

# » Datenschutz bei RFID-Anwendungen «



Kontakt:  
Marco Andres  
FTK Forschungsinstitut für Telekommunikation e.V.  
Martin-Schmeißer-Weg 4  
44227 Dortmund

Tel.: +49 (231) 97 50 56-54  
E-Mail: [mandres@ftk.de](mailto:mandres@ftk.de)

[www.rfid-support-center.de](http://www.rfid-support-center.de)

Stand September 2007



Gefördert mit Mitteln der Europäischen Union  
und des Landes Nordrhein-Westfalen

## Inhalt

|   |    |
|---|----|
| 1. Vorwort .....                                  | 3  |
| 2. Einführung .....                               | 4  |
| 3. Grundlagen der RFID-Technologie .....          | 5  |
| 4. Rechtliche Aspekte des Datenschutzes .....     | 9  |
| 5. Stand der Diskussion - Expertenmeinungen ..... | 17 |
| 6. Umfrage-Ergebnisse .....                       | 23 |
| 7. Checkliste für RFID-Projekte .....             | 33 |
| 8. Weiterführende Informationen .....             | 35 |

## 1. Vorwort

Die Radiofrequenz-Identifikation ist eine Technologie, die innerhalb kürzester Zeit in allen wirtschaftlichen und gesellschaftlichen Bereichen bis hinein in die Privatsphäre zu spürbaren Veränderungen führen wird. Es ist nicht überraschend, dass um das Thema RFID eine kontroverse Diskussion geführt wird, bei der nicht nur Fragen des Datenschutzes, sondern auch der allgemeine Wunsch nach Akzeptanz im Vordergrund stehen.

In der Debatte um die Möglichkeiten und Grenzen der RFID-Technologie haben sich zwei gegenüberstehende Positionen herauskristallisiert: Auf der einen Seite werden die Chancen gesehen, die sich aus der Nutzung von RFID ergeben, auf der anderen Seite hingegen werden vor allem mögliche Risiken, Bedrohungen und Beschränkungen thematisiert. Um eine möglichst objektive und von allen Interessengruppen nachvollziehbare Beurteilung der Chancen und Risiken der RFID-Technologie zu ermöglichen, ist eine offene, sachliche und umfassende Information unbedingt erforderlich. Eine möglichst hohe Transparenz in der Diskussion um RFID und Datenschutz innerhalb der einzelnen Akteursgruppen ist ein notwendiger Schritt zur Versachlichung der Diskussion und der gesellschaftlichen Meinungsbildung.

Die vorliegende Studie wurde im Rahmen des Projektes RFID-Support-Center erstellt. Sie soll insbesondere kleine und mittelständische Unternehmen (KMU) mit dem Thema Datenschutz vertraut machen und diese dazu bewegen, im Rahmen der Durchführung von RFID-Projekten unternehmensbezogene RFID-Privacy Grundsätze zu berücksichtigen. Den KMU sollen Kompetenzen zur Bewertung, Gestaltung und Implementierung von datenschutzintensiven RFID-Lösungen einschließlich der Sensibilisierung der beteiligten Mitarbeiter vermittelt werden.

Im Rahmen der Studie wurde eine Online-Befragung bei über 700 Unternehmen durchgeführt. Die überaus große Resonanz mit einer Beteiligung von 23 Prozent lässt erkennen, dass das Thema Datenschutz im Zusammenhang mit der Nutzung von RFID-Technologie einen hohen Stellenwert besitzt. Die Ergebnisse der Befragung werden in Kapitel 6 vorgestellt.

Um den Unternehmen eine möglichst praxisnahe Hilfestellung beim Umgang mit den Einflussfaktoren und Akzeptanzfragen im Zusammenhang mit den Aspekten des Datenschutzes bieten zu können, wurden Statements, Einschätzungen und Handlungsempfehlungen verschiedener Experten aus dem RFID-Umfeld erfragt und aufbereitet.

Wir danken an dieser Stelle den Experten für ihre freundliche Unterstützung sowie allen Personen, die an der Befragung teilgenommen haben.

## 2. Einführung

Technische Entwicklungen wie die RFID-Technologie rufen nicht nur eine hohe Datenmenge hervor, sondern bieten auch neue Möglichkeiten der Datenerfassung und -verarbeitung. Der Einsatz von RFID-Systemen ermöglicht durch die sicht- und kontaktlose Funktionsweise neue Anwendungen wie zum Beispiel die Verfolgung oder Ortung von Produkten in den Bereichen Produktion oder Logistik. Vielversprechende Anwendungsfelder zeichnen sich unter anderem in Bereichen wie Pharma (z.B. Erkennung gefälschter Medikamente), Luftfahrt (z.B. Vorbeugende Wartung der Flugzeuge und Überwachung der Zulässigkeit von Werkzeugen), Automotive (z.B. Verkürzung von Lieferzyklen, Vermeidung gefälschter Teile) sowie Handel und Konsum (z.B. automatische Steuerung der Nachbevorratung von Supermärkten sowie Vermeidung leerer Regale) ab.

Vor dem Hintergrund der technischen Möglichkeiten, die in Verbindung mit der Radiofrequenzidentifikation bestehen, wird klar, dass der Einsatz der Technologie Auswirkungen auf die verschiedensten Ebenen der IT-Sicherheit und der Gesellschaft haben wird. Themen wie Privatsphäre und Datenschutz sind dabei schnell ins Zentrum der RFID-Diskussion gerückt. Verbraucherschützer befürchten im Zuge einer zukünftig breiten Anwendung der RFID-Technologie eine Einschränkung der Freiheits- und Persönlichkeitsrechte.

Als Grund für die häufig geäußerte Skepsis gegenüber der Technologie wird hauptsächlich die Möglichkeit eines unberechtigten und unbemerkten Auslesens der verwendeten Transponder genannt. Durch eine mögliche Verknüpfung personenbezogener Daten (z.B. Alter oder Adresse auf einer Kundenkarte) mit Produktdaten ist es vorstellbar, dass das Kaufverhalten eines Kunden mit Hilfe der Transpondertechnologie unberechtigt und unbemerkt nachvollzogen werden könnte, um dieses beispielsweise für interne Marketingzwecke oder Verhaltensforschungen zu nutzen.

Analog zu den personenbezogenen Daten bei Verbrauchern sind aber auch Unternehmensinterna vor dem unbefugten Zugriff und vor unberechtigter Weitergabe zu schützen. Produktdaten können von Unternehmen auf Transpondern für interne Zwecke gespeichert und während des Produktionsprozesses bearbeitet und aktualisiert werden. Falls diese nicht in verschlüsselter Form vorliegen, ist es potenziell für konkurrierende Unternehmen bzw. auch für Kunden möglich, Firmeninterna auszulesen, wenn diese vorher nicht zerstört oder verschlüsselt wurden.

Als Basis für eine sachliche Diskussion über den Schutz von Daten im Zusammenhang mit RFID-Anwendungen sind sowohl Kenntnisse über die technischen Grundlagen als auch über die rechtlichen Aspekte des Datenschutzes notwendig. In den Kapiteln 3. und 4. werden hierzu einführende Informationen zur Verfügung gestellt.

### 3. Grundlagen der RFID-Technologie

Das Verständnis für die verschiedenen Fragestellungen der Datenschutz-Thematik im Zusammenhang mit dem Einsatz der Radiofrequenz-Technologie setzt die Kenntnis einiger technischer Grundlagen voraus. Im Folgenden werden die Grundbegriffe der RFID-Technologie kurz erläutert.

#### Funktionsweise

RFID-Systeme werden der Gruppe der automatischen Identifikationssysteme zugerechnet. Die eigentliche Kernfunktionalität eines RFID-Systems kommt der Identifikation von Objekten und Personen sowie der Informationsbereitstellung zu.

Die RFID-Technologie bietet die Möglichkeit der berührungslosen Datenübertragung auf der Basis elektromagnetischer Wechselfelder. Auf diesem Wege können Daten automatisch ohne manuelles Zutun ausgelesen werden. So lassen sich Objekte identifizieren, auch wenn sie in Bewegung sind.

