktiv tätig werden, um entstandene digitale Spuren zu entfernen. Doch Besorgnis und Zutrauen liegen nicht weit auseinander. So werden viele der mit dem Schlagwort Web 2.0 umschriebenen neuen Anwendungen und Dienste bereits nach kurzer Zeit ausgiebig und extensiv auch von Nutzern in Deutschland genutzt. Dies legt die Vermutung nahe, dass Einschätzungen zu den möglichen Folgen einer solchen Nutzung für das eigene oder das Recht anderer auf informationelle Selbstbestimmung oftmals vernachlässigt werden oder aber bei einer Nutzen-Risiko-Abwägung der Nutzen zu überwiegen scheint. Ein Beispiel hierfür stellen einmal mehr die Sozialen Netzwerke als wesentlicher Kern des Web 2.0 dar. Schon die ersten Formen wurden sehr ausgiebig von

[1] siehe u. a. „Datenschutz im digitalen Zeitalter – Trends und Spannungsfelder“, Studie von TNS im Auftrag von Microsoft, Mai/Juni 2011, abrufbar unter: *download.microsoft.com/.../TNS_Studie_Datenschutz_im_Internet2011.pdf;* „Die Einstellung der Deutschen zum Thema Datenschutz“, Studie des Instituts für Demoskopie Allensbach im Auftrag der SCHUFA Holding AG, September 2010; "Datenschutz im Internet", BITKOM, Juni 2011, abrufbar unter: http://www.bitkom.org/files/documents/BITKOM_Publikation_Datenschutz_im_Internet.pdf

mehreren Millionen Menschen unterschiedlichen Alters weltweit genutzt. Bis heute haben sie nichts an ihrer Attraktivität eingebüßt. Im Gegenteil: rasante gesellschaftliche und auch politische Veränderungen lassen sich weltweit u. a. auch auf Soziale Netzwerke als Kommunikationsinstrument zurückführen. Die auf der Mitteilung und Eingabe von personenbezogenen Daten (z. B. Lebensweisen, Gewohnheiten und Präferenzen) basierenden Netzwerke haben sich jedoch auch schon als Bumerang für manchen Nutzer erwiesen. Insbesondere dann, wenn Dritte sich unberechtigt Zugang zu schützenswerten Daten verschafft haben oder bereits eingestellte personenbezogene Daten nachträglich nicht mehr „zurückgeholt“ werden konnten. Besonderen Aufwand erfordern auch die datenschutzrechtlichen Grundeinstellungen für die Nutzer. So gelten pseudonyme Nutzungen bei Facebook als mit den AGB unvereinbar. Ein Teil der eingestellten Daten und Informationen steht zunächst allen Mitgliedern und teilweise auch der Öffentlichkeit zur Verfügung, wenn diese nicht aktiv von sich aus Veränderungen an den Einstellungen vornehmen.

In der digitalen Gesellschaft zeichnet sich eine Entwicklung dahingehend ab, dass Dienste oder Anwendungen, die mit einer Individualisierung einhergehen, als attraktiver wahrgenommen werden. Eine solche Individualisierung setzt die Eingabe oder Bereitstellung personenbezogener Daten durch den Nutzer selbst voraus. Oft erheben und verarbeiten auch die Anbieter vom Nutzer zunächst unbemerkt Daten, um individualisierte Dienste zur Verfügung zu stellen. Der Nutzer und sein Verhalten werden damit zum Mittelpunkt. Bei vielen Diensten und Anwendungen werden aber auch personenbezogene Daten erhoben, obwohl dies nicht unmittelbar zu einem erkennbaren Mehrwert für den Nutzer führt.

Für den Nutzer hat all dies zur Folge, dass er sich fortlaufend an die veränderten Gegebenheiten anpassen muss, will er neue Dienste bzw. die Weiterentwicklung bestehender Dienste weiterhin nutzen und dabei wirksam von seinem Recht auf informationelle Selbstbestimmung Gebrauch machen. Hierzu bedarf es nicht nur des notwendigen Wissens und damit eines entsprechend kompetenten Umgangs mit dem Medium Internet, sondern auch einer permanenten Aktualisierung und Erweiterung des Wissens über die Funktionsweisen und Auswirkungen der vorhandenen und benutzten Anwendungen und Dienste.

