I

(Entschließungen, Empfehlungen und Stellungnahmen)

STELLUNGNAHMEN

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

Stellungnahme des Europäischen Datenschutzbeauftragten zur Stärkung des Vertrauens in die Informationsgesellschaft durch die Förderung des Schutzes von Daten und Privatsphäre

(2010/C 280/01)

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 7 und 8,

gestützt auf die 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 ([1]),

gestützt auf die 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 ([2]),

gestützt auf die Richtlinie 45/2001/EG des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ([3]), insbesondere auf Artikel 41 —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. EINLEITUNG

1. Informations- und Kommunikationstechnologien (IKT) eröffnen unglaubliche Möglichkeiten in fast allen Bereichen unseres Lebens — der Art, wie wir arbeiten, spielen, soziale Kontakte pflegen und erziehen. Sie sind für die heutige Informationswirtschaft und die Gesellschaft im Allgemeinen unverzichtbar.

2. Die Europäische Union ist eine weltweit führende Kraft in der modernen IKT und entschlossen, dies auch zu bleiben. Um dieser Herausforderung zu begegnen, wird die Europäische Kommission voraussichtlich demnächst eine neue europäische digitale Agenda verabschieden, die Kommissionsmitglied Kroes als Priorität bestätigt hat ([4]).

3. Der Europäische Datenschutzbeauftragte (EDSB) sieht den Nutzen der IKT und schließt sich der Auffassung an, dass die EU alles in ihren Kräften Stehende tun sollte, um deren Entwicklung und generelle Einführung zu beschleunigen. Darüber hinaus stimmt er der Meinung der Kommissionsmitglieder Kroes und Reding zu, dass im Mittelpunkt dieses neuen Umfelds der einzelne Nutzer stehen sollte ([5]). Der Nutzer sollte sich darauf verlassen können, dass die IKT in der Lage sind, die Sicherheit seiner Daten zu schützen und ihre Verwendung zu kontrollieren, und er sollte darauf vertrauen können, dass seine Datenschutzrechte im digitalen Raum gewahrt bleiben. Die Achtung dieser Rechte ist entscheidend, wenn es gilt, das Vertrauen der Verbraucher zu gewinnen. Und dieses Vertrauen ist unabdingbar, wenn die Bürger neue Dienste annehmen sollen ([6]).

([1]) ABl. L 281 vom 23.11.1995, S. 31.
([2]) ABl. L 201 vom 31.7.2002, S. 37.
([3]) ABl. L 8 vom 12.1.2001, S. 1.

([4]) Antworten von Kommissionsmitglied Neelie Kroes zu einem Fragebogen des Europäischen Parlaments im Zusammenhang mit den Anhörungen im EP vor ihrer Ernennung.
([5]) Antworten von Kommissionsmitglied Neelie Kroes zu einem Fragebogen des Europäischen Parlaments im Zusammenhang mit den Anhörungen im EP vor ihrer Ernennung; Rede von Kommissionsmitglied Reding „A European Digital Agenda for the New Digital Consumer“ vor dem BEUC Multi-stakeholder Forum on Comsumer Privacy and Online Marketing. „Market Trends and Policy Perspectives“, Brüssel, 12. November 2009.
([6]) Siehe z. B. RISEPTIS Report, „Trust in the Information Society“, A Report of the Advisory Board, RISEPTIS (Research and Innovation on Security, Privacy and Trustworthiness in the Information Society). Abrufbar unter: http://www.think-trust.eu/general/news-events/riseptis-report.html Siehe auch: J. B Horrigan, Broadband Adoption and Use in America, FCC Omnibus Broadband Initiative, OBI Working Paper Series No 1.

4. Die EU verfügt über einen starken Rechtsrahmen zum Datenschutz/Schutz der Privatsphäre, dessen Grundsätze im digitalen Zeitalter uneingeschränkt ihre Gültigkeit behalten. Selbstgefälligkeit können wir uns jedoch nicht leisten. In vielen Fällen werfen IKT neue Fragen auf, die im vorhandenen Rahmen nicht berücksichtigt werden. Deshalb sind Maßnahmen notwendig, um sicherzustellen, dass die im EU-Recht verankerten individuellen Rechte auch in diesem neuen Umfeld weiterhin einen wirksamen Schutz bieten.

5. In dieser Stellungnahme wird erörtert, welche Maßnahmen die Europäische Union fördern oder ergreifen könnte, um die Privatsphäre des Einzelnen und den Datenschutz in einer globalisierten Welt zu gewährleisten, die auch in Zukunft technologiegeprägt sein wird. Es geht dabei um Rechtsinstrumente und Instrumente außerhalb der Gesetzgebung.

6. Nach einem Überblick über die IKT als neue Entwicklung, die sowohl Chancen als auch Risiken birgt, wird die Notwendigkeit erörtert, Datenschutz und Privatsphäre in der Praxis von Anfang an in neue Informations- und Kommunikationstechnologien zu integrieren (Grundsatz des „eingebauten Datenschutzes", auch als „Privacy by Design" bezeichnet). Es wird erörtert, dass dieser Grundsatz, wenn seine Einhaltung sichergestellt werden soll, auf mindestens zwei Wegen in den rechtlichen Rahmen des Datenschutzes eingebettet werden muss: erstens durch Aufnahme als allgemeiner, verbindlicher Grundsatz und zweitens durch Einbindung in spezielle IKT-Bereiche, die besondere Risiken für Privatsphäre/Datenschutz bergen, welche sich durch eine angemessene Gestaltung von technischer Architektur und Design verringern lassen. Diese Bereiche sind die Funkfrequenzkennzeichnung (RFID), soziale Netzwerke und Browser-Anwendungen. Abschließend werden in der Empfehlung Vorschläge zu anderen Instrumenten und Grundsätzen zum Schutz der Privatsphäre und der Daten des einzelnen Bürgers im IKT-Bereich formuliert.

7. Zu diesem Thema enthält die Stellungnahme Ausführungen zu einigen Aussagen der Artikel-29-Datenschutzgruppe in ihrem Beitrag zur öffentlichen Konsultation über die Zukunft der Privatsphäre [1]. Sie stützt sich zudem auf frühere Stellungnahmen des EDSB, z. B. auf die Stellungnahme vom 25. Juli 2007 zur Durchführung der Datenschutzrichtlinie, die Stellungnahme vom 20. Dezember 2007 zur RFID und seine beiden Stellungnahmen zur Datenschutzrichtlinie für elektronische Kommunikation [2].

II. IKT BIETEN NEUE CHANCEN, BRINGEN ABER AUCH NEUE RISIKEN MIT SICH

8. IKT sind mit anderen wichtigen Erfindungen der Vergangenheit, z. B. der Elektrizität, verglichen worden. Für eine Bewertung ihrer tatsächlichen historischen Bedeutung mag es zwar noch zu früh sein, doch die Beziehung zwischen IKT und Wirtschaftswachstum in den Industrieländern ist eindeutig. IKT schaffen Arbeitsplätze, bringen wirtschaftliche Vorteile und tragen zum allgemeinen Wohl bei. Die Bedeutung der IKT geht über die rein wirtschaftliche Dimension hinaus, da sie eine wichtige Rolle als Motor für Innovation und Kreativität spielen.

9. Darüber hinaus haben IKT die Art, wie Menschen arbeiten, soziale Kontakte pflegen und interagieren, verändert. Viele Menschen nutzen beispielsweise IKT zunehmend für soziale und wirtschaftliche Kontakte. Die Bürger können die verschiedensten neuen IKT-Anwendungen nutzen, z. B. elektronische Gesundheitsdienste, elektronische Verkehrsdienstleistungen, elektronische Behördendienste sowie innovative interaktive Unterhaltungs- und Lernsysteme.

10. Angesichts dieser Vorteile haben sich alle europäischen Institutionen verpflichtet, die IKT als notwendiges Instrument zur Erhöhung der Wettbewerbsfähigkeit der europäischen Industrie und Beschleunigung des wirtschaftlichen Wiederaufschwungs in Europa zu fördern. So verabschiedete die Kommission im April den Bericht über die digitale Wettbewerbsfähigkeit Europas [3] und leitete eine öffentliche Konsultation über angemessene Strategien zur Förderung der IKT ein. Am 7. Dezember 2009 legte der Rat einen Beitrag zu dieser Konsultation mit dem Titel „Post-i2010 Strategie - hin zu einer offenen, grünen und wettbewerbsfähigen Wissensgesellschaft" vor [4]. Das Europäische Parlament hat kürzlich einen Bericht

[1] Stellungnahme der Artikel-29-Datenschutzgruppe: Die Zukunft des Datenschutzes. Gemeinsamer Beitrag zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz der personenbezogenen Daten, angenommen am 1. Dezember 2009.

[2] Stellungnahme vom 25. Juli 2007 zu der Mitteilung der Kommission an das Europäische Parlament und an den Rat „Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie", ABl. C 255 vom 27.10.2007, S. 1; Stellungnahme des Europäischen Datenschutzbeauftragten zu der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zum Thema „Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen" (KOM(2007) 96), ABl. C 101 vom 23.4.2008, S. 1; Stellungnahme vom 10. April 2008 zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung unter anderem der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Richtlinie über den Schutz der Privatsphäre und elektronische Kommunikation), ABl. C 181 vom 18.7.2008, S. 1; Zweite Stellungnahme vom 9. Januar 2009 zur Überprüfung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

[3] Europe's Digital Competitiveness Report-Main achievements of the i-2010 strategy 2005-2009, (SEC(2009) 1060).

[4] Schlussfolgerungen des Rates „Post i-2010 Strategy- Towards and Open, Green and Competitive Knowledge Society" (Post-i2010 Strategie — hin zu einer offenen, grünen und wettbewerbsfähigen Wissensgesellschaft) (17107/09), angenommen am 18.12.2009.

verabschiedet, der der Kommission Anleitung für die Festlegung einer digitalen Agenda bieten soll ([1]).

11. Die Entwicklung der IKT bringt aber neben Chancen und Vorteilen auch neue Risiken, vor allem für die Privatsphäre und den Schutz personenbezogener Daten mit sich. IKT führen oft dazu, dass immer mehr Daten (oft ohne dass der einzelne Bürger es merkt) gesammelt, sortiert, gefiltert, übertragen oder anderweitig gespeichert werden und sich die damit zusammenhängenden Risiken somit vervielfachen.

12. So treten beispielsweise RFID-Chips bei (einigen) Verbraucherprodukten an die Stelle von Strichcodes. Durch Verbesserung des Informationsflusses in der Lieferkette (und Verringerung der Notwendigkeit von „Sicherheits"-Beständen, Ermöglichung genauerer Voraussagen usw.) soll das neue System sowohl der Wirtschaft als auch den Verbrauchern zugute kommen. Gleichzeitig erhöht sich die beunruhigende Möglichkeit, zu verschiedenen Zwecken und von verschiedenen Einrichtungen über mit RFID-Etiketten versehene persönliche Gegenstände beobachtet zu werden.

13. Ein weiteres Beispiel ist das „Cloud Computing", im Grunde genommen die Bereitstellung gehosteter Verbraucheranwendungen und anderer Dienste über das Internet. Das Spektrum reicht von Fotoarchiven, Kalendern, Webmail- und Kundendatenbanken bis zu komplexeren Unternehmensdiensten. Die Vorteile für Unternehmen und einzelne Nutzer sind klar: geringere Kosten (die Grenzkosten sinken), Ortsungebundenheit (leichter Zugang zu Daten von überall auf der Welt), Automatisierung (es sind keine spezialisierten IT-Ressourcen erforderlich, Software muss nicht auf dem neuesten Stand gehalten werden) usw. Gleichzeitig existieren sehr reale Risiken von Sicherheitsproblemen und Hackerangriffen. Dazu kommt die Befürchtung, Zugang zu und Kontrolle über die eigenen Daten zu verlieren.

