EUROPEAN EXPERT GROUP FOR IT-SECURITY

eicar

# EICAR TASK FORCE ON RFID

## LEITFADEN: RFID UND DATENSCHUTZ

IMPRESSUM:

**HERAUSGEBER:**
EICAR e.V.

Der Leitfaden wurde innerhalb der EICAR-Arbeitsgruppe RFID in Zusammenarbeit mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfD), dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie GS1 erstellt.

# INHALT:

# I. VORWORT

*Der vorliegende Leitfaden ist ein Ergebnisdokument, das in der EICAR Task Force on RFID (Radio Frequency Identification) erarbeitet wurde*

Die European Expert Group for IT-Security – EICAR (www.EICAR.org) – wurde 1991 als eingetragener Verein in Deutschland gegründet. Zunächst mit dem Ziel, Know-how im Bereich der Antivirenforschung zu bündeln, gilt die EICAR mittlerweile als anerkanntes IT-Security-Expertennetzwerk. Das Institut versteht sich als Plattform für den Informationsaustausch für alle Sicherheitsexperten, die in den Bereichen Forschung und Entwicklung, Implementierung sowie Management tätig sind. Hierdurch soll die globale Zusammenarbeit im Bereich der Computersicherheit gefördert werden. Ziel des Instituts ist es, Lösungen und Präventivmaßnahmen gegenüber allen Arten der Computerkriminalität, wie z.B. das Schreiben und Verbreiten von Computer-Viren, Betrug sowie das Ausspähen von personenbezogenen Daten, zu entwickeln. Dabei arbeitet das Institut sowohl sehr eng mit Unternehmen, politischen Organisationen oder universitären Einrichtungen als auch mit Medien, Technik- und Rechtsexperten zusammen.

## Warum eine Arbeitsgruppe RFID?

Vor zwei Jahren hat die EICAR eine Task Force zum Thema RFID ins Leben gerufen. In der öffentlichen Diskussion standen Themen wie Privacy und Datenschutz zu diesem Zeitpunkt an oberster Stelle. Die Task Force hat es sich daher zur Aufgabe gemacht, eine sachliche Diskussion zu führen und sowohl Chancen als auch Risiken der RFID-Technologie kritisch zu betrachten. Vor allem unter den Aspekten des Datenschutzes und der IT-Sicherheit.
Mitglieder der EICAR Task Force on RFID sind renommierte Unternehmen aus Industrie, aber auch Vertreter von Behörden und Organisationen.

## Ziele und Nutzen des Leitfadens

Der Leitfaden richtet sich in seiner jetzigen Fassung an Unternehmen, die zukünftig RFID-Technologien einsetzen wollen. Sie erhalten im Leitfaden Hinweise in Bezug auf Datenschutz-relevante Aspekte im Zusammenhang mit dem Einsatz von RFID, insbesondere im Consumerbereich, bei dem sich künftig eine Verknüpfung von Logistikdaten auf einem RFID-Chip und personenbezogenen Daten möglich sein wird.
Der Leitfaden soll demjenigen, der RFID im kundennahen Bereich einsetzt, eine Hilfestellung für die Praxis geben und gleichzeitig das notwendige Bewusstsein schaffen, das für die Beachtung datenschutzrechtlicher Vorgaben notwendig ist.
Der Leitfaden kann somit beispielsweise einen Appendix für Allgemeine Geschäftsbedingungen oder Projektverträge darstellen, die sich auf den Einsatz von RFID-Technologien beziehen. Ein Entscheider kann damit prüfen, welche Datenschutz-relevanten Kriterien greifen und was er genau tun muss, um diesen zu entsprechen.
Aufgrund der Tatsache, dass Datenschutz-relevante Kriterien abhängig von dem jeweiligen Einsatzgebiet der RFID-Technologien sind, hat sich die Arbeitsgruppe zunächst für die Unterteilung in drei Szenarien entschieden:

### 1. Szenario 1:

*Tags, die entfernt werden, wenn der Konsument die Ware erwirbt und somit nicht mit Kundendaten verknüpft werden*

## 2. Szenario 2:

*Auslesen der auf den RFID-Tags enthaltenen Produktdaten, z. B. zum Bezahlen an der Kasse und Verbindung mit Kundendaten*

## 3. Szenario 3:

*Tags, die zur Erstellung von Nutzungsprofilen verwendet werden*

Der Leitfaden ist ein dynamisches Papier, das kontinuierlich an aktuelle Entwicklungen angepasst wird. Es ist durchaus denkbar, dass der Leitfaden in Zukunft weitere Einsatz-Szenarien der RFID-Technologie beleuchten wird.

*Die Autoren im März 2006*

# I. EINLEITUNG

RFID (Radio Frequency Identification)- Systeme werden zunehmend für eine Reihe unterschiedlicher Anwendungen eingesetzt. Sie gehören – wie die schon seit 1970 verbreiteten Barcode-Systeme - zu den sog. Automatic Identification (Auto-ID)-Systemen.
Die Basistechnologien der Mikro-, bzw. Informationselektronik unterliegen in unserer Gesellschaft einem rasanten Entwicklungsprozess. Immer mehr Prozesse laufen elektronisch ab und sind für den Verbraucher unsichtbar.

Darüber hinaus funktionieren diese Prozesse immer öfter dezentral und sind daher schwer nachvollziehbar.

