I

(Entschließungen, Empfehlungen und Stellungnahmen)

STELLUNGNAHMEN

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

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)

(2008/C 101/01)

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 286,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 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,

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,

gestützt auf die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, insbesondere auf Artikel 41 —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. **EINLEITUNG**

1. Die Kommission hat am 15. März 2007 die Mitteilung „Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen" ([1]) (nachstehend „Mitteilung" genannt) angenommen. Nach Artikel 41 der Verordnung (EG) Nr. 45/2001 ist der Europäische Datenschutzbeauftragte (EDSB) für die Beratung der Organe und Einrichtungen der Gemeinschaft in allen die Verarbeitung personenbezogener Daten betreffenden Angelegenheiten zuständig. Gemäß diesem Artikel nimmt der EDSB hiermit Stellung.

2. Diese Stellungnahme ist als Reaktion des EDSB auf die Mitteilung sowie auf andere Maßnahmen im RFID-Bereich zu sehen, die seit der Annahme der Mitteilung erfolgt sind. Zu den anderen einschlägigen Maßnahmen, die in dieser Stellungnahme berücksichtigt wurden, gehört Folgendes:

   — der Beschluss der Kommission vom 28. Juni 2007 zur Einsetzung der Sachverständigengruppe für Funkfrequenzkennzeichnung (RFID) ([2]), eine direkte Folgemaßnahme zu der Mitteilung. Diese Gruppe ist auch als RFID-Interessengruppe bekannt. Entsprechend Artikel 4 Absatz 4 Buchstabe b des Beschlusses wirkt der EDSB an den Arbeiten der Gruppe als Beobachter mit,

   — die Entschließung des Rates vom 22. März 2007 zu einer Strategie für eine sichere Informationsgesellschaft in Europa ([3]),

   — das vom Europäischen Parlament initiierte Projekt „RFID und Identitätsmanagement" ([4]),

([1]) Dok. KOM(2007) 96 endg.
([2]) Beschluss 467/2007/EG (ABl. L 176 vom 6.7.2007, S. 25).
([3]) ABl. C 68 vom 24.3.2007, S. 1.
([4]) Projekt „RFID and identity management — Case studies from the frontline of the development towards ambient intelligence", durchgeführt von der Europäischen Gruppe für Technikfolgenabschätzung (European Technology Assessment Group/ETAG) im Auftrag des Dienstes des Europäischen Parlaments für die Bewertung wissenschaftlicher und technischer Optionen (Scientific and Technological Option Assessment/STOA): http://www.europarl.europa.eu/stoa/default_en.htm

— die im Juni 2007 abgegebene Stellungnahme Nr. 4/2007 der Artikel-29-Datenschutzgruppe zu dem Begriff „personenbezogene Daten“ ([1]),

— die Mitteilung der Kommission an das Europäische Parlament und an den Rat zum Thema „Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie“ ([2]) und die Stellungnahme des EDSB vom 25. Juli 2007 zu dieser Mitteilung ([3]),

— die Annahme des Vorschlags für eine Richtlinie zur Änderung (u. a.) der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation durch die Kommission ([4]).

3. Der EDSB begrüßt die Mitteilung der Kommission über die Funkfrequenzkennzeichnung, da sie auf die wichtigsten Fragen im Zusammenhang mit dem Einsatz der RFID-Technologie eingeht, ohne dabei die entscheidenden Aspekte der Privatsphäre und des Datenschutzes außer Acht zu lassen. Die kohärenten und intensiven Vorbereitungsarbeiten haben sich positiv auf die Mitteilung ausgewirkt. So fanden im Vorfeld der Mitteilung fünf thematische Workshops und eine öffentliche Online-Anhörung ([5]) statt, die von der Kommission in Auftrag gegeben worden waren.

4. Der EDSB schließt sich der Auffassung an, dass RFID-Systeme bei der Entwicklungsphase der Informationsgesellschaft, die für gewöhnlich „Internet der Dinge“ genannt wird, eine Schlüsselrolle spielen könnten, und er teilt voll und ganz die in Abschnitt 3.2 der Mitteilung geäußerten Bedenken, dass RFID-Systeme möglicherweise eine Gefährdung des Rechts des Einzelnen auf Privatsphäre und Datenschutz bewirken. So benannte der EDSB bereits in seinem Jahresbericht für das Jahr 2005 die Funkfrequenzkennzeichnung zusammen mit biometrischen Systemen, intelligenten Umgebungen und Identitätsmanagementsystemen als technologische Entwicklungen, bei denen davon auszugehen ist, dass sie erhebliche Auswirkungen auf den Datenschutz mit sich bringen werden.

5. Nach Auffassung des EDSB werden die „Domestizierung“ der RFID-Technologien und ihre breite Akzeptanz nicht nur durch die von ihnen gebotenen Annehmlichkeiten oder neuen Dienste erreicht, sondern auch durch die positive Wirkung maßgeschneiderter und kohärenter Datenschutzgarantien gefördert.

6. Kurz gesagt: Der EDSB stuft RFID als eine grundlegend neue technologische Entwicklung ein, die in der Mitteilung der Kommission zu Recht als Wegbereiter für eine neue Entwicklungsphase der Informationsgesellschaft bezeichnet wird.

7. Diese Entwicklung wirft in verschiedenen Bereichen wichtige Fragen auf — auch im Bereich Datenschutz und Privatsphäre. Der EDSB beschränkt sich in seiner Stellungnahme auf diesen Bereich.

II. SCHWERPUNKT DER STELLUNGNAHME

8. Im Mittelpunkt dieser Stellungnahme stehen die möglichen Auswirkungen der betreffenden Entwicklungen auf Datenschutz und Privatsphäre. Derzeit herrscht Ungewissheit in Bezug auf diese Auswirkungen, was auch darauf zurückzuführen ist, dass die Entwicklung, was RFID-Systeme und ihre Domestizierung betrifft, sich noch in vollem Gange befindet und keineswegs klar ist, wo sie hinführen wird.

9. Vor diesem Hintergrund vertritt der EDSB folgenden Ansatz:

— erstens muss verdeutlicht werden, welche praktischen Auswirkungen der Einsatz von RFID-Systemen auf den Datenschutz und die Privatsphäre hat,

— zweitens sind diese Auswirkungen vor dem Hintergrund des bestehenden Rechtsrahmens für Datenschutz und Privatsphäre genau zu erfassen,

— drittens geht der EDSB auf die Frage ein, ob diese Auswirkungen speziellere Regeln erfordern, um die mit dem Einsatz der RFID-Technologien verbundenen Datenschutzfragen zu klären. Diese Frage, auf die der EDSB bereits in seiner Stellungnahme zu der Mitteilung über die Datenschutzrichtlinie eingegangen ist, soll in der vorliegenden Stellungnahme weiter vertieft werden.

10. Mit diesem Ansatz möchte der EDSB erreichen, dass bei der Entwicklung von RFID-Systemen und ihrer Domestizierung auch die berechtigten Belange des Datenschutzes und der Privatsphäre berücksichtigt werden.

III. VERDEUTLICHUNG DER AUSWIRKUNGEN

RFID-Systeme und Funketiketten

11. Auch wenn, wie bereits angemerkt, die Entwicklungen noch in vollem Gange sind und sich das Ergebnis dieses Prozesses noch nicht absehen lässt, ist es sehr wohl möglich, die Hauptmerkmale dieser Entwicklungen hinsichtlich ihrer Auswirkungen auf den Datenschutz zu beschreiben.

([1]) Auf der Website der Gruppe veröffentlichtes Dokument WP 136.
([2]) Mitteilung der Kommission an das Europäische Parlament und an den Rat vom 7. März 2007 zum Thema „Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie“, Dok. KOM(2007) 87 endg.
([3]) ABl. C 255 vom 27.10.2007, S. 1. Siehe ferner: „Stellungnahme zu der Mitteilung über die Datenschutzrichtlinie“.
([4]) Vorschlag vom 13. November 2007 für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, KOM(2007) 698 endg. Die Richtlinie 2002/58/EG wird nachstehend als „Datenschutzrichtlinie“ für elektronische Kommunikation bezeichnet.
([5]) http://www.rfidconsultation.eu/

12. Bei der Bewertung der potenziell den Datenschutz und die Privatsphäre betreffenden Aspekte der RFID-Technologie ist es von größter Wichtigkeit, nicht nur die RFID-Funketiketten, sondern die gesamte RFID-Infrastruktur zu berücksichtigen, d. h. das Funketikett, das Lesegerät, das Netz, die Referenzdatenbank und die Datenbank, in der die von der Verbindung Funketikett/Lesegerät generierten Daten gespeichert werden. Wie in der Einleitung der Mitteilung kurz angemerkt wird, umfasst RFID mehr als bloße „elektronische Etiketten" und daher werden sich die Datenschutzfragen nicht ausschließlich auf die Funketiketten beschränken, sondern sich auf die gesamte RFID-Infrastruktur erstrecken. Jede RFID-Komponente hat erforderlichenfalls ihren Beitrag zur Umsetzung des europäischen Rechtsrahmens für den Datenschutz zu leisten. Triebkräfte der RFID-Entwicklung sind die Haupttendenzen der sich weiterentwickelnden Informationsgesellschaft wie etwa eine nahezu unbegrenzte Bandbreite, allgegenwärtige Netzanschlüsse und eine schier unerschöpfliche Speicherkapazität.