14. Dass es sowohl Nutzen als auch Risiken gibt, hat sich auch in anderen Bereichen gezeigt, in denen IKT zum Einsatz kommen. Ein Beispiel sind die elektronischen Gesundheitsdienste, mit denen sich die Effizienz steigern, die Kosten verringern, die Zugänglichkeit verbessern und die allgemeine Qualität der Gesundheitsversorgung verbessern lassen. In Verbindung mit elektronischen Gesundheitsdiensten stellt sich jedoch oft die Frage nach der Legitimität einer Weiterverwendung von Gesundheitsdaten, die eine gründliche Prüfung der Zwecke erforderlich macht, zu denen sie potenziell wiederverwendet werden könnten ([2]). Mit dem zunehmenden Einsatz elektronischer Gesundheitsakten, sind zudem die Systeme selbst Gegenstand von Skandalen geworden, und es wurden bereits viele Fälle bekannt, in denen elektronische Gesundheitsakten gehackt wurden.

15. Zusammenfassend ist zu sagen, dass auch bei richtiger Bewertung und Durchführung der notwendigen Maßnahmen wahrscheinlich ein gewisses Restrisiko bleibt. Eine risikofreie Situation ist unrealistisch. Wie im Folgenden noch erörtert wird, können und müssen jedoch Maßnahmen ergriffen werden, um diese Risiken auf ein angemessenes Niveau zu verringern.

III. „EINGEBAUTER DATENSCHUTZ" ALS SCHLÜSSELINSTRUMENT ZUR GEWINNUNG VON NUTZERVERTRAUEN IN DIE IKT

16. Die potenziellen Vorteile der IKT können in der Praxis nur genutzt werden, wenn es gelingt, Vertrauen in sie zu wecken, oder — anders ausgedrückt — bei den Nutzern die Bereitschaft zu schaffen, sich aufgrund der Merkmale und des Nutzens der IKT auf sie zu verlassen. Dieses Vertrauen kann nur gewonnen werden, wenn IKT zuverlässig, sicher und vom einzelnen Nutzer kontrollierbar sind und wenn der Schutz der personenbezogenen Daten und der Privatsphäre garantiert ist.

17. Verbreitete Risiken und Mängel wie die oben geschilderten gefährden, besonders, wenn sie den Missbrauch personenbezogener Daten und die Verletzung der Privatsphäre durch ihre Weitergabe zur Folge haben, mit einiger Wahrscheinlichkeit das Vertrauen der Nutzer in die Informationsgesellschaft. Dadurch könnte die Entwicklung der IKT und ihr potenzieller Nutzen ernsthaft gefährdet werden.

18. Die Lösung für diese Risiken in Bezug auf Privatsphäre und Datenschutz kann jedoch nicht darin liegen, die Verwendung von IKT zu unterbinden bzw. auszuschließen oder ihre Förderung zu verweigern. Dies wäre weder praktikabel noch realistisch, es würde die Bürger daran hindern, die Vorteile der IKT zu nutzen, und den potenziellen Gesamtnutzen stark verringern.

19. Der EDSB hält eine positivere Lösung für möglich: die Achtung von Privatsphäre und Datenschutz bei der Planung und Entwicklung von IKT. Es ist deshalb von entscheidender Bedeutung, dass Privatsphäre und Datenschutz in den gesamten Lebenszyklus der Technologie — von der ersten Planungsphase an bis zum tatsächlichen Einsatz, ihrer Nutzung und Entsorgung — eingebettet sind. Dies wird üblicherweise als „eingebauter Datenschutz" bezeichnet und im Folgenden erörtert.

20. „Eingebauter Datenschutz" kann, je nach Situation oder Anwendung, verschiedene Maßnahmen umfassen. In manchen Fällen kann diese Vorgehensweise z. B. den Ausschluss/die Verringerung personenbezogener Daten oder die Verhinderung einer nicht notwendigen bzw. unerwünschten Verarbeitung erfordern. In anderen Fällen kann „eingebauter Datenschutz" bedeuten, dass Tools angeboten werden, die den Nutzern mehr Kontrolle über

([1]) Bericht über die Festlegung einer neuen digitalen Agenda für Europa: von der Initiative i2010 zur Initiative digital.eu (2009/2225(INI), angenommen am 18.3.2010.

([2]) So muss z. B. sorgfältig geprüft werden, ob Gesundheitsdaten, die zu Behandlungszwecken erhoben wurden, nicht verkauft oder zur Standortwahl von dezentralen Behandlungseinrichtungen, zur Einrichtung ambulanter Operationszentren oder anderweitig zur Planung künftiger Aktivitäten mit finanziellen Implikationen verwendet werden dürfen.

ihre personenbezogenen Daten ermöglichen. Solche Maßnahmen sollten bei der Festlegung von Standards bzw. beispielhaften Verfahren erwogen werden. Sie lassen sich auch in die Architektur von Informations- und Kommunikationssystemen oder den Aufbau der Einrichtungen einbauen, die personenbezogene Daten verarbeiten.

III.1. **Der Grundsatz des „eingebauten Datenschutzes": Anwendung in verschiedenen IKT-Umgebungen und Auswirkungen**

21. Der Grundsatz des „eingebauten Datenschutzes" ist in vielen verschiedenen IKT-Umgebungen notwendig. So werden z. B. im Gesundheitswesen zunehmend IKT-Infrastrukturen genutzt, die oft eine zentrale Speicherung von Gesundheitsdaten beinhalten. Die Anwendung des „eingebauten Datenschutzes" im Gesundheitswesen würde eine Bewertung der Angemessenheit verschiedener Maßnahmen erforderlich machen, z. B. der Möglichkeit, die zentral gespeicherten Daten auf ein Minimum zu reduzieren oder auf einen Index zu beschränken, Verschlüsselungsinstrumente zu verwenden, Zugangsrechte streng nach dem Grundsatz „Kenntnis notwendig" zu vergeben, nicht mehr benötigte Daten zu anonymisieren usw.

22. Auch Verkehrssysteme werden zunehmend standardmäßig mit modernen IKT-Anwendungen ausgestattet, die zu verschiedenen Zwecken und für verschiedene Funktionen mit dem Fahrzeug und seiner Umgebung interagieren. Immer mehr PKWs sind z. B. mit neuen IKT-Funktionen (GPS, GSM, Sensorennetz usw.) ausgestattet, die in Echtzeit Angaben nicht nur über den Standort, sondern auch über die technischen Bedingungen liefern. Diese Daten könnten beispielsweise verwendet werden, um das bestehende Steuersystem zur Finanzierung des Straßennetzes durch eine nutzungsabhängige Maut zu ersetzen. Die Anwendung des „eingebauten Datenschutzes" auf die Planung und Architektur solcher Systeme sollte dazu führen, dass möglichst wenig personenbezogene Daten verarbeitet und weitergeleitet werden ([1]). Nach diesem Grundsatz wäre eine dezentrale oder semizentrale Architektur, bei der die Übermittlung von Standortdaten an eine zentrale Stelle begrenzt ist, zentralisierten Systemen vorzuziehen.

23. Die genannten Beispiele zeigen, dass die Risiken für Privatsphäre und Datenschutz deutlich verringert werden können, wenn Informations- und Kommunikationstechnologien nach dem Grundsatz des „eingebauten Datenschutzes" gestaltet werden.

([1]) Siehe Stellungnahme des Europäischen Datenschutzbeauftragten vom 22. Juli 2009 zu der Mitteilung der Kommission über einen Aktionsplan zur Einführung intelligenter Verkehrssysteme in Europa und dem dazugehörigen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung eines Rahmens für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern, abrufbar unter: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_DE.pdf

III.2. **Es werden nicht genug nach dem Grundsatz des „eingebauten Datenschutzes" geplante IKT eingesetzt**

24. Eine wichtige Frage lautet: Sind IKT-Hersteller/Anbieter und die für die Datenverarbeitung Verantwortlichen an einer Vermarktung und Umsetzung des „eingebauten Datenschutzes" in den IKT interessiert? In diesem Zusammenhang muss auch die Nachfrage nach „eingebautem Datenschutz" bei den Nutzern bewertet werden.

25. 2007 veröffentlichte die Kommission eine Mitteilung, in der sie Unternehmen aufforderte, ihre Innovationskraft dafür einzusetzen, Technologien zum Schutz der Privatsphäre zu schaffen und einzuführen, um den Schutz der Privatsphäre und der personenbezogenen Daten von Anfang an in den Entwicklungszyklus einzubinden ([2]).

26. Bislang zeigen jedoch die vorliegenden Nachweise, dass es weder IKT-Herstellern noch datenverarbeitenden Stellen (sowohl in der Privatwirtschaft als auch im öffentlichen Sektor) gelungen ist, „eingebauten Datenschutz" konsequent umzusetzen oder zu vermarkten. Dafür werden verschiedene Gründe angeführt, u. a. fehlende wirtschaftliche Anreize oder institutionelle Unterstützung, unzureichende Nachfrage usw ([3]).

27. Auch die Nutzer zeigen eine relativ geringe Nachfrage nach „eingebautem Datenschutz". Nutzer von IKT-Produkten und -Dienstleistungen gehen möglicherweise mit gutem Recht davon aus, dass ihre Privatsphäre und ihre personenbezogenen Daten *de facto* geschützt sind, auch wenn dies vielfach nicht der Fall ist. In manchen Fällen sind sie einfach nicht in der Lage, die notwendigen Sicherheitsmaßnahmen zu ergreifen, um ihre eigenen personenbezogenen Daten oder die anderer zu schützen. In vielen Fällen liegt das daran, dass sie über die Risiken nicht umfassend oder auch nur teilweise informiert sind. So lassen z. B. junge Menschen die Risiken für die Privatsphäre im Allgemeinen unberücksichtigt, wenn sie personenbezogene Informationen in sozialen Netzen veröffentlichen, und ignorieren oft die Datenschutzeinstellungen. Andere Nutzer sind sich der Risiken bewusst, verfügen aber u. U. nicht über die notwendigen technischen Fachkenntnisse, um Sicherheitsverfahren — z. B. zum Schutz ihrer Internetverbindung — einzusetzen oder die Browsereinstellungen zu ändern, um ein Profiling durch Beobachtung ihres Surfverhaltens möglichst weitgehend zu verhindern.

28. Die Risiken für den Schutz der Privatsphäre und den Datenschutz sind jedoch sehr real. Werden Privatsphäre und Datenschutz nicht von Anfang an berücksichtigt, ist es oft zu spät und wirtschaftlich zu aufwändig, die Systeme zu bereinigen und den bereits entstandenen Schaden zu beheben. Die wachsende Zahl von Sicherheitsverletzungen in

([2]) Mitteilung des Europäischen Parlaments und des Rates vom 2.5.2007 (KOM(2007) 228 endg.) über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre.

([3]) Studie über die wirtschaftlichen Vorteile von Technologien zum Schutz der Privatsphäre (PET) jls/2008/D4/036.

den letzten Jahren macht dieses Problem deutlich und unterstreicht die Notwendigkeit eines „eingebauten Datenschutzes".