Zum Datenaustausch und zur Speicherung von Informationen dienen „Transponder“ oder „Tags“, die sich an der Ware anbringen lassen. Wiederbeschreibbare Tags lassen sich auch mit neuen Daten beschreiben. Ein Tag oder Transponder besteht aus einem Mikrochip mit Kupfer- oder Aluminium-Antenne. Wie beim Barcode lassen sich Informationen auf einem Datenträger an Objekten anbringen und auslesen. Mit einem Unterschied: die Daten werden berührungslos und bei Bedarf auch automatisiert gelesen. Die Antenne des Transponders kommuniziert mit dem Lesegerät (Reader), das wiederum den Inhalt des integrierten Transponderchips ausliest.

Auf dem Markt befinden sich viele unterschiedliche RFID-Systeme, die sich durch die jeweilige Transponderbauform, die Energie- und Datenübertragung, die Übertragungsfrequenz und die Reichweite unterscheiden. Je nach Anwendung, Produkt und Verpackungsmaterial kommen unterschiedliche Transponder, Reader und Antennen zum Einsatz.

#### Bauformen von Transpondern

Ob Glasröhrchen, Ohrenmarke, Scheckkarte, Scheibe oder hitzeresistente Modelle für die Automobilindustrie: Für fast jedes Anwendungsgebiet gibt es eine passende Transpondervariante. Deshalb kann nicht von "dem" Transponder gesprochen werden.

Klassische Tag-Formen sind z.B. die Scheckkarte, die für Zugangskontrollen genutzt wird oder die im Zündschlüssel integrierte Wegfahrsperre. Hier werden schon seit den 90er Jahren RFID-Systeme zuverlässig eingesetzt, auch wenn dies dem Nutzer oft nicht bekannt ist. Denn der Transponder für die Wegfahrsperre ist im Autoschlüssel verbaut und deswegen nicht erkennbar.



Darüber hinaus ermöglichte die fortschreitende Miniaturisierung auch die Entwicklung von „Smart Labels“. Diese passiven Transponder werden mit einer Antenne auf Folie aufgebracht. Vorteil: Sie sind bedruckbar und lassen sich wie Papier weiterverarbeiten. Die Energie zum Auslesen der Daten liefert

das Lesegerät. Transponder in Etikettenform sind beispielsweise für den Einsatz in Logistikunternehmen interessant. Dort werden Paletten, Pakete und Sendungen direkt mit dem Transponder beklebt; dadurch lassen sich die Warensendungen identifizieren.

### **Aktive und passive Transponder**

Transponder können als aktive oder passive Variante vorkommen. Während die aktiven Transponder über eine eigene Energieversorgung durch eine eingebaute Batterie verfügen und sich lesen und beschreiben lassen, beziehen passive Transponder die nötige Energie aus dem elektromagnetischen Frequenzfeld des Lesegerätes. Auch der Speicherinhalt passiver Tags kann überschrieben werden. Die Menge der auf dem Tag gespeicherten Daten ist ebenfalls variabel je nach Transponder.

Beide Transponderarten haben unterschiedliche Eigenschaften und eignen sich deshalb für unterschiedliche Anwendungsbereiche. Das Fehlen der Batterie bei passiven Tags reduziert Kosten, Gewicht und Größe des Transponders. Nachteilig ist die geringere Reichweite. Diese Tags werden oft zur Produktidentifizierung und -auszeichnung bei hohen Stückzahlen verwendet. Eine Datenfortschreibung ist hier vielmals nicht notwendig. Auf dem Tag wird die eindeutige Produkt-Identifikationsnummer abgelegt; lediglich in der Datenbank werden Änderungen vollzogen. Passive Etiketten sind günstiger und werden oft bei Massenartikeln verwendet.

Aktive Transponder funken im Vergleich zu passiven Tags durch ihre eigene Energieversorgung deutlich weiter. Diese Eigenschaften machen sie für Bereiche interessant, bei denen Überwachungs- bzw. Protokollierungsaufgaben übernommen werden. Aktive Tags werden zum Beispiel bei der

Temperaturüberwachung von Lebensmitteltransporten eingesetzt. Wegen der komplexeren Bauweise und Ausstattung sind aktive Tags wesentlich teurer als ihre passiven Verwandten. Sie werden daher meist bei Produkten eingesetzt, die ebenfalls hochwertig und teuer sind.

### Frequenzbereiche

Die RFID-Technologie ist in der Anwendung vielseitig. Trotzdem gibt es keine Systemlösung, die sich für alle Bereiche eignet. Die Auswahl der jeweils passenden Technik hängt vom Anwendungskontext ab. Technisch begrenzt sich die Reichweite der Transponder durch die Antennengröße, den verwendeten Transpondertyp und die Übertragungsfrequenz.

Frequenzen von 125 kHz (Niederfrequenz, NF), 13,56 MHz (Hochfrequenz, HF), 860 MHz bis 960 MHz (Ultrahochfrequenz, UHF) und 2,45 GHz (Mikrowellenbereich) sind im Einsatz. Welcher Bereich sich eignet, hängt von der Art der Anwendung ab. Bei Niedrig- und Hochfrequenz-Transpondern sind Störungen durch Wasser und Metall geringer als im Ultrahochfrequenzbereich (UHF).

|   | LF<br>Niederfrequenz<br>125 kHz – 135<br>KHz | HF<br>Hochfrequenz<br>13,56 MHz | UHF<br>Ultrahochfrequenz<br>860 MHz – 960 MHz               | Mikrowelle<br>2,45 GHz                                 |
|---|--|---------------------------------|---|--|
| <b>Energie-<br/>Versorgung</b>                            | Passiv                                       | Passiv                          | Passiv  | aktiv  |
| <b>Reichweiten</b>  | Weniger als 1m                               | Max. 1,7 m                      | Max. ca. 6m (passiv)<br>Max100m (aktiv)                     | Max. ca. 6m (passiv)<br>Max100m (aktiv)                |
| <b>Übertragungs-<br/>Raten</b>                            | Niedrig                                      | Mittel                          | Hoch  | Sehr hoch  |
| <b>Störung durch<br/>Flüssigkeiten</b>                    | Kein Einfluß                                 | Geringer<br>Einfluß             | Starker Einfluß   | Starker Einfluß  |
| <b>Störung durch<br/>Metall</b>                           | Starker Einfluß                              | Starker Einfluß                 | Bei direkter Aufbrin-<br>gung ggf. keine Lese-<br>fähigkeit | Bei direkter Aufbrin-<br>gung keine Lesefä-<br>higkeit |
| <b>Ausrichtung des<br/>Transponders<br/>beim Auslesen</b> | Nicht nötig                                  | Nicht nötig                     | Teilweise nötig   | Immer nötig  |

Quelle: RFID - Eine Chance für kleine und mittlere Unternehmen,  
EC-Ruhr und ECC Stuttgart-Heilbronn, 2007

Niederfrequenzsysteme werden bei Zugangs-Kontrollsystemen, der Tierkennzeichnung, bei Wegfahrsperrern und in der Produktion verwendet. Transponder dieses Bereichs eignen sich für viele Einsatzbereiche, da der Markt viele Bauformen anbietet. Niedrige Anschaffungskosten und der unproblematische Umgang mit Feuchtigkeit und Metall zeichnen sie aus. Sie eignen sich daher gut für den Einsatz in rauer Umgebung. Ein Nachteil ist die kurze Lesereichweite (weniger als ein Meter) und die lange Übertragungsdauer großer Daten-Mengen.

Hochfrequenzsysteme findet man beispielsweise bei Ticketing- oder Bibliothekssystemen oder im ÖPNV. Sie erzielen Reichweiten bis zu 1,7 Metern und hohe Lesegeschwindigkeiten. Nachteil dieser Technik: die Flüssigkeitsempfindlichkeit. Der niedrige Preis lässt den Einsatz bei Massenverarbeitungen und Einweganwendungen zu.