Auswirkungen von RFID-Systemen und Funketiketten

13. Zwar ist, wie im vorangegangenen Absatz vermerkt, ein umfassenderer Ansatz erforderlich, doch ist es aus verschiedenen Gründen gerechtfertigt, den Schwerpunkt zunächst auf die Verwendung von RFID bei der Etikettierung von einzelnen Verbraucherprodukten wie etwa im Einzelhandel zu legen. Ein naheliegender Grund ist die hier geplante Ausweitung des RFID-Einsatzes, der sich offenbar immer mehr durchsetzt. Gegenüber anderen RFID-Anwendungen mit begrenzter oder eingeschränkter Verwendung hat die Warenetikettierung das Potenzial, sich zu einer Massenmarktanwendung zu entwickeln. Schon jetzt sind viele Verbraucherprodukte mit RFID-Etiketten ausgestattet. Diese RFID-Etikettierung wird sich auf eine Vielzahl von Einzelpersonen auswirken, deren personenbezogene Daten wahrscheinlich jedes Mal verarbeitet werden, wenn sie ein Produkt erwerben, das mit einem RFID-Etikett versehen ist.

14. Den Auswirkungen der RFID-Etikettierung auf die Eigentümer der Artikel sollte besondere Aufmerksamkeit gewidmet werden. RFID-Systeme bewirken möglicherweise eine Erweiterung der Beziehung zwischen einem Artikel und seinem Eigentümer. Sobald diese Beziehung erweitert worden ist, kann der Eigentümer mit einem Scanner erfasst und im Hinblick auf künftige Geschäftsvorgänge als „Erwerber mit geringer Kaufkraft" oder „attraktive Zielperson" eingestuft werden; die exzessive Herstellung von Eins-zu-eins-Zuordnungen ([1]) könnte zur automatischen „Ahndung" bestimmter Verhaltensweisen (Wiederverwertungsverpflichtungen, Abfallverhalten usw.) führen. Menschen dürfen nicht einem Prozess von für sie nachteiligen automatisierten Entscheidungen unterworfen sein. Durch die Katalysatorwirkung dieses RFID-Merkmals nimmt die Gefahr zu, dass die Informationsgesellschaft immer weiter auf eine Lage zusteuert, in der automatisierte Entscheidungen getroffen werden und die Technik missbraucht wird, um menschliches Verhalten zu steuern.

15. Bei den in einem RFID-Etikett gespeicherten oder von diesem erzeugten Daten kann es sich um personenbezogene Daten im Sinne des Artikels 2 der Datenschutzrichtlinie handeln. So enthalten für Reisezwecke verwendete Chipkarten möglicherweise sowohl Daten zur Identifizierung als auch Informationen über die jüngsten Reisen des Karteninhabers. Wollte eine skrupellose Person die Bewegungen einzelner Personen nachvollziehen, so bräuchte sie lediglich an strategischen Stellen Lesegeräte aufstellen, die ihr Informationen über die Reisebewegungen der Karteninhaber liefern, wodurch deren Privatsphäre und der Schutz ihrer personenbezogenen Daten verletzt würden.

16. Zu ähnlichen Bedrohungen der Privatsphäre könnte es selbst dann kommen, wenn die im RFID-Etikett gespeicherten Informationen nicht die Namen einzelner Personen enthalten. RFID-Etiketten enthalten Kennungen, die dem jeweiligen Verbraucherprodukt unverwechselbar zugeordnet sind: Wenn jedes Etikett eine eindeutige Identitätskennzeichnung aufweist, lässt sich diese Kennung auch zu Überwachungszwecken verwenden. Trägt eine Person beispielsweise eine Armbanduhr mit einem RFID-Etikett, das mit einer Identifizierungsnummer versehen ist, so könnte dies auch als eindeutige Kennung für den Träger der Uhr verwendet werden, selbst wenn dessen Identität unbekannt ist. Je nach der Art der Verwendung der betreffenden Informationen — entweder in Bezug auf die Uhr selbst oder auf die Einzelperson — könnte die Richtlinie gelten oder nicht gelten. Sie würde beispielsweise dann gelten, wenn Informationen über den Aufenthaltsort von Personen generiert werden, die voraussichtlich zur Überwachung ihres Verhaltens oder etwa für Preisdifferenzierungen, Zugangsverweigerungen oder unaufgeforderte Werbung verwendet werden.

17. Es muss in diesem Zusammenhang dafür gesorgt werden, dass RFID-Anwendungen zusammen mit den technologischen Maßnahmen eingesetzt werden, die erforderlich sind, um das Risiko einer ungewollten Weitergabe von Informationen auf ein Minimum zu reduzieren. Zu diesen Maßnahmen könnte die Vorgabe gehören, die RFID-Infrastruktur — insbesondere die RFID-Etiketten — so zu konzipieren, dass derartige Auswirkungen ausgeschlossen sind. So können RFID-Etiketten mit einer Außerbetriebsetzungsfunktion („kill command") versehen sein, die ihre Deaktivierung ermöglicht. Auf diese Option soll in Kapitel IV weiter eingegangen werden.

18. Dadurch, dass RFID-Systeme die Weiterverfolgung von Produkten auch nach dem Verlassen des Verkaufsorts ermöglichen, wird die Debatte über die Privatsphäre um neue Aspekte erweitert. Diesbezüglich sind zwei Fragen bei der Folgenabschätzung zu berücksichtigen: die Frage, wie sehr der Artikel als personenbezogen angesehen wird, und die Frage der Mobilität des Artikels ([2]).

19. Auch der Lebenszyklus eines Objekts könnte für die erforderliche Risikoanalyse herangezogen werden und in die quantitative Bewertung der potenziellen Bedrohungen für die Privatsphäre einfließen. Dadurch, dass ein Etikett nicht deaktiviert werden kann, kann ein Endverbraucherprodukt mit einem langen Lebenszyklus mehr Informationen über den Eigentümer des Produkts zusammentragen und ein genaueres Profil liefern. Dagegen sind Produkte mit kurzen Lebenszyklen wie etwa Limonadendosen von der Herstellung bis zur Wiederverwertung möglicherweise mit geringeren Risiken behaftet und könnten somit weniger strenge Maßnahmen erfordern als Produkte mit einem sehr viel längeren Lebenszyklus.

([1]) Dr. Sarah Spiekermann, Geschäftsführerin des Berliner Forschungszentrums Internetökonomie, in einem Beitrag zu dem im Rahmen des Transatlantischen Verbraucherdialogs am 13. März 2007 veranstalteten Workshop über RFID und die Allgegenwärtigkeit der Informationsverarbeitung.

([2]) Dara J. Glasser, Kenneth W. Goodman und Norman G. Einspruch: Chips, tags and scanners: Ethical challenges for radio frequency identification, Ethics and Information Technology, Bd. 9, Nr. 2, 2007.

Fragen der Privatsphäre und des Datenschutzes beim Einsatz von RFID-Systemen

20. Zum besseren Verständnis der Auswirkungen von RFID-Systemen auf die Privatsphäre und den Datenschutz werden im Folgenden fünf grundlegende Aspekte der Privatsphäre und der Sicherheit unterschieden.

21. Der erste Aspekt ist die Identifizierung der betroffenen Person. Vor mehr als sechzig Jahren bestand der Zweck der RFID-Etiketten in der „Freund-Feind-Erkennung" ankommender Objekte. Heute können RFID-Systeme nicht nur allgemeine Bestandteile eines Objekts erkennen, sondern letztendlich auch zur Identifizierung einer Person verwendet werden und müssen daher datenschutzfreundlich gestaltet werden.

22. Der zweite Aspekt betrifft die Identifizierung des/der für die Datenverarbeitung Verantwortlichen. Bei RFID-Systemen ist die Identifizierung des für die Datenverarbeitung Verantwortlichen im Sinne des Artikels 2 Buchstabe d der Datenschutzrichtlinie möglicherweise schwieriger und muss deshalb näher untersucht werden. Diese Identifizierung ist jedoch nach wie vor ein entscheidender Schritt bei der Festlegung der Verantwortlichkeiten, die jeder der einschlägigen Akteure im Hinblick auf die Einhaltung des rechtlichen Rahmens für den Datenschutz übernehmen muss. Während des Lebenszyklus des Funketiketts kann der für die Datenverarbeitung Verantwortliche je nach den Zusatzdiensten, die ggf. in Bezug auf das mit einem Etikett versehene Objekt erbracht werden, mehrmals wechseln.