29. Die vorstehenden Ausführungen lassen klar erkennen, dass Hersteller und Anbieter von IKT-Technologien zur Verarbeitung personenbezogener Daten gemeinsam mit den datenverarbeitenden Stellen Verantwortung dafür tragen sollen, dass diese mit eingebauten Mechanismen zum Schutz von Daten und Privatsphäre geplant werden. In vielen Fällen würde das bedeuten, dass sie mit datenschutzfreundlichen Voreinstellungen („Privacy by Default") ausgestattet werden.

30. Vor diesem Hintergrund müssen wir prüfen, welche Schritte politische Entscheidungsträger ergreifen könnten, um „eingebauten Datenschutz" in der IKT-Entwicklung zu fördern. Eine erste Frage lautet: Enthält der bestehende Rechtsrahmen für den Datenschutz angemessene Bestimmungen, um die Anwendung des Grundsatzes eines „eingebauten Datenschutzes" sowohl durch für die Datenverarbeitung Verantwortliche als auch durch Hersteller/Entwickler zu gewährleisten? Eine zweite Frage lautet: Was sollte im Zusammenhang mit der europäischen digitalen Agenda unternommen werden um sicherzustellen, dass die IKT-Branche Vertrauen bei den Verbrauchern schafft.

IV. VERANKERUNG DES GRUNDSATZES DES „EINGEBAUTEN DATENSCHUTZES" IN GESETZEN UND POLITIK DER EU

IV.1. Der bestehende Rechtsrahmen für Datenschutz und Privatsphäre

31. Die EU verfügt über einen robusten Rechtsrahmen für Datenschutz und Privatsphäre, der in der Richtlinie 95/46/EG ([1]), der Richtlinie 2002/58/EG ([2]) und der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte ([3]) und des Gerichtshofs verankert ist.

32. Die Datenschutzrichtlinie gilt für „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten" (Erhebung, Speicherung, Weitergabe usw.). Sie schreibt vor, dass Personen oder Einrichtungen, die personenbezogene Daten verarbeiten („für die Verarbeitung Verantwortliche") bestimmte Grundsätze und Verpflichtungen einhalten. Sie räumt natürlichen Personen Rechte ein, z. B. das Recht auf Zugang zu personenbezogenen Daten. Die Datenschutzrichtlinie für elektronische Kommunikation beschäftigt sich speziell mit dem Schutz der Privatsphäre in der elektronischen Kommunikation ([4]).

33. In der geltenden Datenschutzrichtlinie ist „eingebauter Datenschutz" nicht ausdrücklich vorgeschrieben. Sie enthält jedoch Bestimmungen, nach denen in verschiedenen Situationen die Anwendung des Grundsatzes des „eingebauten Datenschutzes" durchaus erforderlich sein kann. Insbesondere Artikel 17 schreibt vor, dass der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen muss, die für den Schutz gegen die ungerechtfertigte Verarbeitung von Daten erforderlich sind ([5]). „Eingebauter Datenschutz" ist somit in sehr allgemeiner Form abgedeckt. Zudem richten sich die Bestimmungen der Richtlinie vor allem an für die Verarbeitung Verantwortliche, die personenbezogene Daten verarbeiten. Sie schreiben nicht ausdrücklich vor, dass Informations- und Kommunikationstechnologien privatsphären- und datenschutzgerecht sind, was auch Anforderungen an die Entwickler und Hersteller von IKT, einschließlich der Aktivitäten in der Standardisierungsphase, mit sich bringen würde.

34. Die Datenschutzrichtlinie für elektronische Kommunikation enthält explizitere Bestimmungen: In Artikel 14 Absatz 3 heißt es: „Erforderlichenfalls können gemäß der Richtlinie 1999/5/EG und dem Beschluss 87/95/EWG des Rates vom 22. Dezember 1986 über die Normung auf dem Gebiet der Informationstechnik und der Telekommunikation Maßnahmen getroffen werden, um sicherzustellen, dass Endgeräte in einer Weise gebaut sind, die mit dem Recht der Nutzer auf Schutz und Kontrolle der Verwendung ihrer personenbezogenen Daten vereinbar ist." Diese Bestimmung wurde jedoch noch nie angewandt ([6]).

35. Die genannten Bestimmungen der zwei Richtlinien sind zwar hilfreich, um den „eingebauten Datenschutz" zu *fördern*, reichen aber in der Praxis nicht aus, um *zu gewährleisten*, dass er in IKT verankert wird.

36. Aufgrund dieser Situation ist in den Rechtsvorschriften nicht hinreichend präzise festgelegt, dass IKT nach dem Grundsatz des „eingebauten Datenschutzes" geplant werden müssen. Auch die Befugnisse der Datenschutzbehörden reichen nicht aus, um eine Verankerung dieses Grundsatzes zu gewährleisten. Das führt zu Ineffizienz. Datenschutzbehörden können möglicherweise Sanktionen verhängen, wenn Bürgern die Dateneinsicht verweigert wird, und besitzen die notwendigen Befugnisse, um bestimmte

([1]) Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (im Folgenden Datenschutzrichtlinie).

([2]) Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates (im Folgenden: Datenschutzrichtlinie für elektronische Kommunikation).

([3]) Rechtsprechung zur Auslegung der wesentlichen Elemente und Bedingungen, die in Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten, verabschiedet in Rom am 4. November 1950, für verschiedene Bereiche festgelegt sind.

([4]) Durch den Lissabon-Vertrag wurde dieser Schutz verstärkt, indem die Achtung des Privatlebens und der Schutz personenbezogener Daten als eigene Grundsätze in Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union anerkannt wurden. Die Charta der Grundrechte wurde mit dem Inkrafttreten des Lissabon-Vertrags verbindlich.

([5]) Artikel 17 lautet: „Die Mitgliedstaaten sehen vor, dass der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen muss, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang — insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden — und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind." In Erwägungsgrund 46 heißt es zudem: „Für den Schutz der Rechte und Freiheiten der betroffenen Personen bei der Verarbeitung personenbezogener Daten müssen geeignete technische und organisatorische Maßnahmen getroffen werden, und zwar sowohl zum Zeitpunkt der Planung des Verarbeitungssystems als auch zum Zeitpunkt der eigentlichen Verarbeitung, um insbesondere deren Sicherheit zu gewährleisten und somit jede unrechtmäßige Verarbeitung zu verhindern."

([6]) Die Kommission hat die Absicht mitgeteilt, die Richtlinie 1999/5/EG gegen Ende 2010 zu aktualisieren.

Maßnahmen zur Verhinderung einer ungerechtfertigten Datenverarbeitung zu fordern. Es ist jedoch nicht immer hinreichend klar, ob ihre Befugnisse ausreichen, um zu verlangen, dass ein System so geplant wird, dass die Wahrnehmung der Datenschutzrechte natürlicher Personen erleichtert wird [1]. Auf der Grundlage der geltenden Rechtsvorschriften ist z. B. nicht klar, ob verlangt werden kann, dass die Architektur eines Informationssystems so geplant wird, dass die Unternehmen Auskunftsersuchen natürlicher Personen leichter beantworten und sie automatisch und schneller bearbeiten können. Zudem können spätere Versuche, die Technologie zu ändern, wenn sie bereits entwickelt oder eingeführt ist, zu einem Flickwerk von Einzellösungen führen, die nicht uneingeschränkt funktionieren und überdies kostspielig sind.

37. Nach Auffassung des EDSB, die von der Artikel-29-Datenschutzgruppe [2] geteilt wird, lässt der gegenwärtige Rechtsrahmen Raum für eine ausdrücklichere Unterstützung des Grundsatzes des „eingebauten Datenschutzes".

IV.2. **Verankerung des „eingebauten Datenschutzes" auf verschiedenen Ebenen**

38. Daher empfiehlt der EDSB der Kommission vier Strategien:

a) Vorschlag zur Aufnahme einer allgemeinen Bestimmung über „eingebauten Datenschutz" in den Rechtsrahmen für den Datenschutz;

b) Ausarbeitung dieser allgemeinen Bestimmung in spezifischen Bestimmungen, wenn spezifische Rechtsinstrumente in verschiedenen Sektoren vorgeschlagen werden. Diese spezifischen Bestimmungen könnten auf der Grundlage von Artikel 17 der Datenschutzrichtlinie (und anderer geltender Rechtsvorschriften) schon jetzt in Rechtsinstrumente aufgenommen werden.

c) Aufnahme des „eingebauten Datenschutzes" als Leitprinzip in die europäische digitale Agenda;

d) Aufnahme des „eingebauten Datenschutzes" in andere EU-Initiativen (vor allem nicht-rechtlicher Art).

Eine allgemeine Bestimmung über den „eingebauten Datenschutz"

39. Der EDSB schlägt vor, den Grundsatz des „eingebauten Datenschutzes" unmissverständlich und ausdrücklich in den bestehenden Regulierungsrahmen für den Datenschutz aufzunehmen. Dies würde den Grundsatz stärker und ausdrücklicher etablieren und für seine wirksame Umsetzung sorgen. Außerdem würde es den Durchsetzungsbehörden mehr Legitimität bei der Forderung seiner *De-facto*-Anwendung in der Praxis verleihen. Dies ist besonders angesichts der geschilderten Fakten notwendig, nicht nur wegen der Bedeutung des Grundsatzes selbst als Vertrauen schaffendes Instrument, sondern auch als Anreiz für die Interessengruppen zur Umsetzung des „eingebauten Datenschutzes" und Verstärkung der im geltenden Rechtsrahmen verankerten Garantien.

40. Dieser Vorschlag stützt sich auf die Empfehlung der Artikel-29-Datenschutzgruppe zur Einführung des Grundsatzes „Privacy by Design" als allgemeinen Grundsatz in den Rechtsrahmen für den Datenschutz, insbesondere in die Datenschutzrichtlinie. Die Artikel-29-Arbeitsgruppe erklärt darin: „Dieser Grundsatz sollte sowohl für die Entwickler und Hersteller der Technologien, als auch für die für die Datenverarbeitung Verantwortlichen, die über den Erwerb und die Nutzung der IKT zu entscheiden haben, verbindlich sein. Sie sollten dazu verpflichtet sein, bereits in der Planungsphase der Informations- und Kommunikationsverfahren und -systeme Technologien zum Datenschutz zu berücksichtigen. Sowohl die Anbieter solcher Systeme oder Dienstleistungen als auch die für die Datenverarbeitung Verantwortlichen sollten zeigen, dass sie alle erforderlichen Maßnahmen ergriffen haben, um diese Anforderungen zu erfüllen."

41. Der EDSB begrüßt auch die Unterstützung des „eingebauten Datenschutzes" durch Kommissionsmitglied Viviane Reding im Zusammenhang mit der Ankündung einer Überarbeitung der Datenschutzrichtlinie [3].

42. Kommen wir nun zum Inhalt solcher Regelungen. Wichtig ist vor allem, dass ein „eingebauter Datenschutz" als allgemeiner Grundsatz technologieunabhängig sein sollte. Es sollte keine Regulierung der Technologie angestrebt werden, d. h. es sollten keine spezifischen technischen Lösungen vorgeschrieben werden. Vielmehr sollte er dazu verpflichten, bestehende Privatsphären- und Datenschutzgrundsätze in Informations- und Kommunikationssysteme und -lösungen zu integrieren. Dies würde es Interessengruppen, Herstellern, für die Datenverarbeitung Verantwortlichen und Datenschutzbehören erlauben, die Bedeutung des Grundsatzes im Einzelfall auszulegen. Zweitens

[1] Siehe Bericht der Datenschutzbehörde des Vereinigten Königreichs (UK Information Commissioner's Office): „Privacy by Design", veröffentlicht im November 2008.

