Orientierungshilfe „Datenschutzgerechter Einsatz von RFID“

Herausgegeben vom
Arbeitskreis „Technische und organisatorische Datenschutzfragen“
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

(Stand: 14. Dezember 2006)

Autoren:

Dirk Bungard (Bund), Dr. Michael Glage (Sachsen-Anhalt), Gabriel Schulz (Mecklenburg-Vorpommern),
Axel Tönjes (Berlin), Rüdiger Wehrmann (Hessen), Dr. Sebastian Wirth (Hamburg)

Inhalt

1 Einleitung

Diese Orientierungshilfe soll Mechanismen und Technologien aufzeigen, die dazu beitragen können, Radio Frequency Identification (RFID) – Systeme möglichst datenschutzfreundlich zu gestalten. Dazu werden in diesem Dokument Anforderungen aus Sicht des Datenschutzes an die RFID-Technologie herausgearbeitet und unter technischen und juristischen Gesichtspunkten betrachtet.

Die Orientierungshilfe richtet sich in erster Linie an Anwender von RFID-Systemen. Sie sollen zu Datenschutzaspekten der RFID-Technologie sensibilisiert werden und erhalten mit diesem Dokument Empfehlungen zum datenschutzgerechten Einsatz dieser Systeme. Das Papier richtet sich aber auch an die Hersteller von RFID-Komponenten. Sie sollen motiviert werden, schon während der Entwicklung und der Produktion von RFID-Systemen datenschutzrechtliche Grundsätze zu beachten. Nicht zuletzt richtet sich die Orientierungshilfe an Kunden und Verbraucher. Sie können sich über die Datenschutz-Risken moderner RFID-Systeme informieren und erhalten somit die Möglichkeit, die Risiken für das Recht auf informationelle Selbstbestimmung durch RFID-Systeme in der Praxis besser einzuschätzen, um ihr Verhalten diesen Risiken anpassen zu können.

2 RFID als Schlüsseltechnologie

Die Allgegenwart von Rechnern ist keine ferne Zukunftsvision mehr. Bei der Entwicklung dieses sog. "Ubiquitous Computing" wird der RFID-Technologie eine Schlüsselrolle zugewiesen. Die Vorstellung des "Ubiquitous Computing" geht u. a. davon aus, dass menschliche Informationsverarbeitung und Kommunikation durch verselbständigte Informations- und Kommunikationsprozesse von Gegenstand zu Gegenstand ergänzt oder ersetzt werden. Als Anwendungsbeispiele seien hier genannt: Der Kühlschrank meldet die Lebensmittel, deren jeweiliges Verfallsdatum erreicht ist, oder bestellt gar eigenständig verbrauchte Gegenstände nach. Die Waschmaschine verständigt sich mit den zu waschenden Kleidungsstücken über die zulässige Höchsttemperatur des bevorstehenden Waschgangs und akzeptiert dabei möglicherweise nur das Waschmittel einer ganz bestimmten Marke. Bei der Warenverwaltung wird die Optimierung der Logistik in Aussicht gestellt. Es wird automatisch kontrolliert, ob während des Transports die Kühlkette bei kühlungsbedürftigen Lebensmitteln nirgends unterbrochen wurde. Auf Flughäfen melden verfügbare, aber irgendwo auf dem Areal abgestellte Gepäckwagen eigenständig ihre Standorte, um zu demjenigen Gepäckband gebracht zu werden, an dem sie benötigt werden. Militär, Museen, Bibliotheken, Krankenhäuser, Automobilhersteller, Handel, öffentlicher Personennahverkehr und sogar Schulen setzen die RFID-Technologie zu Informations- und Überwachungszwecken ein. Bei der Tierkennzeichnung, für die Zeitnahme bei Marathonläufen, in Reisepässen und auf Eintrittskarten für Großveranstaltungen finden RFID-Tags Verwendung. Selbst über die Integration in Euroscheine wird bereits diskutiert.

Unzweifelhaft gibt es Felder, auf denen der Einsatz von RFID mit Vorteilen verbunden ist, aber auch Felder, auf denen aus verschiedenen Gründen besser auf RFID verzichtet werden sollte. RFID birgt in vielen Fällen datenschutzrechtliche Risiken und Nebenwirkungen, die individuell und in ihren gesamtgesellschaftlichen Folgen nicht unterschätzt werden dürfen. Beispielsweise können Daten aus dem Speicher des RFID-Tags ausgelesen werden, ohne dass der Besitzer der Ware davon Kenntnis erlangt. Mit diesen Daten wäre es prinzipiell möglich, detaillierte Verhaltens-, Nutzungs- und Bewegungsprofile einzelner Personen (Kunden) ohne deren Wissen zu erstellen, wenn sie entsprechend gekennzeichnete Gegenstände erworben haben und mit sich führen. Immer dann, wenn die Kontrolle über die Gegenstände zu einer Überwachung der Menschen führen kann oder gar das primäre Ziel darstellt, ist Sensibilität für den Datenschutz, also für das Recht auf informationelle Selbstbestimmung gefragt.

3 Funktionsweise

RFID ist die Abkürzung für Radio Frequency Identification und steht für technische Verfahren, in denen durch Funkwellen eine kontaktlose Kommunikation zwischen RFID-Tag (auch als Transponder bezeichnet) und den dazugehörigen Lese- und/oder Schreibgeräten ermöglicht wird. RFID-Systeme gehören – wie die schon seit 1970 verbreiteten Barcode-Systeme – zu den so genannten Automatic Identification (Auto-ID)-Systemen [1] und dienen der automatischen Identifikation von Gegenständen.

Die überwiegende Mehrzahl der verwendeten RFID-Tags arbeitet nach dem Prinzip des so genannten Transponders (Transmitter und Responder). Diese RFID-Tags (passive Systeme) bestehen mindestens aus einem Speicherchip und einer Antenne, wobei es Chip und Antenne in verschiedenen Ausführungen und Bauformen gibt. Passive RFID-Tags beziehen ihre Energie aus den empfangenen Funkwellen der Lesegeräte. Auf dem RFID-Tag gespeicherte Daten können deshalb erst dann vom Lesegerät ausgelesen werden, wenn sich der Chip im Funkfeld des Lesegeräts befindet. Insofern ist der oft verwendete Begriff „Funk-Chip“ etwas irreführend, da passive RFID-Tags nicht selbständig Daten senden können.

Sind RFID-Tags mit einer eigenen Energiequelle ausgestattet, können sie die auf ihnen gespeicherten Daten selber aktiv funken. Diese aktiven Systeme werden in der Regel nur in anspruchsvollen, industriellen Anwendungen eingesetzt. Durch den aufwendigeren Aufbau sind aktive RFID-Tags wesentlich teurer und kommen daher für den Massenmarkt nicht in Frage.

Bauweise und Leistungsfähigkeit der RFID-Tags weisen jeweils eine große Variationsbreite auf. Die Bauformen können verschiedenen Einsatzzwecken angepasst werden [2]. Die unterschiedliche Beschaffenheit der RFID-Tags führt dazu, dass in praktisch jedem Einsatzszenario – selbst bei extremen Umwelteinflüssen – eine hohe Zuverlässigkeit gewährleistet werden kann. Die Entwicklungsfortschritte führen zu einer ständigen Miniaturisierung und steigenden Vielfalt der verwendbaren Materialien (z. B. flexible, in Kleidung nicht wahrnehmbar integrierbare Tags, sog. Smart Labels oder Smart Tags). Das kontaktlose Auslesen von Daten ist durch Stoff und Leder hindurch problemlos möglich [3]. Selbst RFID-Tags, die Menschen und Tieren implantiert werden, sind bereits im Einsatz.

Die Leistungsfähigkeit der RFID-Tags reicht von einfachen Speichermedien bis zu komplexen Systemen mit auf dem RFID-Tag integrierten Mikroprozessoren. Es gibt bereits RFID-Tags mit einer Speicher-Kapazität von 500 Kbyte und einem Prozessor, der für Datenverschlüsselungen ausreicht [4]. Die Übertragungsreichweite variiert zwischen wenigen Millimetern und zweistelligen Meterzahlen.

Um einzelne Gegenstände mit Hilfe von RFID-Tags zu identifizieren, müssen die Tags in RFID-Systeme eingebunden werden. Die zur Zeit verfügbaren Systeme bestehen in der Regel aus folgenden Komponenten:

- der RFID-Tag, der an das zu identifizierende Objekte angebracht wird und die zu übermittelnden Informationen enthält,
- die Schreibeinheit zum Schreiben von Daten auf den RFID-Tag und
- die Leseeinheit, welche die im RFID-Tag enthaltenen Informationen ausliest.

Charakteristisch für RFID-Systeme ist u. a. die Nicht-Erforderlichkeit eines Sichtkontaktes zwischen Tag und Lesegerät und das Potenzial, gleichzeitig mehrere Datenträger in einem Lesevorgang zu erfassen (Pulk-Erfassung). RFID-Lesegeräte sind je nach Frequenzbereich in der Lage, bis zu 200 RFID-Tags in der Sekunde auszulesen. Schreib- und Lesegerät sind in der Regel in einer Einheit zusammengefasst, die häufig mit einer zusätzlichen Schnittstelle ausgestattet wird, um die vom RFID-Tag empfangenen Daten an ein Hintergrundsystem (z. B. Datenbank, Automatensteuerung) weiterzuleiten [5].

Mittlerweile werden verschiedene Varianten von RFID-Systemen auf dem Markt angeboten. Um einen Überblick zu geben und die verschiedenen Systeme sinnvoll zu klassifizieren, bieten sich als Unterscheidungsmerkmale die Speicherkapazität, die Rechenleistung, die Form der Energieversorgung, die Reichweite, verwendete Frequenzen sowie Datenübertragungsverfahren an. Eine umfassende Darstellung ist u. a. der Studie des BSI [6] zu entnehmen. Darin werden auch weitere technische Schutzmaßnahmen aufgezeigt.