23. Der dritte Aspekt ist die gesunkene Bedeutung der traditionellen Unterscheidung zwischen Privatsphäre und öffentlichem Raum. Obwohl auch in der Vergangenheit nicht immer eine eindeutige Trennung zwischen Privatsphäre und öffentlichem Raum bestand, so sind sich die meisten Menschen doch über die Grenzen zwischen diesen Bereichen (und auch über die Grauzonen) im Klaren und richten ihr Handeln — bewusst oder intuitiv — entsprechend aus. Laut Hall ([1]) definiert sich der private Raum für gewöhnlich anhand der physischen Distanz zu anderen Menschen. Das Privatsphärenmanagement kann auch als ein dynamischer Grenzsetzungsprozess betrachtet werden ([2]). Daher kann es nicht überraschen, dass der „drahtlose Charakter" der Kommunikation über Funketiketten sowie die dadurch bestehende Möglichkeit, Daten außerhalb der Sichtweite auszulesen, Bedenken in Bezug auf den Schutz der Privatsphäre aufwerfen, da diese herkömmliche Grenzen verwischen und entsprechende Gestaltungsmöglichkeiten beeinträchtigt werden. So besteht die Befürchtung, dass dem Einzelnen die bisher ausgeübte Kontrolle über die Distanzgestaltung teilweise oder gar vollständig entgleitet. Dementsprechend wurde die Leseentfernung der ersten Anwendungen von RFID-Systemen von deren Befürwortern und Gegnern gleichermaßen ins Visier genommen.

24. Der vierte Aspekt betrifft die Größe und die materiellen Eigenschaften der RFID-Etiketten. Da diese Etiketten grundsätzlich klein und preiswert sein müssen, sind die Sicherungsvorkehrungen, mit denen dieser Teil des RFID-Systems ausgestattet werden könnte, naturgemäß begrenzt. Durch die Drahtlosigkeit der Kommunikation entsteht jedoch auch eine zusätzliche Risikoebene im Vergleich zur drahtgebundenen Kommunikation, was zusätzliche Sicherheitsanforderungen notwendig macht.

25. Der fünfte Aspekt ist eine mangelnde Transparenz bei der Verarbeitung. Mit RFID-Systemen könnten unbemerkt Informationen zusammengetragen und verarbeitet werden, die sich zur Erstellung eines Persönlichkeitsprofils verwenden ließen. Diese Auswirkung lässt sich sehr gut durch den Vergleich von RFID-Systemen mit Mobiltelefonen veranschaulichen — ein Vergleich, der des Öfteren herangezogen wird. Die Mobiltelefonie genoss eine sehr hohe technologische Akzeptanz — trotz der Gefahr von Verletzungen der Privatsphäre. Man könnte daraus folgern, dass RFID genau so akzeptiert werden wird. Gleichzeitig muss jedoch darauf hingewiesen werden, dass es sich bei einem Mobiltelefon um ein sichtbares Objekt handelt, das sich insoweit noch unter der Kontrolle des Endverbrauchers befindet, als es abgeschaltet werden kann. Dies ist bei RFID nicht der Fall.

26. Auch wenn das oben erwähnte unbemerkte Zusammentragen und Verarbeiten von Informationen durchaus rechtmäßig sein kann, so ist es ebenso gut möglich — und unter verschiedenen Umständen auch sehr wahrscheinlich —, dass es zu einer unrechtmäßigen Erfassung und Verarbeitung derartiger Daten kommt.

27. Die in diesem Kapitel enthaltenen Verdeutlichungen gestatten folgende Schlussfolgerung: Der breite Einsatz der RFID-Technologie ist von Grund auf neuartig und kann sich in fundamentaler Weise auf unsere Gesellschaft und auf den Schutz der Grundrechte in dieser Gesellschaft, wie Privatsphäre und Datenschutz, auswirken. RFID kann qualitative Veränderungen bewirken.

IV. GENAUE ERFASSUNG DER AUSWIRKUNGEN

Einleitung

28. Dieses Kapitel behandelt im Wesentlichen die Auswirkungen der RFID-Technologie auf den Schutz der Grundrechte in unserer Gesellschaft, zu denen die Rechte auf Privatsphäre und Datenschutz gehören. Die entsprechenden Ausführungen erfolgen in zwei Schritten, wobei in einem ersten Schritt kurz beschrieben wird, wie diese Grundrechte in dem derzeitigen Rechtsrahmen geschützt werden. In einem zweiten Schritt wird der EDSB darauf eingehen, wie dieser Rahmen umfassend genutzt werden kann. Dieses Bestreben wurde bereits mit den Worten „vollständige Umsetzung der derzeitigen Bestimmungen der Richtlinie" in der Stellungnahme zu der Mitteilung über die Datenschutzrichtlinie thematisiert.

29. Ausgangspunkt für diese Überlegungen ist der Umstand, dass neue technologische Entwicklungen wie RFID-Systeme sich eindeutig auf die Anforderungen an einen wirksamen rechtlichen Rahmen für den Datenschutz auswirken. Zugleich kann es zur Gewährleistung eines wirksamen Schutzes der personenbezogenen Daten von Einzelpersonen erforderlich werden, dem Einsatz dieser neuen Technologien Grenzen zu setzen. Die Interaktion ist daher wechselseitig: Die Technologie beeinflusst die Rechtsvorschriften und die Rechtsvorschriften beeinflussen die Technologie ([3]).

([1]) Edward T. Hall, 1966, The Hidden Dimension (1. Auflage), Garden City, N.Y.: Doubleday.

([2]) Altman, I., 1975, The Environment and Social Behaviour, Brooks/Cole Monterrey.

([3]) Siehe die auf der Website des EDSB veröffentlichten Kommentare des EDSB vom März 2006 zu der Mitteilung der Kommission über die Interoperabilität der europäischen Datenbanken.

Schutz von Grundrechten

30. Der Schutz der Grundrechte auf Privatsphäre und Datenschutz in der Europäischen Union wird in erster Linie durch einen Rechtsrahmen gewährleistet, der erforderlich ist, weil es sich hier um Rechte handelt, die in Artikel 8 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten und in den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union anerkannt werden. Der für Datenschutz und RFID geltende Rechtsrahmen besteht im Wesentlichen aus der Datenschutzrichtlinie 95/46/EG und der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG ([1]).

31. Der allgemeine Rechtsrahmen für den Datenschutz nach Maßgabe der Richtlinie 95/46/EG gilt insoweit für die RFID-Technologie, als die von RFID-Systemen verarbeiteten Daten unter die Definition des Begriffs „personenbezogene Daten" fallen. Während RFID-Anwendungen in bestimmten Fällen ganz eindeutig personenbezogene Daten verarbeiten und zweifellos unter die Datenschutzrichtlinie fallen, gibt es auch Anwendungen, bei denen möglicherweise weniger offensichtlich ist, dass die Datenschutzrichtlinie für sie gilt. Die Stellungnahme Nr. 4/2007 der Artikel-29-Datenschutzgruppe zu dem Begriff „personenbezogene Daten" soll zu einer präzisieren und allgemein anerkannten Auslegung des Begriffs „personenbezogene Daten" beitragen und damit diese Unsicherheit verringern ([2]).

32. In Bezug auf die Datenschutzrichtlinie für elektronische Kommunikation stellt sich die Lage wie nachstehend beschrieben dar. Bisher ist unklar, ob diese Richtlinie für RFID-Anwendungen gilt. Daher enthält der Vorschlag der Kommission vom 13. November 2007 zur Änderung der Richtlinie eine Bestimmung, mit der präzisiert werden soll, dass die Richtlinie effektiv für bestimmte RFID-Anwendungen gilt. Andere RFID-Anwendungen fallen jedoch möglicherweise nicht unter die Richtlinie, weil diese auf die Verarbeitung personenbezogener Daten im Zusammenhang mit der Erbringung von öffentlich verfügbaren elektronischen Kommunikationsdiensten in öffentlichen Kommunikationsnetzen beschränkt ist.

33. Der Schutz der personenbezogenen Daten kann durch eine Reihe von Selbstregulierungsinstrumenten (rechtsetzungsunabhängiger Rahmen) ergänzt werden. Der Rückgriff auf diese Instrumente wird in beiden Richtlinien aktiv gefördert, und zwar insbesondere in Artikel 27 der Datenschutzrichtlinie, wo bestimmt ist, dass die Mitgliedstaaten und die Kommission die Ausarbeitung von Verhaltensregeln fördern, die zur ordnungsgemäßen Umsetzung dieser Richtlinie beitragen sollen. Ferner könnten Selbstregulierungsinstrumente wirksam zur Durchführung der nach Artikel 17 der Datenschutzrichtlinie und Artikel 14 der Datenschutzrichtlinie für elektronische Kommunikation vorgeschriebenen Sicherheitsmaßnahmen beitragen.