[2] Siehe Stellungnahme 168 der Artikel-29-Datenschutzgruppe: Die Zukunft des Datenschutzes. Gemeinsamer Beitrag zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz der personenbezogenen Daten, angenommen am 1. Dezember 2009.

[3] Der „eingebaute Datenschutz" liegt im Interesse sowohl der Bürger als auch der Unternehmen. Er wird zu einem besseren Schutz für den Einzelnen, aber auch zu Vertrauen in neue Dienste und Produkte führen, die sich wiederum positiv auf die Wirtschaft auswirken werden. Es gibt einige ermutigende Beispiele, doch es muss noch viel mehr geschehen. Grundsatzrede zum Datenschutztag am 28. Januar 2010, Europäisches Parlament, Brüssel.

sollte die Einhaltung des Grundsatzes auf verschiedenen Stufen obligatorisch sein, von der Festlegung von Standards und der Planung der Architektur bis zu ihrer Umsetzung durch die für die Datenverarbeitung Verantwortlichen.

Bestimmungen in spezifischen Rechtsinstrumenten

43. Aktuelle und künftige Rechtsinstrumente müssen den Grundsatz des „eingebauten Datenschutzes" auf der Grundlage des aktuellen Rechtsrahmens und, nach der Verabschiedung der oben vorgeschlagenen allgemeinen Bestimmung, auf der Basis dieser Bestimmung verankern. So trägt die Kommission beispielsweise im Rahmen der laufenden Initiativen zu intelligenten Verkehrssystemen gerade zu Anfang besondere Verantwortung bei der Festlegung von Maßnahmen, Standardisierungsinitiativen, Verfahren und bewährten Verfahren. Bei der Erfüllung dieser Aufgaben sollte „eingebauter Datenschutz" als Leitprinzip fungieren.

44. Des Weiteren weist der EDSB darauf hin, dass der „eingebaute Datenschutz" auch im Bereich der Freiheit, der Sicherheit und des Rechts von besonderer Bedeutung ist, insbesondere in Bezug auf die Ziele der im Stockholm-Programm vorgesehenen Informationsmanagement-Strategie ([1]). In seiner Stellungnahme zum Stockholmer Programm betonte der EDSB, dass die Systemarchitektur für den Informationsaustausch auf dem Grundsatz des „eingebauten Datenschutzes" aufbauen sollte ([2]). „Konkret bedeutet dies, dass Informationssysteme, die zum Zwecke des Schutzes der öffentlichen Sicherheit konzipiert werden, immer nach dem Grundsatz des ‚eingebauten Datenschutzes' entwickelt werden sollten".

45. In der Stellungnahme der Artikel-29-Datenschutzgruppe zur Zukunft des Datenschutzes ([3]) wird noch ausdrücklicher erklärt, dass in einem Raum der Freiheit, der Sicherheit und des Rechts, in dem die Behörden die wichtigsten Akteure sind und in dem sich Maßnahmen, die auf eine wachsende Überwachung abzielen, direkt auf das Grundrecht auf Privatsphäre und Datenschutz auswirken können, solche Anforderungen zur zwingenden Vorschrift werden sollten. Durch Einführung dieser Anforderungen für Informationssysteme würden die Regierungen den „eingebauten Datenschutz" auch in ihrer Eigenschaft als Pilotkunden fördern.

([1]) Das Stockholmer Programm — Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, angenommen vom Europäischen Rat im Dezember 2009.

([2]) Stellungnahme vom 10. Juli 2009 zu der Mitteilung der Kommission an das Europäische Parlament und den Rat mit dem Titel „Ein Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger", ABl. C 276, vom 17.11.2009, S. 8, Punkt 60.

([3]) Stellungnahme 168 der Artikel-29-Datenschutzgruppe: Die Zukunft des Datenschutzes — Gemeinsamer Beitrag zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz der personenbezogenen Daten, angenommen am 1. Dezember 2009.

„Eingebauter Datenschutz" als Leitprinzip in der europäischen digitalen Agenda

46. Informations- und Kommunikationstechnologien sind zunehmend komplex und bringen immer größere Risiken für die Privatsphäre und den Datenschutz mit sich. Allgemein sind digitalisierte Daten, bei denen Zugriff, Kopieren und Übermittlung leichter sind, viel stärker gefährdet als Informationen in Papierform. Mit der Verbreitung von Netzen untereinander verbundener Gegenstände werden diese Risiken wachsen. Je größer die Risiken für Privatsphäre und Datenschutz, desto mehr wächst auch die Nachfrage nach verstärkten Schutzmaßnahmen für den Datenschutz/die Privatsphäre. Daraus ergibt sich im IKT-Sektor eine zwingende Notwendigkeit, den „eingebauten Datenschutz" einzuführen. Außerdem ist, wie bereits erörtert, das Vertrauen in die IKT von entscheidender Bedeutung, wenn die Bürger diese neuen Dienste annehmen sollen, und Privatsphäre und Datenschutz sind Schlüsselelemente dieses Vertrauens.

47. All dies macht deutlich, dass in einer Strategie für die IKT-Entwicklung die Notwendigkeit bekräftigt werden muss, sie mit einem eingebauten Element zum Privatsphären- und Datenschutz auszustatten, d. h. den Grundsatz des „eingebauten Datenschutzes" zu berücksichtigen.

48. Deshalb sollte in der europäischen digitalen Agenda das Prinzip des eingebauten Datenschutzes ausdrücklich als notwendiges Element hervorgehoben werden, um das Vertrauen der Bürger in die IKT und Online-Dienste zu gewährleisten. Es sollte anerkannt werden, dass Privatsphäre und Vertrauen Hand in Hand gehen und dass der „eingebaute Datenschutz" ein maßgeblicher Faktor bei der Entwicklung eines vertrauenswürdigen IKT-Sektors sein sollte.

„Eingebauter Datenschutz" als Grundsatz in anderen EU-Initiativen

49. Die Kommission sollte den „eingebauten Datenschutz" als Leitprinzip zur Umsetzung von Strategien, Maßnahmen und Aktivitäten in spezifischen IKT-Sektoren betrachten, z. B. im Gesundheits- und Beschaffungswesen (eHealth und eProcurement), der Sozialversicherung (eSocial Security), dem Bildungsbereich (eLearning) usw. Viele diese Initiativen werden Aktionspunkte der europäischen digitalen Agenda sein.

50. Das bedeutet z. B., dass Initiativen zur effizienteren und moderneren Gestaltung staatlicher Anwendungen zur Interaktion der Bürger mit der Verwaltung auch die Anforderung enthalten sollten, dass diese nach dem Grundsatz des „eingebauten Datenschutzes" geplant und betrieben werden. Das gilt auch für Strategien der Kommission für ein schnelleres Internet, digitale Inhalte oder die allgemeine Förderung der Festnetz- und Drahtlos-Kommunikation und -Datenübertragung.

51. Ebenso gilt dies auch für Bereiche, in denen die Kommission für große IT-Systeme, z. B. SIS und VIS (Schengener Informationssystem und Visa-Informationssystem) zuständig ist, sowie für Fälle, in denen sich die Zuständigkeit der Kommission auf die Entwicklung und Pflege der gemeinsamen Infrastruktur eines solchen Systems beschränkt, z. B. beim Europäischen Strafregisterinformationssystem (ECRIS).

52. Wie der Grundsatz des „eingebauten Datenschutzes" genau entwickelt wird, hängt vom einzelnen Sektor und der jeweiligen Situation ab. Werden z. B. Initiativen der Kommission von Gesetzesvorschlägen zu einem bestimmten IKT-Sektor begleitet, ist es in vielen Fällen angemessen, darin ausdrücklich darauf hinzuweisen, dass das Konzept des „eingebauten Datenschutzes" auf die betreffende IKT-Anwendung/das System anzuwenden ist. Werden Aktionspläne für einen bestimmten Bereich geplant, sollte darin die Anwendung des Rechtsrahmens sichergestellt und gewährleistet werden, dass die betreffende IKT-Technologie unter Berücksichtigung des „eingebauten Datenschutzes" konzipiert wird.

53. In Bezug auf die Forschung sollten das 7. Rahmenprogramm und seine Nachfolgeprogramme genutzt werden, um Projekte zu unterstützen, die sich mit der Frage beschäftigen, wie IKT-Technologien und -Architektur dem Datenschutz und insbesondere dem Grundsatz des „eingebauten Datenschutzes" besser gerecht werden können. Außerdem sollte der „eingebaute Datenschutz" stets bei umfassenderen IKT-Projekten berücksichtigt werden, bei denen es um die Verarbeitung personenbezogener Daten geht.

Bereiche von besonderer Bedeutung

54. In manchen Fällen kann es aufgrund der besonderen Risiken für die Privatsphäre und den Datenschutz oder anderer Faktoren (Widerstand der Industrie gegen die Bereitstellung von Produkten für „eingebauten Datenschutz", Nachfrage der Verbraucher usw.) notwendig sein, explizitere und spezifischere Maßnahmen für den „eingebauten Datenschutz" festzulegen, die in ein bestimmtes Produkt oder eine Technologie der Informations- und Kommunikationstechnologie integriert werden müssen — gegebenenfalls in Form von Rechtsinstrumenten.

55. Der EDSB hat verschiedene Bereiche ermittelt (RFID, soziale Netze und Browseranwendungen, die seiner Meinung nach in dieser Phase von der Kommission sorgfältig geprüft und den oben genannten praktischeren Maßnahmen unterzogen werden sollten. Diese drei Bereiche werden weiter unten erörtert.

V. **FUNKFREQUENZKENNZEICHNUNG (RFID)**

56. RFID-Etiketten können an Gegenständen, Tieren und Menschen angebracht werden. Sie können verwendet werden, um personenbezogene Informationen, wie z. B. medizinische Daten, zu sammeln und zu speichern, die Bewegungen einer Person zu verfolgen oder für verschiedene Zwecke ein Profil ihres Verhaltens zu erstellen. Dies kann geschehen, ohne dass die beobachtete Person es merkt ([1]).

57. Wirksame Garantien in Bezug auf Datenschutz, Privatsphäre und alle damit verbundenen ethischen Dimensionen sind entscheidend für das Vertrauen der Öffentlichkeit in die RFID und ein künftiges „Internet der Dinge". Nur wenn dieses Vertrauen besteht, kann die Technologie ihren großen wirtschaftlichen und gesellschaftlichen Nutzen entfalten.

V.1. **Die Lücken des geltenden Rechtsrahmens zum Datenschutz**

58. Die Datenschutzrichtlinie und die Datenschutzrichtlinie für elektronische Kommunikation gelten für die Datenerfassung durch RFID-Anwendungen ([2]). Sie schreiben u. a. vor, dass beim Betrieb von RFID-Anwendungen angemessene Datenschutzvorkehrungen getroffen werden müssen ([3]).

59. Dieser Rechtsrahmen berücksichtigt jedoch nicht alle Bedenken im Hinblick auf Datenschutz und Privatsphäre, die durch diese Technologie aufgeworfen werden. Das liegt daran, dass die Richtlinien nicht hinreichend detailliert auf die Art der Vorkehrungen eingehen, die bei RFID-Anwendungen getroffen werden sollten. Die bestehenden

([1]) RFID steht für Radio Frequency Identification (Funkfrequenzkennzeichnung). Die wichtigsten Komponenten der Funkfrequenzkennzeichnungstechnologie *oder* –infrastruktur sind ein Etikett, *Tag* genannt (d. h. ein Microchip), ein Lesegerät und eine Anwendung, die über Middleware mit Tags und Lesegeräten verbunden ist und die generierten Daten verarbeitet. Der Tag besteht aus einem elektronischen Schaltkreis, der Daten speichert, und einer Antenne, die die Daten über Funk überträgt. Das Lesegerät ist mit einer Antenne und einem Demodulator ausgestattet, der die per Funk übertragenen analogen Signale in digitale Daten umwandelt. Die Daten können dann über Netzwerke an Datenbanken und Server geschickt und dann von einem Computer verarbeitet werden.