Auch für die Anbieter steigt durch diese Ausrichtung ihrer Geschäftstätigkeit die Verantwortung im Umgang mit den Daten und Informationen ihrer Kunden. Hinreichend konkrete Vorgaben für die Einhaltung und Umsetzung datenschutzrechtlicher Bestimmungen stärken dabei sowohl das Vertrauen der Nutzer als auch die Rechtssicherheit der Anbieter. In diesem Zusammenhang sollte der Datenschutz nicht als Grenze technologischer Entwicklungen gesehen, sondern auch als Chance zur Erhöhung der Akzeptanz neuer Technologien ausgestaltet werden.

Die Beratungen in der Enquete-Kommission zum Thema Datenschutz und Persönlichkeitsrechte haben gezeigt, dass es einen breiten Konsens über die Grundprinzipien, Ziele und Werte des Datenschutzes gibt. Alle Mitglieder der Enquete-Kommission heben hervor, dass Datenschutz und eine Gewährleistung des Grundrechts auf informationelle Selbstbestimmung Akzeptanz und Vertrauen schaffen. Beide sind unabdingbar für den technologischen Fortschritt in einer digitalen Gesellschaft.

Vor diesem Hintergrund gibt die Enquete-Kommission nachfolgende Handlungsempfehlungen:

## II. Vorgaben für nationalen, europäischen und internationalen Datenschutz

Die Zukunft des Datenschutzes liegt längst nicht mehr allein auf nationaler, sondern auf europäischer und insbesondere auf internationaler Ebene. Die Enquete-Kommission begrüßt daher grundsätzlich das Ziel der Mitteilung der Europäischen Kommission vom 04.11.2010 - KOM (2010) 609 -, das bestehende Datenschutzrecht auf europäischer Ebene zu novellieren und zu modernisieren, um es so an die neuen technischen Anforderungen des digitalen Zeitalters anzupassen. Insbesondere die Zielsetzung der Kommission, die Rechte des Einzelnen zu stärken, den Verwaltungsaufwand für die Unternehmen zu verringern und ein einheitlich hohes Schutzniveau in und außerhalb der EU zu gewährleisten, unterstützt die Enquete-Kommission grundsätzlich.

Aber auch die Anstrengungen der EU-Kommission, die Zusammenarbeit mit Drittstaaten und internationalen Organisationen, einschließlich Vereinter Nationen, Europarat und OECD sowie internationalen Normungsorganisationen wie dem Europäischen Komitee für Normung (CEN), der Internationalen Organisation für Normung (ISO), dem World Wide Web Consortium (W3C) und der Internet Engineering Task Force (IETF) zu verbessern, finden die Unterstützung durch die Enquete-Kommission. Aus Sicht der Enquete-Kommission sollte daher die Bundesregierung sowohl prüfen, ob sie ihre eigenen Anstrengungen in den vorgenannten Gremien im Hinblick auf den Datenschutz intensivieren kann als auch ob es der Anregung weiterer Verhandlungsmandate für die EU-Kommission bedarf.

1. Die Enquete-Kommission sieht Handlungsbedarf darin, die Wettbewerbsposition deutscher Anbieter von Internetdiensten gegenüber ausländischen Mitbewerbern durch den Gesetzgeber weiter fortlaufend zu analysieren. Gerade im Bereich der sozialen Netzwerke halten sich ausländische Anbieter, die keinen Sitz in Deutschland haben, teilweise nicht an nationale datenschutzrechtliche Bestimmungen. Zugleich besteht auf nationaler Ebene ein Vollzugsdefizit, das geltende Recht auch wirksam gegenüber ausländischen Anbietern von Diensten umzusetzen, wenn diese über keinen inländischen Sitz verfügen. Die Enquete-Kommission regt daher eine kurzfristige Befassung des Deutschen Bundestags an, wie die Probleme des

Anwendungsbereichs und bestehende Vollzugsdefizite zielgerichtet behoben werden können. Im Rahmen einer solchen Diskussion gibt die Enquete-Kommission zu bedenken, dass nationales Datenschutzrecht nicht immer bei weltweiten Angeboten angewendet werden kann.

2. Aus Sicht der Enquete-Kommission sollte die Bundesregierung prüfen, ob zukünftig bei international und europaweit tätigen Unternehmen mit mehreren Niederlassungen in Mitgliedstaaten der EU in Fragen des Datenschutzes im Internet eine stärkere Koordinierung der datenschutzrechtlichen Aufsicht sowohl auf europäischer Ebene wie auch nationaler Ebene, etwa durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, wahrgenommen werden sollte. Hierzu wäre die Schaffung eines derartigen verbindlichen Abstimmungsverfahrens erforderlich.