Schon jetzt ist aber die nächste Generation von RFID-Tags absehbar, die neben einem einfachen Speichermodul auch Sensorik und Aktuatorik enthalten. Denkbar sind beispielsweise Tags, die die Umgebungstemperatur messen und eigenständig die Kühlung ansteuern oder über GPRS oder GSM Meldungen absetzen [1]. Auch wurden bereits so genannte RFIDsecure-Chips vorgestellt, die über eine eingebaute Zugangskontrolle auf der Basis verschiedener Verschlüsselungsstufen verfügen. Der Chip kann somit in unterschiedlichen Nutzermodi arbeiten, die beispielsweise auf den Besitzer des Chips, den Anwender der verarbeiteten Daten oder die aufsetzende Anwendung gerichtet sind [7].

4 Charakteristische Datenschutz-Risiken von RFID

RFID-Tags tragen selbst in ihrer simpelsten Variante mindestens eine eindeutige Seriennummer. Wo immer sie eingesetzt werden, ob an/in Sachen, Tieren oder Menschen, bewirken sie damit eine weltweit einmalige und somit eindeutige Kennzeichnung des Trägermediums. Bei Handelsprodukten etwa geht es damit nicht mehr um ein Exemplar aus einer bestimmten Fertigungsserie von einem Fertigungsort innerhalb eines gewissen zeitlichen Fertigungsrahmens, sondern es geht speziell um das weltweit eindeutig identifizierbare Einzelprodukt, also beispielsweise genau um diese Flasche Mineralwasser und um keine andere.

Ein mit einem RFID versehenes Produkt (Brille, Armbanduhr usw.) kann einem bestimmten Menschen dauerhaft zugeordnet werden. Damit wird die technische Möglichkeit umfassender Profilbildungen über diesen Menschen eröffnet. Die mit RFID verbundenen Risiken für das Recht auf informationelle Selbstbestimmung sind maßgeblich dadurch bedingt, dass RFID-Tags an Gegenständen versteckt angebracht werden können, und dass sie ihre Kommunikation mit dem Lese-/Schreibgerät ohne Sichtkontakt, sondern lediglich per Funk und damit ohne Wissen und Wollen der Person, die den Gegenstand mit dem RFID-Tag bei sich hat, abwickeln können. Wenn der Käufer eines Produktes nichts über die Existenz des RFID-Tags weiß, kann er auch keine Schutzmaßnahmen ergreifen, um ein unbemerktes Auslesen zu verhindern. Das führt dazu, dass der weitere Umgang mit den erhobenen (personenbezogenen) Daten weitgehend intransparent ist. Zudem kann für (unberechtigte) Dritte die Möglichkeit bestehen, die Kommunikation abzuhören, also mitzulesen und personenbezogene Daten des RFID-Tags ohne Wissen des Nutzers zu speichern.

Bei dauerhafter Zuordnung eines (mit RFID versehenen) Gegenstandes zu einer Person (Brille, Armbanduhr) wäre ein globales Registrierungssystem denkbar, da der Gegenstand als Identifikationsmerkmal der Person dienen kann. Jedes Lesegerät weltweit könnte dann dieses Identifizierungsmerkmal (unbefugt) auslesen. Ebenso denkbar wäre die Erstellung von Bewegungs- und Konsumprofilen. So wären die (mit RFID versehenen) Handelswaren aus dem Kaufhaus A und aus der Apotheke B auch in der geschlossenen Einkaufstasche in Laden C komplett erkennbar. Würde etwa am Geldautomaten oder Bankschalter registriert, welche Geldscheine mit welchen RFID-Tags an welche Person ausgegeben worden sind, so würde dies zum Verlust der Anonymität bei der Zahlung mit Bargeld führen können.

Der Hauptgrund für die Anwendung von RFID ist, dass die weltweit eindeutige Kennung in den verschiedensten Anwendungszusammenhängen in jeweils unterschiedliche Hintergrundsysteme der Datenverarbeitung eingebettet werden kann. Datenschutzfragen müssen dabei nicht zwangsläufig relevant sein. Erinnert sei an die Gepäckwagen auf dem Flughafen – eine Anwendung, die ohne jedes personenbeziehbare Datum auskommt und damit in datenschutzrechtlicher Hinsicht unproblematisch ist. Datenschutzrechtlich relevant wird es immer dann, wenn personenbezogene Daten entweder im Hintergrundsystem verarbeitet werden, das mit der RFID-Anwendung verknüpft ist, oder wenn auf dem RFID-Tag selbst automatisierte Verarbeitungsprozesse personenbezogener Daten stattfinden. Solche Hintergrundsysteme mit Verarbeitung personenbezogener Daten sind beispielsweise Verleihsysteme (Bibliotheken, Autovermietungen usw.) und alle Arten der nicht-anonymen Bezahlweise (Kreditkarten, Kundenkarten, Bonusprogramme usw.).

5 Datenschutzrechtliche Rahmenbedingungen

5.1 Grundlagen

Bei der Anwendung der RFID-Technologie ist der Schutz der verfassungsrechtlich abgesicherten Persönlichkeitsrechte der Betroffenen, insbesondere das Grundrecht auf informationelle Selbstbestimmung, zu berücksichtigen. Werden daher Informationen mit Personenbezug verwendet, sind die datenschutzrechtlichen Rahmenbedingungen zu beachten.

Für die rechtliche Einordnung des Handelns maßgeblich ist zuerst, ob öffentliche oder nicht-öffentliche Stellen tätig werden und ob spezialgesetzlich geregelte Vorschriften oder die allgemeinen Datenschutzgesetze einschlägig sind. Für öffentliche Stellen im Bund wie in den Ländern kommen zunächst bereichspezifische Bestimmungen zur Anwendung, die gegebenenfalls vom allgemeinen Datenschutzrecht ergänzt werden. Für die öffentlichen Stellen des Bundes ist dies das Bundesdatenschutzgesetz (BDSG) und für die öffentlichen Stellen der Länder sind dies die jeweiligen Landesdatenschutzgesetze. Ein Beispiel: Sollen in einem Land alle gefährlichen Hunde mit RFID-Tags "verchipt" werden, um über das zugehörige Hintergrundsystem die jeweilige Halterin oder den jeweiligen Halter des Tieres auch in deren oder dessen Abwesenheit ermitteln zu können, bedarf es einer normenklaren spezialgesetzlichen Grundlage für die Verarbeitung der Daten der Halterinnen und Halter. Flankiert und ergänzt wird die Spezialregelung dann durch das allgemeine Landesdatenschutzrecht, das beispielsweise Bestimmungen über Auskunfts-, Berichtigungs- und Löschungsrechte enthält. Für nicht-öffentliche Stellen gilt ebenfalls der Vorrang bereichsspezifischer Regelungen, die durch das Bundesdatenschutzgesetz ergänzt werden.

Die nach dem Bundes- und nach den Landesdatenschutzgesetzen vorgesehenen Pflichten beim Umgang mit personenbeziehbaren Daten gelten auch für den Einsatz von RFID-Systemen. Zu nennen sind hier beispielsweise die Grundsätze von Datenvermeidung und Datensparsamkeit, Auskunfts-, Berichtigungs- und Löschungsrechte der Betroffenen, umfangreiche Informations- und Benachrichtigungspflichten, Klarheit über die Identität der verantwortlichen Stelle, über die Zweckbestimmung der Datenverarbeitung und gegebenenfalls über weitere Stellen. Sollen nicht nur im Hintergrundsystem, sondern auf dem RFID-Tag direkt Datenverarbeitungen stattfinden, kommen weitere Anforderungen hinzu (z. B. Durchführung einer Vorabkontrolle).

5.2 Personenbezogene Daten

Die datenschutzrechtlichen Schranken sind erst zu berücksichtigen, wenn das Persönlichkeitsrecht einer Einzelperson betroffen ist. Dies setzt die Verwendung personenbezogener Daten voraus. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Erfasst sind alle Informationen, die über Betroffene etwas aussagen.

Die Bestimmbarkeit einer Person ist schon dann möglich, wenn die Identifikation zwar nicht mit Hilfe der vorhandenen Daten allein vorgenommen werden kann, jedoch durch Hinzuziehen weiterer Informationen (Zusatzwissen) die Identität ermittelbar ist. Der Gesetzgeber hat bewusst auch die nur bestimmbaren Personen geschützt. Es ist daher nicht erforderlich, dass die Identifizierung gerade Zweck des Vorgehens sein muss, sondern es sind auch mögliche beiläufige Bestimmbarkeiten vom Schutzzweck des Gesetzes erfasst. Die Annahme der Be-

stimmbarkeit richtet sich nach dem technischen und intellektuellen Aufwand der Identifizierung.

In der nachfolgenden Tabelle wird die Personenbeziehbarkeit anhand unterschiedlicher Einsatzszenarien von RFID-Tags erläutert. Dabei ist zu beachten, dass nicht nur dann ein Personenbezug besteht, wenn im RFID-Tag selbst Personendaten gespeichert sind, sondern auch andere Daten einen Personenbezug ermöglichen.