Mit dieser Dezentralisierung durch Miniaturisierung geht auch das Verschwinden bzw. das Unsichtbarwerden der physikalischen Systemkomponenten einher, mit denen die Nutzer intuitiv kommunizieren. Hieraus resultieren immense Möglichkeiten, obgleich die Faszination mit ganz natürlicher Skepsis einhergeht. Ist bei der Benutzung des Mobiltelefons ein klarer direkter Nutzen gegeben, so liegt dieser bei der RFID-Technologie für den Konsumenten nur indirekt vor. Der nicht-offensichtliche Nutzen gepaart mit der Nicht-Sichtbarkeit mündet in notwendige Fragen hinsichtlich der informatorischen Selbstbestimmtheit des Konsumenten.
Dies führt dazu, dass die Themen Privatsphäre und Datenschutz ins Zentrum der RFID-Diskussion rücken. Verbraucher haben zunehmend Angst, dass ihre persönlichen Daten verbraucht werden – vor allem dann, wenn sie kaum eine Möglichkeit haben, den elektronischen Austauschprozess der Daten nachzuvollziehen. Für den speziellen Fall von RFID hat Simons Garfinkel (Mitarbeiter des AutoID Centers am MIT, Cambridge) daher bereits 2002 „A RFID Bill of Rights" vorgeschlagen, die die Kernforderungen der Datenschützer enthielt.
Obwohl sowohl Entwickler als auch die ersten Anwender der Problematik gewahr waren, sind die notwendigen Diskurse zeitversetzt zu ersten Pilotapplikationen und strategischen Potenzialaussagen angestoßen worden.

Die rechtzeitige Abbildung der neuen Technologiemöglichkeiten im Rahmen der *technischen, organisatorischen sowie rechtlichen* Maßnahmen blieb aus, so dass sich etwa seit 2002 eine

verhärtete Konfliktlage zwischen Befürwortern und Gegnern der technologischen Möglichkeiten entwickeln konnte. Die Argumentationsbasis der Diskussionen gründet dabei vielfach auf unvollständige Informationen zu den oben genannten Maßnahmenanforderungen.

Zur Vervollständigung der Debatte um diese revolutionierenden Technologien werden auch die *strategischen* Fragen der Notwendigkeit ihrer Nutzung, der Art und der Zeitpunkt der Einführung sowie der *psychologische* Aspekt der Wahrnehmung und Akzeptanz Raum einnehmen.

Dieser Leitfaden hat daher zum Ziel, die aktuellen Fakten zusammenzustellen, um vor allem Anbietern der RFID-Technologie einen Entscheidungsrahmen in Bezug auf Datenschutz-relevante Kriterien zu verschaffen.

# II. FUNKTIONSWEISE DER RFID-TECHNOLOGIE

## 1. Allgemeine Funktionsweise

Die RFID-Technik basiert auf winzigen Chips (in RFID-Tags oder Transpondern), welche per Funk Informationen übermitteln, ohne dass eine Übertragung äußerlich bemerkbar ist. Der Chip ist so klein, dass er auf Transport- oder Produktverpackungen angebracht und sogar in Textilien eingearbeitet werden kann. Ein Lesegerät („Reader") sendet in einer festgelegten Frequenz (Nieder-, Hochfrequenz oder UHF-Bereich) Funksignale aus, die von dem RFID-Tag erkannt werden. Danach werden die in diesem Chip gespeicherten Daten dem Lesegerät übermittelt. RFID-Lesegeräte sind je nach Frequenzbereich in der Lage, bis zu 200 Transponder in Sekundenschnelle auszulesen.

## 1. Spezielle Funktionsweise

RFID nutzt Radiowellen die, wie der Name bereits zum Ausdruck bringt, vergleichbar sind mit üblichen Radio- und Fernsehsystemen. Wie bei diesen ist in der Masse der angebotenen RFID-Konzepte das Medium (Tag, Label, Etikett, Transponder etc.) lediglich ein Empfänger, der nicht selbstständig sendet, sondern ein ausgesendetes Radiofeld mit spezifischen Veränderungen sozusagen „reflektiert". Insofern ist der landläufig gebrauchte Begriff des „Funkchips" irreführend und wenig hilfreich. Transponder, die nur Empfänger und keine Sender sind, werden als *passive* Tags bezeichnet. Der Aufbau ist relativ einfach (Chip und Antenne), so dass der Preis für Massenanwendungen (Handel und Logistik) gering genug ist. Demgegenüber werden in einigen industriellen Anwendungen auch aufwendige und *aktive* Systeme zum Einsatz gebracht, die so funktionieren, wie es von den WLAN-Systemen bekannt ist (Access Point und WLAN-Karte sind Sende- und Empfängersysteme).

Transpondersysteme unterscheiden sich einerseits durch die Betriebsfrequenz, den damit möglichen Formfaktoren (Größe, Dicke) des Bauelements, der Speichergröße sowie der Protokollstruktur (z.B. Lesetransponder, Schreib-/Lesetransponder, Sicherheitsfunktionen etc.). Die Größe eines RFID-Chips kann heute bereits weit unter einem Quadratmillimeter liegen, jedoch ist die funktionale Einheit Chip und Antenne determiniert durch die Antennengröße selbst. Übliche Formfaktoren für Antennen sind im Bereich einiger Quadratzentimeter angesiedelt, so dass

die Anbringung an Objekte des Materialflusses beliebig herausfordernd sein kann. Die Größe der Antenne ist jedoch ein entscheidender Faktor im Hinblick auf die Lesedistanz.
Betrachtet man den Masseneinsatz von RFID in Konsumgüterindustrie und dem Handel, werden hauptsächlich passive, einmal beschreibbare Tags mit einer geringen Speicherkapazität eingesetzt.