3. Aus Sicht der Enquete-Kommission ist es fraglich, ob die bisherigen nationalen und europäischen Regelungen zur Auftragsdatenverarbeitung für eine rechtssichere Teilnahme von Unternehmen am so genannten Cloud Computing ausreichend sind. Im Zuge der Novellierung der Datenschutzrichtlinie 95/46/EG sollten daher Regelungen geschaffen werden, die Unternehmen die Nutzung von Cloud Computing und neue Entwicklungen in diesem Bereich ermöglichen. Diese Regelungen sollten gleichzeitig ein hohes Datenschutzniveau sicherstellen und damit die Belange der Nutzer berücksichtigen sowie den Wirtschaftsstandort Europa stärken.

4. Aus Sicht der Enquete-Kommission muss ein novelliertes europäisches Datenschutzrecht der modernen Arbeitsweise international organisierter Konzerne stärker als bisher Rechnung tragen. Datenschutz und Datenaustausch in verbundenen Unternehmen müssen unter Beachtung des Rechts auf informationelle Selbstbestimmung rechtssicher und damit ggf. vereinfacht ausgestaltet werden.

5. Die Enquete-Kommission regt eine Prüfung auf europäischer Ebene an, ob dem Datenschutzrecht ein wettbewerbsschützender Charakter zugeschrieben werden kann. Schließlich könnte dies zu einer stärkeren gegenseitigen Kontrolle der Marktteilnehmer im nicht-öffentlichen Bereich und somit zu einer besseren Durchsetzbarkeit des Datenschutzes führen.

## III. Datenschutz als Standortfaktor

Die Einhaltung von datenschutzrechtlichen Bestimmungen und die Schaffung eines hohen Datenschutzniveaus könnten gerade im europäischen und internationalen Vergleich zu einem positiven Wirtschaftsfaktor und somit zu einem vermarktungsfähigen Alleinstellungsmerkmal werden. Diese dürfen daher nicht nur als möglicher Kostenfaktor ge-

sehen werden. Das Bewusstsein der Nutzer für datenschutzfreundliche Angebote muss jedoch weiter gestärkt werden, damit sie den Markt entsprechend mitgestalten.

Die Enquete-Kommission regt an, nationale und verstärkt auch internationale Initiativen für Datenschutz zusammenzufassen.

Nationale Initiativen könnten dabei unter einem Markenzeichen wie beispielsweise „Made in Germany“ oder „Made in Europe“ zusammengeführt werden, um so das hohe nationale Datenschutzniveau als Qualitätsmerkmal besser herausstellen und vermarkten zu können. Einen wichtigen Beitrag hierzu können freiwillige Gütesiegel und Audits, die auf verbindlichen Auditierungsverfahren beruhen und von unabhängiger Stelle angeboten und durchgeführt werden, leisten.

## IV. Einwilligung

Die Enquete-Kommission hat in ihrem Bericht herausgearbeitet, dass eine informierte und freiwillige Einwilligung des Einzelnen oft nicht stattfindet – und zwar aus unterschiedlichen Gründen. Darüber hinaus ist ein Überblick für die Nutzerinnen und Nutzer über bereits erteilte Einwilligungen nur schwer zu behalten.
Deshalb empfiehlt die Enquete-Kommission dem Deutschen Bundestag,

1. die Informationspflichten so auszugestalten, dass die Informationen von der Art und vom Umfang her die Grundlage für informierte und freiwillige Einwilligungen bilden,

2. die 2009 verabschiedete Regelung der elektronischen Einwilligung nach § 28 Abs. 3a BDSG in den Allgemeinen Teil des BDSG unter § 4a BDSG zu übernehmen, damit ihr Anwendungsbereich sich nicht nur auf Werbeeinwilligungen, sondern auf alle elektronischen Einwilligungen erstreckt,

3. zu prüfen, ob es erforderlich erscheint, § 13 Abs. 2 TMG im Hinblick auf ein gesetzlich geregeltes Opt-in-Verfahren (bei dem Betroffene aktiv in die Datenerhebung und –verarbeitung einwilligen, z. B. durch Ankreuzen, Haken setzen etc.) zu konkretisieren und die Anforderungen technikneutral auszugestalten,