Einsatz-Szenarium	**Personenbezug?**
1-Bit-Transponder	Kein Personenbezug
RFID-Tag nur mit eindeutiger Identifikations-Nummer (ID-Nr.)	Die Speicherung einer eindeutigen ID-Nr. auf einem RFID-Tag kann dafür genutzt werden, ein Bewegungsprofil einer Person zu erstellen. Anhand der ID-Nr. kann die Person an verschiedenen Orten wieder erkannt werden. Wird ein solcher RFID-Tag auf einen Gegenstand angebracht, den eine Person regelmäßig mit sich trägt, wie z.B. eine Brille, eine Armbanduhr oder einen Schlüsselanhänger, ergibt sich die Gefahr der Profilbildung. So können z. B. die Ankunftszeit, der Besuch unterschiedlicher Filialen, aber auch weitere Konsum- bzw. Nutzungsgewohnheiten zu dieser ID-Nr. erfasst werden. Derartige Informationen können sowohl von der "ausgebenden" Stelle aber auch von Dritten zur ID-Nr. gespeichert werden, wobei sich das Gefährdungspotential mit der Zahl der Institutionen erhöht, die ihre Daten abgleichen. Ein Profil zu dieser Person kann auch dann erstellt werden, wenn der Name der Person nicht bekannt ist. Bei der Verwendung einer eindeutigen Nummer kann sich also ein Personenbezug ergeben, so dass datenschutzrechtlichen Regelungen dann zu beachten sind.
RFID-Tag mit ID-Nr., die zur Zuordnung von personenbezogenen Daten eines Hintergrundsystems genutzt wird	Die verantwortliche Stelle, die die Daten des Hintergrundsystems nutzt, kann anhand der ID-Nr. die personenbezogenen Daten hieraus dem RFID-Tag zuordnen, da sie über das dafür erforderliche Zusatzwissen verfügt. Auch die ID-Nr. ist personenbeziehbar. Es besteht daher ein Personenbezug.
RFID-Tag mit weiteren gespeicherten "sprechenden" Daten wie z.B. ISBN (International Standard Book Number), EPC (Electronic Product Code) oder EAN (European Article Number)	Die auf dem Chip gespeicherte Information kann funkgestützt abgerufen und einer Person zugeordnet werden, auch ohne dass auf dem Chip oder in einem Hintergrundsystem weitere personenbezogene Daten gespeichert sind. Die Kennzeichnungen wie ISBN, EPC etc. sind nicht nur für die ausgebende Stelle interpretierbar, sondern haben auch für Dritte aufgrund der offen gelegten Definition Informationsgehalt. Mit Zusatzwissen kann diese Information einer konkreten Person zugeordnet werden. Ob dieses Zusatzwissen vorhanden ist, hängt von den jeweiligen Einsatzbedingungen ab. Trägt z. B. eine Person ein Medikament mit einer eindeutigen Medikamenten-Nr. bei sich, können ggf. Rückschlüsse auf deren Gesundheitszustand gezogen werden. Diese Information kann von allen Lesegeräten ausgelesen werden, in deren Reichweite die Person kommt. Bei definierten Zugängen zu Gebäuden oder Räumen, wie z. B. an der Empfangsschleuse beim Pförtner, könnte diese Information durch das Zusatzwissen der Pförtnerin oder des Pförtners über diese Person zugeordnet werden. Eine Mitwirkung des Betroffenen ist nicht erforderlich. Der Blick in die Taschen von Arbeitnehmern, Versicherungsnehmern, Patienten etc. wäre möglich.

	Damit besteht ein Personenbezug auch bei diesem Einsatzfeld.
Speicherung von weiteren personenbezogenen Daten auf dem RFID-Tag	Der Personenbezug ist offensichtlich

5.3 Datensparsamkeit, Datenvermeidung, Erforderlichkeit

Die Gestaltung und Auswahl von Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten hat sich nach § 3a BDSG oder den jeweiligen Regelungen der Landesdatenschutzgesetze an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verwenden. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen. Für die Nutzung der RFID-Technologie bedeutet dies, dass die verantwortliche Stelle immer erst Alternativen in Betracht ziehen muss, die das gleiche Ziel ohne die Verarbeitung personenbezogener Daten erreichen können.

Das Erheben, Verarbeiten und Nutzen personenbezogener Daten hat sich am Grundsatz der Erforderlichkeit zu orientieren. Bei öffentlichen Stellen heißt dies, dass die Daten für die Erfüllung der gesetzlichen Aufgabe unerlässlich sein müssen. Der Begriff der Erforderlichkeit ist dabei eng auszulegen. Erforderlich sind personenbezogene Daten nur dann, wenn die Aufgabe sonst nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllt werden kann. Der Grundsatz der Erforderlichkeit gilt auch in zeitlicher Hinsicht. Erforderlich sind die Daten erst dann und auch nur so lange, wie die Aufgabe aktuell zu erfüllen ist.

Im nicht-öffentlichen Bereich bemisst sich die Erforderlichkeit daran, ob die betreffenden Daten für die Erfüllung eigener Geschäftszwecke verwendet werden sollen, also für die Erfüllung eines Vertragsverhältnisses oder die Wahrung berechtigter Interessen der verarbeitenden Stelle erforderlich sind. Die Verwendung personenbezogener Daten steht jedoch immer unter dem Vorbehalt einer Interessenabwägung. Die berechtigten Interessen der verantwortlichen Stelle sind immer gegenüber den schutzwürdigen Interessen Betroffener abzuwägen.

5.4 Zweckbindung

Kann nach gründlicher Prüfung der Frage, ob das angestrebte Ziel nicht auch ohne die Verwendung personenbezogener Daten erreichbar ist, nicht auf personenbezogene oder –beziehbare Daten verzichtet werden, so ist zwingend ein hinreichend präziser Verwendungszweck zu bestimmen. Dies hat im öffentlichen Bereich in gesetzlicher Form zu erfolgen. Im nicht-öffentlichen Bereich sind die erlaubten Verwendungszwecke im BDSG normiert. Die Festlegung der Zweckbindung im Vorhinein soll die verfassungsrechtlichen Anforderungen an die Überschaubarkeit von Datenverarbeitungen für die davon betroffenen Menschen gewährleisten. Spätere Zweckänderungen sind zwar nicht generell ausgeschlossen, bedürfen aber spezieller rechtlicher Rechtfertigungen. Die Einhaltung von Zweckbindungen ist insbesondere durch technische und organisatorische Maßnahmen sicherzustellen.

5.5 Technische und organisatorische Maßnahmen

Werden personenbezogene Daten erhoben, verarbeitet oder genutzt, sind technische und organisatorische Maßnahmen zu treffen, die nach dem jeweils einschlägigen Gesetz erforderlich sind, um die Sicherheit der Datenverarbeitung im Interesse des Schutzes des Persönlichkeitsrechtes zu gewährleisten. Insbesondere wenn personenbezogene Daten automatisiert erhoben, verarbeitet oder genutzt werden, sind die Sicherheitsziele der Vertraulichkeit, der Integrität, der Verfügbarkeit, der Authentizität, der Revisionsfähigkeit und der Transparenz zu verwirklichen.

5.6 Zulässigkeit der Datenverarbeitung aufgrund rechtlicher Bestimmungen

Die Erhebung und Verarbeitung personenbezogener Daten sowie deren Nutzung im öffentlichen Bereich sind nur zulässig, wenn dies durch eine spezialgesetzliche Vorschrift oder durch das Bundes- oder das jeweilige Landesdatenschutzgesetz erlaubt ist. Im nicht-öffentlichen Bereich sind neben möglichen spezialgesetzlichen Regelungen die Bestimmungen des Bundesdatenschutzgesetzes zu berücksichtigen. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten in bestimmten Fällen zulässig.

So erlaubt § 28 Abs. 1 Nr. 1 BDSG die Erhebung und Verarbeitung personenbezogener Daten im Rahmen der Zweckbestimmung eines Vertragsverhältnisses. Sollen hingegen Daten zur Wahrung berechtigter Interessen der verantwortlichen Stelle erhoben oder verarbeitet werden, muss zunächst geprüft werden, ob schutzwürdige Interessen der Betroffenen überwiegen (§ 28 Abs. 1 Nr. 2 BDSG). Entscheidend für die Anwendbarkeit der hier genannten Rechtsvorschriften ist jedoch, ob und ggf. wann ein Personenbezug hergestellt wird. Dazu ist es nicht zwingend erforderlich, dass personenbezogene Daten auf dem RFID-Tag gespeichert werden. Der Personenbezug kann beispielsweise auch dann hergestellt werden, wenn auf dem Chip lediglich Produktdaten gespeichert sind, diese jedoch bei Kauf einer Ware mit den personenbezogenen Daten der Käuferinnen und Käufer verknüpft werden. Diese Möglichkeit besteht regelmäßig bei der Zahlung mit Kunden-, EC- oder Kreditkarten. Die Verknüpfung personenbezogener Daten von EC- oder Kreditkarten mit den Produktinformationen, die aus RFID-Tags beim Verkauf einer Ware ausgelesen werden, ist jedoch regelmäßig kein Bestandteil eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses (§ 28 Abs. 1 Nr. 1 BDSG). Das Bezahlen von Waren mit diesen Karten kann somit nicht als Einwilligung in die Verknüpfung von personenbezogenen Daten der Käuferinnen und Käufer mit aus den RFID-Tags ausgelesenen Daten der erworbenen Produkte gewertet werden.

5.7 Zulässigkeit der Datenverarbeitung aufgrund von Einwilligungen

Rechtsgrundlage für die Verarbeitung personenbezogener Daten kann auch eine Einwilligung der betroffenen Person sein. Dabei bedarf es einer "informierten Einwilligung“. Betroffene können grundsätzlich nur in diejenigen Umstände rechtswirksam einwilligen, von denen sie sich eine hinreichend bestimmte Vorstellung machen können. Demgemäß ist bei der Einholung der Einwilligung auf die Bedeutung der Einwilligung, den Zweck der Erhebung, die Verarbeitung und Nutzung sowie auf das Recht und die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf grundsätzlich der Schriftform, das äußere Er-

scheinungsbild der Erklärung ist hervorzuheben. Ein Widerruf ist jederzeit mit Wirkung für die Zukunft möglich.

Eine rechtswirksame Einwilligung setzt also insbesondere die Transparenz über den Einsatz von RFID-Tags und das damit zusammenhängende Gefährdungspotential voraus. Die Information der Betroffenen ist somit von zentraler Bedeutung. Die Nutzung von RFID-Tags mit Personenbezug auf der Basis eines vermeintlichen Einverständnisses, etwa durch den bloßen Kauf ohne eine gezielte, ausführliche Information, erfüllen nicht die datenschutzrechtlichen Anforderungen an eine informierte Einwilligung. Von einer Einwilligung kann nur dann ausgegangen werden, wenn die Betroffenen bei der Ausgabe z. B. von Kunden- oder Bonuskarten ausführlich über den Zweck der Datenverarbeitung und den weiteren Umgang mit den erhobenen Daten informiert werden. Hierzu gehört auch der Hinweis auf das Widerspruchsrecht.