Ultrahochfrequenzen verwendet beispielsweise der Handel zur Palettenidentifikation. In der Lagerwirtschaft, der Verfolgung und Identifikation der Waren und bei der Distribution wird die Frequenz verstärkt eingesetzt. UHF-Systeme profitieren von ihrer sehr hohen Daten-Übertragungsrate und hohen Reichweiten. Passive Transponder funken maximal sechs Meter weit. Aktive Transponder senden ihre Informationen über Distanzen von bis zu 100 Metern an den Empfänger. Transponder, die die Mikrowellenfrequenz (2,45 GHz) nutzen, finden sich bei der automatischen Mauterfassung sowie der Waren-, Container- und Palettenverfolgung und im Flottenmanagement. Die Reichweite ist den UHF-Systemen überlegen.

### **Einsatzbereiche**

Die RFID-Technologie gilt als eine der zentralen Enabling-Technologien des Ubiquitous Computing (Allgegenwärtigkeit der Informationsverarbeitung). Dementsprechend breit gefächert sind die möglichen Anwendungen und Anwendungsfelder. Aufgrund ihrer Funktionsweise bietet sie sich in all den Bereichen an, in denen eine Identifizierung, Authentifizierung und oder Kommunikation mit Objekten erforderlich bzw. sinnvoll ist. Der sichtkontaktlose und in der Leseentfernung skalierbare Datenaustausch, die mögliche Menge und Variabilität der Daten ebenso wie Zusatzfunktionalitäten verschaffen dieser Technologie einen erheblichen Mehrnutzen gegenüber den „bisherigen klassischen“ Identtechnologien wie z.B. Barcode oder Magnetstreifen.

Die Nutzung der RFID-Technologie beschränkt sich somit nicht auf eine bestimmte Branche oder einen speziellen Einsatzbereich. Wegen der Vielfältigkeit kann sie überall dort eingesetzt werden, wo Produkte oder Objekte automatisch identifiziert bzw. verwaltet werden. RFID wird daher auch als Querschnittstechnologie bezeichnet. Der Technologie-Einsatz ist nicht nur in klassischen Anwendungsbereichen wie Produktion, Logistik und

Verkehr sowie Handel und Konsum erfolgversprechend. Vielmehr gewinnen auch Anwendungen in Bereichen wie Sicherheit, Pflege, Gesundheit und Freizeit zunehmend an Bedeutung.

#### **4. Rechtliche Aspekte des Datenschutzes**

Die folgenden Informationen finden Anlehnung an das Rechtsgutachten „RFID - rechtliche Dimensionen der Radiofrequenz-Identifikation“ des Informationsforums RFID.

##### **Anwendbarkeit des Datenschutzrechts**

Ziel und Zweck des Datenschutzes ist nicht der Schutz von Daten, sondern der Schutz von Personen vor Missbrauch und unberechtigtem Zugriff auf personenbezogene Daten. Ein wichtiger Aspekt hierbei ist die informationelle Selbstbestimmung. Grundsätzlich darf jeder selbst über die Verbreitung persönlicher Daten entscheiden. „Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer Person“ (§3, BDSG). Daten werden zu personenbezogenen Daten durch Verknüpfung von z.B. Namen mit Geburtsdatum, Kfz-Kennzeichen, Kontonummer oder Gesundheitsdaten. RFID-Anwendungen, bei denen keine Personen betroffen sind (u.a. zur Tieridentifikation) werfen dahingehend keine datenschutzrechtlichen Probleme in Bezug auf personenbezogene Daten auf.

Die Verwendung von RFID-Technologie bedarf einer differenzierten Betrachtung zur juristischen Bewertung. Zu unterscheiden sind drei Fälle von RFID-Anwendungen:

1. Auf den Tags wird ausschließlich ein elektronischer Produktcode (EPC) gespeichert.

Dieser Anwendungsbereich ist vor allem im Handel vorstellbar, z.B. bei automatischer Erfassung im Kassensbereich. Die zentrale Fragestellung ist, ob personenbezogene Daten erhoben oder verarbeitet werden. Ist auf einem Tag lediglich ein elektronischer Produktcode gespeichert, so handelt es sich hierbei, mangels Bestimmbarkeit einer Person, nicht um ein personenbezogenes Datum und das Datenschutzrecht ist somit nicht anwendbar.

2. Der EPC wird mit Kundendaten verknüpft, die in Datenbanken hinterlegt sind.

Wie im ersten Fall wird hier auf dem Tag ausschließlich ein Produktcode oder eine Seriennummer gespeichert. Im Unterschied dazu wird jedoch eine Verknüpfung zu personenbezogenen Daten hergestellt, die in der Regel in einer Datenbank hinterlegt sind. Ein Beispiel für diesen zweiten Fall ist eine Kundenkarte, die beim Bezahlen zum Einsatz kommt. Die Tags auf den erworbenen Produkten enthalten keine personenbezogenen

Daten. Durch die Kundenkarte werden die Produktdaten jedoch mit der Person verbunden und Umsatzarten und -größen unter Umständen gespeichert. Die Vorschriften des BDSG finden daher Anwendung.

3. Persönliche Kundendaten werden direkt auf dem Tag gespeichert. Ist das BDSG anwendbar, wie in den Fällen 2 und 3, so ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach § 4 Abs. 1 BDSG nur dann zulässig, wenn der Betroffene eingewilligt hat, oder das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet. Als ein solcher Erlaubnistatbestand ist vor allem § 28 Abs. 1 S. 1 BDSG in Erwägung zu ziehen. Auch die weiteren datenschutzrechtlichen Grundsätze wie das Prinzip der Erforderlichkeit, der Transparenz- und der Zweckbindungsgrundsatz sind zu beachten. Werden mobile Speichermedien eingesetzt, bestehen zusätzliche Unterrichtungspflichten des Verwenders nach § 6c BDSG. Dies ist z.B. bei der Verwendung von Kundenkarten der Fall.

### **Datenschutzrechtliche Grundlagen**

Der Umgang mit verschiedenen Daten und unterschiedlichen Datenerfassungssystemen ist rechtlich eingebettet. Bereits 1995 veröffentlichte die Europäische Union eine „Datenschutzrichtlinie für elektronische Kommunikation“. Inhalt dieser Richtlinie ist die Formulierung von Mindestvorgaben im Datenschutz. Das Bundesdatenschutzgesetz (BDSG) ist die nationale Umsetzung der europäischen Richtlinie. Es ist nicht immer unumgänglich, dass personenbezogene Daten erhoben, bzw. weiterverarbeitet werden. Bei Kauf von elektronischen Eintrittskarten (z.B. für die Fußball-Weltmeisterschaft 2006) ist die Angabe persönlicher Daten erforderlich. Das Datenschutzgesetz dokumentiert hierfür den vorgeschriebenen Umgang mit personenbezogenen Daten, die in RFID-Systemen und allen anderen elektronischen Systemen bearbeitet werden. Es regelt sowohl den Datenschutz für Privatpersonen als auch für Unternehmen (nicht-öffentliche Stellen).

Das Europäische Institut für Computer Anti-Viren Forschung (EICAR) hat hierzu einen Leitfaden (EICAR-RFID-Leitfaden) erarbeitet, der konkrete Anwendungsszenarien vorstellt und hinsichtlich datenschutzrechtlicher Aspekte bewertet. EICAR ist eine Plattform für den Informationsaustausch im Bereich der Computer Anti-Viren Forschung. Mitglieder der Arbeitsgruppen kommen sowohl aus rechtlichen, als auch technischen Bereichen von Wissenschaft, Industrie und Verbraucherschutzorganisationen.

Im Folgenden wird näher auf die einzelnen Bestimmungen des BDSG eingegangen. Es sei nochmals darauf hingewiesen, dass diese nur zur Anwendung kommen, wenn die unter „Anwendbarkeit des Datenschutzrechtes“ angegebenen Voraussetzungen zutreffen.