4. zu prüfen, ob eine zeitliche Befristung von Einwilligungen sinnvoll und zielführend ist und welche Konsequenzen sich hieraus für das bestehende Recht der Einwilligung ergeben könnten,

5. in Betracht zu ziehen, den Widerruf der Einwilligung im BDSG klarstellend zu regeln. Dies gilt insbesondere mit Blick auf die Weitergabe von Daten. Hier wird empfohlen, dass bereits der Widerruf bei der Stelle genügt, die erstmals die Daten

erhoben und weitergegeben hat. Der Widerruf wäre durch diese Stelle an die weiteren Stellen weiterzureichen,

6. die in der E-Privacy-Richtlinie[2] vorgesehenen Anforderungen an Information und Zustimmung bei der Platzierung von Cookies für einen wirksamen Schutz bei der Verarbeitung personenbezogener Daten durch den Gesetzgeber in deutsches Recht umzusetzen.

## V. AGB und Datenschutz

Insbesondere die in kurzem zeitlichen Abstand erfolgenden mehrfachen Änderungen von Datenschutzbestimmungen in Allgemeinen Geschäftsbedingungen von Anbietern von Diensten im Internet, darunter auch Anbieter Sozialer Netzwerke, werfen rechtliche Fragen auf. Die Enquete-Kommission fordert, gesetzlich klarzustellen, dass Anbieter von Diensten verpflichtet sind, den rechtzeitigen Vorabzugang veränderter Datenschutzbestimmungen an alle Nutzer sicherzustellen.

Auch wenn es Ziel aller Anbieter von Diensten sein sollte, den Nutzern Datenschutzinformationen in prägnanter und kurzer Form anzubieten, um so eine bewusste Kenntnisnahme deutlich zu erleichtern und das Vertrauen in netzbasierte Anwendungen und Transaktionen zu stärken, gelingt dies nur in den wenigsten Fällen. Nach wie vor müssen viele Nutzer zunächst umfangreiche und teilweise auch schwer verständliche und oft juristisch formulierte Allgemeine Geschäftsbedingungen zur Kenntnis nehmen. Die Bundesregierung sollte daher prüfen,

1. ob die Möglichkeit besteht, leicht verständliche und nachvollziehbare Datenschutzerklärungen zu entwickeln, die für eine Vielzahl von Angeboten im Internet anwendbar sind. Damit könnte die Transparenz für die Nutzer erhöht und eine erhebliche Vereinfachung für die betroffenen Unternehmen erzielt werden,

2. ob die Möglichkeit besteht, Verwender von Datenschutzerklärungen in Allgemeinen Geschäftsbedingungen gesetzlich zu verpflichten, diese bereits auf der Startseite kurz und verständlich zum Abruf bereit zu halten.

[2] 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. EG Nr. L 201 vom 31. Juli 2002, geändert durch Artikel 2 Nr. 5 der Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009, ABl. EU Nr. L 337 vom 18. Dezember 2009.

## VI. Privacy by design / by default

„Privacy by design“ und „privacy by default“ orientieren sich an den Vorgaben der Datenvermeidung und Datensparsamkeit und damit an den zentralen Leitlinien des Datenschutzrechts.

Elemente von „privacy by design“ sind beispielsweise eine grundsätzliche Verschlüsselung von Daten oder die automatisierte Löschung von Daten nach Funktionserfüllung.

Die Enquete-Kommission empfiehlt dem Deutschen Bundestag, das Prinzip „privacy by design“ grundsätzlich als verpflichtende Vorgabe bei der Entwicklung und dem Einsatz neuer Technologien zu formulieren.

Der Grundsatz „privacy by default“ gewährleistet, dass die Nutzer bei der Reduzierung des Schutzniveaus von Diensten, Technologien und Anwendungen aktiv entscheiden müssten, welche Veränderungen des höchstmöglichen Schutzniveaus sie zulassen möchten.

Die Enquete-Kommission sieht im Prinzip des „privacy by default“ eine wichtige Option zur Gestaltung von elektronischen Diensten und Anwendungen im Internet (z. B. bei deutschen sozialen Netzwerken oder so genannten „location based services“). Die Anwendung von datenschutzfreundlichen Voreinstellungen erscheint gerade angesichts der Vielfalt der einzelnen technischen Einstellungen vieler webbasierter Angebote und der oftmals nicht leicht erkennbaren Konsequenzen sinnvoll. Sie begrüßt daher, dass viele Anbieter von Diensten im Internet sich bereits freiwillig zu einer Umsetzung von „privacy by default“ verpflichtet haben.