Wirksame Einwilligungserklärungen setzen Freiwilligkeit bei den Erklärenden voraus. Ob diese Voraussetzung tatsächlich gegeben ist, muss immer geprüft werden. Dies ist gerade in den Bereichen zu beachten, in denen nicht in jedem Fall von einer Freiwilligkeit ausgegangen werden kann, wie beispielsweise bei Arbeitsverhältnissen. Im Verhältnis zwischen Staat und Bürgerinnen und Bürgern kann der Einsatz von RFID-Tags in einigen Ländern nur auf gesetzlicher Grundlage erfolgen – es sei denn, die gesetzliche Regelung selbst sieht eine Einwilligungslösung vor. Die jeweiligen Voraussetzungen sind anhand der datenschutzgesetzlichen Vorgaben zu überprüfen.

5.8 Mobile personenbezogene Speicher- und Verarbeitungsmedien

Nach § 3 Abs. 10 BDSG sind Datenträger dann mobile personenbezogene Speicher- und Verarbeitungsmedien, wenn funktional auf ihnen über die Speicherung hinaus durch die ausgebende oder eine andere Stelle Daten automatisiert verarbeitet werden können. In den Landesdatenschutzgesetzen ist dieser Begriff teilweise unterschiedlich festgelegt. Für Datenträger, die unter diesen Begriff fallen, sind die Regelungen zu mobilen personenbezogenen Speicher- und Verarbeitungsmedien des § 6c BDSG oder die entsprechenden Regelungen der Landesdatenschutzgesetze anzuwenden, wenn automatisierte Verfahren ganz oder teilweise auf den (in einzelnen Landesdatenschutzgesetzen auch "durch die") mobilen Medien ablaufen. Stellen, die ein solches Verfahren einsetzen, müssen die Betroffenen über die gesetzlich vorgegebenen Aspekte informieren. Hierzu gehören die Informationspflicht über die Identität der handelnden Stelle, die Beschreibung der Funktionsweise des Datenträgers einschließlich der Art der zu verarbeitenden personenbezogenen Daten in allgemeinverständlicher Form, der Hinweis auf die Rechte der Betroffenen (Auskunft, Berichtigung, Löschung und Sperrung) sowie die Information über die bei Verlust oder Zerstörung des Datenträgers zu treffenden Maßnahmen. Der jeweils datenschutzrechtlich relevante Vorgang des Erhebens, Verarbeitens oder Nutzens muss für die Betroffenen erkennbar sein. Es gilt das Transparenzgebot. Sind die Vorschriften des § 6c BDSG anwendbar, müssen beispielsweise auch Kommunikationsvorgänge, die auf dem RFID-Tag eine Datenverarbeitung auslösen, für die Betroffenen eindeutig erkennbar sein. Das unbemerkte Auslesen der Daten - etwa beim Vorbeigehen an einem versteckten Lesegerät - ist nicht zulässig. RFID-Tags fallen unter die obigen Regelungen, wenn sie mit einem integrierten Prozessor ausgestattet sind. Dies gilt unabhängig davon, ob die personenbezogenen Daten auf dem RFID-Tag gespeichert sind oder der Personenbezug erst über Hintergrundsysteme hergestellt werden kann. Aber auch bei RFID-Tags die lediglich EEPROMs (Electrically Erasable Programmable Read-Only Memory) enthalten, ist die Voraussetzung für die Anwendbarkeit der Vorschriften bezüglich der mobilen personenbezogenen Speicher-

medien gegeben, da jeweils Ergebnisse aktueller Verarbeitungen auf diese Chips geschrieben werden können [8].

In einigen Ländern dürfen öffentliche Stellen derartige Verfahren nur einsetzen, wenn dies durch eine Rechtsvorschrift vorgesehen ist. Die Regelungen zu mobilen personenbezogenen Datenträgern einzelner Datenschutzgesetze der Länder sind zu berücksichtigen.

6 Handlungsempfehlungen

6.1 Für Anwender von RFID-Systemen

Datenschutzpolitisch sollten sich Stellen, die mit RFID arbeiten wollen und dabei auf die Personenbeziehbarkeit nicht verzichten können, mindestens an den folgenden, nicht in jedem Einzelfall abschließenden 11-Punkte-Katalog halten:

1. Vor dem Einsatz von RFID-Systemen mit Personenbezug ist zu prüfen, ob das angestrebte Ziel auch ohne Verarbeitung personenbezogener Daten erreicht werden kann. Es ist zu überlegen, ob es ganz andere Möglichkeiten gibt, das Ziel zu erreichen.
2. Eine Technikfolgenabschätzung bzw. Vorabkontrolle ist durchzuführen, um die Risiken für die Rechte der Betroffenen bewerten zu können.
3. Der Zweck der Verarbeitung personenbezogener Daten ist eindeutig festzulegen. Spätere Änderungen oder Erweiterungen sind nicht zulässig.
4. Die Grundsätze der Datensparsamkeit und der Erforderlichkeit sind zu berücksichtigen. Die Menge personenbezogener Daten muss demnach so gering wie möglich sein. Das zulässige Ausmaß der Verarbeitung hat sich auf den unabdingbar nötigen Umfang zu beschränken.
5. Personenbezogene Daten dürfen nur so lange gespeichert werden, wie sie zur Zweckerreichung erforderlich sind.
6. In einem Sicherheitskonzept sind angemessene technische und organisatorische Maßnahmen für das gesamte RFID-System (also auch für das Hintergrundsystem) festzulegen. Dabei sind Datensicherheitsaspekte wie sichere Verschlüsselung der Daten, wirksame Authentisierung der beteiligten Geräte und eine Systemgestaltung, die keine unbemerkte oder ungewollte Profilerstellung ermöglicht, zu berücksichtigen.
7. Die betroffenen Personen sind umfassend zu informieren über z. B. den Einsatz und die Funktionsweise des Systems, die Art der zu verarbeitenden Daten, den Verarbeitungszweck, ihre Rechte auf Auskunft, Berichtigung und Löschung der Daten zur eigenen Person usw.
8. Mit RFID-Tags versehene Produkte sowie zum System gehörende Lesegeräte sind zu kennzeichnen.
9. Den betroffenen Personen ist die Wahrnehmung ihrer Rechte zu gewährleisten.
10. Den betroffenen Personen ist der einzelne Verarbeitungsvorgang transparent zu machen, z. B. durch die eindeutige Erkennbarkeit von Kommunikationsvorgängen, die eine Verarbeitung personenbezogener oder -beziehbarer Daten auslösen (optisches/ akustisches Signal).
11. Den betroffenen Personen sind Möglichkeiten zur Blockierung, Deaktivierung, Löschung oder Entfernung von RFID-Tags zur Verfügung zu stellen; es darf keinen faktischen Nutzungszwang geben. Im Handel z. B. müssen anonyme Kaufmöglichkeiten erhalten bleiben, ohne dass Nachteile in Kauf genommen werden müssten.

6.2 Für Kunden als Betroffene von RFID-Systemen

Auch dem Betroffenen (Kunde, Verbraucher) können Möglichkeiten eingeräumt werden, das Missbrauchspotential der RFID-Technologie selbst zu minimieren. Dazu müssten den Betroffenen Mechanismen an die Hand gegeben werden, mit denen sie die Kommunikation zwischen dem RFID-Tag und den Lese-/Schreibgeräten ab einem bestimmten Zeitpunkt selbst

unterbinden können. Derartige Mechanismen bergen jedoch die Gefahr in sich, dass die Verantwortung für den Schutz der Privatsphäre der Kunden von den Herstellern und dem Handel auf die Schultern der Konsumenten verlagert wird [9].
Wenn die Möglichkeit besteht, die Kommunikation zwischen RFID-Tag und Lesegeräten zu beeinflussen oder wenn Tags entfernt oder wirksam und endgültig gelöscht bzw. deaktiviert werden, muss sichergestellt werden, dass der Kunde keine Benachteiligungen zu erwarten hat. Beispielsweise wäre es unzulässig, dass Händler Garantieleistungen, besondere Rabatte oder den Umtausch von Waren ausschließlich an die Bedingung knüpfen, dass an dem betreffenden Produkt ein funktionstüchtiger RFID-Tag auch nach dem Kauf verbleibt. Solche Fälle sind durch gesetzliche Regelungen auszuschließen. Möglichkeiten zur unkomplizierten Deaktivierung in Form von Terminals oder ähnlichem müssen deutlich sichtbar und in ausreichender Zahl in den Verkaufsräumen vorhanden sein, denn die Deaktivierungsmöglichkeit der Transponder ist eine Mindestanforderung, die der Einzelhandel erfüllen muss, um dem Datenschutz gerecht zu werden.

6.2.1 Blocker-Tags

Blocker-Tags bewirken eine derartige Überlastung der Lesegeräte, dass eine Identifikation des richtigen Signals nicht möglich ist [10]. Das Blocker-Tag simuliert gegenüber dem Lesegerät eine so große Zahl adressierbarer RFID-Tags, die sich unmöglich alle nacheinander abfragen lassen. Eine Kommunikation mit den "echten" Tags im Lesebereich kommt mit hoher Wahrscheinlichkeit nicht zustande, da das Lesegerät eine sehr große Anzahl von vergeblichen Tag-Anforderungen abarbeiten muss.
Bislang sind solche Geräte in Europa jedoch noch nicht erfolgreich getestet, da sie nur ein bestimmtes Kommunikationsprotokoll wirksam stören können. Allerdings darf die Verfügbarkeit solcher Geräte nicht dazu führen, dass es zu einem "Zwei-Klassen"-Datenschutz kommt. Die wirksame Durchsetzung des Rechts auf informationelle Selbstbestimmung darf nicht davon abhängen, ob der Verbraucher ein solches Blocker-Tag besitzt.