### *Exurs: Nächste Generation von Tags*

Die fortschreitende Entwicklung in der Mikroelektronik wird aber in der Zukunft auch RFID-Tags ermöglichen, die neben einem Speichermodul auch Sensorik bis zur Aktuatorik enthalten werden. Diese aufwendigen Tags werden naturgemäß für empfindliche Güter (gefrostete Lebensmittel, Frischware, Medikamente etc.) Anwendung finden. Tags verbunden mit Aktuatorik könnten in der Zukunft z.B. bei festgestellter Erhöhung der Umgebungstemperatur eigenständig die Kühlung ansteuern oder über GPRS eine SMS absetzen. Im Rahmen der erhöhten Anforderungen an das Nachverfolgbarkeitsprinzip in der Konsumgüterindustrie lassen sich entsprechende Vorteile für die Konsumentensicherheit erwarten.

## III. AKTIVE UND PASSIVE RFID-TAGS

RFID-Tags werden – wie bereits oben beschrieben – in „aktive" und „passive" untergliedert. Aktive Tags verfügen über eine eigene Stromversorgung, welche in der Regel eine höhere Lesereichweite oder eine autarke Aufzeichnung von Daten (z.B. Temperaturverläufe in der Tiefkühllogistik) ermöglichen. Passive Tags beziehen ihre Energie zur Übertragung der Informationen aus den empfangenen Funkwellen.

Man unterscheidet des Weiteren einmal beschreibbare Transponder im Gegensatz zu mehrfach beschreibbaren Tags. Ein letztes Unterscheidungskriterium ist die Kapazität zur Speicherung von Daten. Alle drei Kriterien (Energieversorgung, Wiederbeschreibbarkeit, Speicherkapazität) haben einen signifikanten Einfluss auf den Preis eines Transponders. Daher werden in der Praxis oftmals passive, einmal beschreibbare Tags mit einer geringen Speicherkapazität eingesetzt.

## IV. ANWENDUNGEN

Es wird eine Unterscheidung zwischen RFID-Anwendungen vorgenommen, die primär zur Personenidentifizierung dienen und Anwendungen, die der Objektidentifizierung dienen. Außerdem lässt sich ein wesentliches Unterscheidungskriterium durch die Nutzungsdauer des Transponders heranziehen.

*(siehe Abbildung)*

| | *PERSONENBEZUG* | *OBJEKTBEZUG* |
|---|---|---|
| *EINWEGTRANSPONDER* | · WM 2006 TICKETS<br>· FAHRKARTE / VERKEHRSVERBUND<br>· SKIPASS<br>· BOARDINGPASS | · KONSUMGÜTER (SCM, PRODUKTPIRATERIE)<br>· NAHRUNGSMITTEL<br>· FLUGGEPÄCK<br>· PAKETE/PACKSTÜCKE<br>· LADE-EINHEITEN |
| *MEHRWEGTRANSPONDER* | · KUNDENKARTE<br>· E-PASSPORT<br>· GESUNDHEITSKARTE<br>· ZUTRITTSMANAGEMENT<br>· SPORT-DAUERKARTEN<br>· WEGFAHRSPERRE | · MEHRWEGTRANSPORT-SYSTEME<br>· WERKZEUGMANAGEMENT<br>· PRODUKTIONSSTEUERUNG<br>· MAUTSYSTEME<br>· BIBLIOTHEKEN |

*Abb: RFID Anwendungsmatrix* *© UbiConsult 2005*

## 1. Identifizierung von Waren

(Anwendungsbereiche in der Matrix: Konsumgüter, Nahrungsmittel, Ladeeinheiten, Mehrwegtransportsysteme, Produktpiraterie)
RFID-Tags können zunächst zur Identifizierung von Waren/logistischen Einheiten entlang der Logistikkette eingesetzt werden (vgl. das Pilotprojekt bezüglich dem Einsatz von RFID in der Logistikkette im „METRO Group Future Store" in Rheinberg). Dadurch wird die Überwachung des ganzen Prozesses von der Produktion über den Wareneingang bis hin zur Auslieferung beim Einzelhändler ermöglicht, so dass man im Wesentlichen folgende Potenziale ausschöpfen kann:

- Prozessbeschleunigung,
- Diebstahlbekämpfung in der Logistikkette,
- Verhinderung von Out of Stock auf der Verkaufsfläche und
- Nachweis der Herkunft (Echtheitsnachweis bzw. Haftung).

Insgesamt soll mit dieser Technik die Warenkennzeichnung mittels Barcode-Technologie ergänzt werden. Barcodes werden in der Konsumgüterindustrie zur Speicherung von EAN-Nummern genutzt und identifizieren ein Objekt als zu einer Kategorie gehörend. Ein wesentlicher Nachteil dieser Technik ist, dass der Code für das Lesegerät sichtbar sein muss (optische Erfassung) und die Etiketten nicht wiederbeschreibbar sind. RFID-Tags können hingegen jedes Objekt mit einer eindeutigen Kennung versehen. Die Menge der gespeicherten Daten kann in Abhängigkeit von der Speicherkapazität des Tags im Vergleich zu Barcodes deutlich größer sein. Darüber hinaus besteht die Möglichkeit wiederbeschreibbare Tags einzusetzen, zum Beispiel um Informationen zu ergänzen oder zu löschen. Ein Sichtkontakt zum Lesegerät ist hierbei nicht erforderlich. RFID-Tags sind zudem robuster gegen Umwelteinflüsse und haben somit eine längere Lebensdauer.