Die Enquete-Kommission regt an, die bereits bestehenden gesetzlichen Vorgaben der Datenvermeidung und Datensparsamkeit (vgl. § 3e BDSG) mit dem Prinzip „privacy by default“ gesetzlich zusammenzuführen.

## VII. Verfallsdaten

Die Enquete-Kommission empfiehlt dem Deutschen Bundestag, die Diskussion um Verfallsdaten im Internet auf nationaler und europäischer Ebene weiter zu verfolgen, denn die Entwicklung von technologischen Lösungen für ein Vergessen im Internet steht erst am Anfang. Die Enquete-Kommission sieht in der Initiative der Bundesregierung, mit Hilfe eines Ideenwettbewerbs entsprechende technische Möglichkeiten zu entwickeln, einen richtigen Ansatz.

Die Enquete-Kommission empfiehlt dem Deutschen Bundestag daher

Anreize zu schaffen, die Verfallsdatentechnik und andere technische Maßnahmen zum Schutz der Privatsphäre (etwa *„sticky policies“*)[3] möglichst intensiv weiterzuentwickeln. Je stärker bereits die technische Infrastruktur datenschutzrechtliche Aspekte berücksichtigt, desto leichter wird es Nutzerinnen und Nutzern fallen, ihre Rechte aktiv wahrzunehmen.

## VIII. Selbstdatenschutz und Medienkompetenz

Die Enquete-Kommission hält die Ausbildung und kontinuierliche Förderung von Kompetenz und Eigenverantwortung der Nutzer digitaler Medien und dem damit verbundenen Umgang mit eigenen und fremden personenbezogenen Daten für unverzichtbar. Sie geht davon aus, dass die Nutzung zukünftiger (mobiler) Internetdienste die Entwicklung hin zu einem nutzerorientierten Datenschutzmanagement noch weiter verstärken wird. (Selbst-)Datenschutz, Datenschutzmanagement und IT-Sicherheit müssen deshalb kontinuierlich thematisiert und gestärkt werden. Bildungsangebote müssen für alle Altersstufen entwickelt und angeboten werden.

Die Enquete-Kommission empfiehlt dem Deutschen Bundestag deshalb, darauf hin zu wirken, dass die bisherigen Akteure, wie beispielsweise die Daten- und Verbraucherschutzverbände, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheitzusammen mit der geplanten Stiftung Datenschutz noch stärker als bisher zur Förderung von Selbstdatenschutz und Medienkompetenz beitragen. Die Enquete-Kommission betont, dass über die finanzielle Ausstattung der Landesbeauftragten für den Datenschutz allein die Länder entscheiden, unterstützt aber eine Fortführung des Engagements in diesem Bereich.

Hinsichtlich weiterer Handlungsempfehlungen wird auf die Projektgruppe Medienkompetenz und die Handlungsempfehlungen zur Stiftung Datenschutz verwiesen.

## IX. Soziale Netzwerke

Aus datenschutzrechtlicher Sicht werfen soziale Netzwerke eine Reihe von spezifischen Fragestellungen auf. Diese können in Abhängigkeit von den konkreten Produkten der

[3] Mit sticky policies wird eine Art von digitalem Rechtemanagement für Daten bezeichnet: Durch angeheftete Metadaten werden zugelassene Verwendungszwecke definiert. Mit "sticky" ist gemeint, dass diese Metadaten bei Kopiervorgängen "haften bleiben", also mitübertragen werden (siehe auch die Studie „Ergänzende und alternative Techniken zu Trusted Computing (TC-Erg./-A.) - Teil 1-“ im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik, 29.01.2010, S. 20 f., abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/TC_ErgA/TC-ErgA_Teil1.pdf)

jeweiligen Netzwerkanbieter variieren. Von grundlegender Bedeutung für die Bewertung ist eine klare Trennung zwischen der Datenverarbeitung durch die Anbieter der Netzwerke selbst und der Datenverarbeitung der Nutzer der Plattformen. Die Enquete-Kommission regt daher an, bestehende Vollzugsdefizite schnellstmöglich zu beseitigen, und empfiehlt zugleich dem Deutschen Bundestag, den Datenschutz bei Sozialen Netzwerken in geeigneter Weise zu verbessern.