### ***Das Recht auf informationelle Selbstbestimmung***

Dieses Recht beruht auf einer Ableitung des Bundesverfassungsgerichts aus Artikeln des Grundgesetzes. Zum einen ist hier die freie Entfaltung der Persönlichkeit nach Art. 2 Abs. 1 GG und der Achtung der Menschenwürde nach Art. 1 Abs. 1 GG anzuführen. Das Recht auf informationelle Selbstbestimmung befugt den Bürger, selbst darüber zu entscheiden, in wie weit, wann und wo seine persönlichen Daten offengelegt werden. Auch unter der Veränderung technologischer Bedingungen, wie dies im RFID-Bereich der Fall ist, muss er immer noch über Erhebung, Verarbeitung und Nutzung seiner Daten bestimmen können.

### ***Das Verbot mit Erlaubnisvorbehalt***

Die Erhebung, Speicherung, Übermittlung, Veränderung, Verarbeitung und Nutzung personenbezogener Daten ist nur mit Einwilligung des Betroffenen nach § 4 Abs. 1 BDSG rechtmäßig, oder wenn eine andere Rechtsvorschrift dies zulässt. Letzteres wird Erlaubnistatbestand genannt. Erlaubnistatbestände liegen vor, wenn der Umgang mit Daten zur Wahrung berechtigter Interessen der verantwortlichen Stelle dient, sofern kein schutzwürdiges Interesse des Betroffenen überwiegt, und wenn er der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen dient. Auf die Einwilligung und die Erlaubnistatbestände (Ausnahmetatbestände) wird im Folgenden eingegangen.

### ***Einwilligungsvorbehalt gem. § 4 Abs. 1 BDSG***

Bei der Einwilligung handelt es sich nach dem BDSG um eine antizipierte Erlaubnis. Sie muss also ausnahmslos der Datenverarbeitung vorausgehen. Die Vorschriften der Willenserklärung aus Geschäftshandlungen sind hier entsprechend anzuwenden. Die Einwilligungserklärung muss auf freier Entscheidung des Betroffenen beruhen und grundsätzlich schriftlich erfolgen. Außerdem muss der Betroffene grundsätzlich auf den Zweck der Erhebung, Verarbeitung und Nutzung, sowie die Folgen einer Verweigerung der Einwilligung hingewiesen werden. Sie ist besonders hervorzuheben, wenn sie schriftlich zusammen mit anderen Erklärungen erfolgt.

### ***Ausnahmetatbestände nach § 28 BDSG***

Zum einen gelten Ausnahmetatbestände, wie oben erwähnt, für die Zweckbestimmung des Vertrages und für die Wahrnehmung berechtigter Interessen.

Die Zulässigkeit der Erhebung, Speicherung, Veränderung oder Übermittlung von personenbezogenen Daten ohne Einwilligung bezieht sich nicht nur auf die Zweckbestimmung des Vertragsverhältnisses, sondern auch auf die vertragsähnlichen Vertrauensverhältnisse. Dies ermöglicht eine Speicherung personenbezogener Daten bereits vor Beginn oder nach Ende eines Vertragsverhältnisses. Zwischen Speicherung und Abwicklung des Vertrages muss jedoch ein unmittelbarer Zusammenhang bestehen. Kauft ein Kunde beispielsweise Waren mit einem RFID-System oder be-

zahlt mit Karte, so dürfen die Daten nicht für Werbekampagnen genutzt werden. Hierzu kann sich der Händler nicht auf einen Ausnahmetatbestand stützen. Bezüglich der Dauer der Speicherung gilt eine Legitimität für die Spanne der Durchführung des Vertrages von der Lieferung bis zum Ende der Gewährleistungsfrist (zwei Jahre). In der Regel dürfen hier die Stammdaten gespeichert werden.

Unter berechtigtem Interesse, das die Speicherung ohne Einwilligung ermöglicht, wenn das schutzwürdige Interesse des Betroffenen nicht überwiegt, ist tatsächliches, wirtschaftliches oder ideelles Interesse zu verstehen. Dienlichkeit ist zur Wahrung des berechtigten Interesses nicht genug. Es wird Erforderlichkeit vorausgesetzt. Ob das berechnete Interesse der Stelle oder das schutzwürdige des Betroffenen überwiegt, wird in Interessensabwägungen ermittelt. Im Zweifel überwiegt das Interesse des Betroffenen. Die Durchführung von Werbekampagnen und Marktanalysen ist nach herrschender Meinung ein berechtigtes Interesse der Stelle, hier des Unternehmens. Bezüglich der Stammdaten lässt sich teilweise kein schutzbedürftiges Interesse feststellen, welches überwiegt. Benutzt der Kunde also Kundenkarten etc., so muss er damit rechnen, dass seine dort erhobenen Daten auch zu Werbezwecken genutzt werden. In Bezug auf RFID lässt sich jedoch kein berechtigtes Interesse des Unternehmens an Aufenthaltsdaten oder Bewegungsdaten von Kunden in Geschäften erkennen, das dem Schutz der Privatsphäre des Kunden überwiegt.

Des Weiteren ist eine Datenverarbeitung zulässig, wenn die Daten allgemein zugänglich sind, wie z.B. in Telefonbüchern, sofern nicht ein entgegenstehendes Interesse des Betroffenen offensichtlich überwiegt. Im Zweifel ist in diesem Fall also eine Speicherung der Daten zulässig.

### ***Transparenzgebot***

Die Transparenz der Erhebungs- und Verarbeitungszusammenhänge ist Grundlage dafür, dass der Betroffene sein Recht auf informationelle Selbstbestimmung überhaupt wahrnehmen kann. Die gespeicherten Daten müssen ihm offengelegt werden, damit er Lösungs- und Änderungswünsche geltend machen kann. Daher müssen ihm Auskunftsrechte gewährt werden (§§19a, 34 BDSG) und es bestehen Benachrichtigungspflichten (§§19, 33 BDSG) der verantwortlichen Stellen. Erfolgt die Datenerhebung in RFID-Systemen ohne Kenntnis des Betroffenen, so ist er zu benachrichtigen. Dies ist nur durch eine vorherige Einwilligung des Betroffenen zum Entfall der Benachrichtigungspflicht zu vermeiden. Auskunftsrechte sind in jedem Fall zu gewähren.

### ***Zweckbindung***

Eine zweckwidrige Nutzung personenbezogener Daten ist unzulässig. Sie dürfen nur für eindeutig festgelegte und rechtmäßige Zwecke erhoben und weiterverarbeitet werden. Insbesondere wird eine Vorratshaltung von personenbezogenen Daten zu unbestimmten Zwecken untersagt, auf Grundlage des Rechts auf informationelle Selbstbestimmung (§14 BDSG).

### ***Prinzip der Erforderlichkeit***

Der Erforderlichkeitsgrundsatz besagt, dass nur für die Bearbeitung der jeweiligen Aufgabe Daten erhoben und verarbeitet werden dürfen. Der Datenverarbeitungsvorgang dient einer bestimmten Sachaufgabe und nur für diese dürfen die Daten genutzt werden. Abschwächungsklauseln haben diesen Grundsatz jedoch für nicht-öffentliche Stellen abgeschwächt, wenn es der Zweckbestimmung eines Vertragsverhältnisses dient, oder wenn es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist (§28 Abs. 1 S. 1 BDSG).

### ***Grundsatz der Datensparsamkeit***

Der Grundsatz der Datenvermeidung- und Sparsamkeit (§3a BDSG) spezifiziert das o.g. Prinzip der Erforderlichkeit. Ziel von Datenverarbeitungssystemen soll sein, keine oder möglichst wenige personenbezogene Daten zu erheben. Sie sollen insbesondere von Anonymisierung und Pseudonymisierung Gebrauch machen. So sollten RFID-Systeme in der Entwicklung datenschutzfreundlich ausgelegt werden, um Gefährdungen der informationellen Selbstbestimmung vorzubeugen.