## 2. Weitere Anwendungsmöglichkeiten

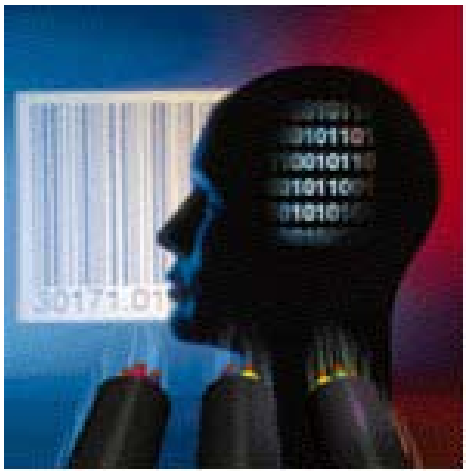
Vielfach wird heute RFID bereits als Zugangsschlüssel zu physischen Objekten genutzt. Neben dem allseits bekannten Funkautoschlüssel, geben immer mehr Firmen kontaktlose Zugangskarten aus, die wartungsarm und bequem das Gebäude/Gelände absichern. Zunehmend interessiert sich auch die Kreditwirtschaft für die kontaktlosen RFID Karten, weil wie bereits erwähnt, neben der wesentlich höheren Sicherheit gegenüber den Magnetstreifen, auch eine bedeutende Steigerung der Zuverlässigkeit gegeben ist. Neben diesen beispielhaften Anwendungen auf der Basis aufwendiger, wiederverwendbarer Karten, werden zunehmend Einwegtickets im Bereich des öffentlichen Nahverkehrs und des Sports eingesetzt.

Zur Fußballweltmeisterschaft 2006 in Deutschland werden die Tickets mit RFID-Tags versehen und an den Stadiontoren ein funkbasiertes elektronisches Zugangskontrollsystem eingesetzt. Begründet wird der Einsatz dieses Systems mit der Motivation, den WM-Ticketerwerb durch Gewalttäter zu vermeiden, gegen Fälschung, Verlust und Diebstahl zu schützen und den Schwarzhandel zu unterbinden.

Im Allgemeinen sind RFID-Tags schon Bestandteil des täglichen Lebens geworden. Ihr Einsatz zur Tierkennzeichnung, bei Straßenmautsystemen und Skipässen sowie zur Diebstahlsicherung als Wegfahrsperre ist bereits eine Tatsache. Im Bereich der Logistik als auch im Bereich der Sicherheit soll die Verwendung der RFID-Technik zu Vereinfachung und Optimierung der Prozesse führen. Die Vorteile sowohl für die Wirtschaft als auch für die einzelnen Verbraucher, die Produkte und Dienstleistungen besserer Qualität genießen werden, machen die RFID-Technik besonders attraktiv.

Bei der Verbreitung von RFID-Tags sind jedoch mögliche datenschutzrechtliche Gefahren auszuschließen. Die Erstellung personalisierter Einkaufs- und Nutzungsprofile ohne Wissen und Zustimmung der betroffenen Personen ist datenschutzrechtlich nicht erlaubt. Die Anwender der Technik sind daher aufge-

fordert, das Datenschutzrecht zu beachten. Werden personenbezogene Daten mit Hilfe der RFID-Technologie verarbeitet, sind die Grundsätze des Datenschutzrechts bei der Einführung und Verwendung dieser Technologie zu berücksichtigen.



# V. DATENSCHUTZRECHTLICHE ASPEKTE

## 1. Anwendbarkeit des Datenschutzrechts

Das Datenschutzrecht kann betroffen sein, wenn entweder der RFID-Tag selbst personenbezogene Daten speichert oder die nicht personenbezogenen Daten auf dem RFID-Chip einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Dies hat zur Folge, dass der Einsatz der RFID-Tags in der Warenwirtschaftskette nicht in den Anwendungsbereich des Datenschutzrechts fällt, weil dort keine Daten mit Personen verknüpft werden.

## 2. Datenschutzrecht: Verbot mit Erlaubnisvorbehalt

Wenn wir uns zunächst einmal veranschaulichen, wie das Datenschutzgesetz personenbezogene Daten definiert, stellen wir fest: Die personenbezogenen Daten werden in § 3 Abs. 1 BDSG als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person definiert. Im Datenschutzrecht gilt das sog. Verbotsprinzip: Grundsätzlich ist die Erhebung und Verarbeitung personenbezogener Daten verboten und nur ausnahmsweise gestattet, wenn entweder die Einwilligung des Betroffenen oder eine gesetzliche Ermächtigung dazu vorliegt.

## 3. Grundsatz der Datenvermeidung und -sparsamkeit (§ 3a BDSG)

Für einen Anwender, der personenbezogene Daten erhebt, gilt:
Nach dem Grundsatz der Datenvermeidung und -sparsamkeit (§ 3a BDSG) soll die verantwortliche Stelle zunächst Alternativen in Betracht ziehen, die das gleiche Ziel ohne die Erhebung von personenbezogenen Daten erreichen. Wenn die personenbezogenen Daten erforderlich sind, dann müssen diese offen und transparent, also für den Betroffenen erkenn- und nachvollziehbar, erhoben werden.

### *4. Rechtsgrundlage für die Datenverarbeitung im nicht-öffentlichen Bereich: §§ 27 ff. BDSG*

*Was ist erlaubt?*
Ohne Einwilligung des Betroffenen ist die Datenverarbeitung im nicht-öffentlichen Bereich unter den Voraussetzungen der §§ 27 ff. BDSG zulässig. Insbesondere ist § 28 BDSG einschlägig, der die Zulässigkeitsvoraussetzungen einer Datenverarbeitung für eigene Zwecke normiert. In § 28 Abs.1 Nr.1 BDSG ist die Nutzung der Daten im Rahmen der Zweckbestimmung eines Vertragsverhältnisses erlaubt. Ferner gestattet § 28 Abs.1 Nr.2 BDSG die Nutzung von Daten im Wege einer Interessenabwägung: Die Nutzung von personenbezogenen Daten ohne Einwilligung ist zulässig, „soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt".