Für soziale Netzwerke sollten datenschutzfreundliche Grundeinstellungen ("privacy by default") gesetzlich vorgeschrieben sein. Diese sollten auch die Funktionalität beinhalten, dass in Sozialen Netzwerken abgelegte Profile in externen Suchmaschinen nur nach ausdrücklicher Zustimmung des Nutzers auffindbar werden. Zudem müssen die Nutzer eines Sozialen Netzwerks jederzeit ihren Account einfach und nachhaltig elektronisch löschen können, d. h. es muss auch zu einer Löschung der Daten auf dem Server des Anbieters kommen. Die Weitergabe von personenbezogenen Daten durch die Betreiber Sozialer Netzwerke an Dritte darf neben gegebenenfalls geltenden gesetzlichen Erlaubnistatbeständen nur nach ausdrücklicher Einwilligung durch den Nutzer zulässig sein.

## X. Datenschutzaufsicht

Die bestehenden Regelungen zur Datenschutzaufsicht sollten aus Sicht der Enquete-Kommission dahingehend überprüft werden, ob sie auch bei den neuen Organisationsformen und vernetzten Prozessen (z. B. Cloud-Computing, Auftragsdatenverarbeitung im Konzern, internationale Diensteanbieter im Internet) einen effektiven Datenschutz sicherstellen. Es sollten die Anordnungsbefugnisse des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit an dessen Aufsichtsbefugnisse angepasst werden.
Darüber hinaus hat das Urteil des Europäischen Gerichtshofes vom 09. März 2010 zur Unabhängigkeit der deutschen Datenschutzbehörden im nicht-öffentlichen Bereich noch einmal die besondere Rolle der Kontroll- bzw. Aufsichtsbehörden für den Datenschutz hervorgehoben. Aus Sicht der Enquete-Kommission ist es daher unabdingbar, dass die Kontroll- und Aufsichtsbehörden über ausreichende finanzielle, personelle und technische Mittel verfügen, um die ihnen übertragenen Aufgaben effizient und angemessen zu erfüllen. Denn es ist wichtig, dass die Kontroll- und Aufsichtsbehörden die vorhandenen gesetzlichen Befugnisse intensiv ausüben können, damit die bestehenden Datenschutzgesetze effektiv durchgesetzt, Rechtssicherheit geschaffen werden kann.

Die Enquete-Kommission regt darüber hinaus an, dass die Entscheidungen des Düsseldorfer Kreises sowie Einzelpositionen der dort vertretenen Kontroll- und Aufsichtsbehörden grundsätzlich zukünftig veröffentlicht werden und nur in begrenzten Ausnahmefällen eine Veröffentlichung unterbleibt. Auch wenn die Entscheidungen des Düsseldorfer Kreises formal keine unmittelbaren normativen Wirkungen entfalten können, können sie für betroffene Unternehmen zumindest grundlegende Anhaltspunkte bei bestehenden Rechtsunsicherheiten bieten.

## XI. Vorbildwirkung öffentlicher IT-Projekte

Die Enquete-Kommission weist darauf hin, dass sowohl bei der Planung von öffentlichen IT-Projekten und eGovernment-Angeboten als auch bei der späteren Aus- und Durchführung die aktuellen technischen und organisatorischen Anforderungen an einen wirksamen Datenschutz in besonderer Weise beachtet und bei technischen Weiterentwicklungen auch fortgeschrieben werden müssen. Nur so können aufkommende Zweifel am sicheren Umgang mit personenbezogenen Daten von Beginn an ausgeräumt werden. Öffentliche IT-Projekte sollten mit Blick auf ihre Vorbildwirkung etwa für die Privatwirtschaft auf hohem Datenschutzniveau durchgeführt werden.