Vollständige Umsetzung des bestehenden Rahmens

34. In der Stellungnahme zu der Mitteilung über die Datenschutzrichtlinie wird eine Reihe von Instrumenten aufgelistet, die für eine bessere Umsetzung der Richtlinie zur Verfügung stehen. Die meisten der in der Stellungnahme genannten nicht verbindlichen Instrumente — wie etwa Mitteilungen zur Auslegung oder andere Mitteilungen, Förderung bewährter Verfahren, Verwendung von Datenschutzgütesiegeln und Datenschutz-Audits durch Dritte — sind auch für die RFID-Technologie von Belang. Auf die Möglichkeit der Annahme spezifischer Vorschriften für den RFID-Bereich wird in Kapitel V eingegangen. Es sind aber auch Verbesserungen innerhalb des derzeit geltenden Rahmens möglich.

Selbstregulierungsinstrumente

35. Der EDSB stimmt der Kommission darin zu, dass in einer ersten Phase Raum für die Selbstregulierung gelassen und es den beteiligten Akteuren ermöglicht werden sollte, rasch ein rechtlich einwandfreies Umfeld zu schaffen und somit zur Verwirklichung eines sichereren Rechtsumfelds beizutragen.

36. Es wird erwartet, dass die Kommission diesen Selbstregulierungsprozess im Benehmen mit der RFID-Interessengruppe belebt und steuert. In diesem Zusammenhang begrüßt der EDSB die in der Mitteilung angekündigte Empfehlung, die spezifische Leitlinien mit den „Grundprinzipien" enthalten soll, „die von den Behörden und anderen Beteiligten im Zusammenhang mit der RFID-Nutzung zu befolgen sind".

37. In der Mitteilung ist vorgesehen, dass die Selbstregulierung in Gestalt eines Verhaltenskodex oder eines Kodex für bewährte Verfahren erfolgt. Der EDSB vertritt die Auffassung, dass die Selbstregulierung unabhängig von ihrer Form Folgendes leisten sollte:

— Bereitstellung konkreter und praktischer Orientierungshilfen für die einzelnen Arten von RFID-Anwendungen und damit Leistung eines Beitrags zur Einhaltung des Rechtsrahmens für den Datenschutz,

— Berücksichtigung spezifischer Datenschutzfragen und -probleme, die im Zusammenhang mit generischen RFID-Anwendungen auftreten,

— Leistung eines Beitrags zur unionsweit einheitlichen und harmonisierten Anwendung der Datenschutzrichtlinie gerade in den Sektoren, in denen EU-weit die gleiche Art von RFID-Anwendungen verwendet werden dürfte,

— Anwendung durch alle einschlägigen Akteure. Die Nichtanwendung sollte negative (möglichst finanzielle) Auswirkungen nach sich ziehen.

([1]) In Nummer 59 dieser Stellungnahme wird auf die Relevanz einer dritten Richtlinie eingegangen, nämlich der Richtlinie 1999/5/EG des Europäischen Parlaments und des Rates vom 9. März 1999 über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität (ABl. L 91 vom 7.4.1999, S. 10).

([2]) Siehe u. a. Nummer 10 der Stellungnahme, auf die in Fußnote 5 verwiesen wird.

38. Der EDSB verweist auf einen Aspekt, bei dem die Selbstregulierung besonders sinnvoll ist. Für die RFID-Anwendungen, bei denen zwangsläufig personenbezogene Daten verarbeitet werden, erlegt die Datenschutzrichtlinie — insbesondere in Artikel 17 (Sicherheit der Verarbeitung) und Artikel 7 (Datenverarbeitung nur bei Erfüllung der entsprechenden rechtlichen Voraussetzungen) — den für die Verarbeitung Verantwortlichen verschiedene Pflichten auf. Nach den betreffenden Bestimmungen müssen die für die Verarbeitung Verantwortlichen zum einen Maßnahmen gegen die unberechtigte Offenlegung der Daten treffen. Zum anderen haben sie dafür zu sorgen, dass die Verarbeitung — wie etwa die Offenlegung von Informationen durch die Lesegeräte — gegebenenfalls nur dann erfolgt, wenn die Person, auf die sich die Daten beziehen, in Kenntnis der Sachlage eingewilligt hat.

39. Diese Bestimmungen der Datenschutzrichtlinie können dahin gehend ausgelegt werden, dass RFID-Anwendungen mit den technischen Lösungen ausgestattet sein müssen, die erforderlich sind, um dem Risiko einer unerwünschten Offenlegung vorzubeugen oder dieses Risiko so gering wie möglich zu halten und zu gewährleisten, dass die Verarbeitung oder Übermittlung der Daten gegebenenfalls nur mit der in Kenntnis der Sachlage gegebenen Einwilligung des Betroffenen erfolgt. Nach Auffassung des EDSB wird sich das Bestehen einer derartigen Verpflichtung (d. h. zur Anwendung der für die Verhütung oder Minimierung der Risiken einer unerwünschten Offenlegung erforderlichen technischen Lösungen) und ihre verbindliche Geltung für den Einsatz von RFID-Anwendungen noch nachhaltiger und deutlicher auswirken, wenn diese Verpflichtung in den noch ausstehenden Verhaltenskodex bzw. Kodex bewährter Verfahren, von dem bereits die Rede war, aufgenommen wird. Daher empfiehlt der EDSB nachdrücklich, in der Empfehlung der Kommission eine entsprechende Auslegung der Datenschutzrichtlinie vorzusehen und darauf hinzuweisen, dass die Verpflichtung besteht, RFID-Anwendungen mit den technischen Maßnahmen einzusetzen, die erforderlich sind, um der unerwünschten Sammlung oder Offenlegung von Informationen vorzubeugen.

Erforderliche Leitlinien

40. Der EDSB empfiehlt, dass die Kommission in enger Abstimmung mit der RFID-Sachverständigengruppe ein oder mehrere Dokumente erstellt, in denen ein klare Orientierung in der Frage vermittelt wird, wie der bestehende rechtliche Rahmen auf den RFID-Bereich angewendet werden soll. Diese Orientierung sollte praktische Hinweise zur Einhaltung der Grundsätze enthalten, die in der Datenschutzrichtlinie und in der Datenschutzrichtlinie für elektronische Kommunikation niedergelegt sind. Für den mit dieser Orientierung zu verfolgenden Gesamtansatz und seine konkrete Ausgestaltung legt der EDSB die nachstehenden Vorschläge vor.

41. Die Leitlinien mit den für den RFID-Einsatz geltenden Grundsätzen sollten hinreichend zielgerichtet sein und einem sektorspezifischen Ansatz folgen. Eine undifferenzierte Einheitslösung wird dem Anliegen, einen präzisen und kohärenten Rahmen zu gewährleisten, nicht dienlich sein. Stattdessen müssen sich die Leitlinien auf genau bezeichnete sektorspezifische RFID-Anwendungen beschränken.

42. Ferner sollten die betreffenden Leitlinien Vorschläge für praktikable und wirksame Methoden zur Entwicklung von Techniken und Normen enthalten, die dazu beitragen könnten, dass die RFID-Systeme dem Datenschutz-Rechtsrahmen entsprechen, und die zur Anwendung des Konzepts „privacy by design“ („eingebauter Datenschutz“) führen.

43. Bei der Anwendung des derzeitigen Rechtsrahmens auf den RFID-Bereich ist der Anwendung der Datenschutzgrundsätze und -pflichten, die für die Datenverarbeitung bei RFID-Anwendungen Verantwortlichen gelten, besondere Aufmerksamkeit zu widmen. Besonders relevant sind folgende Verpflichtungen und Grundsätze:

— der Grundsatz des Rechts auf Information einschließlich des Rechts, informiert zu werden, wenn Daten durch Lesegeräte erfasst werden und — gegebenenfalls — dass Produkte mit Funketiketten ausgestattet sind,

— das Konzept der Einwilligung als eine der rechtlichen Voraussetzungen für die Verarbeitung von Daten. Dieses Konzept findet seinen Niederschlag in der Verpflichtung, die RFID-Etiketten am Verkaufsort zu deaktivieren, es sei denn, der Betroffene hat der Verarbeitung zugestimmt ([1]). Das Recht auf Deaktivierung der RFID-Etiketten dient auch dem Zweck, die Sicherheit der Informationen zu gewährleisten, d. h. dafür Sorge zu tragen, dass die über RFID-Etiketten verarbeiteten Daten nicht gegenüber Dritten, bei denen dies nicht gewünscht wird, offen gelegt werden,

— das Recht des Einzelnen, keinen für ihn nachteiligen Entscheidungen unterworfen zu werden, die allein auf der automatisierten Verarbeitung eines definierten Persönlichkeitsprofils beruhen.

44. Was das Recht auf Information anbelangt, so sollte in den Leitlinien festgelegt werden, dass den betroffenen Personen Informationen über die Verarbeitung ihrer personenbezogenen Daten bereitgestellt werden müssen. Sie sollten unter anderem unterrichtet werden über: i) die Präsenz von Lesegeräten und die Präsenz aktivierter RFID-Etiketten auf Produkten oder Produktverpackungen; ii) die Auswirkungen einer derartigen Präsenz hinsichtlich der Erhebung von Informationen; und iii) den Zweck, für den die erhobenen Informationen verwendet werden sollen.