*Szenario 1:*

Tags, die entfernt werden, wenn der Konsument die Ware erwirbt und somit nicht mit Kundendaten verknüpft werden

*Szenario 2:*

Auslesen der auf den RFID-Tags enthaltenen Produktdaten, z. B. zum Bezahlen an der Kasse und Verbindung mit Kundendaten

*Szenario 3:*

Tags, die zur Erstellung von Nutzungsprofilen verwendet werden

## VI. EINSATZMÖGLICHKEITEN & DATENSCHUTZRECHTLICHE BEWERTUNG VON RFID-TAGS IM ENDKUNDENBEREICH

*Für den Einsatz von RFID-Technologie ist Folgendes generell zu beachten:*
Die Datenschutzerfordernisse bei der Nutzung von RFID-Tags sind anhand des konkreten Einsatzes zu bestimmen. Im Endkundenbereich erscheint die Unterscheidung in drei Gruppen sinnvoll.

Die datenschutzrechtlichen Anforderungen sowie die technischen und organisatorischen Maßnahmen, die das Unternehmen treffen muss, sind bei diesen drei möglichen Lösungen unterschiedlich.

*Szenario 1:*

Tags, die entfernt werden, wenn der Konsument die Ware erwirbt und somit nicht mit Kundendaten verknüpft werden

### *a) Rechtliche Bewertung: Keine Anwendbarkeit des BDSG*

Bei diesem Anwendungsszenario werden RFID-Tags zum Beispiel zur Erhöhung der Sicherheit eingesetzt. Die Kaufhäuser sichern ihre Artikel mit RFID-Tags zum Zwecke der Diebstahlabsicherung. Die verwendeten Tags werden an der Kasse entfernt und oftmals wiederverwendet.

### *b) Organisation:*

In organisatorischer Hinsicht ist jedoch zu empfehlen, dass das Unternehmen die Kunden auf den Einsatz von RFID-Tags, die für die Warenidentifikation eingesetzt werden, im Geschäft hinweist und die notwendigen Informationen über diese Technologie und über den genauen Ort der Anbringung der RFID-Tags und die Möglichkeit ihrer Entfernung ohne Zerstörung des Produktes selbst bereitstellt. Damit wird die Transparenz des Einsatzes von RFID-Tags gewährleistet. Eine explizite gesetzliche Verpflichtung liegt jedoch nicht vor.

## *Szenario 2:*

## Auslesen der auf den RFID-Tags enthaltenen Produktdaten, z. B. zum Bezahlen an der Kasse und Verbindung mit Kundendaten

Mit der Verwendung von RFID-Tags wird innerhalb des Handels eine Vielzahl von Anwendungsbereichen angestrebt, wie zum Beispiel die Unterstützung von Inventurprozessen, die Verbesserung der Warenpräsenz oder weitere Erleichterungen des Kassiervorganges. Die Tags sind deaktivierbar (z.B. durch Unterdrückung der Auslesbarkeit) oder leicht zu entfernen.

### *a) Datenschutzrechtliche Zulässigkeit § 28 Abs. 1 Nr. 1 BDSG*

Bei diesem Szenario werden im RFID-Tag selbst keine personenbezogenen Daten verarbeitet. An der Kasse werden – analog zum Barcode – Produktdaten ausgelesen und die relevanten Produktinformationen wie z. B. der Preis und die Artikelbezeichnung für dieses Produkt aus dem Warenwirtschaftssystem abgerufen. Der Einsatz dient der schnelleren Abwicklung an der Kasse. Bei Barzahlung ergeben sich somit datenschutzrechtlich keine Besonderheiten.

Der Bezug zu einer natürlichen Person kann jedoch möglich sein, wenn die Bezahlung mit Kunden-, EC- oder Kreditkarten vorgenommen wird. Erst durch eine Bezahlung mit solchen Karten kann ein Personenbezug hergestellt werden. Dies hat zur Folge, dass der Anwendungsbereich des Datenschutzrechts eröffnet wird, so dass eine gesetzliche Grundlage für die Verarbeitung von personenbezogenen Daten erforderlich ist. Diese Grundlage stellt § 28 Abs. 1 BDSG dar.

§ 28 Abs. 1 S. 1 Nr. 1 BDSG lässt die Verarbeitung von personenbezogenen Daten zu, sofern dies zur Abwicklung eines Vertragsverhältnisses erforderlich ist. Diese Vorschrift stellt die Grundlage für die Datenverarbeitung zur Durchführung eines Vertragsverhältnisses oder zur Abwicklung eines vertragsähnlichen Vertrauensverhältnisses dar.

Die erhobenen Kundendaten sind bei Bezahlung mit Kunden-, EC- oder Kreditkarten zur Abwicklung des Vertrags erforderlich (§ 28 Abs. 1 S. 1 Nr. 1 BDSG) und können ohne Einwilligung des Betroffenen zu diesem Zweck (z.B. Bezahlung und/oder Rabattabwicklung bei Kundenkarten) verwendet werden. Die personenbezogenen Daten dürfen jedoch nur für den speziellen Zweck verwendet werden, für den sie ursprünglich erhoben wurden und auch nur solange wie notwendig gespeichert bleiben (Zweckbindungsgrundsatz).

Des Weiteren muss die verantwortliche Stelle hierbei die im BDSG verankerten Informations- und Hinweispflichten erfüllen. Eine Einwilligung des Kunden ist jedoch nicht notwendig.