([2]) Die Datenschutzrichtlinie für elektronische Kommunikation nimmt in Artikel 3 Bezug auf RFID: „Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft." Ergänzt wird diese durch Erwägungsgrund 56: „Der technische Fortschritt erlaubt die Entwicklung neuer Anwendungen auf der Grundlage von Datenerfassungs- und Identifizierungsgeräten, bei denen es sich auch um kontaktlos mit Funkfrequenzen arbeitende Geräte handeln könnte. So werden beispielsweise in RFID-Funkfrequenzerkennungsgeräten (Radio Frequency Identification Devices) Funkfrequenzen genutzt, um von eindeutig gekennzeichneten Etiketten Daten abzulesen, die dann über bestehende Kommunikationsnetze weitergeleitet werden können. Die breite Nutzung solcher Technologien kann erhebliche wirtschaftliche und soziale Vorteile bringen und damit einen großen Beitrag zum Binnenmarkt leisten, wenn ihr Einsatz von den Bürgern akzeptiert wird. Um dieses Ziel zu erreichen, muss gewährleistet werden, dass sämtliche Grundrechte des Einzelnen, einschließlich des Rechts auf Privatsphäre und Datenschutz, gewahrt bleiben. Werden solche Geräte an öffentlich zugängliche elektronische Kommunikationsnetze angeschlossen oder werden elektronische Kommunikationsdienste als Grundinfrastruktur genutzt, so sollten die einschlägigen Bestimmungen der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation), einschließlich der Vorschriften über Sicherheit, Datenverkehr, Standortdaten und Vertraulichkeit, zur Anwendung kommen".

([3]) Artikel 17 der Datenschutzrichtlinie verpflichtet z. B. zur Durchführung der geeigneten technischen und organisatorischen Maßnahmen, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung oder die unberechtigte Weitergabe personenbezogener Daten erforderlich sind.

Regelungen müssen durch zusätzliche Bestimmungen ergänzt werden, die spezielle Vorkehrungen vorschreiben und vor allem zur Einbettung technischer Lösungen („eingebauter Datenschutz") in die RFID-Technologie verpflichten. Vorgeschrieben werden sollte z. B., dass Etiketten, die personenbezogene Informationen speichern, durch einen „Kill"-Befehl deaktiviert werden können, und bei Tags, die bestimmte Arten personenbezogener Daten speichern, Verschlüsselungsverfahren eingesetzt werden.

V.2. **Selbstregulierung als erster Schritt**

60. Im März 2007 verabschiedete die Kommission eine Mitteilung ([1]), in der sie es u. a. für notwendig erklärte, ausführliche Leitlinien für die praktische Einführung neuer Technologien wie RFID zu erlassen, und sich für die Verabschiedung von Gestaltungskriterien aussprach, um Datenschutz- und Sicherheitsrisiken von vornherein auszuschließen.

61. Zu diesem Zweck verabschiedete die Kommission im Mai 2009 eine Empfehlung zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen ([2]). Im Einzelhandel sollen RFID-Etiketten am Verkaufsort deaktiviert werden, es sei denn, die Verbraucher haben ihrer weiteren Verwendung zugestimmt. Dies gilt nur dann nicht, wenn eine Datenschutzfolgenabschätzung ergeben hat, dass die RFID-Etiketten wahrscheinlich keine Bedrohung für die Privatsphäre oder den Schutz personenbezogener Daten darstellen. In diesem Fall können sie auch nach Verlassen des Verkaufsorts betriebsfähig bleiben. Die Verbraucher müssen allerdings jederzeit die Möglichkeit haben, sie kostenfrei zu deaktivieren.

62. Der EDSB unterstützt das Konzept der Kommission, das Selbstregulierungsinstrumente vorsieht. Wie weiter unter beschrieben, ist es jedoch denkbar, dass die Selbstregulierung nicht zu den erwarteten Ergebnissen führen könnte; deshalb fordert er die Kommission auf, sich auf einen möglichen Einsatz alternativer Maßnahmen einzustellen.

V.3. **Wichtige Bereiche und mögliche Zusatzmaßnahmen, wenn die Selbstregulierung versagt**

63. Der EDSB befürchtet, dass Organisationen, die RFID-Anwendungen im Einzelhandel betreiben, die Möglichkeit einer unerwünschten Überwachung von RFID-Etiketten durch Dritte übersehen könnten. Dadurch könnten eventuell auf dem Tag gespeicherte personenbezogene Daten weitergegeben werden; zudem könnten Dritte in die Lage versetzt werden, eine Person zu verfolgen oder zu erkennen, indem sie einfach die Kenncodes (unique identifiers) in einem oder mehreren Etiketten auslesen. Dies ist sogar außerhalb der Reichweite der RFID-Anwendung möglich. Grund zur Sorge sieht er überdies darin, dass die Betreiber von RFID-Anwendungen versucht sein können, ungerechtfertigt ein stillschweigendes Einverständnis vorauszusetzen und deshalb das Etikett auch nach Verlassen des Verkaufsorts betriebsfähig zu belassen.

64. Geschieht dies, ist es möglicherweise zu spät, um die Risiken für den Datenschutz und die Privatsphäre der Kunden einzudämmen, die vielleicht schon verletzt wurden. Aufgrund des Wesens der Selbstregulierung könnten die Kontrollbehörden außerdem in einer schwächeren Position sein, wenn sie Einrichtungen, die RFID-Anwendungen betreiben, die Durchführung von Maßnahmen des „eingebauten Datenschutzes" auferlegen.

65. Deshalb fordert der EDSB die Kommission auf, sich darauf einzustellen, Rechtsinstrumente zur Regelung der wichtigsten Belange der RFID-Nutzung vorzuschlagen, sofern die effektive Anwendung des geltenden Rechtsrahmens fehlschlägt. Die Bewertung der Kommission sollte nicht unnötig aufgeschoben werden; eine Verzögerung könnte Risiken für die einzelnen Bürger verursachen und wäre auch für die Industrie kontraproduktiv, da die Rechtsunsicherheit zu groß ist und die einschlägigen Probleme dadurch wahrscheinlich größer und schwerer behebbar werden.

66. Im Rahmen der vorzuschlagenden Maßnahmen empfiehlt der EDSB das „Opt-in-Prinzip" beim Verlassen des Verkaufsorts, d. h die standardmäßige Deaktivierung aller RFID-Etiketten an Verbraucherprodukten am Verkaufsort. Es ist unter Umständen nicht erforderlich, dass die Kommission festlegt, welche Technologie in der Praxis verwendet wird. Stattdessen muss im EU-Recht die rechtliche Verpflichtung verankert werden, eine vorherige Zustimmung einzuholen („Opt-in"). Wie sie erfüllt wird, können die Betreiber selbst entscheiden.

V.4. **Weitere zu prüfende Fragen: Verwaltung des „Internets der Dinge"**

67. Von RFID-Etiketten übermittelte Daten — zum Beispiel Produktinformationen — können längerfristig Eingang in ein globales Kommunikations-Infrastrukturnetz finden, das üblicherweise als „Internet der Dinge" bezeichnet wird. Probleme in Bezug auf Datenschutz/die Wahrung der Privatsphäre entstehen dadurch, dass Gebrauchsgegenstände durch RFID-Etiketten gekennzeichnet sein können, die neben Produktinformationen möglicherweise personenbezogene Daten enthalten.

68. Viele offene Fragen gibt es noch dazu, wer die Speicherung von Daten aus so gekennzeichneten Gegenständen verwalten wird. Wie wird sie organisiert? Wer hat Zugang dazu? Im Juni 2009 verabschiedete die Kommission eine Mitteilung über das Internet der Dinge ([3]), in der das Potenzial dieses Phänomens zur Verursachung von Problemen beim Daten- und Privatsphärenschutz ausdrücklich angesprochen wird.

([1]) Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen, KOM(2007) 96 endgültig.

([2]) Empfehlung der Kommission vom 12. Mai 2009 zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen (K(2009) 3200 endg.).

([3]) Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen — Internet der Dinge — ein Aktionsplan für Europa, 18.6.2009, KOM(2009) 278 endg.

69. Der EDSB möchte einige der in der Mitteilung angesprochenen Punkte hervorheben, die seiner Meinung nach bei der Entwicklung des Internets der Dinge besonderes Augenmerk verdienen. Erstens kann durch eine dezentrale Architektur möglicherweise die Rechenschaftspflicht und die Durchsetzbarkeit des EU-Rechtsrahmens gefördert werden. Zweitens sollte das Recht des Einzelnen, nicht „verfolgt" zu werden, in größtmöglichem Maße geschützt werden. Mit anderen Worten: Eine Verfolgung von Personen durch RFID-Etiketten ohne ihr Einverständnis sollte nur in streng begrenzten Fällen erfolgen. Es sollte eine ausdrückliche Zustimmung erforderlich sein. Dies wird oft als „Schweigen der Chips" bezeichnet bzw. als das Recht, in Frieden gelassen zu werden. Schließlich sollte bei der Planung des Internets der Dinge der „eingebaute Datenschutz" als Leitprinzip fungieren. Das würde z. B. erfordern, dass konkrete RFID-Anwendungen, die mit Mechanismen zur Kontrolle durch die Nutzer ausgestattet sind, mit datenschutzfreundlichen Voreinstellungen versehen werden.

70. Der EDSB erwartet, dass er bei den in der Mitteilung vorgestellten Maßnahmen konsultiert wird, insbesondere bei der Ausarbeitung der Mitteilung über Datenschutz und Vertrauen in der allgegenwärtigen Informationsgesellschaft.

VI. SOZIALE NETZWERKE UND DIE NOTWENDIGKEIT DATENSCHUTZFREUNDLICHER VOREINSTELLUNGEN

71. Soziale Netze sind aktuell sehr „angesagt". Sie sind offenbar inzwischen beliebter als E-Mail. Sie verbinden Menschen miteinander, die ähnliche Interessen bzw. Aktivitäten pflegen. Die Nutzer können ihre Profile online stellen und Mediendateien, wie z. B. Videos, Fotos, Musik und ihre beruflichen Profile austauschen.

72. Vor allem junge Menschen haben die sozialen Netzwerke schnell angenommen, und der Trend setzt sich fort. Das Durchschnittsalter der Internetnutzer in Europa ist in den letzten Jahren gesunken. 9-10-Jährige gehen heute mehrmals in der Woche ins Netz, 12-14-Jährige sind täglich, oft eine bis drei Stunden lang, online.

VI.1. Soziale Netzwerke und der geltende Rechtsrahmen für Datenschutz und Privatsphäre

73. Die Entwicklung der sozialen Netze versetzt die Nutzer in die Lage, Informationen über sich und Dritte ins Internet zu stellen. Nach Aussage der Artikel-29-Datenschutzgruppe [1] handeln Internetnutzer für die von ihnen hochgeladenen Daten im Sinne von Artikel 2 Buchstabe d der Datenschutzrichtlinie als für die Datenverarbeitung Verantwortliche [2]. In den meisten Fällen gilt für eine solche Datenverarbeitung jedoch die „Ausnahmeklausel für Privathaushalte" gemäß Artikel 3 Absatz 2 der Richtlinie. Gleichzeitig gelten Anbieter sozialer Netzwerkdienste insofern als die „für die Verarbeitung von Benutzerdaten Verantwortlichen", als sie die Mittel für die Verarbeitung der Benutzerdaten und alle „Basisdienste" für die Benutzerverwaltung (z. B. Registrierung und Löschung von Profil- und Verkehrsdaten) bereitstellen.