45. Die Verwendung von Logos ist möglicherweise eine zweckdienliche Unterrichtungsmaßnahme. Logos können verwendet werden, um auf die Präsenz von Lesegeräten und von RFID-Etiketten hinzuweisen, die aktiv bleiben sollen. Die Verwendung von Logos allein wird jedoch nicht ausreichen, um eine faire Verarbeitung von Informationen zu gewährleisten; dazu ist erforderlich, dass die Informationen den Betroffenen in eindeutiger und verständlicher Form vermittelt werden. Die Verwendung von Logos sollte als eine die Bereitstellung ausführlicher Informationen ergänzende Maßnahme angesehen werden.

([1]) Siehe die ausführlichere Darlegung in den Nummern 46-50.

Der Grundsatz der vorherigen Zustimmung („Opt-in-Prinzip") als Eckpfeiler

46. Bei allen einschlägigen RFID-Anwendungen sollten die gewählten Lösungen mit dem Grundsatz der vorherigen Zustimmung am Verkaufsort im Einklang stehen und ihn zur Grundvoraussetzung machen. Eine Aktivierung der RFID-Etiketten in der Form, dass sie nach Verlassen des Verkaufsorts weiterhin Informationen übermitteln, wäre unrechtmäßig, wenn der für die Verarbeitung Verantwortliche keine angemessenen rechtlichen Gründe geltend machen kann. Angemessene rechtliche Gründe wären in der Regel nur: a) die Einwilligung des Betroffenen; oder b) der Umstand, dass die Offenlegung notwendig ist, um auf ausdrücklichen und freien Wunsch der betreffenden Person eine Dienstleistung zu erbringen ([1]). Diese beiden rechtlichen Gründe wären dann als vorherige Zustimmung („opt in") anzusehen.

47. Entsprechend dem Opt-in-Prinzip sollten die Funketiketten am Verkaufsort deaktiviert werden, es sei denn, der Erwerber des mit einem Funketikett ausgestatteten Produkts wünscht, dass das Etikett aktiviert bleibt. Mit der Ausübung des Rechts, das Etikett aktiviert zu lassen, würde die betreffende Person der Weiterverarbeitung ihrer Daten, beispielsweise einer Übermittlung der Daten an das Lesegerät bei ihrem nächsten Besuch bei dem für die Verarbeitung Verantwortlichen, zustimmen.

48. Der EDSB betont, dass ein flexibles Vorgehen erforderlich ist, um der zunehmenden Diversifizierung der RFID-Anwendungen Rechnung zu tragen und die Entwicklung neuer innovativer Geschäftsmodelle zu erleichtern. Bei der Anwendung des Opt-in-Prinzips muss daher für Flexibilität gesorgt werden.

49. Für das Opt-in-Prinzip gibt es vielfältige Anwendungsmöglichkeiten. So könnte beispielsweise alternativ zur Entfernung der Funketiketten erwogen werden, das Etikett zu blockieren, es zeitweise außer Funktion zu setzen oder ein als „resurrecting duckling model" („Entchenprägungsmodell") ([2]) bezeichnetes Sicherheitsmodell zugrunde zu legen, bei dem nur ein spezifischer Nutzer Zugang hat. Im Falle eines Funketiketts mit kurzem Lebenszyklus könnte die Adresse des Etiketts, die auf in einer Datenbank gespeicherte Informationen verweist, auch aus der Referenzdatenbank gelöscht werden, um die weitere Verarbeitung der von dem Funketikett gesammelten zusätzlichen Daten auszuschließen.

50. Fazit: Obschon der EDSB die Auffassung vertritt, dass das „Opt-in-Prinzip" am Verkaufsort eine rechtliche Verpflichtung ist, die in den meisten Fällen bereits aufgrund der Datenschutzrichtlinie besteht, so sprechen dennoch gute Gründe dafür, diese Verpflichtung in Selbstregulierungsinstrumenten festzuschreiben, um nicht zuletzt zu gewährleisten, dass das Prinzip auf die am besten geeignete Art und Weise umgesetzt wird. Eine spezifische Umsetzung ist in jedem Fall für alle RFID-Anwendungen erforderlich, die nicht in den Anwendungsbereich der Datenschutzrichtlinie fallen.

Unbedingt erforderlich: der „eingebaute Datenschutz"

51. Zur Minimierung der Risiken für die Wahrung der Privatsphäre und den Datenschutz wird in Nummer 3.2 der Mitteilung der Kommission auf Seite 8 die Ausarbeitung und Verabschiedung von Gestaltungskriterien befürwortet. Der EDSB begrüßt diesen Ansatz. In der Tat wird die Annahme von Spezifikationen und Gestaltungskriterien auch als „beste verfügbare Technik" („Best Available Techniques/BAT") bezeichnet, einen wirksamen Beitrag zur Ausgestaltung der Datenschutzvorschriften und der Sicherheitsanforderungen leisten. Diese Ausarbeitung technischer und organisatorischer Kriterien wird — eine regelmäßige Überprüfung vorausgesetzt — das Modell einer Symbiose von Datenschutz- und Sicherheitsanforderungen stärken, das die Europäische Union derzeit entwickelt.

52. Die Festlegung sachgerechter BAT für Datenschutz und Sicherheit bei RFID-Systemen wird ferner sowohl für die Schaffung eines zuverlässigen Umfelds, das die Akzeptanz dieser Systeme bei den Endnutzern erhöht, als auch für die Wettbewerbsfähigkeit der europäischen Industrie von ausschlaggebender Bedeutung sein.

53. Der Prozess der Auswahl von BAT für RFID-Systeme sollte mit Datenschutz- und Sicherheitsfolgenabschätzungen untermauert werden, für die noch einiges getan werden muss. Nach Auffassung des EDSB kann die Europäische Agentur für Netz- und Informationssicherheit (ENISA) zusammen mit den im Verbund mit den einschlägigen Akteuren aus der Industrie agierenden Gemeinsamen Forschungsstellen der Europäischen Kommission einen Beitrag zur Ermittlung dieser bewährten Verfahren und zur Entwicklung entsprechender Methoden beitragen. Mit der jüngst erfolgten Einleitung eines Projekts für technische Leitlinien im RFID-Bereich hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein gutes Beispiel ([3]) für bewährte Verfahren gegeben, die es nunmehr auf europäischer Ebene zu entwickeln gilt.

54. Auch Normen können bei der frühzeitigen Anwendung des Grundsatzes des „eingebauten Datenschutzes" eine entscheidende Rolle spielen. Die Kommission sollte daher dazu beitragen, dass bei der Entwicklung internationaler RFID-Normen Sicherheitsgarantien für die Wahrung der Privatsphäre und den Datenschutz festgelegt werden. Die Artikel-29-Datenschutzgruppe hat in ihrem Arbeitsdokument über RFID ([4]) genau dargelegt, wie Normen zur datenschutzfreundlichen Gestaltung von RFID-Systemen beitragen können.

([1]) Bei einigen RFID-Anwendungen gibt es möglicherweise noch andere Gründe, auf denen die Datenverarbeitung beruhen kann, wie etwa Artikel 7 Buchstabe f (berechtigtes Interesse des für die Verarbeitung Verantwortlichen, sofern angemessene Schutzmaßnahmen getroffen werden).

([2]) Der Name dieses von Frank Stajano und Ross Anderson von der Universität Cambridge entwickelten Modells geht auf die Frage zurück, wie ein Gänseküken davon ausgehen kann, das es sich bei dem ersten beweglichen Objekt, das es sieht, um seine Mutter handeln muss.

([3]) http://www.bsi.bund.de/veranst/rfid/index.htm

([4]) Arbeitsdokument WP 105 vom 19. Januar 2005 über die mit der RFID-Technologie verbundenen Datenschutzfragen.

55. Ferner begrüßt der EDSB den von der Kommission vertretenen Standpunkt zu Forschung und Entwicklung in Bezug auf RFID-Technologien und zu der Notwendigkeit, die Risiken für den Datenschutz zu minimieren. So muss der Grundsatz des „eingebauten Datenschutzes“ so früh wie möglich bei der Entwicklung von Technologien zum Tragen kommen, was verstärkt dazu beitragen wird, dass diese Technologien dem rechtlichen Rahmen für den Datenschutz entsprechen. Der EDSB wird — wie in seinem Jahresbericht 2006 kurz vermerkt — selbst zum Erreichen dieses Ziels beitragen, indem er im konkreten Fall Stellungnahmen und Empfehlungen zu Projekten des 7. Rahmenprogramms (2007-2013) abgibt.