6.2.2 Clipped-Tags

Der Käufer eines mit RFID-Tag versehenen Produkts kann die Kommunikation prinzipiell auch dadurch einschränken oder ganz unterbrechen, indem er die Antenne vom den RFID-Tags abtrennt (Clipped-Tags). Das Auslesen auf Distanz ist dann praktisch nicht mehr möglich. Die nachfolgend beschriebenen Verfahren befinden sich allerdings erst im Versuchsstadium.

Für die Realisierung von Clipped-Tags gibt es verschiedene Ansätze. So könnte der Sender einfach wie bei einem Rubbel-Los mit dem Fingernagel abgekratzt werden. Auch eine Lösung, bei der die Antenne an einem perforierten Stück untergebracht ist, das der Nutzer mit der Hand abreißen kann, ist denkbar. Zudem erwägen die Forscher die Unterbringung in einem Material-Sandwich. Löst man einen Aufkleber, so wird dadurch auch gleichzeitig der Sender entfernt [11].

Voraussetzung für die Nutzung von Clipped-Tags ist eine entsprechende Information an Kunden, dass das Produkt mit einem solchen RFID-Tag ausgestattet ist. Bei Transpondern, die zur Produktkennzeichnung eingesetzt werden und keine weiteren personenbezogenen Daten enthalten, wäre eine gesetzlich verankerte Hinweispflicht bei der Verwendung zu fordern, um Transparenz zu gewährleisten. Der Verbraucher muss das Recht haben zu erfahren, wann und

wo RFID-Tags genutzt und ausgelesen werden. Dazu sollten die entsprechenden Produkte so markiert werden, dass eindeutig und leicht zu erkennen ist, dass sie mit einem Transponder versehen sind.

7 Kontrollfragen zum Datenschutz

Im Abschnitt 8 werden einige Nutzungsszenarien für die RFID-Technologie beschrieben. Die folgenden Fragen sollen helfen, die Datenschutzfreundlichkeit der einzelnen Einsatzszenarien, in denen personenbezogene Daten verarbeitet werden, zu beurteilen.

- *Wann und wie kommt es zum Personenbezug?*
  Der Personenbezug kann sofort beim Kauf eines Produktes der Komponente oder erst später bei der Verarbeitung von Daten in Hintergrundsystemen erfolgen. Er kann durch Speicherung personenbezogener Daten auf den RFID-Tags selbst oder durch Verknüpfung von Kundendaten mit Produktdaten in Hintergrundsystemen entstehen.
- *Auf welcher Rechtsgrundlage sollen die Daten verarbeitet werden?*
  Es müssen sowohl die Rechtsgrundlagen für die Verarbeitung personenbezogener Daten auf den RFID-Tags selbst als auch die für die Verarbeitung in den weiteren Komponenten des RFID-Systems (Schreib-/Lesegeräte, Hintergrundsysteme) benannt werden.
- *Ist der Datenvermeidungs- / Erforderlichkeitsgrundsatz erfüllt?*
  Es muss nachgewiesen werden, dass vor dem Einsatz eines RFID-Systems geprüft wurde, dass die zu erhebenden und zu verarbeitenden Daten für die jeweilige Aufgabe erforderlich sind. Darüber hinaus muss sichergestellt werden, dass so wenig personenbezogene Daten wie möglich verarbeitet werden und dass nicht mehr benötigte, personenbezogene Daten gelöscht werden. Die Entscheidung kann / sollte der Betroffene treffen.
- *Wer kann wie auf welche Daten zugreifen?*
  Die Zugriffsrechte müssen detailliert dokumentiert sein.
- *Wie wird ein unbefugter Zugriff auf Daten verhindert?*
  In einem Datenschutz- und Sicherheitskonzept müssen alle technischen und organisatorischen Maßnahmen dokumentiert sein, die sicherstellen, dass nur Berechtigte auf personenbezogene Daten zugreifen können. Das Konzept muss vor Inbetriebnahme des RFID-Systems vollständig umgesetzt sein.
- *Sind die Sicherheitsmaßnahmen geeignet und angemessen, um unbefugte Zugriffe zu verhindern?*
- In einer Risikoanalyse muss die Geeignetheit und Angemessenheit der getroffenen Maßnahmen nachgewiesen werden. In diesem Zusammenhang muss immer eine Abwägung erfolgen, welche Konsequenzen für den Betroffenen eintreten können.
- *Ist die Anwendung für den Betroffenen transparent?*
  Die Betroffenen müssen die Möglichkeit haben, sich vollständig über alle Umstände der Verarbeitung ihrer personenbezogenen Daten zu informieren.
- *Wie kann der Betroffene seine Auskunftsrechte geltend machen?*
  Es sind technische Maßnahmen zu realisieren, die dem Betroffenen die Einsicht der auf den RFID-Tags oder der in einer Hintergrund-Datenbank gespeicherten Daten ermöglicht.
- *Sind Kommunikationsvorgänge, die auf einem RFID-Tag eine Verarbeitung personenbezogener Daten auslösen, für den Betroffenen eindeutig erkennbar?*
  Die Betreiber von RFID-Systemen müssen in diesem Fall die Anforderungen des § 6c BDSG vollständig umgesetzt haben.

- *Ist die Möglichkeit zur Löschung/Deaktivierung von RFID-Tags im jeweiligen Geschäft gegeben?*
  Es muss sichergestellt sein, dass zum frühestmöglichen Zeitpunkt die Daten auf dem RFID-Tag gelöscht bzw. der RFID-Tag deaktiviert werden kann. Auf diese Weise sollen die Prinzipien der Erforderlichkeit und der Datensparsamkeit umgesetzt werden.

8 RFID-Szenarien

8.1 Öffentlicher Personennahverkehr

8.1.1 Post-Paid-Systeme

Die Verkehrsverbünde des öffentlichen Personennahverkehrs (ÖPNV) wollen den Erwerb und das Bezahlen von Fahrkarten vereinfachen, indem mit Hilfe von Chipkarten bargeldlos bezahlt wird. Über Schreib-/Lesegeräte in den Verkehrsmitteln oder an den Bahnhöfen bzw. Haltestellen wird die Verbindung zwischen Chipkarte und Hintergrundsystem hergestellt. Mit Hilfe der Daten über das Aus- und Einsteigen werden die Entgelte berechnet und zum Monatsende vom Konto des Fahrgastes abgebucht (Post-Paid-Karten). Da der Ein- und Ausstieg aber möglichst nicht länger dauern soll als bisher, wird oftmals eine kontaktlose Lösung mit RFID-Technik vorgesehen.

Bei der Ausgabe der Chipkarte werden Daten des Besitzers (Name, Adresse, Kontoverbindung) durch das kartenausgebende Unternehmen erhoben und gespeichert. Wenn der Kunde seine Karte erhält, wird zusätzlich gespeichert, welche Karte ihm gehört. Die Zuordnung von Karte und Fahrgast erfolgt über die eindeutige Kartennummer. Damit sind die auf der Chipkarte gespeicherten Daten personenbezogen und das Datenschutzrecht ist anwendbar.

Die Teilnahme an diesem Zahlverfahren erfolgt auf freiwilliger Basis. Bei Vertragsabschluss wird der Kunde informiert, welche Daten über ihn gespeichert werden. Dazu gehören auch Informationen, wo und wie lange welche Daten - zum Beispiel die Daten seiner Fahrten - gespeichert werden. In diese Speicherungen muss er einwilligen, um am Verfahren teilnehmen zu können.

Die Fahrtdaten können nur von zugelassenen Schreib-/Lesegeräten generiert werden. Kontrolleure haben nur lesenden Zugriff und müssen ein zugelassenes Lesegerät benutzen. Um unbefugte Zugriffe auf die Karten zu verhindern, identifizieren und authentifizieren sich die beteiligten technischen Komponenten gegenseitig durch kryptografische Verfahren (Challenge-Response-Verfahren). Das Lesegerät erkennt somit, ob es sich um eine zugelassene Karte handelt, und die Karte kommuniziert nur mit Lesegeräten, die zum System gehören. Darüber hinaus werden die Daten verschlüsselt übertragen. Mit den beschriebenen Maßnahmen ist eine unbefugte Kenntnisnahme der Daten weitgehend ausgeschlossen.

Die Anwendung ist für den Kunden transparent, weil ihm die Abläufe verständlich beschrieben wurden und er Kommunikationsvorgänge zwischen der Chipkarte und Schreib-/Lesegeräten feststellen kann. Transparenz wird auch dadurch erzeugt, indem die zugelassenen Lesegeräte ein optisches und akustisches Signal erzeugen. Der Kunde bemerkt also, wenn seine Karte gelesen wird.

Seine Auskunftsrechte kann er beispielsweise dadurch wahrnehmen, indem er die auf der Chipkarte gespeicherten Daten mit Lesegeräten in den Geschäftsstellen lesen und sich auf einem Bildschirm anzeigen lassen kann.

8.1.2 Pre-Paid-Systeme

Bei Pre-Paid-Systemen wird das Entgelt für eine Fahrt sofort von einer auf der Chipkarte befindlichen elektronischen Geldbörse abgebucht. Bei der Ausgabe dieser Karten werden keine Personalien des Besitzers benötigt. Der Kunde kann somit die Verkehrsmittel ohne Angabe des Namens und seiner Kontendaten nutzen. Diese auch als White-Card bezeichneten Chipkarten werden in der Regel gegen einen Pfandbetrag oder ein Serviceentgeld ausgegeben.

Bei der Nutzung einer solchen Pre-Paid-Card können dennoch personenbezogene Daten anfallen. Da diese Karten eine eindeutige Kartennummer haben, besteht die Möglichkeit zur „Verfolgung“ einzelner Karten. Durch Auswertung mehrerer Zahlvorgänge einer Karte (Verkettung) und durch Zusammenführen mit weiteren Informationen kann prinzipiell ein Personenbezug hergestellt werden (Tracking). Ist zudem der aktuelle Betrag einer Pre-Paid-Card auf dem RFID-Tag unzureichend gegen unbefugtes Auslesen geschützt, kann selbst diese Information einer Person zugeordnet oder auch verändert werden.

Da auch bei Pre-Paid-Cards ein Personenbezug nicht auszuschließen ist, sind die Datenschutzgesetze anzuwenden und geeignete technische und organisatorische Maßnahmen zu treffen.