Der Einsatz von RFID-Tags in Verbindung mit EC-, Kunden-, und Kreditkarten ist deshalb datenschutzrechtlich nicht zu beanstanden, solange und soweit die folgenden im BDSG verankerten Informations- und Hinweispflichten erfüllt werden und die verantwortliche Stelle sich an die weiteren datenschutzrechtlichen Verpflichtungen hält. Dann unterscheidet sich der Vorgang rechtlich nicht von gegenwärtigen Kassenvorgängen.

## *b) Informationspflichten*

### *Informationspflichten nach § 4 Abs. 3 BDSG*

Die verantwortliche Stelle muss nach § 4 Abs. 3 BDSG den Betroffenen schon bei Erhebung der Daten unterrichten über:

- **die Identität der verarbeitenden Stelle**
- **die Zweckbestimmungen der Erhebung, Datenverarbeitung und Nutzung**
- **die Kategorien von Empfängern, sofern der Betroffene nicht mit der Übermittlung an diese rechnen muss.**

### *Informationspflichten nach § 6c BDSG*

Beim Einsatz von RFID-Chipkarten wäre darüber hinaus § 6c BDSG einschlägig, der weitgehende Informationspflichten bei „mobilen personenbezogenen Speicher- und Verarbeitungsmedien" fordert. Dabei handelt es sich nach § 3 Abs. 10 BDSG um Datenträger,

- **die an den Betroffenen ausgegeben werden,**
- **auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und**
- **bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.**

Erfasst werden dementsprechend Medien, auf denen personenbezogene Daten über die Speicherung hinaus automatisiert verarbeitet werden können, die also mit einem Prozessorchip ausgestattet sind. Diese Voraussetzung kommt allerdings nur in Betracht, wenn personenbezogene Daten auf dem RFID-Tag selbst gespeichert werden, was momentan in Handel nicht relevant ist.

Gemäß § 6c Abs. 1 BDSG muss sowohl die ausgebende Stelle als auch die Stelle, die auf das Medium Verarbeitungsverfahren aufbringt, den Betroffenen über ihre Identität und Anschrift (Nr. 1), die Funktionsweise des Mediums (Nr. 2), seine Rechte auf Auskunft und Korrektur (Nr. 3) und die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen unterrichten.

Allgemein ist darauf hinzuweisen, dass die Informationspflicht nicht nur den Anforderungen nach § 4 Abs. 3 BDSG und eventuell § 6c BDSG genügen muss, sondern dass ferner zu empfehlen ist, auch auf den genauen Ort der Anbringung der RFID-Tags und die Möglichkeit zu ihrer Entfernung ohne Zerstörung des Produkts selbst aufmerksam zu machen.

## *c) Technische und organisatorische Maßnahmen (§ 9 BDSG)*

Nach § 9 BDSG haben die verarbeitenden Stellen die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine datenschutzgerechte Verarbeitung personenbezogener Daten sicherzustellen. Der Aufwand für die Maßnahmen muss unter Berücksichtigung des Standes der Technik in

einem angemessenen Verhältnis zu dem angestrebten Zweck stehen. Die Datensicherheit kann dann als wirksam angesehen werden, wenn die getroffenen Maßnahmen in ihrer Gesamtheit einen hinreichenden Schutz der Daten vor Missbrauch leisten. Sicherungsziele sind die Gewährleistung der Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität der Daten.

## d) Rechte des Betroffenen

*Benachrichtigungspflicht: § 33 BDSG*

§ 33 BDSG sieht eine Benachrichtigung des Betroffenen bei der erstmaligen Speicherung über die Speicherung, die Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Identität der verantwortlichen Stelle vor. Gemäß § 33 Abs. 1 BDSG ist der Betroffene, wenn personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung ohne Kenntnis des Betroffenen gespeichert werden, von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen.

In organisatorischer Hinsicht ist somit ein Hinweis auf den RFID-Einsatz am Eingang zum Geschäft zu empfehlen. Dies kann am sinnvollsten durch eine Tafel am Eingang zum Geschäft geschehen. Nur bei Vorliegen dieser Allgemeinen Hinweispflicht über die Verwendung von RFID-Tags im Geschäft ist von einer rechtskonformen Anwendung auszugehen.

*Auskunftsansprüche: § 34 BDSG*

Der Betroffene hat ferner gemäß § 34 BDSG Auskunftsansprüche gegen die verantwortliche Stelle. Mitzuteilen sind die zur Person des Betroffenen gespeicherten Daten (sowie ihre Herkunft), die Empfänger oder Kategorien von Empfänger, an die Daten weitergegeben werden, und der Zweck der Speicherung.

*Deaktivierung der RFID-Tags.*

Eine Löschungspflicht besteht zunächst, wenn die Datenerhebung und -speicherung unzulässig ist (§ 35 Abs. 2 Nr. 1 BDSG). Des Weiteren ist die Löschung geboten, wenn die Speicherung nicht mehr zur Erfüllung des Zwecks erforderlich ist (§ 35 Abs. 2 Nr. 3 BDSG). Das Unternehmen muss somit die mit Hilfe von RFID-Tags erhobenen Daten, die es in seinem EDV-System gespeichert hat, löschen, wenn der Verwendungszweck entgültig weggefallen ist. Die Daten, die auf den RFID-Tag selbst gespeichert sind, sind auch zu löschen, sofern sie personenbezogenen Charakter haben. Die Löschung der Daten auf dem RFID-Tag steht hierbei nicht im Ermessen des Unternehmens. Dies ist allerdings momentan nicht praxisnah, denn es werden in den meisten Fällen noch keine RFID-Tags, die personenbezogenen Daten speichern, eingesetzt.