### ***Die Phasen des Datenumgangs nach §3 BDSG***

Das Erheben ist das gezielte Beschaffen von Daten über den Betroffenen. Hiermit ist nicht das zufällige Auslesen von anderen Daten gemeint, die nicht dem Ziel dienen, z.B. wenn der Reader mehr Tags im Umfeld erfasst als gewollt. Diese Daten dürfen dann jedoch nicht weiterverwendet werden und sind unverzüglich zu löschen.

Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Diese Begriffe sind im Gesetzestext definiert. Speichern ist das Erfassen, Aufnehmen oder Aufbewahren dieser Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung. Verändern ist das inhaltliche Umgestalten gespeicherter personenbezogener Daten. Das Herausnehmen aus dem Zusammenhang und die Verfälschung und Berichtigung sind hierbei schon ein inhaltliches Umgestalten. Übermitteln ist das Bekanntgeben personenbezogener Daten an einen Dritten. Sperren ist das Kennzeichnen gespeicherter personenbezogener Daten, um ihre Verarbeitung oder Nutzung einzuschränken. Löschen ist das Unkenntlichmachen dieser Daten. Das Löschen ist das Ende der Verarbeitung. Beim Löschen dürfen die Daten nicht rekonstruierbar sein, so wie beim Deaktivieren eines RFID-Tags. Nutzen ist jede Verwen-

dung personenbezogener Daten (§3 Abs. 5 BDSG), wenn sie nicht zur Verarbeitung zählt.

### ***Sondervorschriften für mobile Speichermedien nach §6c Abs. 1 BDSG***

Mobile Speichermedien sind Datenträger, auf denen personenbezogene Daten nicht nur gespeichert werden können, sondern auch automatisiert durch die erhebenden oder weiteren Stellen weiterverarbeitet werden können. Der Betroffene kann diese Verarbeitung nur über den Gebrauch des mobilen Speichermediums beeinflussen. Besondere Unterrichtungspflichten im Rahmen des Transparenzgebots bestehen, weil dem Betroffenen die Kontrolle aufgrund der fehlenden Schnittstelle zwischen Mensch und Gerät entzogen wird. Der Unternehmer muss dem Kunden seine Identität und Anschrift mitteilen und ihn über die Funktionsweise des Mediums verständlich aufklären. Weiterhin muss er den Kunden informieren, wie er seine Rechte auf Auskunft und Korrektur unter den Umständen der mobilen Technologie ausüben kann. Betroffen sind meist nur Anwendungen, bei denen personenbezogene Daten direkt auf dem Tag gespeichert werden.

Bei den Transpondern selbst wird unterschieden, ob eine über die Speicherung hinausgehende automatisierte Weiterverarbeitung erfolgen kann. Dies ist am oberen Ende des Segments der Fall. Am unteren Ende des Segments der Transponder können auf diesen keine Daten zusätzlich gespeichert oder gar weiterverarbeitet werden. Das mittlere Segment ist zu prüfen. Bei dauerhaften und unveränderlichen Speicherungen wie auf ROM-Speichern findet §6c BDSG keine Anwendung. Dies ist vor allem im Handel beim Einsatz von passiven RFID-Tags der Fall. Hier ist nur der EPC gespeichert. Read-Write Systeme dagegen eröffnen die Möglichkeiten eine automatisierte Weiterverarbeitung der Daten und daher findet §6c BDSG hier Anwendung.

### **Konsequenzen für Unternehmen und Privatpersonen**

#### ***Rechtlicher Schutz für Unternehmen und Privatpersonen***

Unternehmen sind grundsätzlich vor unberechtigtem Umgang oder Weiterverarbeitung interner Daten durch konkurrierende Firmen zu schützen. Generell bietet eine umfangreiche Datensicherheit die beste Grundlage zur Wahrung von Unternehmensgeheimnissen. Firmeninterne Produktdaten (z.B. Herstelldatum, Name des Bearbeiters) können in diesem Zusammenhang auch als personenbezogene Daten aufgefasst werden. Somit gilt hierfür der gleiche rechtliche Schutz wie für Privatpersonen (zu Rechtlicher Schutz für Privatpersonen).

Oberste Maxime des Datenschutzes ist die Wahrung des Persönlichkeitsrechts. „Zweck dieses Gesetzes ist es, das Individuum davor zu schützen,

dass es durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird." (§ 1 Abs. 1, BDSG). Ein Eingriff in die Privatsphäre ist grundsätzlich bei automatischer Verarbeitung der personenbezogenen Daten möglich, sei es durch Erhebung, Verarbeitung oder Nutzung.

Verbraucher bzw. Personen, die mit automatisierter Datenverarbeitung in Kontakt kommen, haben grundsätzlich das Recht, selbst darüber zu bestimmen, an wen und zu welchem Zweck sie persönliche Daten weitergeben möchten. Ein wichtiger Grundsatz des BDSG stellt die Einwilligungspflicht des Betroffenen dar (§4 BDSG). Der Betroffene muss nicht nur der Datenerhebung zustimmen, sondern „dem Betroffenen ist auf Antrag Auskunft zu erteilen über Zweck, Empfänger und über die gespeicherten Daten" (§19 BDSG).

### ***Rechtliche Vorgaben für Unternehmen***

Unternehmen, die RFID-Systeme im Einsatz haben oder ihre Produkte mit RFID-Tags ausstatten, müssen auch die rechtlichen Vorgaben des Datenschutzes beachten. Unter dem Prinzip der Selbstverpflichtung sind sie angehalten, das allgemeine Persönlichkeitsrecht zu wahren (§1 Abs. 1 BDSG). Das Bundesdatenschutzgesetz stellt auch hierzu die Rechtsgrundlage dar. Nur im Rahmen der Einhaltung des allgemeinen Persönlichkeitsrechts und mit der Einwilligung des Betroffenen ist eine Datenerhebung rechtlich abgesichert (§4 BDSG).

Ebenso regelt das BDSG

- Gebot der Datenvermeidung und der Datensparsamkeit (§3 BDSG) - Der Anbieter ist angehalten „keine oder so wenig personenbezogene Daten wie möglich" zu verarbeiten
- Meldepflicht (§4d BDSG) - Grundsätzlich sind Systeme mit automatisierter Datenverarbeitung meldepflichtig
- Datengeheimnis (§5 BDSG) - Es ist verboten, personenbezogene Daten unbefugt zu erheben
- Schadensersatz (§7 BDSG) - Der Anwender eines automatisierten Datenverarbeitungssystems ist verpflichtet, dem Betroffenen bei unbefugtem Umgang mit personenbezogenen Daten, Schadensersatz zu leisten
- Datenverarbeitung (§14 BDSG) - Die Datenverarbeitung seitens eines Anwenders ist zulässig, wenn sie der Aufgabe und dem Zweck der verantwortlichen Stelle dienen

Neben den allgemeinen Vorschriften gelten für Privatunternehmen, sogenannte nicht-öffentliche Stellen, Zusatzvorschriften für die interne Datenverarbeitung. Die Datenerhebung bzw. -verarbeitung muss einerseits einem benannten, auch im Vertragsverhältnis vereinbarten Zweck dienen und andererseits müssen diese Daten auch allgemein zugänglich sein

(§28 BDSG). Weiterhin dürfen Unternehmen personenbezogene Daten erheben bzw. nutzen, wenn das Interesse des Betroffenen nicht offensichtlich das Interesse der verantwortlichen Stelle überwiegt.

Zusätzlich zur Zweckbestimmung der Datenerhebung ist es Unternehmen erlaubt, unter den Voraussetzungen des §29 BDSG geschäftsmäßig Daten zu erheben und zu speichern, um sie zu übermitteln. Dies betrifft insbesondere Tätigkeiten, die der Werbung oder Markt- und Meinungsforschungen dienen. Weiterhin dürfen nicht-öffentliche Stellen Daten in anonymisierter Form übermitteln (§29).