V. **SIND SPEZIELLE RECHTSETZUNGSMASSNAHMEN ERFORDERLICH?**

56. Die Selbstregulierung reicht möglicherweise nicht aus, um den bestehenden Rahmen für Datenschutz und Wahrung der Privatsphäre vollständig umzusetzen. Auch wenn die Selbstregulierung den vorgenannten Anforderungen genügt, ist ihre Einhaltung freiwillig und kann die Nichteinhaltung nicht immer wirksam geahndet werden. So sind möglicherweise zusätzlich verbindliche Rechtsvorschriften erforderlich, um den Schutz der Rechte des Einzelnen auf Privatsphäre und Datenschutz zu gewährleisten. Dies ist um so notwendiger, wenn der Selbstregulierungsansatz nicht greift.

57. Eine Kernfrage ist die Ermittlung der Rechtsvorschriften, die erforderlich sind, um zu gewährleisten, dass RFID-Anwendungen wirklich mit den erforderlichen technischen Lösungen ausgestattet werden, mit denen den Risiken für Datenschutz und Privatsphäre vorgebeugt werden kann bzw. diese Risiken auf ein Mindestmaß begrenzt werden können, und dass die für die Verarbeitung Verantwortlichen die geeigneten Maßnahmen treffen, um ihren Verpflichtungen aufgrund des bestehenden rechtlichen Rahmens nachzukommen. Dies wirft einige weitere Fragen auf:

— Sind spezifische Vorschriften erforderlich?

— Wenn dies bejaht wird, können diese Vorschriften innerhalb des vorhandenen Rechtsrahmens, beispielsweise im Wege der bestehenden Ausschussverfahren, angenommen werden?

— Oder ist vielmehr ein neuer Rechtsetzungsakt erforderlich, um den wirksamen Einsatz von RFID-Anwendungen mit „eingebauten“ Technologien zur Erhöhung des Datenschutzes sicherzustellen?

58. In diesem Kapitel soll auf die Möglichkeiten des Erlasses von verbindlichen Rechtsvorschriften innerhalb des bestehenden rechtlichen Rahmen eingegangen werden; die Frage der Notwendigkeit eines neuen Rechtsetzungsakts, bei der es sich um einen gesonderten Aspekt handelt, wird in Kapitel VI behandelt.

59. In erster Linie sollte Artikel 17 der Richtlinie 95/46/EG, Artikel 14 Absatz 3 der Richtlinie 2002/58/EG und Artikel 3 Absatz 3 Buchstabe c der Richtlinie 1999/5/EG besondere Aufmerksamkeit gewidmet werden. Artikel 14 Absatz 3 der Richtlinie 2002/58/EG gestattet es den Mitgliedstaaten, gemäß der Richtlinie 1999/5/EG ([1]) mit entsprechenden Maßnahmen 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. In Artikel 3 Absatz 3 Buchstabe c der Richtlinie 1999/5/EG ist vorgesehen, dass die Kommission — im Wege eines Ausschussverfahrens — festlegen kann, dass Geräte in bestimmten Geräteklassen oder bestimmte Gerätetypen so hergestellt sein müssen, dass sie über Sicherheitsvorrichtungen zum Schutz personenbezogener Daten und der Privatsphäre des Benutzers und des Teilnehmers verfügen. Bisher ist von der zuletzt genannten Bestimmung noch kein Gebrauch gemacht worden.

60. Die genannten Bestimmungen geben dem Gesetzgeber — sowohl auf einzelstaatlicher Ebene als auch auf der Ebene der Gemeinschaft — die Befugnis, vorzuschreiben, dass in den Prozess der Herstellung von RFID-Systemen Sicherheitsvorkehrungen zur Wahrung der Privatsphäre und zum Datenschutz integriert werden, was als Konzept des „eingebauten Datenschutzes“ bekannt ist ([2]). Dieses Konzept verlangt zudem den Einsatz der besten verfügbaren Technologie.

61. Der EDSB empfiehlt im Hinblick auf eine verbindliche Anwendung des Konzepts „des eingebauten Datenschutzes“, dass die Kommission von dem Verfahren nach Artikel 3 Absatz 3 Buchstabe c der Richtlinie 1999/5/EG unter Heranziehung der RFID-Sachverständigengruppe Gebrauch macht.

62. In zweiter Linie ist es möglich, die Anwendung des bestehenden rechtlichen Rahmens auf den RFID-Bereich vorzuschreiben, indem die Richtlinien selbst geändert werden. Wie bereits erwähnt, hat die Kommission gerade einen Vorschlag zur Änderung der Datenschutzrichtlinie für elektronische Kommunikation vorgelegt, der eine neue Bestimmung mit dieser Zielrichtung enthält. Der EDSB begrüßt diese erste Bestätigung des Umstands, dass die Richtlinie für RFID-Anwendungen gilt. Er wird sich in seiner für Anfang 2008 vorgesehenen Stellungnahme zu dem Änderungsvorschlag mit den spezifischen Fragen befassen, die durch das Verhältnis zwischen der Datenschutzrichtlinie für elektronische Kommunikation und der RFID-Technologie aufgeworfen werden.

63. Da die Kommission jedoch auf kurze Sicht keine Änderung der Datenschutzrichtlinie plant ([3]), sind die Möglichkeiten für Vorschriften über eine Anwendung des bestehenden Rechtsrahmens auf die RFID-Technologie begrenzt.

VI. **IST EIN SPEZIELLER RECHTLICHER RAHMEN FÜR RFID ERFORDERLICH?**

Absichten der Kommission

64. In der Mitteilung ([4]) wird die Bedeutung von Sicherheit und „eingebautem Datenschutz“ hervorgehoben. Ferner wird die Einbindung aller betroffenen Akteure gefordert. Das Hauptergebnis der Tätigkeiten der Kommission soll darin

([1]) Und gemäß dem Beschluss 87/95/EWG des Rates vom 22. Dezember 1986 über die Normung auf dem Gebiet der Informationstechnik und der Telekommunikation (ABl. L 36 vom 7.2.1987, S. 31).

([2]) Siehe Kapitel IV.

([3]) Der EDSB unterstützt diese Vorgehensweise; siehe Nummer 64.

([4]) Siehe Nummer 4.1 der Mitteilung.

bestehen, eine „Empfehlung zu Grundprinzipien" zu „veröffentlichen, die von den Behörden und anderen Beteiligten im Zusammenhang mit der RFID-Nutzung anzuwenden sind". Diese Empfehlung wird voraussichtlich im Frühjahr 2008 angenommen. Die in der Mitteilung genannten Rechtsetzungsambitionen umfassen zwei Schritte. Die Kommission äußert die Absicht:

— in Betracht zu ziehen, in den anstehenden Vorschlag für eine Änderung der Datenschutzrichtlinie für elektronische Kommunikation geeignete Bestimmungen über RFID aufzunehmen. Wie bereits bemerkt, hat die Kommission im November 2007 eine entsprechende Änderung der Datenschutzrichtlinie für elektronische Kommunikation vorgeschlagen und dabei bestätigt, dass die Richtlinie auf RFID-Anwendungen anwendbar ist ([1]); sie hat in diesem Zusammenhang aber nicht vorgeschlagen, den Anwendungsbereich der Richtlinie auf private Netze auszuweiten,

— zu bewerten, ob weitere Rechtsetzungsmaßnahmen zur Gewährleistung von Datenschutz und Privatsphäre erforderlich sind.

65. Daraus lässt sich ableiten, dass die Kommission nicht — jedenfalls nicht kurzfristig — die Absicht hat, neue spezifische Rechtsvorschriften zur Gewährleistung des Datenschutzes und der Wahrung der Privatsphäre im RFID-Bereich vorzuschlagen.

Parameter für den Gesetzgeber

66. Der EDSB führte in seiner Stellungnahme zu der Mitteilung über die Datenschutzrichtlinie einige Grundzüge für Rechtsetzung in Bezug auf die Verarbeitung personenbezogener Daten auf, die sich wie folgt zusammenfassen lassen:

— in erster Linie sollten die Grundprinzipien des Datenschutzes eingehalten werden: „Es sind keine neuen Prinzipien erforderlich, aber es besteht ein eindeutiger Bedarf an anderen Verwaltungsregelungen, die einerseits wirksam und angemessen für eine vernetzte Gesellschaft sind und andererseits die Verwaltungskosten minimieren" ([2]),

— zum zweiten sollten Rechtsetzungsvorschläge nur vorgelegt werden, wenn ihre Notwendigkeit und Verhältnismäßigkeit ausreichend nachgewiesen sind. Aus diesem Grund sollte der allgemeine Rechtsetzungsrahmen für den Datenschutz kurzfristig nicht geändert werden,

— drittens kann ein gesellschaftlicher Wandel zur Festlegung spezifischer rechtlicher Rahmenbedingungen führen, mit denen die in der Datenschutzrichtlinie vorgegebenen Grundsätze an die durch spezielle Technologien wie RFID aufgeworfenen Aspekte angepasst werden sollen. Natürlich müssen auch in diesem Fall die Kriterien der Notwendigkeit und der Verhältnismäßigkeit erfüllt sein.