## e) Sanktionen

Bei Verletzungen der Bestimmungen des Datenschutzrechts sind in § 7 BDSG Schadensersatzansprüche vorgesehen. Ferner stellen die Verstöße gegen das BDSG Ordnungswidrigkeiten (§ 43 BDSG) dar, die auch strafbar sein können (§ 44 BDSG).
Nur bei selbstverpflichtender Einhaltung der Anforderungen durch das Unternehmen, insbesondere der dargestellten Informations- und Hinweispflichten über die Verwendung von RFID-Tags im Geschäft sowie dem Angebot zur Deaktivierung der RFID-Tags nach ihrer Verwendung, kann von einer rechtskonformen RFID-Anwendung gesprochen werden.

*Szenario 3:*

**Tags, die zur Erstellung von Nutzungsprofilen verwendet werden**

Bei dieser – in der Praxis noch nicht relevanten – Konstellation sind die RFID-Tags nicht deaktivierbar und werden zur Erstellung von Nutzungsprofilen verwendet.

## *a) Rechtliche Bewertung: Zulässigkeit nur mit Einwilligung des Kunden*

Zu prüfen ist zunächst die Zulässigkeitsklausel des § 28 BDSG. Wenn die dort genannten Voraussetzungen vorliegen würden, wäre dieses Szenario legitimiert. Die Voraussetzungen des § 28 Abs. 1 S. 1 Nr. 1 BDSG (Zweckbestimmung eines Vertragsverhältnisses) sind regelmäßig nicht erfüllt: Die Erfassung von RFID-Daten bei dem zugrunde liegenden Fall ist zur Erfüllung der Pflichten oder zur Wahrnehmung der Rechte aus dem Vertrag offensichtlich nicht erforderlich. Ebenso wenig relevant ist der Zulässigkeitstatbestand des § 28 Abs. 1 S. 1 Nr. 3 BDSG (Daten aus allgemein zugänglichen Quellen).

Allenfalls könnte § 28 Abs. 1 Nr. 2 BDSG in Betracht kommen. Danach ist die Nutzung von personenbezogenen Daten zulässig, soweit sie zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Ein berechtigtes Interesse i. S. dieser Vorschrift ist „ein nach vernünftiger Erwägung durch die Sachlage gerechtfertigtes Interesse, das auch wirtschaftlicher Natur sein kann". Inwieweit die schutzwürdigen Interessen des Betroffenen den berechtigten Interessen der verantwortlichen Stellen vorrangig sind, kann im Rahmen einer Interessenabwägung ermittelt werden. Angesichts der Art der erhobenen Daten und ihrer Aussagekraft einerseits und der Belange der verantwortlichen Stelle andererseits, liegen beim Einsatz von RFID in dieser Konstellation die Voraussetzungen der § 28 Abs. 1 Nr. 2 BDSG regelmäßig nicht vor.

Es ist zunächst nicht ersichtlich, warum die Erfassung von Bewegungen des Kunden in einem Geschäft erforderlich ist, um berechtigte Interessen des Geschäftes zu wahren. Selbst bei Annahme eines berechtigten Interesses des Kaufhauses sind diese Daten zur Wahrung eines wirtschaftlichen Interesses des Geschäfts nicht erforderlich. Des Weiteren liegt regelmäßig ein überwiegendes Interesse des Kunden gegen die Erstellung von personenbezogenen Nutzungsprofilen vor. Als Ergebnis ist also festzuhalten, dass weder § 28 Abs. 1 Nr. 2 BDSG noch die übrigen gesetzlichen Erlaubnistatbestände des BDSG in Betracht kommen können.

*Zwischenergebnis:*
Es liegt bei diesem Szenario kein Erlaubnistatbestand gemäß § 28 BDSG vor. Der Einsatz von RFID-Tags in dieser Konstellation ist deshalb nur mit Einwilligung des Kunden zulässig. Ohne die wirksame Einwilligung des Betroffenen stellen die Verfolgung der Bewegungen des Kunden im Geschäft und die Erstellung von Nutzungsprofilen einen gravierenden Verstoß gegen das Recht auf informationelle Selbstbestimmung des Einzelnen dar.

## *b) Anforderung an eine wirksame Einwilligung*

Das BDSG geht von dem Konzept der informierten Einwilligung aus: Die Einwilligung muss auf der freien Entscheidung des Betroffenen beruhen (§ 4a Abs. 1 S. 1 BDSG). Der Betroffene muss die vorgesehene Verarbeitung kennen, so dass er eine hinreichend bestimmte Erklärung abgeben kann. Das Gesetz verlangt explizit, dass der Betroffene vorher über die Tragweite seiner Einwilligung aufzuklären ist (§ 4a Abs. 1 S. 2 BDSG).

Auch bei der Datenverarbeitung auf Grundlage einer Einwilligung muss die verantwortliche Stelle über ihre Identität, die Zweckbestimmungen der Datenverarbeitung und die Kategorien von Empfängern unterrichten (§ 4 Abs. 3 BDSG) und gegebenenfalls die Informationspflichten aus § 6c BDSG erfüllen. Die Unterrichtung des Betroffenen über diese Angaben erfolgt jedoch in der Regel bereits im Rahmen der Einholung der Einwilligungserklärung, so dass eine besondere Unterrichtung nach § 4 Abs. 3 BDSG bzw. § 6c BDSG grundsätzlich nicht notwendig ist. Des Weiteren ist die allgemeine Hinweispflicht über die Verwendung von RFID-Tags im Geschäft und die Informationspflicht über den genauen Ort der Anbringung der Tags und die Möglichkeit zu ihrer Entfernung zu beachten.