Die Pre-Paid-Card ist aus Datenschutzsicht insgesamt positiv zu bewerten, sofern der Personenbezug soweit erschwert wird, dass dieser nur unter technisch-organisatorisch sehr hohem Aufwand hergestellt werden kann bzw. unmöglich wird.

8.2 Diebstahlsicherung

8.2.1 Einzelhandel

Weit verbreitet ist die Verwendung von RFID-Tags als Diebstahlsicherung in Geschäften und Kaufhäusern. Sie sind entweder in Etiketten oder vor allem bei Bekleidung in ca. 3 bis 5 cm große Hartplastikscheiben oder -riegel integriert und enthalten einen 1-bit-Transponder, der lediglich eine ja/nein-Information im Sinne von bezahlt/nicht bezahlt speichern kann. Beim Bezahlen wird die Diebstahlsicherung entfernt oder durch Anlegen eines starken Magnetfeldes deaktiviert. Sollte ein Kunde mit einem noch nicht deaktivierten Transponder das Geschäft verlassen wollen, geben Lesegeräte im Ausgangsbereich akustischen oder optischen Alarm, der in der Regel eine Prüfung des Vorfalls nach sich zieht. In diesem Zusammenhang ist nicht auszuschließen, dass die Identität des entsprechenden Kunden festgestellt wird. Bei einem ordnungsgemäß abgewickelten Kauf ist ein Personenbezug jedoch nicht herstellbar, so dass derartige RFID-Tags datenschutzrechtlich unbedenklich sind.

8.2.2 Kraftfahrzeuge

Bei Kraftfahrzeugen hat sich mittlerweile zur Realisierung eines wirkungsvollen Diebstahlschutzes die Wegfahrsperre auf Basis von RFID-Systemen durchgesetzt. Der Transponder

befindet sich dabei im Autoschlüssel, das Lesegerät ist in der Nähe des Zündschlosses platziert. Manche Schließsysteme kommen heute bereits ohne Zündschlüssel, also nur mit einem RFID-Tag aus. Das Fälschen eines elektronischen RFID-Schlosses wird durch kryptographische Verfahren zur Authentifizierung zwischen RFID-Tag und Fahrzeug verhindert. Auch hier werden keine personenbezogenen Daten verarbeitet, so dass diese Anwendungen keine Datenschutzrelevanz haben.

8.3 Bibliotheken

Um den personalintensiven Ausleihprozess zu rationalisieren, werden so genannte Selbstverbuchungsstationen eingesetzt, an denen die Nutzer entliehene oder zurückzugebende Medien selbst registrieren. Wird jedes Medium mit einem RFID-Tag versehen, muss es nicht einzeln an einem Lesegerät vorbeigeführt werden, so dass der Verbuchungsprozess erheblich beschleunigt wird. Gleichzeitig kann am Ausgang überprüft werden, ob alle mitgeführten Medien bereits verbucht sind. Insofern kann das Verfahren gleichzeitig zur Diebstahlssicherung genutzt werden.

Für den Verbuchungsprozess ist es erforderlich, dass die eindeutige Kennzeichnung eines Mediums dem Ausleiher zugeordnet wird. Da der Ausleiher mit Namen und Anschrift bekannt ist, werden personenbezogene Daten verarbeitet. Die Einwilligung im Rahmen der Beantragung eines Benutzerausweises bildet die Rechtsgrundlage für die Verarbeitung. Allerdings müssen die Datenverarbeitungsprozesse und insbesondere auch die auf dem RFID-Tag gespeicherten Daten und deren Nutzung dem Nutzer transparent erläutert werden.

Um das Prinzip der Datensparsamkeit umzusetzen, sollte ausschließlich die eindeutige Kennung des jeweiligen Mediums oder die ID-Nr. des RFID-Tags im Verbuchungsprozess verarbeitet werden. Auf die Speicherung zusätzlicher Angaben wie Buchtitel, Katalognummer des Mediums, die ISBN-Nummer oder den EPC (Electronic Product Code) sollte verzichtet werden, um Rückschlüsse auf den Benutzer zu vermeiden. Bei einer Nutzung einer nichtsprechenden Nummer wären dann auch kein starker Zugriffsschutz gegen ein unautorisiertes Auslesen der RFID-Tags erforderlich. Weitere personenbezogene Daten, insbesondere der Name oder die Benutzer-Nummer des aktuellen Ausleihers, Angaben zur Ausleihhistorie oder der Buchtitel in Klarschrift, sollten aus Gründen der Datensparsamkeit nicht auf dem RFID-Tag gespeichert werden, da die Zuordnung über das Hintergrundsystem erfolgt.

Um auch dann einen reibungslosen Verbuchungsablauf zu gewährleisten, wenn das Hintergrundsystem nicht zur Verfügung steht bzw. um die Medienannahme zu beschleunigen, können ggf. weitere Datenfelder erforderlich sein, wie z. B. die Bibliotheksangabe oder die Angabe, ob es sich um ein mehrteiliges Medium handelt. Da das Verfahren in der Regel auch gleichzeitig zum Diebstahlschutz genutzt werden soll, kann hierfür ebenfalls ein Datenfeld erforderlich sein. Wenn neben der ID-Nr. des Chips weitere Daten gespeichert werden können, sollten diese gegen unautorisierten Zugriff geschützt werden.

Transparenz für die Nutzer kann beispielsweise realisiert werden, indem die Lese-Prozesse, mit denen die RFID-Tags ausgelesen werden, für den Nutzer klar erkennbar sind. Die Lese-Stationen sollten daher entsprechend deutlich gekennzeichnet sein. Ein verdecktes Auslesen z. B. innerhalb der Bibliothek mit dem Ziel, das Nutzungsverhalten näher zu studieren, muss ausgeschlossen werden. Über die Anwendung der RFID-Tags müssen die Bibliotheksnutzer ausführlich informiert werden und entsprechende Erläuterungen sollten auch in die Nutzerordnung aufgenommen werden.

8.4 Zutrittskontrollsysteme

8.4.1 Arbeitsplatz

Ein weiteres Einsatzgebiet der RFID-Technologie sind Zutrittskontrollsysteme. Bei ausreichender Reichweite der RFID-Tags ist das Passieren einer mit einem Lesegerät gesicherten Tür möglich, ohne dass der RFID-Tag aus der Tasche geholt werden muss. Oft wird dieser gleichzeitig auch zur Zeiterfassung benutzt, die dadurch weitgehend automatisiert werden kann.

In der Regel werden bei solchen Systemen personenbezogene Daten wie z. B. Personalnummer, der Name und die jeweiligen Berechtigungen gespeichert. Die Daten auf der Karte und im Hintergrundsystem werden über ein eindeutiges Merkmal verbunden, etwa die Karten-ID. Es handelt sich bei solchen RFID-Anwendungen um eine Verarbeitung personenbezogener Daten.
Häufig werden solche Zugangskontrollsysteme ggf. in Verbindung mit einer Zeiterfassung oder weiteren Anwendungsmöglichkeiten im Rahmen von Beschäftigungsverhältnissen eingesetzt. In solchen Zusammenhängen kommt eine Einwilligung meist nicht in Betracht, da die Freiwilligkeit insbesondere dann nicht gegeben ist, wenn den Beschäftigten keine alternativen Methoden etwa eine Karte mit Magnetstreifen angeboten wird. Rechtsgrundlagen für diese Anwendungen sind Dienstvereinbarungen, da diese Zugangskontrollsysteme nach den §§ 87 Abs. 1 Nr. 6 BetrVG, 75 Abs. 3 Nr. 17 und 76 Abs. 2 Nr. 7 BPersVG (bzw. den entsprechenden Vorschriften der Landespersonalvertretungsgesetze) mitbestimmungspflichtig sind.

Da RFID-Tags möglicherweise auch ohne Mitwirkung der Betroffenen ausgelesen werden können, besteht die Gefahr, dass die Daten zu einer verdeckten Leistungs- oder Verhaltenskontrolle missbraucht werden. Daher sollte zunächst geprüft werden, ob die angestrebten Ziele der RFID-Anwendung auch mit einer anderen Technologie erreicht werden können, die ein geringeres Gefährdungspotenzial aufweist. Wenn der RFID-Einsatz erforderlich ist, sind geeignete technische und organisatorische Maßnahmen zu treffen, die das Missbrauchspotential verringern. Eine der zu treffenden Maßnahmen könnte z. B. sein, dass der Betroffene die Karte vor dem Auslesen aus einer Hülle nehmen muss, die ein Auslesen verhindert. Dadurch wird die Mitwirkung erforderlich und ein verdecktes Auslesen der Karte weitgehend verhindert.

8.4.2 Großveranstaltungen

In ihrer Antwort auf eine Kleine Anfrage der Fraktion Bündnis 90/Die Grünen hat die Bundesregierung erklärt, dass RFID-Tags für den Masseneinsatz auf Großveranstaltungen geeignet seien [12]. Nach dem Einsatz von RFID-Tags in Eintrittskarten zur FIFA-WM 2006 ist daher zu erwarten, dass künftig auch Eintrittskarten weiterer Großveranstaltungen mit RFID-Tags versehen werden, auf denen personenbezogene Daten gespeichert werden.

Die Ausstattung der WM-Tickets mit RFID-Tags sollte unter anderem Ticketfälschungen erschweren und sicherstellen, dass nur Personen, die ihr Ticket offiziell erworben haben, in die WM-Stadien gelangen. Dazu wurden schon bei der Online-Ticketbestellung umfangreiche personenbezogene Daten erhoben, und in Hintergrundsystemen der WM-Stadien für spätere Kontrollzwecke gespeichert. Einige der bei der Ticketbestellung erhobenen personenbezogenen Daten, wie Name, Geburtsdatum, Pass- oder Personalausweisnummer wurden auf die Eintrittskarte gedruckt. Im RFID-Tag selbst war eine Nummer gespeichert. Diese enthielt einen Hash-Wert, der sich aus der Reservierungsnummer und der Chip-ID zusammensetzt.