Der Datenschutz spielt innerhalb des Verbraucherschutzes eine wichtige Rolle. Eine Nichteinhaltung des Verbraucherschutzes wirkt sich auch auf das Unternehmen negativ aus, da Schadensersatzansprüche, Sanktionen oder Imageverluste entstehen können.

### **Verstoß gegen datenschutzrechtliche Vorschriften**

Der Verstoß gegen datenschutzrechtliche Vorschriften ist bußgeld- und ggf. strafbewehrt. Nach § 43 Abs. 2 Nr. 1 BDSG ist das vorsätzliche oder fahrlässige unbefugte Erheben oder Verarbeiten personenbezogener Daten, die nicht allgemein zugänglich sind, eine Ordnungswidrigkeit und kann mit einer Geldbuße von bis zu 250.000 € geahndet werden. Wird eine Handlung nach § 43 Abs. 2 Nr. 1 BDSG gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begangen, handelt es sich gem. § 44 Abs. 1 StGB um eine Straftat, die mit Freiheitsstrafe von bis zu zwei Jahren oder mit Geldstrafe bestraft werden kann.

## 5. Stand der Diskussion - Expertenmeinungen

Daten- und Verbraucherschutz sind für den erfolgreichen Einsatz von RFID von hoher Bedeutung und stellen einen wichtigen Akzeptanzfaktor für einen zukünftigen Einsatz der Technologie, insbesondere im Endverbraucherbereich dar. Die aktuelle Diskussion zum Thema RFID und Datenschutz könnte ein wichtiger Schritt hin zu mehr Akzeptanz und Transparenz sein. Experten aus Wissenschaft und Praxis sind sich darüber einig, dass die Diskussion über das Thema Datenschutz sachgerecht und konstruktiv geführt werden sollte, damit das Potenzial in Entwicklung, Produktion und Anwendung der RFID-Technologie voll ausgeschöpft werden kann. Die folgenden Ausführungen basieren auf Statements, Einschätzungen und Handlungsempfehlungen ausgewiesener Experten aus dem RFID-Umfeld, die im Rahmen dieser Studie befragt wurden.

Dr. Kai Kuhlmann, Bereichsleiter Electronic Business-Recht beim Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. - BITKOM hält im Rahmen einer sachlichen Diskussion zum Thema Datenschutz vor allem die Betrachtung der bestehenden gesetzlichen Regelungen für zentral: "Zum einen muss beachtet werden, welchen Schutz das Bundesdatenschutzgesetz schon jetzt bietet. In der gegenwärtigen Diskussion unterbleibt dieser Abgleich von Forderungen nach Datenschutz mit dem gesetzlichen Status Quo bedauerlicherweise häufig. Übersehen wird dadurch, dass in vielen Konstellationen das Bundesdatenschutzgesetz, aber auch das Telekommunikationsgesetz oder das Strafgesetzbuch Anwendung finden und ein differenziertes und effektives Regelungsgefüge bieten." Die Aufstellung von Forderungen ohne die Einordnung in das bestehende Regelungsgefüge erwecke den unzutreffenden Eindruck, dass sich RFID-Anwendungen in einem rechtsfreien Raum bewegen. Die Diskussion über einen etwaigen Ergänzungsbedarf der bestehenden Regelungen werde dadurch erheblich erschwert.

Für den Schutz personenbezogener Daten existiert nach Auffassung des BITKOM in Deutschland ein klares und bewährtes Regelwerk. Demnach sind die Instrumente des Bundesdatenschutzgesetzes auf RFID anwendbar und bieten einen effektiven Schutz gegen unbefugte Datenverarbeitung. Der technologieneutrale Regelungsansatz der Richtlinie 95/46/EG und des Bundesdatenschutzgesetzes (BDSG) bewähre sich bei RFID, so Kai Kuhlmann. Um den häufig geäußerten Bedenken gleichwohl Rechnung zu tragen, existierten bereits mehrere Selbstverpflichtungserklärungen und Richtlinien von Wirtschaftsorganisationen, die Grundregeln für den Einsatz der RFID -Technologie (auch im Bereich nicht-personenbezogener Daten) regeln. "Diese Regeln werden sukzessive der Entwicklung der Technologie angepasst. Für ein Eingreifen des Gesetzgebers besteht nach alledem kein Bedarf" erläutert Kuhlmann.

Prof. Dr. Bernd Holznagel, Leiter des ITM Institut für Informations-, Telekommunikations- und Medienrecht an der Universität Münster verdeutlicht, dass die allgemeinen Grundsätze des Bundesdatenschutzgesetzes (BDSG) bei der Entwicklung, der Einführung und der Verwendung von RFID-Technologien berücksichtigt werden müssen. So sei nach dem Grundsatz der Datensparsamkeit das Erheben von Daten nicht erlaubt, wenn das gleiche Ziel ohne die Erhebung personenbezogener Daten erreicht werden kann. Auch die übrigen Datenschutzgrundsätze, wie z. B. der strikte Zweckbindungsgrundsatz und die Löschungspflicht, seien einzuhalten. Auch Prof. Holznagel stellt klar, dass das BDSG, soweit derzeit absehbar, keine Lücken in Bezug auf die RFID-Technologie aufweist und betont: "Entscheidender Faktor für die Akzeptanz bei Verbrauchern ist und bleibt eine größtmögliche Transparenz der Datenverwendung. Werden personenbezogene Daten erhoben und verarbeitet, muss offengelegt und für die Betroffenen erkennbar sein, für welchen Zweck diese Daten bei wem gespeichert sind." Darüber hinaus sei es sinnvoll, auch Objekte zu kennzeichnen, die mit RFID-Tags versehen sind, auch wenn keine personenbezogenen Daten verarbeitet werden sollen. "Nicht das Rechtssystem muss sich dem technologischen Fortschritt anpassen, sondern der technologische Fortschritt muss sich unumgänglichen gesetzlichen Schutznormen unterwerfen, um RFID als Standard-Technologie der Zukunft annehmen zu können", so Prof. Holznagel.

Nach Auffassung der Gesellschaft für Datenschutz und Datensicherung e. V. (GDD) in Bonn ist es nicht sinnvoll, bei jeder neuen Technologie wie z.B. RFID nach gesetzlichen Regelungen zu rufen. Potenzielle Gefahren für die Persönlichkeitsrechte im Rahmen der Anwendung von RFID-Technologien gingen in erster Linie von den nachgelagerten Systemen, deren Vernetzung und der Aufbereitung der erfassten Daten und nicht von der Technologie selbst aus. So plädiert die GDD dafür, das gesamte Datenschutzrecht in Hinblick darauf zu überprüfen, ob es den neuen gesellschaftlichen und technologischen Herausforderungen noch adäquat gewachsen ist. Kernelemente eines modernen Datenschutzrechts sollten demnach der Systemdatenschutz sein, welcher die Wirtschaft verpflichtet, neue Technologien und Verfahren à priori datenschutzfreundlich zu gestalten, sowie der Selbstdatenschutz, der den informierten Menschen voraussetzt und ihm Mittel und Wege aufzeigt, wie er sich selbst vor missbräuchlicher Verarbeitung seiner Daten schützen kann. Im Hinblick auf die RFID-Technologie setzt sich die GDD für angemessene Selbstverpflichtungen der Wirtschaft ein, die einerseits die Prinzipien des Systemdatenschutzes berücksichtigen und andererseits für eine umfassende Aufklärung der betroffenen Nutzer Sorge tragen.

Die GS1 Germany GmbH, bekannt als Dienstleistungs- und Kompetenzzentrum für unternehmensübergreifende Geschäftsabläufe in der deutschen Konsumgüterwirtschaft und ihren angrenzenden Wirtschaftsbereichen ist der Überzeugung, dass die Akzeptanz der RFID-Technologie

durch den Verbraucher der Schlüssel für eine erfolgreiche Einführung und Nutzung von RFID sein wird. Daher sei es erforderlich, dass die Verbraucher über die Technologie und Anwendungen informiert sein müssen.