74. Rechtlich bedeutet dies, dass Internetnutzer und Anbieter sozialer Netzwerkdienste gemeinsam für die Verarbeitung personenbezogener Daten als „für die Verarbeitung Verantwortliche" im Sinne von Artikel 2 Buchstabe d der Richtlinie zuständig sind, wenn auch in unterschiedlichem Umfang und mit unterschiedlichen Pflichten.

75. Deshalb sollten die Nutzer wissen und verstehen, dass für sie, wenn sie eigene personenbezogene Daten und die anderer verarbeiten, Bestimmungen des EU-Datenschutzrechts gelten, die u. a. vorschreiben, dass die informierte Einwilligung derjenigen Personen einzuholen ist, deren Daten hochgeladen werden, und dass diesen Personen ein Recht auf Berichtigung, Einspruch usw. einzuräumen ist. Außerdem müssen die Anbieter sozialer Netzwerkdienste u. a. geeignete technische und organisatorische Maßnahmen ergreifen und dabei die Risiken der Verarbeitung und die Art der Daten berücksichtigen. Dies bedeutet wiederum, dass die Anbieter sozialer Netzwerke für datenschutzfreundliche Voreinstellungen sorgen sollten, und auch für Einstellungen, die den Zugriff auf die vom Nutzer selbst ausgewählten Kontakte begrenzen. In den Voreinstellungen sollte auch eine ausdrückliche Zustimmung des Nutzers gefordert werden, ehe ein Profil für Dritte zugänglich wird, und geschützte Profile sollten von internen Suchmaschinen nicht gefunden werden.

76. Leider klafft eine Lücke zwischen den rechtlichen Bestimmungen und ihrer Einhaltung in der Praxis. Internetnutzer unterliegen zwar rechtlich als „für die Datenverarbeitung Verantwortliche" dem EU-Rechtsrahmen für Datenschutz und Privatsphäre, in der Praxis ist ihnen dies jedoch oft nicht bewusst. Allgemein kann man sagen, dass ihnen nur unzureichend bewusst ist, dass sie personenbezogene Daten verarbeiten und dass die Veröffentlichung solcher Informationen Risiken für den Datenschutz und die Privatsphäre birgt. Vor allem junge Menschen stellen Inhalte online und unterschätzen dabei die Folgen, die das für sie selbst und andere, z. B. bei einer Bewerbung auf einen Studienplatz oder eine Stelle, haben könnte.

[1] Siehe Artikel-29-Datenschutzgruppe 163: Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, angenommen am 12. Juni 2009.

[2] „für die Verarbeitung Verantwortlicher" [bezeichnet] die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten in einzelstaatlichen oder gemeinschaftlichen Rechts- und Verwaltungsvorschriften festgelegt, so können der für die Verarbeitung Verantwortliche bzw. die spezifischen Kriterien für seine Benennung durch einzelstaatliche oder gemeinschaftliche Rechtsvorschriften bestimmt werden.

77. Gleichzeitig wählen Anbieter sozialer Netzwerke die voreingestellten Standardeinstellungen oft nach dem „Opt-out"-Prinzip und erleichtern so die Weitergabe personenbezogener Daten. Manche ermöglichen in der Voreinstellung, dass normale Suchmaschinen auf Profile zugreifen können. Dies wirft zwei Fragen auf: Haben die Nutzer tatsächlich der Weitergabe zugestimmt, und handeln die sozialen Netzwerke gemäß Artikel 17 der Richtlinie (siehe oben), der die Durchführung geeigneter technischer und organisatorischer Maßnahmen gegen die unberechtigte Verarbeitung vorschreibt?

VI.2. **Risiken durch soziale Netzwerke und vorgeschlagene Abhilfemaßnahmen**

78. Die oben geschilderte Situation führt zu steigenden Risiken für die Privatsphäre des einzelnen Bürgers und den Datenschutz. Sie setzt Internetnutzer und all diejenigen, deren Daten hochgeladen wurden, der Gefahr eklatanter Verstöße gegen ihre Rechte auf Privatsphäre und Datenschutz aus.

79. Vor diesem Hintergrund sollte sich die Kommission mit der Frage beschäftigen, wie dagegen vorgegangen werden sollte und kann. Diese Stellungnahme bietet keine umfassende Antwort auf diese Frage, sondern lediglich eine Reihe von Vorschlägen, die weiter geprüft werden sollten.

In die Information der Internetnutzer investieren

80. Der erste Vorschlag betrifft Investitionen in die Information der Nutzer. Die EU-Institutionen und die nationalen Behörden sollten in die Unterrichtung über und Sensibilisierung für die Gefahren investieren, die durch soziale Netzwerke im Internet entstehen. So führt die GD Informationsgesellschaft beispielsweise das Programm „Sichereres Internet" durch, das darauf abzielt, Kinder und Jugendliche zu stärken und zu schützen, z. B. durch Sensibilisierungsaktivitäten ([1]). Kürzlich haben die EU-Institutionen die Kampagne „Erst denken, dann klicken" gestartet, die für die Risiken des Austauschs personenbezogener Daten mit Fremden sensibilisieren soll.

81. Der EDSB fordert die Kommission auf, Aktivitäten dieser Art auch weiterhin zu unterstützen. Die Betreiber sozialer Netzwerke selbst sollten jedoch ebenfalls eine aktive Rolle spielen, da sie rechtliche und soziale Verantwortung dafür tragen, dass die Nutzer darüber unterrichtet werden, wie sie ihre Dienste sicher und datenschutzfreundlich nutzen können.

82. Wie oben beschrieben, können Informationen, die in sozialen Netzwerken eingestellt werden, standardmäßig für verschiedene Gruppen sichtbar sein. Es ist z. B. möglich, dass diese Informationen für die allgemeine Öffentlichkeit zugänglich sind, auch für Suchmaschinen, die sie indexieren und somit direkt verlinken können. Die Informationen können aber auch nur für „ausgewählte Freunde" zugänglich sein oder vollständig privat bleiben. Natürlich werden bei verschiedenen Netzwerken unterschiedliche Genehmigungen und Begriffe verwendet.

83. Wie bereits erwähnt, wissen jedoch nur sehr wenige Nutzer sozialer Netzwerkdienste, wie sie den Zugang zu den von ihnen eingestellten Informationen kontrollieren oder gar die Privatsphäre-Voreinstellungen ändern können. Die Privatsphäre-Einstellungen bleiben meist unverändert, weil die Nutzer nicht wissen, welche Folgen es haben kann, sie nicht zu ändern, oder nicht wissen, wie sie sie ändern können. In der Mehrzahl der Fälle bedeutet die Beibehaltung der Privatsphäre-Voreinstellungen also nicht, dass die Nutzer eine informierte Entscheidung für die Weitergabe der Daten getroffen haben. In diesem Zusammenhang ist es besonders wichtig, dass Dritte, z. B. Suchmaschinen, nicht auf individuelle Profile verlinken, weil von der Annahme ausgegangen wird, dass die Nutzer (indem sie die Privatsphäre-Einstellungen nicht geändert haben) der unbeschränkten Weitergabe der Informationen zugestimmt haben.

84. Die Information der Nutzer kann zwar zur Behebung dieser Situation beitragen, reicht aber allein nicht aus. Wie von der Artikel-29-Datenschutzgruppe in ihrer Stellungnahme zur Nutzung sozialer Online-Netzwerke empfohlen, sollten die Anbieter sozialer Netzwerke kostenlos datenschutzfreundliche Voreinstellungen anbieten. Dadurch würden die Nutzer sich ihres Handelns stärker bewusst und könnten besser entscheiden, ob und an wen sie Informationen weitergeben möchten.

Rolle bei der Selbstregulierung

85. Die Kommission hat eine Vereinbarung mit 20 Betreibern sozialer Netzwerke geschlossen, die als „Safer Social Networking Principles for the EU" (Grundsätze zur Sicherheit in sozialen Netzwerken) bekannt ist ([2]). Ziel ist die Erhöhung der Sicherheit von Minderjährigen beim Umgang mit sozialen Online-Netzwerken in Europa. Diese Grundsätze beinhalten viele Vorgaben, die sich aus der Anwendung des oben beschriebenen Rechtsrahmens für den Datenschutz ergeben. Dazu gehört z. B. die Forderung, die Nutzer durch Tools und Technologie zu stärken, um sicherzustellen, dass sie die Verwendung und Verbreitung ihrer persönlichen Informationen steuern können. Eine weitere Anforderung sind datenschutzfreundliche Voreinstellungen.

86. Anfang Januar 2010 veröffentlichte die Kommission die Ergebnisse eines Berichts, in dem die Umsetzung der Grundsätze bewertet wurde ([3]). Der EDSB ist besorgt, dass, wie dieser Bericht zeigt, einige Schritte unternommen

([1]) Informationen über dieses Programm sind abrufbar unter: http://ec.europa.eu/information_society/activities/sip/index_en.htm

([2]) Abrufbar unter http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

([3]) Report on the assessment of the implementation of the Safer Social Network Principles for the EU, abrufbar unter: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf

wurden, viele andere aber noch ausstehen. So werden in dem Bericht z. B. Probleme bei der Kommunikation der Sicherheitsmaßnahmen und der auf den Internetseiten verfügbaren Tools festgestellt. Außerdem wird festgestellt, dass weniger als die Hälfte der Unterzeichner der Vereinbarung den Zugriff auf die Profile Minderjähriger ausschließlich auf deren Freunde beschränken.

Notwendigkeit obligatorischer datenschutzfreundlicher Voreinstellungen

87. In diesem Zusammenhang lautet die Kernfrage, ob zusätzliche politische Maßnahmen notwendig sind, um sicherzustellen, dass soziale Netzwerke ihre Dienste mit datenschutzfreundlichen Voreinstellungen versehen. Das ehemalige Kommissionsmitglied für die Informationsgesellschaft Viviane Reding erklärte zu dieser Frage, Rechtsvorschriften seien möglicherweise notwendig ([1]). Ähnlich äußerte sich der Europäische Wirtschafts- und Sozialausschuss, der erklärte, zusätzlich zur Selbstregulierung müssten Mindest-Datenschutzstandards gesetzlich vorgeschrieben werden ([2]).

88. Wie oben erwähnt, lässt sich die Verpflichtung für Betreiber sozialer Netzwerke zur Einführung datenschutzfreundlicher Voreinstellungen indirekt aus Artikel 17 der Datenschutzrichtlinie ([3]) ableiten, der die für die Datenverarbeitung Verantwortlichen verpflichtet, geeignete technische und organisatorische Maßnahmen („sowohl zum Zeitpunkt der Planung des Verarbeitungssystems als auch zum Zeitpunkt der eigentlichen Verarbeitung") durchzuführen, um deren Sicherheit zu gewährleisten und somit jede unrechtmäßige Verarbeitung zu verhindern, wobei die von der Verarbeitung ausgehenden Risiken und die Art der zu schützenden Daten zu berücksichtigen sind.