Die Kontrolle des Zugangs zu den Stadien wurde in mehreren Phasen durchgeführt. Bei einer stichprobenartig durchgeführten Ausweiskontrolle erfolgte zunächst ein optischer Abgleich des Ausweispapiers mit dem Ticketaufdruck. Im Rahmen weiterer technischen Kontrollen bestand dann die Möglichkeit zu prüfen, ob die auf dem RFID-Chip gespeicherte Nummer mit den Daten aus dem Ticketverkaufsystem (Hintergrundsystem) identisch und der Inhaber des Tickets rechtmäßiger Eigentümer ist. Allerdings wurde während der Einlasskontrolle nur ein geringer Bruchteil der Tickets tatsächlich kontrolliert, und nur in vergleichsweise wenigen Fällen wurden die Daten des Inhabers mit den im Hintergrundsystem gespeicherten Daten abgeglichen [13].

Auch vor diesem Hintergrund ist sicher fraglich, ob das Konzept der personalisierten Tickets unter Nutzung der RFID-Technologie mit dem Datenschutz vereinbar ist, und ob dem Grundsatz der Datenvermeidung und Datensparsamkeit angemessen Rechnung getragen wird. Darüber hinaus müssen bei derartigen Anwendungen Fragen der Transparenz im Vordergrund stehen. Für die Käufer der Eintrittskarten muss nachvollziehbar sein, welche Daten wo und für welche Zwecke und für welchen Zeitraum gespeichert werden.

8.5 Sportveranstaltungen

Vielfältige Einsatzmöglichkeiten für RFID-Systeme gibt es auch bei Sportveranstaltungen. So können beispielsweise Transponder in die Schuhe von Marathonläufern integriert werden, um auch bei großer Teilnehmerzahl die zurückgelegte Strecke und die benötigte Zeit zu messen.

8.6 Transport, Lagerwesen, Großhandel

Im Transport- und Lagerwesen sowie in den Bereichen Logistik und Distribution hat die Verwendung von RFID-Systemen zu beträchtlichen Effizienzsteigerungen durch die Erhöhung des Automatisierungsgrades und Vereinfachung von Abläufen geführt. An Containern und Paletten werden RFID-Tags angebracht, auf denen beispielsweise der Inhalt, der Hersteller, der Empfänger, Versandanweisungen, Gefahrenhinweise, der bisherige Verlauf des Transports usw. gespeichert werden können. Verbunden mit Datenbanksystemen kann so der Lagerbestand relativ detailliert und zuverlässig erfasst werden, die Lagerplatzvergabe lässt sich vereinfachen und Verwechslungen und aufwendiges Suchen werden vermieden. Auch könnte automatisch kontrolliert werden, ob während des Transports die Kühlkette bei kühlungsbedürftigen Lebensmitteln nirgends unterbrochen wurde.

Auch im Großhandel werden schon heute oft RFID-Tags etwa zur Kennzeichnung von Paletten eingesetzt. Es ist jedoch eine wesentlich umfassender Nutzung der RFID-Technologie geplant. In Verbindung mit stationären Lesegeräten an den Ein- und Ausgängen von Lagern und an Regalen sowie mobilen Lesegeräten zusammen mit entsprechenden Software-Lösungen hofft man, beim Warentransfer von der Fabrik bis zum Ladenregal erhebliche Kosteneinsparungen realisieren zu können. Der Warenfluss soll mittels RFID-Systemen weitgehend automatisiert werden. Die zuverlässige, lückenlose und schnelle Datenerfassung und -übertragung soll möglichst in Echtzeit dazu führen, dass jede Transportverpackung jederzeit eindeutig identifiziert und lokalisiert werden kann. Beim Sortieren und Kommissionieren von Waren sowie dem Zusammenstellen von verschiedenen Gütern für den Transport werden Effizienzsteigerungen und eine Senkung der Fehlerquote erwartet.

Sofern diese Logistikdaten nicht mit personenbezogenen Daten zusammengeführt werden, sind derartige Anwendungen datenschutzrechtlich unbedenklich. Selbst eine Zusammenführung kann im Einzelfall unbedenklich sein, wenn die von den Datenschutzgesetzen vorgegebenen Rahmenbedingungen (z. B. Zweckbestimmung, technische und organisatorische Maßnahmen) eingehalten werden.

8.7 Warenwirtschaft und Einzelhandel

Der Einzelhandel verspricht sich neben dem schon erwähnten Einsatz der RFID-Tags zum Schutz vor Diebstahl auch in anderen Bereichen einen hohen Nutzen durch die umfassende Nutzung dieser Technologie. So ist denkbar, dass künftig möglichst jedes einzelne Produkt einen RFID-Tag erhält, der den bisher auf die Verpackungen aufgedruckten Bar- bzw. Strichcode erweitert und langfristig vollständig ersetzt. Barcodes enthalten heute die EAN (European Article Number), eine ursprünglich nur in Europa, mittlerweile aber weltweit verwendete Produktnummer für Handelsartikel. Der Nachfolger der EAN soll im Rahmen weltweiter RFID-Standards der Electronic Product Code (EPC) werden. Dieser Code wurde von der Standardisierungsinitiative EPCglobal entwickelt. Diese Initiative wurde vom US-amerikanischen Uniform Code Council (UCC) und EAN International, die momentan die Standards für Barcodes verwalten, ins Leben gerufen [14].

Im Gegensatz zur bisher verwendeten EAN hat der EPC mit einer Länge von 96 Bit eine ausreichende Kapazität, um Unternehmen 16 Millionen so genannter Objektklassen zur Verfügung zu stellen. In jeder Objektklasse lassen sich wiederum bis zu 68 Milliarden eindeutige Seriennummern vergeben [15]. Der EPC kann auf einfachen passiven RFID-Tags gespeichert werden. Mit entsprechend leistungsfähigen Datenbanken der Hintergrundsysteme soll es somit möglich sein, jedes Produkt weltweit eindeutig zu identifizieren. Allerdings ist zu erwarten, dass Barcodes und RFID-Etiketten in den nächsten Jahren nebeneinander existieren werden, da es weiterhin Anwendungen gibt, bei den Barcodes vorteilhafter sind.

Während die Kennzeichnung von Paletten häufig datenschutzrechtlich unbedenklich ist (siehe Punkt 8.4), entsteht bei der Kennzeichnung von Einzelprodukten ein Gefährdungspotential für die Rechte der Verbraucher. Dies soll anhand von einigen Beispielen [16] aufgezeigt werden.

Eine Handelskette gibt an ihre Kunden beispielsweise mit RFID-Tags versehene Pfandmünzen für Einkaufswagen aus, die bei jedem Einkauf wieder verwendet werden können. Mit Hilfe der auf der Pfandmünze gespeicherten Identifikationsnummer könnte eine Datei erstellt werden, aus der ersichtlich wäre, welche Produkte eine durch die Pfandmünze identifizierte Person kauft, wie häufig sie diese Produkte kauft und welche Filialen der Handelskette sie aufsucht. Die Filialen könnten Rückschlüsse auf das Einkommen, den Gesundheitszustand, den Lebensstil, die Einkaufsgewohnheiten usw. des Kunden ziehen. Diese Informationen wiederum könnten bestimmte Verkäuferentscheidungen beeinflussen, z. B. die Marketingstrategie oder gar eine dynamische Preispolitik. Da der Kunde mit Hilfe der Pfandmünze jedes Mal identifiziert würde, wenn er die Verkaufsräume betritt, könnten seine gespeicherten Einkaufsgewohnheiten für individuelle Werbeaktionen genutzt werden. Neben den einzelnen Filialen könnten aber auch Dritte diese Angaben erhalten. Auf diese Weise könnten eine Reihe von Entscheidungen über die identifizierte Person getroffen werden, ohne dass diese hierzu in voller Kenntnis der Sachlage ihre Einwilligung gibt. Ähnlich wie bei der Verwendung von Cookies im Internet lässt sich die betroffene Person, selbst wenn sie nicht sofort und unmittelbar anhand eines bestimmten Produkts identifiziert werden kann, auf der assoziativen Ebene problemlos identifizieren, und zwar über die Masse der sie umgebenden bzw. über sie ge-

speicherten Informationen. Die erhobenen Daten können sogar die Art beeinflussen, in der die betroffene Person behandelt oder beurteilt wird. Auch diese RFID-Anwendung löst schwerwiegende daten- und verbraucherschutzrechtliche Befürchtungen aus.

Datenschutzrechtliche Bedenken ergeben sich auch in Situationen, in denen die Verwendung von RFID-Tags die Verarbeitung personenbezogener Daten nach sich zieht, selbst wenn keine weiteren eindeutigen Kenndaten verwendet werden. Angenommen die Person Z betritt das Geschäft C mit einer Tasche, in der sich Produkte mit RFID-Tags aus den Geschäften A und B befinden. Geschäft C scannt diese Tasche, und die darin befindlichen Produkte (wahrscheinlich eher ein Wirrwarr an Zahlen) werden erfasst. Geschäft C speichert diese Zahlen. Kommt der Kunde Z am nächsten Tag wieder in das Geschäft, wird er wieder gescannt. Das Produkt Y, das bereits am Vortag gescannt wurde, wird wieder erkannt - die Nummer steht für die Armbanduhr, die der Kunde täglich trägt. Geschäft C erstellt eine Datei mit der Nummer des Produktes Y als "Schlüssel". Nun kann der Kunde beim Betreten des Geschäfts anhand der ID-Nr. der Armbanduhr erkannt werden. Geschäft C kann jetzt für den Kunden Z (dessen Name ihm nicht bekannt ist) ein Profil erstellen und verfolgen, was der Kunde bei späteren Besuchen in seiner Einkaufstasche hat. Auf diese Weise verarbeitet Geschäft C personenbezogene Daten. Folglich findet das Datenschutzrecht Anwendung.