67. In einem nächsten Schritt sollten sinnvollerweise die Erwartungen präzisiert werden, mit denen sich der Gesetzgeber im RFID-Bereich konfrontiert sieht:

— erstens müssen die Rechtsvorschriften flexibel sein und Raum für Innovation und technologische Entwicklung lassen. Dies sollte dazu führen, dass hinreichend „technologieneutrale" Rechtsvorschriften erlassen werden,

— zweitens müssen die Rechtsvorschriften Rechtssicherheit gewährleisten. Dies sollte zur Verabschiedung hinreichend spezifischer Rechtsvorschriften führen. Die betroffenen Akteure müssen genau wissen, welche Regeln für ihr Verhalten gelten,

— Drittens müssen die Rechtsvorschriften alle in Frage stehenden berechtigten Interessen wirksam schützen. Dies erfordert in jedem Fall die Durchsetzung der Rechtsvorschriften und eine klare Bestimmung der Zuständigkeiten (welche Seite ist für welches Verhalten rechenschaftspflichtig?) ([3]) Diese Anforderungen fallen umso stärker ins Gewicht, wenn es um Wahrung der Privatsphäre und Datenschutz und damit um Grundrechte des Einzelnen geht, die in der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten und in der Charta der Grundrechte der Europäischen Union verankert sind.

Standpunkt des EDSB

68. Der EDSB ist sich darüber im Klaren, dass nicht alle technologischen Entwicklungen eine Reaktion des europäischen Gesetzgebers erfordern. Technologische Entwicklungen können schnell eintreten, während die Annahme und das Inkrafttreten von Rechtsvorschriften Zeit erfordern und auch erfordern sollten. Rechtsvorschriften sollten das Ergebnis einer Abwägung aller in Frage stehenden Interessen sein. Wird als Rechtsetzungsakt eine Richtlinie gewählt, so ist der Zeitbedarf noch größer, da Richtlinien vollständig in die Rechtsordnungen der Mitgliedstaaten übernommen werden müssen.

69. RFID stellt jedoch, wie bereits mehrfach in dieser Stellungnahme betont wurde, nicht einfach irgendeine weitere technologische Entwicklung dar. In der Mitteilung wird ausgeführt, dass die RFID-Technik den Weg in eine neue Entwicklungsphase der Informationsgesellschaft ebnet, die häufig als das „Internet der Dinge" bezeichnet wird, und dass RFID-Etiketten einen Kernbestandteil von „intelligenten Umgebungen" ausmachen werden. Diese Umgebungen sind auch bedeutende Schritte in der Entwicklung der sogenannten „Überwachungsgesellschaft" ([4]). Daher können Rechtsetzungsmaßnahmen im RFID-Bereich angebracht sein. RFID kann qualitative Veränderungen bewirken.

([1]) Siehe vorgeschlagene Neufassung des Artikels 3 der Richtlinie 2002/58/EG.

([2]) Nummer 24 der Stellungnahme zu der Mitteilung über die Datenschutzrichtlinie.

([3]) In datenschutzrechtlicher Hinsicht erfordert dies die genaue Identifizierung des „für die Verarbeitung Verantwortlichen".

([4]) Diese Botschaft wurde in der am 2. November 2006 in London abgegebenen Erklärung der europäischen Datenschutzbehörden erneut aufgegriffen; die Erklärung kann auf der Website des EDSB abgerufen werden: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51

70. Vor diesem Hintergrund empfiehlt der EDSB die Annahme von Gemeinschaftsvorschriften (bzw. eines entsprechenden Vorschlags) in Betracht zu ziehen, in denen die Hauptaspekte der RFID-Verwendung in den einschlägigen Sektoren geregelt werden, falls es nicht gelingt, den bestehenden Rechtsrahmen ordnungsgemäß umzusetzen. Nach ihrem Inkrafttreten ist eine derartige Rechtsetzungsmaßnahme als *„lex specialis"* gegenüber dem allgemeinen Datenschutzrahmen anzusehen.

71. Der Erlass eines entsprechenden Rechtsaktes böte folgende Vorteile:

— der Rechtsetzungsakt könnte die wesentlichen Parameter für die Selbstregulierungsmechanismen vorgeben,

— die Aussicht auf die Annahme eines Rechtsetzungsakts wird sich möglicherweise als wirksamer Anreiz für die betroffenen Akteure erweisen, Selbstregulierungsmechanismen zu schaffen, die den erforderlichen Schutz bieten.

72. Im Hinblick auf eine größere Praxisnähe könnte die Kommission ersucht werden, ein Konsultationsdokument über das Für und Wider spezifischer Rechtsvorschriften und ihrer Hauptbestandteile auszuarbeiten. Selbstverständlich könnten die betroffenen Akteure aufgefordert werden, aktiv an dieser Konsultierung mitzuwirken. Desgleichen könnte auch die Artikel-29-Datenschutzgruppe herangezogen werden.

Mögliche Modalitäten

73. Der Gesetzgeber könnte für einen maßgeschneiderten rechtlichen Rahmen sorgen, bei dem eine Kombination von Regelungsinstrumenten den bestehenden Rechtsrahmen präzisiert und ergänzt. Dieser maßgeschneiderte Rechtsrahmen sollte auf den bekannten Grundsätzen des Datenschutzes beruhen und schwerpunktmäßig auf die Aufteilung der Zuständigkeiten und die Wirksamkeit der Kontrollmechanismen abstellen.

74. Ein spezieller Grund, aus dem derartige maßgeschneiderte Rechtsvorschriften erforderlich werden könnten, liegt darin, dass es nicht bei allen RFID-Anwendungen zwangsläufig zur Verarbeitung personenbezogener Daten kommt. Anders gesagt, wenn RFID-Anwendungen nicht zur Verarbeitung personenbezogener Daten führen, so sind die mit Herstellung und Verkauf von RFID-fähigen Produkten befassten Parteien rechtlich nicht verpflichtet, technische Maßnahmen anzuwenden, die das Abfangen von Daten oder die Einrichtung von Lesegeräten ohne ordnungsgemäße Unterrichtung der betroffenen Personen verhindern würden. Allerdings gehen nachweislich auch von solchen RFID-Anwendungen durch die mögliche Überwachung von Personen Gefahren für den Datenschutz aus, so dass auch die gleichen Datenschutzmechanismen erforderlich sind. Dies kann gerade bei der Etikettierung von Verbraucherprodukten vor dem Eintreffen am Verkaufsort der Fall sein. Insgesamt betrachtet, können RFID-Anwendungen, bei denen keine personenbezogenen Daten verarbeitet werden, immer noch eine Gefährdung der Privatsphäre des Einzelnen darstellen, wenn mit ihnen die heimliche Überwachung und die Verwendung der betreffenden Informationen für unzulässige Zwecke ermöglicht wird.

75. Nach Auffassung des EDSB sollten derartige unerwünschte Auswirkungen vermieden werden. Da sich mit den derzeitigen Rechtsvorschriften teilweise — zumindest hinsichtlich der RFID-Anwendungen, bei denen keine personenbezogenen Daten verarbeitet werden — dieser Gefährdung der Privatsphäre nicht begegnen lässt und überdies die Mängel des nicht zwingenden Rechts („soft law") zu berücksichtigen sind, erscheint es notwendig, verbindliche Rechtsvorschriften zu erlassen, um zu einem zufrieden stellenden Ergebnis zu gelangen.

76. Diese Rechtsvorschriften sollten in jedem Fall:

— die Anwendung des Grundsatzes der vorherigen Zustimmung („Opt-in-Prinzip") am Verkaufsort als eine ausdrückliche und bestreitbare Verpflichtung auch für die RFID-Anwendungen vorschreiben, die nicht in den Anwendungsbereich der Datenschutzrichtlinie fallen [1],

— dafür sorgen, dass RFID-Anwendungen obligatorisch mit den geeigneten technischen Vorkehrungen oder „eingebautem Datenschutz" ausgestattet werden.

VII. DER ORDNUNGSPOLITISCHE ASPEKT

77. Während die inhärente grenzüberschreitende Dimension der RFID-Systeme in der Mitteilung nur im Zusammenhang mit dem Binnenmarkt gesehen wird, vertritt der EDSB die Auffassung, dass dieser Dimension auf einer über den Binnenmarkt hinausreichenden Ebene Rechnung getragen werden muss. In einer Verkaufsstelle wirken RFID-Systeme bereits „grenzüberschreitend", da die Reichweite des Etiketts möglicherweise nicht am Verkaufsort endet. Auf der Ebene des globalen RFID-Systems werden diese Technologien auch „grenzüberschreitend", wenn die Übermittlung personenbezogener Daten an ein Drittland stattfindet, weil der Hersteller des etikettierten Artikels, der Teil des RFID-Systems ist, außerhalb der europäischen Union niedergelassen ist [2].