EPCglobal, eine von Unternehmen getragene internationale Organisation für Standardisierung im Bereich RFID, GS1 Germany und die durch GS1 Germany vertretenen Wirtschaftsbereiche treten für einen datenschutzkonformen Umgang mit RFID ein. In einem ersten Schritt wurden von EPCglobal daher auf internationaler Ebene Richtlinien zur Verwendung des EPC bei Konsumgütern verabschiedet und veröffentlicht ([http://www.epcglobalinc.org/public/ppsc\\_guide/](http://www.epcglobalinc.org/public/ppsc_guide/)). Diese Richtlinien sind Teil der EPCglobal-Umsetzungsbedingungen von EPC/RFID und gelten für alle EPCglobal-Mitglieder. Darüber hinaus haben GS1 Germany und seine Anwenderunternehmen aus Industrie, Dienstleistung und Handel ein nationales Positionspapier vorgelegt, das Grundsätze zum Umgang mit der RFID-Technologie in Anwendungsbereichen mit einem mittelbaren oder unmittelbaren Verbraucherbezug enthält ([http://www.gs1-germany.de/content/e39/e466/e468/datei/epc\\_rfid/daten\\_verbraucherschutz.pdf](http://www.gs1-germany.de/content/e39/e466/e468/datei/epc_rfid/daten_verbraucherschutz.pdf)). In einzelnen Punkten geht die Wirtschaft darin bereits über die nach dem geltenden Datenschutzrecht bestehenden Verpflichtungen hinaus:

Laut GS1 kann die RFID-Technologie ihre Stärken in der Waren- und Objekterkennung in offenen unternehmensübergreifenden Anwendungsbereichen ausspielen. Insbesondere innerhalb der unternehmensübergreifenden Logistik gelinge mit RFID eine effizientere Steuerung der Waren- und Materialflüsse. Den Schlüssel hierfür bilde der sogenannte Elektronische Produkt-Code (EPC) als weltweit gültiger branchenübergreifender Standard. Demnach beinhalte der EPC sowohl technische Spezifikationen, etwa Codierverfahren, als auch Nummerierungssysteme wie die EAN-Artikelnummer oder die Nummer zur Packstückidentifikation. Ein EPC-Transponder wird laut GS1 Germany nur zur Speicherung von objektbezogenen Informationen verwendet, die datenschutzrechtlich nicht relevant sind. Die Speicherung personenbezogener Daten seien nicht vorgesehen.

Dennoch besteht bei vielen Verbrauchern die Sorge, dass sie zum so genannten „gläsernen Kunden“ werden könnten. Nach Auffassung von Mirko Auerbach vom Forschungsinstitut für Rationalisierung (FIR) sind diese im Grunde genommen aber unbegründet und sind insbesondere auf die Unkenntnis der technischen Möglichkeiten und der rechtlichen Rahmenbedingungen zurückzuführen. Auch aus Sicht des BITKOM ist offenbar festzustellen, dass sich sowohl die öffentliche als auch die fachliche Diskussion zum Thema RFID und Datenschutz oft auf unzutreffende technische Annahmen und unrealistische Missbrauchsszenarien stützt. Eine Versachlichung sei daher erforderlich.

Dr. Kai Kuhlmann erläutert weiter: "Bei der datenschutzrechtlichen Bewertung von RFID muss beachtet werden, dass RFID eine Basistechnologie für eine Vielzahl von Anwendungen ist. Eine pauschale Bewertung der Technologie verbietet sich auf Grund der Vielfalt der auf RFID basierenden Anwendungen. Relevant für die datenschutzrechtliche Betrachtung kann immer nur die einzelne Anwendung sein und die Art der Daten, die durch sie verarbeitet werden".

Eine zentrale Frage ist die, welchen Stellenwert der Datenschutz bei den Unternehmen einnimmt, die sich bereits mit der Realisierung von RFID-Projekten beschäftigen. Mirko Auerbach vom FIR in Aachen hat in diesem Zusammenhang festgestellt, dass viele Unternehmen im Bekleidungseinzelhandel – der häufig als Pilotbranche für RFID auf Artelebene genannt wird – noch keine RFID-Projekte durchgeführt haben und Sicherheitsaspekten eine geringe Bedeutung zumessen. Erst wenn tatsächlich Projekte durchgeführt werden, würden Sicherheitsaspekte in den Fokus rücken.

Um den Kunden die Angst zu nehmen, dass Ihre Daten nicht ausreichend geschützt werden, erscheint es notwendig, dass RFID-Anwendungen hinsichtlich Datensicherheit und Datenschutz objektiv überprüft werden können. Um dies zu erreichen, wird im Rahmen des Forschungsprojektes „Trusted-RFID“ ein Vertrauenssiegel entwickelt, das auf objektiven Kriterien beruht und von neutralen Dritten vergeben werden soll. "Verbraucher können so der RFID-Anwendung auf Produktebene vertrauen und der Handel kann diese überprüft anbieten", so Auerbach. Unter der Webadresse [www.trusted-rfid.de](http://www.trusted-rfid.de) finden sich Informationen zum Projekt und zu zwei bundesweit durchgeführten Studien im Bekleidungseinzelhandel und bei Verbrauchern.

In der allgemeinen Diskussion um RFID und Datenschutz stehen vor allem die Aktivitäten und Projekte von Handelsunternehmen in der Kritik. Das Informationsforum RFID gibt in diesem Zusammenhang zu bedenken, dass der Handel nicht die einzige Branche ist, bei der die Möglichkeit besteht, dass Transponder bis zum Endverbraucher gelangen und empfiehlt: "Wird die RFID-Technologie nicht nur in geschlossenen Kreisläufen eingesetzt, sollten Unternehmen prüfen, inwieweit Informationen über den RFID-Einsatz auch bei ihren Produkten notwendig sind. Selbst wenn der Transponder keine Funktion mehr besitzt, kann es nötig sein, auf ihn hinzuweisen, denn fehlende Informationen können das Kundenvertrauen beschädigen."

Das Informationsforum RFID sieht in der Aufklärung einen wichtigen Baustein des Verbraucherschutzes. Mit der Webseite [www.rfidabc.de](http://www.rfidabc.de) stellt die Organisation die Möglichkeit bereit, sich auf leicht verständliche Weise über die Technologie zu informieren. Zudem unterstützt das Informationsforum den Dialog zwischen Handel und Verbraucherschützern zur Erarbei-

tung einer Selbstverpflichtung. Diese soll dem Handel klare Richtlinien bieten und dem Verbraucher eine erhöhte Vertrauenswürdigkeit bieten.

Um Vertrauen bei Verbrauchern aber auch bei Geschäftspartnern aufzubauen, stehen Anbietern und Anwendern der Radiofrequenztechnologie mittlerweile vielfältige Möglichkeiten zur Verfügung. Prof. Dr.-Ing. Ingo Wolff, Geschäftsführer der IMST GmbH in Kamp-Lintfort macht deutlich, dass mit Hilfe so genannter Datenschutztechnologien (privacy enhancing technologies, PET) die Belange des Datenschutzes durch technische Maßnahmen berücksichtigt werden können. Hierzu zählen beispielsweise die Deaktivierung von Transpondern durch abziehbare Antennen sowie Software-Ansätze oder elektrotechnische Ansätze, die ein unerwünschtes Auslesen blockieren („blocker tags“). Außerdem seien etablierte Verschlüsselungstechnologien und abhörsichere Protokolle für die Datenübertragung wirkungsvolle Möglichkeiten, Vertrauen zu schaffen.