Zur Wahrung des Datenschutzes beim Einsatz von RFID in der Warenwirtschaft sind deshalb u. a. Hinweise an den Regalen oder im Eingangsbereich zur Verwendung der RFID-Tags in den Geschäften, eine Deaktivierungsmöglichkeit an den Kassen, und eine genaue Hinweispflicht, wenn Tags versteckt angebracht sind und wo sich diese befinden, erforderlich.

8.8 Ausweisdokumente

Wer in Deutschland einen Reisepass beantragt, erhält seit dem 1. November 2005 einen Pass mit einem integriertem RFID-Tag, auf dem neben seinen alphanumerischen Daten (Name, Adresse, Geburtsdatum usw.) auch ein Lichtbild als weiteres biometrisches Merkmal gespeichert wurde. Damit wird es grundsätzlich möglich sein, diese Daten in externen Datenbanken zu speichern und nach der abgebildeten Person zu suchen [17].

Das Auslesen dieser auf dem RFID-Tag gespeicherten Daten durch Unbefugte soll durch ein Verfahren namens Basic Access Control (BAC) unterbunden werden. Dabei ist das Auslesen des RFID-Tags nur dann möglich, wenn zuvor die maschinenlesbare Zone des Passes optisch gelesen wurde, das Dokument also einem Beamten oder einer im Besitz eines Lesegerätes befindlichen Person ausgehändigt wurde. Das Lesegerät muss sich mit den Daten aus der maschinenlesbaren Zone am RFID-Chip anmelden. Schlägt diese Anmeldung fehl, so bleibt der Chip stumm. Nur zugelassene Lesegeräte sollen den Chip auslesen können, die Kommunikation zwischen Lesegerät und Chip erfolgt verschlüsselt.

Ab Frühjahr 2007 ist geplant, dass in den RFID-Tag auch die Daten von Fingerabdrücken aufgenommen wird. Diese sollen zusätzlich durch das Authentifizierungsverfahren Extended Access Control (EAC) geschützt werden soll. BAC und EAC werden als Authentifizierungsverfahren dann nebeneinander bestehen.

Die Bundesregierung hat bereits angekündigt, dass künftig auch der Personalausweis mit der gleichen Technik ausgestattet werden soll, wie der Reisepass, d. h. auch der Personalausweis wird künftig einen RFID-Tag erhalten.

Ähnliches gilt auch für Visa, für die bereits im Jahr 2003 die Europäische Kommission erste Entwürfe zur Änderung der entsprechenden EU-Verordnungen vorgelegt hat.

9 Zusammenfassung und Ausblick

Es ist damit zu rechnen, dass RFID-Systeme in zunehmendem Maße in vielen Bereichen des täglichen Lebens eingesetzt werden. Die Zukunftsvision der allgegenwärtigen Datenverarbeitung (Ubiquitous Computing) mittels RFID könnte schon bald realer sein, als es so manchem lieb ist. Weite Einsatzbereiche wie die Kennzeichnung von Büchern in Bibliotheken oder RFID-Kundenkarten als Bezahlmittel im ÖPNV werden bald alltäglich sein. Nur durch einen transparenten Umgang mit dieser neuen Technologie können auch künftig die in den Datenschutzgesetzen geforderte Zweckbindung, Datensparsamkeit und Vertraulichkeit bei der Verarbeitung personenbezogener Daten sichergestellt werden.

Hierzu bedarf es jedoch einer individuellen Betrachtung beim Einsatz von RFID, da allgemeingültige Regeln für so vielfältige Anwendungsbereiche nur schwer zu formulieren sind. Bereits im März 2004 hat die 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung [18] die Notwendigkeit hervorgehoben, Datenschutzprinzipien zu berücksichtigen, wenn RFID-Tags verknüpft mit personenbezogenen Daten eingeführt werden sollen. Alle Grundsätze des Datenschutzrechts müssen beim Design, der Einführung und der Verwendung von RFID-Technologie berücksichtigt werden. Hierzu gehören insbesondere,

- dass jeder Datenverarbeiter vor der Einführung von RFID-Tags, die mit personenbezogenen Daten verknüpfbar sind oder die zur Bildung von Konsumprofilen führen, zunächst Alternativen in Betracht ziehen sollte, die das gleiche Ziel ohne die Erhebung personenbezogener Daten erreichen,
- dass Objekte, die RFID-Tags enthalten, gekennzeichnet werden,
- dass bei unverzichtbarer Verarbeitung von personenbezogenen Daten diese offen und transparent erhoben, verarbeitet und genutzt werden,
- dass diese Daten nur für den speziellen Zweck verwendet werden, für den sie ursprünglich erhoben wurden und nur so lange aufbewahrt werden, wie es zur Erreichung dieses Zwecks erforderlich ist, und
- dass RFID-Tags, die im Besitz von Personen sind, die Möglichkeit zur Löschung der gespeicherten Daten oder zur Deaktivierung oder Zerstörung der Etiketten bieten.

Beim Einsatz von RFID im Handel ist darüber hinaus eine Selbstverpflichtungserklärung zur Verarbeitung und zum Schutz der Daten zu empfehlen [19] [20]. Einer Datenschutz-Zertifizierung von RFID-Tags und von Prozessabläufen bei ihrem Einsatz kommt zukünftig ebenfalls eine bedeutende Rolle zu. Datenschutzgerechte Schutzprofile (Protection Profiles) etwa könnten die Transparenz erhöhen und für mehr Akzeptanz beim Einsatz von RFID sorgen.

Das Bundesverfassungsgericht hat den Gesetzgeber mehrfach darauf hingewiesen, dass wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels die technischen Entwicklungen aufmerksam zu beobachten sind und notfalls durch ergänzende Rechtsetzung korrigierend einzugreifen ist. Daher sind die besonderen Gegebenheiten, die mit dem Einsatz der RFID-Technologie verbunden sind, vom Gesetzgeber daraufhin zu untersuchen, ob für alle Risiken adäquate und rechtliche Schutzmechanismen vorhanden sind. Hierauf sowie auf die wesentlichen Kriterien des Schutzes der Persönlichkeitsrechte (Transparenz, Kennzeichnungspflicht, keine heimliche Profilbildung, Vermeidung der unbefugten Kenntnisnahme, Deaktivierung) hat die 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 2006 in einer Entschließung hingewiesen [21]. Ähnlich laute-

tet die Empfehlung der obersten Aufsichtsbehörden für den Datenschutz im nicht-öfffentlichen Bereich zur Entwicklung und Anwendung von RFID-Technologie vom November 2006 [22].

Abkürzungsverzeichnis

Auto-ID	Automatic Identification
BAC	Basic Access Control
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
EAC	Extended Access Control
EAN	European Article Number
EEPROM	Electrically Erasable Programmable Read-Only Memory
EPC	Electronic Product Code
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
ID-Nr.	Identifikations-Nummer
ISBN	International Standard Book Number
ÖPNV	Öffentlicher Personennahverkehr
RFID	Radio Frequency Identification
UCC	Uniform Code Council

Literaturverzeichnis

[1] Leitfaden: RFID und Datenschutz; Hrsg: RA Robert Niedermeier EICAR e.V.

[2] http://de.wikipedia.org/wiki/RFID, Juli 2006

[3] http://www.ean.co.at/html/5_2_1anw.html, Juli 2006

[4] http://www.heise.de/newsticker/meldung/75558, Juli 2006

[5] Finkenzeller, Klaus: RFID-Handbuch: Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten, 3. Auflage: Carl Hanser Verlag München Oktober 2002

[6] Bundesamt für Sicherheit in der Informationstechnik: Stand und Perspektiven der RF-Chip-Technologie Technische Beschreibung und Sicherheitsbetrachtung 03/2004 http://www.bsi.bund.de/fachthem/rfid/studie.htm

[7] http://www.heise.de/newsticker/meldung/73243, Mai 2006

[8] Lahner, C.M.: Anwendung des § 6 c BDSG auf RFID, Datenschutz und Datensicherheit DuD 28 (2004) 12, S. 723 ff

[9] http://www.foebud.org/rfid, Juli 2006

[10] http://www.heise.de/newsticker/meldung/39880, August 2003

[11] http://www.silicon.de/enid/client_server_host/?con_id=15581, November 2005

[12] http://www.heise.de/newsticker/meldung/75693, Juli 2006

[13] http://www.heise.de/newsticker/meldung/74140, Juni 2006

[14] http://www.epcglobalinc.org, Juli 2006

[15] http://www.zdnet.de/itmanager/tech/0,39023442,2137193-3,00.htm, April 2004

[16] Artikel-29-Datenschutzgruppe: Datenschutzfragen im Zusammenhang mit der RFID-Technik, Arbeitspapier, 19.01.2005

[17] http://www.bfdi.bund.de/cln_029/nn_533592/DE/Schwerpunkte/Biometrie/Artikel/BiometrischeMerkmaleAusweise.html

[18] Entschließung der 67. Datenschutzkonferenz vom 25.3.2004 zu RFID http://www.bfdi.bund.de/cln_029/nn_531946/DE/Oeffentlichkeitsarbeit/Entschliessungssammlung/DSBund-Laender/67DSK-Radio-Frequency-Identification.html

[19] BfDI Faltblatt zu RFID http://www.bfdi.bund.de/cln_029/nn_531950/SharedDocs/Publikationen/Faltblaetter/RFIDFunkchipsFuerJedeGelegenheit.html

[20] http://www.bfdi.bund.de/cln_029/nn_531002/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2006/PM-30-06PeterSchaarFordertVerbindliche Regelungen-FuerDenEinsatzVonRFID-Chips.html, August 2006

[21] http://www.bfdi.bund.de/cln_029/nn_531946/DE/Oeffentlichkeitsarbeit/Entschliessungssammlung/DSBund-Laender/72DSK-RFID,templateId=raw,property=publicationFile.pdf/72DSK-RFID.pdf

[22] http://www.bfdi.bund.de/cln_029/nn_531946/DE/Oeffentlichkeitsarbeit/Entschliessungssammlung/DuesseldorferKreis/DKreisNovember2006RFID,templateId=raw,property=publicationFile.pdf/DKreisNovember2006RFID.pdf