78. Von einer stärker zukunftsgerichteten Warte aus gesehen stellt auch die ordnungspolitische Behandlung der RFID-Referenzdatenbanken einen entscheidenden Aspekt im Hinblick auf eine angemessene Durchsetzung des europäischen Rechtsrahmens für den Datenschutz dar. Der EDSB verlangt nachdrücklich, dass hier eine Lösung gefunden wird, da eine weitere Erosion dieses Rahmens nicht hinnehmbar wäre.

79. Der EDSB schätzt die Frage des ordnungspolitischen Umgangs mit der RFID-Thematik als eine große Herausforderung ein, die beträchtliche Investitionen erfordern wird. Es müssen das richtige Verhandlungsforum und die am besten geeignete Regelungsinfrastruktur gefunden werden, damit gewährleistet ist, dass die Datenschutzrechte im internationalen Umfeld angemessen gewahrt werden.

---

[1] In Kapitel IV wurde vorgebracht, dass die Anwendung des Opt-in-Prinzips am Verkaufsort eine rechtliche Verpflichtung ist, die bereits aufgrund der Datenschutzrichtlinie besteht.

[2] Die Verpflichtungen, die bei der Übermittlung personenbezogener Daten eine Rolle spielen, sind in den Artikeln 25 und 26 der Datenschutzrichtlinie geregelt.

80. Daher ersucht der EDSB die Kommission, ihren Standpunkt zum ordnungspolitischen Aspekt — gegebenenfalls nach Rücksprache mit der RFID-Interessengruppe — darzulegen.

VIII. **FAZIT**

81. Der EDSB begrüßt die Mitteilung der Kommission über die Funkfrequenzkennzeichnung, da sie auf die wichtigsten Fragen im Zusammenhang mit dem Einsatz der RFID-Technologie eingeht, ohne dabei die entscheidenden Aspekte der Privatsphäre und des Datenschutzes außer Acht zu lassen. Er schließt sich der Auffassung an, dass RFID-Systeme bei der Entwicklungsphase der Informationsgesellschaft, die für gewöhnlich „Internet der Dinge" genannt wird, eine Schlüsselrolle spielen könnten.

Verdeutlichung der Auswirkungen

82. Der breite Einsatz der RFID-Technologie ist von Grund auf neuartig und kann sich in fundamentaler Weise auf unsere Gesellschaft und den Schutz der Grundrechte in dieser Gesellschaft, wie etwa des Rechts auf Privatsphäre und Datenschutz, auswirken. RFID kann qualitative Veränderungen bewirken.

83. Es lassen sich fünf grundlegende Aspekte der Privatsphäre und der Sicherheit unterscheiden:

— die Identifizierung der betroffenen Person,

— die Identifizierung des/der für die Verarbeitung Verantwortlichen,

— die gesunkene Bedeutung der traditionellen Unterscheidung zwischen Privatsphäre und öffentlichem Raum,

— die mit der Größe und den materiellen Eigenschaften der RFID-Etiketten verknüpften Auswirkungen,

— die mangelnde Transparenz bei der Verarbeitung.

Genaue Erfassung der Auswirkungen

84. Der allgemeine Rechtsrahmen für den Datenschutz nach Maßgabe der Richtlinie 95/46/EG gilt insoweit für die RFID-Technologie, als die von RFID-Systemen verarbeiteten Daten unter die Definition des Begriffs „personenbezogene Daten" fallen.

85. Was in Bezug auf die Datenschutzrichtlinie für elektronische Kommunikation betrifft, so enthält der Vorschlag der Kommission vom 13. November 2007 zur Änderung der Richtlinie eine Bestimmung, mit der präzisiert werden soll, dass die Richtlinie effektiv für bestimmte RFID-Anwendungen gilt. Einige andere RFID-Anwendungen fallen jedoch möglicherweise nicht unter die Richtlinie, weil diese auf die Verarbeitung personenbezogener Daten im Zusammenhang mit der Erbringung von öffentlich verfügbaren elektronischen Kommunikationsdiensten in öffentlichen Kommunikationsnetzen beschränkt ist.

86. Der Schutz personenbezogener Daten kann durch eine Reihe von Selbstregulierungsinstrumenten ergänzt werden. Es sollte Raum für eine derartige Selbstregulierung gelassen werden, sofern diese:

— konkrete und praktische Orientierungshilfe für die einzelnen Arten von RFID-Anwendungen bietet,

— auf spezifische Datenschutzfragen und -probleme, die im Zusammenhang mit generischen RFID-Anwendungen auftreten, eingeht,

— einen Beitrag zur einheitlichen und harmonisierten Anwendung der Datenschutzrichtlinie in der gesamten Union leistet,

— von allen einschlägigen Akteuren praktiziert wird.

87. Der EDSB empfiehlt, dass die Kommission in enger Abstimmung mit der RFID-Sachverständigengruppe ein oder mehrere Dokumente erstellt, in denen ein klare Orientierung in der Frage vermittelt wird, wie der bestehende rechtliche Rahmen auf den RFID-Bereich angewendet werden soll.

88. Die Leitlinien mit den für den RFID-Einsatz geltenden Grundsätzen sollten hinreichend zielgerichtet sein und einem sektorspezifischen Ansatz folgen. Sie sollten Vorschläge für praktikable und wirksame Methoden zur Entwicklung von Techniken und Normen enthalten, die dazu beitragen könnten, dass die RFID-Systeme dem Datenschutz-Rechtsrahmen entsprechen, und die zur Anwendung des Konzepts „privacy by design" („eingebauter Datenschutz") führen.

89. Der EDPS begrüßt den von der Kommission in ihrer Mitteilung vertretenen Ansatz, wonach die Ausarbeitung und Verabschiedung von Gestaltungskriterien befürwortet wird.

90. Auch wenn nach Auffassung des EDSB das „Opt-in-Prinzip" am Verkaufsort eine rechtliche Verpflichtung darstellt, die in den meisten Fällen bereits aufgrund der Datenschutzrichtlinie besteht, so sollte diese Verpflichtung dennoch in Selbstregulierungsinstrumenten festgeschrieben werden.

Sind spezielle Rechtsetzungsmaßnahmen erforderlich?

91. Der EDSB empfiehlt im Hinblick auf eine verbindliche Anwendung des Konzepts des „eingebauten Datenschutzes", dass die Kommission von dem Verfahren nach Artikel 3 Absatz 3 Buchstabe c der Richtlinie 1999/5/EG unter Heranziehung der RFID-Sachverständigengruppe Gebrauch macht.

92. Der EDSB empfiehlt, die Annahme von Gemeinschaftsvorschriften (bzw. eines entsprechenden Vorschlags) in Betracht zu ziehen, in denen die Hauptaspekte der RFID-Verwendung in den einschlägigen Sektoren geregelt werden, falls es nicht gelingt, den bestehenden Rechtsrahmen ordnungsgemäß umzusetzen. Nach ihrem Inkrafttreten ist eine derartige Rechtsetzungsmaßnahme als *„lex specialis"* gegenüber dem allgemeinen Datenschutzrahmen anzusehen. Diese Rechtsetzungsmaßnahme sollte auch den die Privatsphäre und den Datenschutz betreffenden Bedenken in Bezug auf bestimmte RFID-Anwendungen (etwa die Etikettierung von Artikeln vor dem Eintreffen am Verkaufsort), bei denen es nicht zwangsläufig zur Verarbeitung personenbezogener Daten kommt, Rechnung tragen.

93. Die Kommission sollte ein Konsultationsdokument über das Für und Wider spezifischer Rechtsvorschriften und ihrer Hauptbestandteile ausarbeiten.

94. Der Gesetzgeber könnte für einen maßgeschneiderten rechtlichen Rahmen sorgen, bei dem eine Kombination von Regelungsinstrumenten den bestehenden Rechtsrahmen präzisiert und ergänzt. Entsprechende Maßnahmen sollten in jedem Fall:

— die Anwendung des Grundsatzes der vorherigen Zustimmung („Opt-in-Prinzip") am Verkaufsort als eine ausdrückliche und unbestreitbare Verpflichtung auch für die RFID-Anwendungen vorschreiben, die nicht in den Anwendungsbereich der Datenschutzrichtlinie fallen ([1]),

— dafür sorgen, dass RFID-Anwendungen obligatorisch mit den geeigneten technischen Vorkehrungen oder „eingebautem Datenschutz" ausgestattet werden.

Der ordnungspolitische Aspekt

95. Der EDSB ersucht die Kommission, ihren Standpunkt zum ordnungspolitischen Aspekt — gegebenenfalls nach Rücksprache mit der RFID-Interessengruppe — darzulegen.

Geschehen zu Brüssel am 20. Dezember 2007.

Peter HUSTINX

Europäischer Datenschutzbeauftragter

([1]) In Kapitel IV wurde vorgebracht, dass die Anwendung des Opt-in-Prinzips am Verkaufsort eine rechtliche Verpflichtung ist, die bereits aufgrund der Datenschutzrichtlinie besteht.