In den letzten Jahren haben verschiedene IT-Großprojekte zum Teil Kritik von Datenschützern erfahren. Die Enquete-Kommission empfiehlt daher,

1. dass öffentliche IT-Projekte auf hohem Schutzniveau basieren und ihrer Vorbildwirkung gerecht werden,

2. dass eGovernment-Angebote im Bereich der Dienstleistungen für Bürgerinnen und Bürger den aktuellsten technischen und organisatorischen Anforderungen an einen wirksamen Datenschutz genügen müssen,

Darüber hinaus empfiehlt die Enquete-Kommission bei zentralen IT-Projekten, auch bei jenen, die von der EU eingeleitet werden,

1. den Datenschutz bereits von Beginn an in der Konzeption zu berücksichtigen. Wo dies nicht der Fall ist, muss es auch weiterhin möglich sein, die Umsetzung entsprechender Projekte zu verweigern. Wenn Aufträge für die Entwicklung solcher Projekte vergeben werden, sollten sie stets die Programmierung entsprechender technischer Begrenzungen beinhalten. Im Interesse der Verwirklichung möglichst vorbildlichen Datenschutzes sollte dies bereits bei der finanziellen Planung berücksichtigt werden.

2. den besonderen datenschutzrechtlichen Herausforderungen eines verwaltungsübergreifenden Arbeitens zu begegnen. Um national wie international bei Outsourcing einen unsensiblen Umgang mit Datenschutzbelangen frühzeitig zu verhindern, bedarf es hier einer stärkeren aktiven Einbeziehung datenschutzrechtlicher Aspekte in alle Planungsetappen.

Zudem empfiehlt die Enquete-Kommission dem Deutschen Bundestag, die Forschung im Bereich des Datenschutzes auch weiterhin mit öffentlichen Mitteln zu fördern und

zusätzliche finanzielle Anstrengungen zu prüfen, um die Entwicklung von Datenschutztechnologien zu fördern.

## XII. Smartgrids und andere intelligente Netze

Die Möglichkeit, mithilfe intelligenter Stromzähler den tatsächlichen Stromverbrauch kontrollieren zu können, kann einen ökonomischen Mehrwert für den Verbraucher schaffen und beträchtliche ökologische Vorteile mit sich bringen. Bei ihrem Betrieb fallen jedoch auch umfangreiche und differenzierte Datenbestände (Lastprofile) an, die durch geeignete technische und organisatorische Maßnahmen wirksam vor dem Zugriff durch Unberechtigte geschützt werden müssen. Auch muss sichergestellt werden, dass die Datenhoheit, insbesondere ausreichende Kontrollmöglichkeiten, grundsätzlich beim Verbraucher verbleiben und dieser selbst darüber entscheiden kann, wem er welche Daten zur Verfügung stellen möchte. Dabei muss angesichts der zunehmenden Bedeutung regenerativer Energien bei der Stromversorgung ein effektives Netzmanagement möglich sein.

Es muss sichergestellt werden, dass personenbezogene Daten in der Regel nur den Verbrauchern zur Verfügung gestellt und Verbrauchswerte nur für die Abrechnung personenbezogen verwendet werden dürfen. Darüber hinaus sollten bei ihrer Verwendung zu Zwecken eines verbesserten Netzmanagements Verschlüsselungstechniken zur Anwendung kommen, die eine datenschutzkonforme Datenübermittlung ermöglichen. Zudem müssen ausreichende Sicherheitsvorkehrungen vorgehalten werden, die einen unerlaubten Zugriff auf die Daten verhindern.

Nicht nur im Energiesektor werden derzeit „intelligente Netze“ aufgebaut, zu deren Betrieb umfassend Daten kommuniziert werden müssen. Auch im Verkehrssektor (Verkehrstelematik und E-Mobility), im Gesundheitswesen (Gesundheitstelematik und E-Health) und dem Bildungswesen (E-Learning) befinden sich „intelligente Netze“ in Planung. In diesen Netzen sollen künftig Daten über das eigene Mobilitätsverhalten bis hin zu sensibler Daten wie dem persönlichen Gesundheitszustand und der Gesundheitshistorie kommuniziert werden.

„Datensparsamkeit“ und „Datenvermeidung“ im Rahmen der für die Nutzung von Zukunftstechnologien erforderlichen Datenverarbeitung sollten Ausgangspunkt entsprechender gesetzgeberischer Initiativen sein. Die Enquete-Kommission empfiehlt dem Deutschen Bundestag, in diesen Bereichen die Notwendigkeit gesetzlicher Vorgaben eingehend zu prüfen und darauf hinzuwirken, dass neue Technologien auch bei „intelligenten Netzen“ datenschutzkonform ausgestaltet werden. Einzelfallgesetze für bestimmte Dienste sind dabei nach Möglichkeit zu vermeiden.