89. Dieser Artikel ist jedoch viel zu allgemein formuliert und auch in diesem Zusammenhang zu wenig spezifisch. Er enthält keine klaren Aussagen dazu, was mit „geeigneten technischen und organisatorischen Maßnahmen" in Bezug auf soziale Netzwerke gemeint ist. Somit besteht derzeit eine Situation der Rechtsunsicherheit, die sowohl für die Regulierungsbehörden, als auch für die einzelnen Bürger, deren Privatsphäre und personenbezogene Daten nicht umfassend geschützt werden, Probleme aufwirft.

90. Aus diesem Grund fordert der EDSB die Kommission nachdrücklich auf, Rechtsvorschriften auszuarbeiten, die mindestens eine übergreifende Bestimmung enthalten, die Privatsphäre-Einstellungen verpflichtend vorschreibt, gekoppelt mit genaueren Anforderungen:

a) Bereitstellung von Einstellungen, die den Zugriff auf Nutzerprofile auf die vom Nutzer selbst gewählten Kontakte beschränken. In den Einstellungen sollte festgelegt werden, dass Dritte nur mit ausdrücklicher Zustimmung des Nutzers Zugriff auf das Profil erhalten.

b) Gewährleistung, dass geschützte Profile von internen/externen Suchmaschinen nicht gefunden werden können.

91. Abgesehen von den obligatorischen datenschutzfreundlichen Voreinstellungen bleibt die Frage, ob zusätzliche spezifische Datenschutz- oder sonstige Maßnahmen (z. B. in Bezug auf den Schutz von Minderjährigen) ebenfalls angemessen sind. Dies führt zu der übergeordneten Frage, ob es sinnvoll wäre, einen spezifischen Rahmen für derartige Dienste zu schaffen, der nicht nur obligatorische Privatsphäre-Einstellungen vorschreibt, sondern auch andere Aspekte regelt. Der EDSB fordert die Kommission auf, diese Frage zu prüfen.

VII. DURCH DATENSCHUTZFREUNDLICHE BROWSER-VOREINSTELLUNGEN DIE INFORMIERTE ZUSTIMMUNG ZUR ANZEIGE VON WERBUNG SICHERSTELLEN

92. Anbieter von Ad-Netzwerken verwenden Cookies und andere Mechanismen, um das Surfverhalten von Internetnutzern zu überwachen, damit sie ihre Interessen katalogisieren und Profile erstellen können. Diese Daten werden dann genutzt, um ihnen gezielte Werbung zu übermitteln ([4]).

VII.1. Weitere Herausforderungen und Risiken im aktuellen Rechtsrahmen für Datenschutz/Privatsphäre

93. Für diese Art der Datenverarbeitung gilt die Datenschutzrichtlinie (wenn es um personenbezogene Daten geht) sowie auch Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation. Dieser Artikel schreibt ausdrücklich vor, dass der Nutzer informiert wird und die Gelegenheit erhält, der Speicherung von Dateien, wie z. B. Cookies, auf seinem Computer oder anderen Geräten zuzustimmen oder sie abzulehnen ([5]).

94. Bisher nutzen die Anbieter von Ad-Netzwerken Browser-Einstellungen und Datenschutzerklärungen, um die Nutzer zu informieren und ihnen die Genehmigung oder Ablehnung von Cookies zu ermöglichen. In den Datenschutzerklärungen der Herausgeber erklären sie, wie die Speicherung von Cookies ganz unterbunden oder von Fall zu Fall

([1]) Viviane Reding, Mitglied der Europäischen Kommission, zuständig für Informationsgesellschaft und Medien: Think before you post! How to make social networking sites safer for children and teenagers? Safer Internet Day, Straßburg, 9. Februar 2010.

([2]) Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zum Thema „Die Auswirkungen von sozialen Netzwerken im Internet auf Bürger und Verbraucher", 4. November 2009.

([3]) Näher erläutert auch unter Punkt 33 dieses Dokuments.

([4]) Verfolgende Cookies sind kleine Textdateien mit einem Kenncode. In der Regel platzieren die Betreiber von Ad-Netzwerken (ebenso wie Betreiber oder Autoren von Internetseiten) Cookies auf der Festplatte des Besuchers, vor allem im Browser, wenn der Nutzer zum ersten Mal auf Seiten von Werbeträgern in ihrem Netzwerk zugreift. Der Cookie ermöglicht es dem Betreiber des Ad-Netzwerks, einen wiederkehrenden Besucher auf dieser Seite und allen Seiten, die zum Ad-Netzwerk gehören, zu erkennen. Solche wiederholten Besuche ermöglichen es dem Netzwerkbetreiber, ein Profil des Besuchers zu erstellen.

([5]) Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation wurde kürzlich geändert, um den Schutz gegen das Abfangen elektronischer Nachrichten z. B. durch Spähsoftware und Cookies, die auf dem Computer oder anderen Geräten des Nutzers gespeichert werden, zu stärken, Nach der neuen Richtlinie sollten den Nutzern bessere Informationen und einfachere Möglichkeiten geboten werden, um zu kontrollieren, ob sie die Speicherung von Cookies auf ihren Endgeräten wünschen.

gestattet werden kann. Damit wollen Sie ihre Verpflichtung erfüllen, den Nutzern das Recht zur Ablehnung von Cookies einzuräumen.

95. Auch wenn diese Methode (über den Browser) theoretisch tatsächlich eine sinnvolle informierte Zustimmung darstellen könnte, sieht die Realität anders aus. Im Allgemeinen fehlt den Nutzern das grundlegende Verständnis für die Erfassung von Daten jeder Art, insbesondere durch Dritte, für den Wert solcher Daten und ihre Verwendung, für die Funktionsweise der Technologie und speziell dafür, wie und wo sie Cookies ablehnen können. Die notwendigen Schritte zur Sperrung von Cookies erscheinen nicht nur übermäßig kompliziert, sondern auch überzogen (sie müssen zunächst ihren Browser so einstellen, dass er Cookies akzeptiert, und dann der Nutzung widersprechen).

96. Das hat zur Folge, dass nur sehr wenige Nutzer von der Widerspruchsmöglichkeit Gebrauch machen, nicht weil sie eine informierte Entscheidung getroffen haben, verhaltensbezogene Werbung zuzulassen, sondern weil ihnen nicht klar ist dass sie sie durch Nichtnutzung der Widerspruchsoption *de facto* akzeptieren.

97. Somit bietet Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation zwar einen wirksamen rechtlichen Schutz, doch in der Praxis wird davon ausgegangen, dass die Internetnutzer der Überwachung zum Zweck der Übermittlung verhaltensbezogener Werbung zustimmen, obwohl sie in vielen, wenn nicht allen Fällen gar nicht wissen, dass diese Überwachung stattfindet.

98. Die Artikel-29-Datenschutzgruppe arbeitet an einer Stellungnahme, in der die rechtlichen Anforderungen an die verhaltensbezogene Werbung geklärt werden sollen. Diese Arbeit ist zu begrüßen. Die Auslegung allein reicht jedoch möglicherweise nicht aus, um in dieser Situation eine Lösung zu finden, und es könnten weitere Maßnahmen der Europäischen Union notwendig werden.

VII.2. **Notwendigkeit weiterer Maßnahmen, vor allem zur Gewährleistung datenschutzfreundlicher Voreinstellungen**

99. Wie oben beschrieben, erlauben Internet-Browser normalerweise ein gewisses Maß an Kontrolle über bestimmte Arten von Cookies. Derzeit werden in den meisten Browsern in den Voreinstellungen alle Cookies akzeptiert. Mit anderen Worten: Die Browser sind standardmäßig so eingestellt, dass alle Cookies, unabhängig von ihrem Zweck, akzeptiert werden. Nur wenn die Nutzerin oder der Nutzer den Browser so einstellt, dass er Cookies ablehnt, was, wie oben beschrieben, nur sehr wenige tun, werden keine Cookies auf seinem/ihrem Computer gespeichert. Außerdem gibt es bei der Erstinstallation oder Aktualisierung des Browsers keinen Assistenten für die Privatsphäre-Einstellungen.

100. Dieses Problem ließe sich u. a. dadurch verringern, dass Browser mit datenschutzfreundlichen Voreinstellungen versehen werden, also mit der Einstellung „Cookies von Drittanbietern sperren". Ergänzend dazu und zur wirksameren Gestaltung dieser Maßnahmen sollten die Browser verlangen, dass die Nutzer bei der Erstinstallation oder Aktualisierung einen Privatsphäre-Assistenten benutzen. Es sind mehr Granularität und klare Informationen über die verschiedenen Arten von Cookies und den Nutzen einiger von ihnen erforderlich. Nutzer, die bereit sind, sich zum Zweck der Übermittlung von Werbung beobachten zu lassen, sollten angemessen informiert werden und die Browser-Einstellungen ändern müssen. Dadurch würden sie mehr Kontrolle über ihre personenbezogenen Daten und ihre Privatsphäre erhalten. Dies wäre nach Auffassung des EDSB ein wirksamer Weg, die Einwilligung der Nutzer zu achten und weiterhin zu ermöglichen [1].

101. Berücksichtigt man einerseits die große Verbreitung des Problems, d. h. die Zahl der Internetnutzer, die derzeit aufgrund einer illusionären Zustimmung überwacht werden, und andererseits die Größenordnung der Interessen, die auf dem Spiel stehen, wird die Notwendigkeit zusätzlicher Schutzmaßnahmen besonders deutlich. Die Anwendung des Grundsatzes eines „eingebauten Datenschutzes" in Browseranwendungen könnte den einzelnen Bürgern sehr viel mehr Kontrolle über die Datenerhebungspraktiken für Werbezwecke verschaffen.

102. Aus diesen Gründen fordert der EDSB die Kommission nachdrücklich auf, rechtliche Maßnahmen zu prüfen, um datenschutzfreundliche Standardeinstellungen in Browsern und die Bereitstellung einschlägiger Informationen verpflichtend zu machen.

VIII. **SONSTIGE GRUNDSÄTZE ZUM SCHUTZ DER PRIVATSPHÄRE UND ZUM DATENSCHUTZ**

103. Der Grundsatz des „eingebauten Datenschutzes" hat ein großes Potenzial zur Verbesserung des Schutzes personenbezogener Daten und des allgemeinen Datenschutzes, doch um das Vertrauen der Verbraucher in die IKT sicherzustellen, müssen ergänzende Grundsätze festgelegt und in Rechtsvorschriften umgesetzt werden. Diesbezüglich verweist der EDSB auf den Grundsatz der Rechenschaftspflicht und die Ausarbeitung eines sektorübergreifenden verbindlichen Rahmens für die Regelung von Sicherheitsverletzungen.

VIII.1. **Der Grundsatz der Rechenschaftspflicht zur Gewährleistung der Einhaltung des Grundsatzes des „eingebauten Datenschutzes"**

104. Im Dokument der Artikel-29-Datenschutzgruppe „Die Zukunft des Datenschutzes" [2] wird empfohlen, den Grundsatz der Rechenschaftspflicht in die Datenschutzrichtlinie aufzunehmen. Dieser Grundsatz, der in einigen

[1] Gleichzeitig ist sich der EDSB bewusst, dass dies das Problem nicht vollständig lösen würde, da es Cookies gibt, die sich nicht über den Browser kontrollieren lassen, z. B. die so genannten „Flash-Cookies". Hierfür müssten die Browser-Entwickler in die Cookie-Steuerung standardmäßig Mechanismen zur Kontrolle von Flash in die neuen Browser-Versionen integrieren.