In der Praxis kann die Einwilligung des Kunden im Rahmen der Ausgabe einer Kundenkarte eingeholt werden. Wenn der Kunde eine Kundenkarte beantragt, kann ihm die Möglichkeit eingeräumt werden, ausdrücklich und schriftlich dem Einsatz von RFID-Tags zum Zwecke der Erstellung eines Nutzungsprofils im Geschäft einzuwilligen.


Die vorformulierten Einwilligungserklärungen müssen natürlich den hohen Anforderungen der Rechtsprechung an AGB-Einwilligungsklauseln zu Verarbeitung von personenbezogenen Daten entsprechen. Eine versteckte Aufnahme solcher Erklärungen im sog. „Kleingedruckten" ist nicht zulässig, denn dem Kunden ist in diesem Fall nicht bewusst, dass er eine Einwilligungserklärung abgibt.

Die Einwilligung des Kunden ist deshalb besonders hervorzuheben, d.h. sie muss an deutlich sichtbarer Stelle und drucktechnisch von dem anderen Text abgesetzt dargestellt werden. Die Klausel muss klar und verständlich formuliert werden, den Kunden auf den Einsatz von RFID-Tags hinweisen und detailliert über die Zwecke der Datenverarbeitung und seine Rechte aus dem Datenschutzrecht informieren. Aus technischer Sicht ist es in Zukunft denkbar, dass Tags ohne Zerstörvorgang deaktiviert werden können. Des Weiteren sollte angegeben werden, wann es zur Löschung der Daten bzw. Deaktivierung des Tags nach dem Bezahlvorgang kommt. Insbesondere auf das Angebot an den Kunden zur Deaktivierung der Tags nach ihrer Verwendung ist hinzuweisen.

Wenn der Betroffene die entsprechende Klausel unterschreibt, ist er sich über die Bedeutung seiner Einwilligung im Klaren: Er weiß, welche Daten abgefragt werden können und zu welchem Zweck dies geschieht. Der ganze Prozess ist somit transparent.

Um dem Transparenzangebot und der Beaufsichtigungspflicht voll umfänglich zu genügen, empfiehlt es sich allerdings, einen Hinweis auf „verborgen" angebrachte Tags am Regal, am Produkt o.ä. anzubringen. Dies korrespondiert mit der Informationspflicht über den genauen Ort der Anbringung der Tags und der Möglichkeit ihrer Entfernung.

*Abb. 2: Das EPC-Warenlogo dient zur Kennzeichnung RFID/EPC-getaggter Ware.*

Der Kunde sollte außerdem auf die Möglichkeit des Widerrufs seiner Einwilligung hingewiesen werden. Es handelt sich, wenn der Kunde dem Einsatz von

RFID-Tags zum Zwecke der Erstellung eines Nutzungsprofils im Geschäft einwilligt, um einen datenschutzrechtlich relevanten Vorgang. Eine einmalige Einwilligung des Kunden bei Beantragung seiner Kundenkarte kann hierbei nicht als Genehmigung für jegliche Profilbildung des Kunden über Jahre hinaus ausreichen. Der Kunde sollte deshalb in bestimmten Abständen darauf hingewiesen werden, dass er eine solche Einwilligung abgegeben hat bzw. zur Aufrechterhaltung der Einwilligung aufgefordert wird.

Des Weiteren gelten auch hier die Informationspflichten und Benachrichtigungs-, Auskunfts-und Löschungsansprüche des Betroffenen, die im Szenario 2 dargestellt wurden.
Nur wenn diese Informations- und Hinweispflichten und das Angebot zur Deaktivierung der RFID-Tags durch das Unternehmen selbstverpflichtend beachtet werden, kann von einer rechtskonformen RFID-Anwendung gesprochen werden.

In technischer und organisatorischer Hinsicht soll die verantwortliche Stelle alle notwendigen Maßnahmen gemäß § 9 BDSG treffen, um das vom Gesetzgeber gewünschte Datenschutzniveau zu gewährleisten.

Beim Einsatz von RIFD Tags im Arbeitnehmerbereich (Zugangskarten) ist auf die entsprechende Einhaltung von Arbeitnehmerdatenschutzbestimmungen zu achten.

### *c) Sanktionen*

Das dritte Szenario wäre dementsprechend nur möglich, wenn der Kunde einwilligt. Fehlt es an einer solchen Einwilligungserklärung, würde dieser Prozess eine unbefugte Erhebung oder Verarbeitung von personenbezogenen Daten darstellen. Dies kann eine Ordnungswidrigkeit (§ 43 BDSG) bzw. eine strafbare Handlung sein (§ 44 BDSG). Auch Schadensersatzansprüche des Betroffenen wären nicht ausgeschlossen (§ 7 BDSG).

## Weitere Informationen finden sich unter:

*http://www.EICAR.org/rfid/index.htm*

*http://www.bsi.bund.de/fachthem/rfid/studie.htm*

*http://www.bitkom.org/de/publikationen/1357_33258.aspx*

*http://www-1.ibm.com/services/us/index.wss/ibvstudy/imc/a1017984*

*http://www.ibm.com/software/de/websphere*

*http://www-5.ibm.com/de/ibm/unternehmen/partner-for-innovation/index.html*

*http://www.rfid-weblog.de*

*http://www.future-store.org*

*http://www.epcglobal.de*

*http://www.bfdi.bund.de*

**Besonderer Dank gilt den Autoren des Leitfadens:**

Dirk Bungard, Dr. Frank Gillert, Manuel Hüttl, Johannes Landvogt, RA Robert Niedermeier, Katrin Springob, Antonia Voerste, Klaus Vogell