[2] Stellungnahme 168 der Artikel-29-Datenschutzgruppe: Die Zukunft des Datenschutzes Gemeinsamer Beitrag zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz der personenbezogenen Daten, angenommen am 1. Dezember 2009.

multinationalen Datenschutzinstrumenten ([1]) anerkannt wird, verpflichtet Organisationen zur Einführung von Verfahren zur Einhaltung geltender Gesetze und Einrichtung von Methoden zur Bewertung und zum Nachweis der Einhaltung von Gesetzen und anderen verbindlichen Instrumenten.

105. Der EDSB unterstützt die Empfehlung der Artikel-29-Datenschutzgruppe uneingeschränkt. Er betrachtet diesen Grundsatz als äußerst relevant für die Förderung einer wirksamen Umsetzung von Datenschutzgrundsätzen und -pflichten. Die Rechenschaftspflicht bedeutet, dass die für die Datenverarbeitung Verantwortlichen nachweisen müssen, dass sie die notwendigen Verfahren zur Einhaltung der geltenden Datenschutzbestimmungen eingeführt haben. Dies dürfte zur wirksamen Umsetzung des „eingebauten Datenschutzes" in IKT-Technologien beitragen, der ein besonders geeignetes Element ist, um der Rechenschaftspflicht nachzukommen.

106. Um die Erfüllung der Rechenschaftspflicht zu messen und nachzuweisen, könnten die für die Datenverarbeitung Verantwortlichen interne Verfahren sowie Prüfungen und andere Kontrollen durch Dritte einsetzen, die dafür Siegel oder Auszeichnungen vergeben könnten. In diesem Zusammenhang fordert der EDSB die Kommission nachdrücklich auf zu prüfen, ob es zweckmäßig wäre, zusätzlich zu einer allgemeinen Rechenschaftspflicht gesetzlich spezifische Maßnahmen vorzuschreiben, z. B. eine Pflicht zur Vorlage von Folgenabschätzungen in Bezug auf Privatsphäre und Datenschutz unter festzulegenden Umständen.

VIII.2. **Sicherheitsverletzungen: Vervollständigung des Rechtsrahmens**

107. Mit der Änderung der Datenschutzrichtlinie für elektronische Kommunikation im vergangenen Jahr wurde die Vorschrift eingeführt, im Falle von Sicherheitsverletzungen die betroffenen Personen und auch die zuständigen Behörden zu benachrichtigen. Eine Datenschutzverletzung lässt sich definieren als eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Weitergabe usw. von personenbezogenen Daten führt, die übertragen, gespeichert oder auf andere Weise im Zusammenhang mit einem Dienst verarbeitet werden. Die Benachrichtigung betroffener natürlicher Personen ist vorgeschrieben, wenn durch die Datenschutzverletzung die personenbezogenen Daten oder Personen in ihrer Privatsphäre beeinträchtigt werden. Dies kann der Fall sein, wenn die Datenschutzverletzung Identitätsdiebstahl, erhebliche Demütigung oder Rufschaden zur Folge haben könnte. Die Benachrichtigung der zuständigen Behörden ist bei jeder Verletzung des Datenschutzes vorgeschrieben, unabhängig davon, ob ein Risiko für Personen besteht.

Sektorübergreifende Anwendung der Bestimmungen über Sicherheitsverletzungen

108. Leider gilt diese Verpflichtung nur für Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste, z. B. Telefongesellschaften, Internetanbieter, Webmail-Anbieter usw. Der EDSB fordert die Kommission nachdrücklich auf, Vorschläge für eine Ausweitung der Geltung der Bestimmungen über Sicherheitsverletzungen auf alle Sektoren vorzulegen. Was den Inhalt betrifft, ist der EDSB der Meinung, dass der in der Datenschutzrichtlinie für elektronische Kommunikation festgelegte Rechtsrahmen für Sicherheitsverletzungen ein angemessenes Gleichgewicht zwischen dem Schutz individueller Rechte, einschließlich des Rechts auf Datenschutz und Privatsphäre, und den Pflichten der Einrichtungen schafft, für die sie gilt. Gleichzeitig hat dieser Rahmen aber auch „Biss", da er durch wirksame Durchsetzungsbestimmungen untermauert wird, welche die Behörden mit ausreichenden Ermittlungs- und Sanktionsbefugnissen im Fall von Verstößen ausstatten.

109. Deshalb fordert der EDSB die Kommission nachdrücklich auf, einen Vorschlag für eine Rechtsvorschrift vorzulegen, mit der die Geltung dieses Rahmens — bei Bedarf mit entsprechenden Anpassungen — auf alle Sektoren ausgedehnt wird. Dadurch würde zudem sichergestellt, dass dieselben Standards und Verfahren sektorübergreifend angewandt werden.

Vervollständigung des Rechtsrahmens aus der Datenschutzrichtlinie für elektronische Kommunikation im Komitologieverfahren

110. Die geänderte Datenschutzrichtlinie für elektronische Kommunikation ermächtigt die Kommission, über ein Komitologieverfahren technische Durchführungsmaßnahmen zu erlassen, d. h. detaillierte Verfahren für die Benachrichtigung bei Sicherheitsverletzungen ([2]). Diese Ermächtigung ist ein gerechtfertigtes Mittel, um eine kohärente Umsetzung und Anwendung des Rechtsrahmens für Sicherheitsverletzungen zu gewährleisten. Eine kohärente Umsetzung trägt dazu bei, dass Bürger in der gesamten Gemeinschaft ein gleiches Schutzniveau genießen und die betroffenen Einrichtungen nicht durch unterschiedliche Benachrichtigungsvorschriften belastet werden.

111. Die Datenschutzrichtlinie für elektronische Kommunikation wurde im November 2009 verabschiedet. Es ist kein Grund ersichtlich, der einen Aufschub des Beginns der Vorarbeiten für den Erlass der technischen Durchführungsmaßnahmen rechtfertigen würde. Der EDSB hat zwei Seminare zum Erfahrungsaustausch und zur Bestandsaufnahme in Bezug auf die Benachrichtigung bei Datenschutzverletzungen organisiert. Er ist gern bereit, die Ergebnisse weiterzugeben und freut sich auf die Zusammenarbeit mit der Kommission und anderen Interessengruppen bei der Feinabstimmung des übergeordneten Rechtsrahmens für Datenschutzverletzungen.

112. Der EDSB fordert die Kommission nachdrücklich auf, zeitnah die notwendigen Schritte einzuleiten. Ehe technische Durchführungsmaßnahmen erlassen werden, muss die Kommission eine umfassende Konsultation durchführen, bei der die ENISA, der EDSB und die Artikel-29-Datenschutzgruppe angehört werden müssen. Außerdem sollten auch andere „relevante Interessengruppen" einbezogen werden, vor allem, um sich über die besten verfügbaren technischen und wirtschaftlichen Methoden für die Durchführung zu informieren.

([1]) Richtlinien der OECD über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten (1989); Madrid Privacy Declaration: on Globale Datenschutz-Standards für eine globale Welt, vom 3. November 2009.

([2]) Das Komitologieverfahren beinhaltet die Verabschiedung technischer Durchführungsmaßnahmen durch einen Ausschuss aus Vertretern der Mitgliedstaaten unter Vorsitz der Kommission. Für die Datenschutzrichtlinie gilt das sogenannte Regelungsverfahren mit Kontrolle. Das bedeutet, dass sowohl das Parlament als auch der Rat von der Kommission vorgeschlagene Maßnahmen ablehnen können. Mehr dazu unter: http://europa.eu/scadplus/glossary/comitology_de.htm

IX. **SCHLUSSFOLGERUNGEN**

113. Vertrauen bzw. fehlendes Vertrauen wurde als entscheidender Faktor für die Durchsetzung und den erfolgreichen Einsatz von Informationstechnologien ermittelt. Wenn die Menschen den IKT nicht vertrauen, werden diese Technologien wahrscheinlich keinen Erfolg haben. Vertrauen in IKT hängt von verschiedenen Faktoren ab. Eine entscheidende Rolle spielt dabei die Gewährleistung, dass solche Technologien nicht die Grundrechte des Einzelnen auf Privatsphäre und Schutz der personenbezogenen Daten aushöhlen.

114. Um den Rechtsrahmen für Datenschutz/Privatsphäre zu verstärken, dessen Grundsätze in der Informationsgesellschaft uneingeschränkt gültig bleiben, schlägt der EDSB der Kommission vor, den „eingebauten Datenschutz" auf verschiedenen Ebenen der Gesetzgebung und Politikgestaltung einzubetten.

115. Er empfiehlt der Kommission vier Strategien:

a) Vorschlag zur Aufnahme einer allgemeinen Bestimmung über „eingebauten Datenschutz" in den Rechtsrahmen für den Datenschutz. Diese Bestimmung sollte technologieneutral und ihre Einhaltung auf verschiedenen Stufen obligatorisch sein;

b) Ausarbeitung dieser allgemeinen Bestimmung in spezifischen Bestimmungen, wenn spezifische Rechtsinstrumente in verschiedenen Sektoren vorgeschlagen werden. Diese spezifischen Bestimmungen könnten auf der Grundlage von Artikel 17 der Datenschutzrichtlinie (und anderer geltender Rechtsvorschriften) schon jetzt in Rechtsinstrumente aufgenommen werden.

c) Aufnahme des „eingebauten Datenschutzes" als Leitprinzip in die europäische digitale Agenda.

d) Aufnahme des „eingebauten Datenschutzes" in andere EU-Initiativen (vor allem nicht-rechtlicher Art).

116. In drei Bereichen der IKT empfiehlt der EDSB der Kommission zu prüfen, ob es notwendig ist, Vorschläge zur Anwendung des Grundsatzes eines „eingebauten Datenschutzes" in spezieller Form vorzulegen:

a) In Bezug auf RFID sollten Vorschläge für Rechtsinstrumente zur Regelung der wichtigsten Belange der RFID-Nutzung ausgearbeitet werden, falls die effektive Anwendung des geltenden Rechtsrahmens fehlschlägt. Insbesondere sollte das „Opt-in-Prinzip" beim Verlassen des Verkaufsorts, d. h die standardmäßige Deaktivierung aller RFID-Etiketten an Verbraucherprodukten am Verkaufsort festgeschrieben werden.

b) In Bezug auf soziale Netzwerke sollten Rechtsvorschriften ausgearbeitet werden, die mindestens eine übergreifende Bestimmung enthalten, die Privatsphäre-Einstellungen verpflichtend vorschreibt, gekoppelt mit genaueren Bestimmungen: Beschränkung des Zugriffs auf Nutzerprofile auf die vom Nutzer selbst gewählten Kontakte und Sicherstellung, dass geschützte Profile von internen/externen Suchmaschinen nicht gefunden werden können.

c) In Bezug auf gezielte Werbung sollte sie erwägen, durch entsprechende Rechtsvorschriften Browser-Einstellungen vorzuschreiben, in denen Cookies von Drittanbietern standardmäßig gesperrt werden und die Nutzer bei der Erstinstallation oder Aktualisierung ihres Browsers einen Privatsphäre-Assistenten benutzen müssen.

104. Abschließend empfiehlt der EDSB:

a) Die Kommission sollte die Einführung des Rechenschaftsprinzips in der geltenden Datenschutzrichtlinie erwägen und

b) einen Regel- und Verfahrensrahmen für die Anwendung der Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation zur Benachrichtigung bei Datenschutzverletzungen ausarbeiten und ihre Gültigkeit auf alle für die Datenverarbeitung Verantwortlichen ausdehnen.

Geschehen zu Brüssel am 18. März 2010.

Peter HUSTINX

Europäischer Datenschutzbeauftragter