Trotz des bereits breiten Einsatzes sieht Prof. Wolff noch erhebliches Innovationspotenzial, wie die Entwicklung von Funkchips mit Polymer- und hybriden Technologien, die Integration von Sensortechnologie oder Softwareaufgaben wie Kommunikationsprotokolle und Sicherheitsmaßnahmen gegen den Missbrauch von RFID. Um dieses Innovationspotenzial für die deutsche Wirtschaft nutzbar zu machen, empfiehlt Prof. Wolf: "Insbesondere unter dem Gesichtspunkt, dass bei vielen RFID-Anwendungen keine Daten mit Personenbezug entstehen, muss die kritische Diskussion über den Schutz der personenbezogenen Daten durch rechtsfeste, einwandfreie Regelungen bzw. technische Lösungen beendet werden. Nur so kann diese Technik flächendeckend eingesetzt und das enorme Potenzial in Entwicklung, Produktion und Anwendung der RFID-Technologie ausgeschöpft werden."

Neben dem Datenschutz spielt auch das Thema Datensicherheit bei der Umsetzung intelligenter RFID-Anwendungen eine wichtige Rolle. Gerade im Bereich der elektronischen Geschäftsprozesse ist die RFID-Technologie nicht mehr wegzudenken. Thomas Faber, Leiter der Landesinitiative "secure-it.nrw", hält es daher für umso wichtiger, wirkungsvolle Schutzmaßnahmen für diese neuen „Lebensadern“ vieler Unternehmen bereitzustellen, denn schließlich müssen alle mit RFID verknüpften Prozesse und Daten ständig verfügbar und sicher vor unberechtigten Zugriffen sein. "In die Sicherheitskonzeption einbezogen werden sollte aber nicht nur die Datensicherheit, sondern immer dann, wenn in Verbindung mit RFID personenbezogene Daten verarbeitet werden, auch Konzepte zum Datenschutz. Erst dann sind die entsprechenden RFID-Anwendungen in besonderem Maße vertrauenswürdig und finden leichter Akzeptanz bei den Nutzern" sagt Faber.

Der Leiter der Landesinitiative ist sich sicher, dass clevere Unternehmen längst erkannt haben, dass sie neue Technologien wie z.B. RFID „ganz-

heitlich“ in ihre unternehmerische IT-Sicherheits-Strategie einbinden müssen. Die Vorteile einer solchen Vorgehensweise liegen für ihn auf der Hand: "Sie erreichen damit nicht nur eine optimal aufeinander abgestimmte IT-Sicherheits-Infrastruktur - die sich auch wesentlich leichter managen lässt als viele Einzellösungen - sondern schaffen damit auch noch enormes Einsparpotenzial, wenn es um Dokumentation oder auch externe Beratung geht. Chancen also, die sich auch der Mittelstand mit Sicherheit nicht entgehen lassen sollte."

Vor dem Hintergrund der vielfältigen Diskussionen um RFID ist nicht zu erwarten, dass schon heute alle Fragen – ob aus technischer Sicht oder der Perspektive des Datenschutzes – vollständig beantwortet werden können. Dies wird nur anhand konkreter Umsetzungen in der Praxis möglich sein. Eine wesentliche Voraussetzung für die Realisierung von RFID-Lösungen im Alltag ist jedoch die Akzeptanz der beteiligten Personengruppen. Ein gemeinsames Ziel der Diskussion sollte sein, ein ausgewogenes Verhältnis herbeizuführen zwischen dem Schutz der Verbraucher und der Flexibilität, die für die Wirtschaft bei Einführung innovativer Technologien unerlässlich ist, um Deutschland im globalen Wettbewerb erfolgreich positionieren zu können.

#### **Befragte Experten und Einrichtungen:**

Mirko Auerbach  
Forschungsinstitut für Rationalisierung (FIR), Aachen

Thomas Faber  
Leiter der Landesinitiative secure-it.nrw

GDD  
Gesellschaft für Datenschutz und Datensicherung e. V. , Bonn

GS1 Germany GmbH, Köln

Prof. Dr. Bernd Holznagel  
Leiter des ITM Institut für Informations-, Telekommunikations- und Medienrecht an der Universität Münster

Informationsforum RFID e.V., Berlin

Dr. Kai Kuhlmann  
Bereichsleiter Electronic Business-Recht beim Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. - BITKOM, Berlin

Prof. Dr.-Ing. Ingo Wolff  
Geschäftsführer der IMST GmbH, Kamp-Lintfort

## 6. Umfrage-Ergebnisse

Im Rahmen der vorliegenden Studie wurde eine Online-Befragung bei über 700 Unternehmen und Einrichtungen durchgeführt. Zu den Befragten zählen u.a. Unternehmen aus dem Umfeld der RFID-Branche, potenzielle Anwender sowie Experten öffentlicher und wissenschaftlicher Einrichtungen. Eine hohe Beteiligungsquote von rund 23 Prozent bildet die Basis für die im Folgenden dargestellten Ergebnisse.

### **RFID ist nicht nur Thema für die "Großen"**

Die Tatsache, dass sich zahlreiche kleine und mittelständische Unternehmen an der bundesweiten Befragung beteiligt haben zeigt, dass RFID durchaus ein Thema für den Mittelstand ist. 67 Prozent der antwortenden Unternehmen beschäftigen weniger als 250 Mitarbeiter und rund ein Viertel der Beteiligten beschäftigen lediglich bis zu zehn Mitarbeiter. 27 Prozent dagegen zählen zu den großen Unternehmen mit mehr als 250 Mitarbeitern. Dass die Nutzung der Technologie immer auch unter dem Aspekt der Globalisierung zu betrachten ist, zeigt insbesondere die Beantwortung der Frage nach dem Standort der Organisationen: Immerhin neun Prozent der Unternehmen stammen aus dem europäischen Ausland und sechs Prozent haben ihren Sitz sogar außerhalb Europas. Die besondere Rolle des Standorts Nordrhein-Westfalen im Bereich der RFID-Aktivitäten bestätigt sich einmal mehr darin, dass 39 Prozent der an der Umfrage beteiligten Unternehmen ihren Standort in NRW haben.

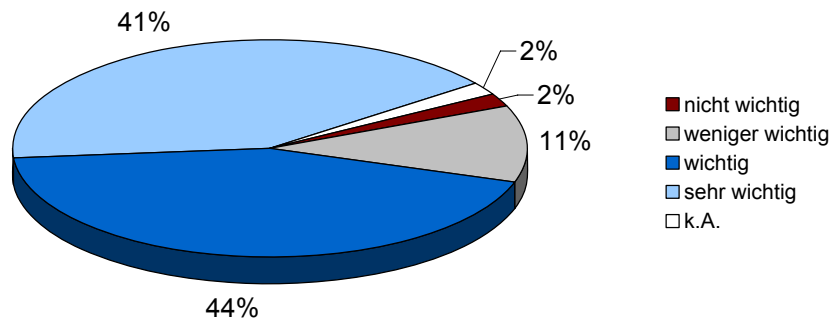
### **Anwendungen in der Logistik bilden einen Schwerpunkt**

14 Prozent der Unternehmen sind Anwender der Technologie aus den verschiedensten Branchen. Neben den Bereichen Automotive, E-Healthcare und Medizin sowie Geoinformation sind insbesondere Anwendungsfelder aus der Logistik wie Lagerhaltung, Verpackung, Distribution, Spedition und Warehouse Management ein deutlicher Schwerpunkt. 86 Prozent der Befragten sind den Bereichen RFID-Hard- und Software zuzuordnen. Davon beschäftigen sich 68 Prozent mit vertrieblichen und 57 Prozent mit beratenden Tätigkeiten.

### **Datenschutz ist ein wichtiges Thema**

Die Diskussion um den Datenschutz ist im Zusammenhang mit der Planung und Umsetzung von RFID-Lösungen zu einem festen Bestandteil geworden. Dennoch gibt es unterschiedliche Auffassungen darüber, welchen Stellenwert der Datenschutz in Verbindung mit RFID generell hat. Insgesamt 85 Prozent der Befragten halten den Datenschutz für wichtig bzw. sehr wichtig. 11 Prozent schätzen das Thema als weniger wichtig ein und lediglich zwei Prozent betrachten den Schutz der Daten in diesem Zusammenhang als nicht wichtig.

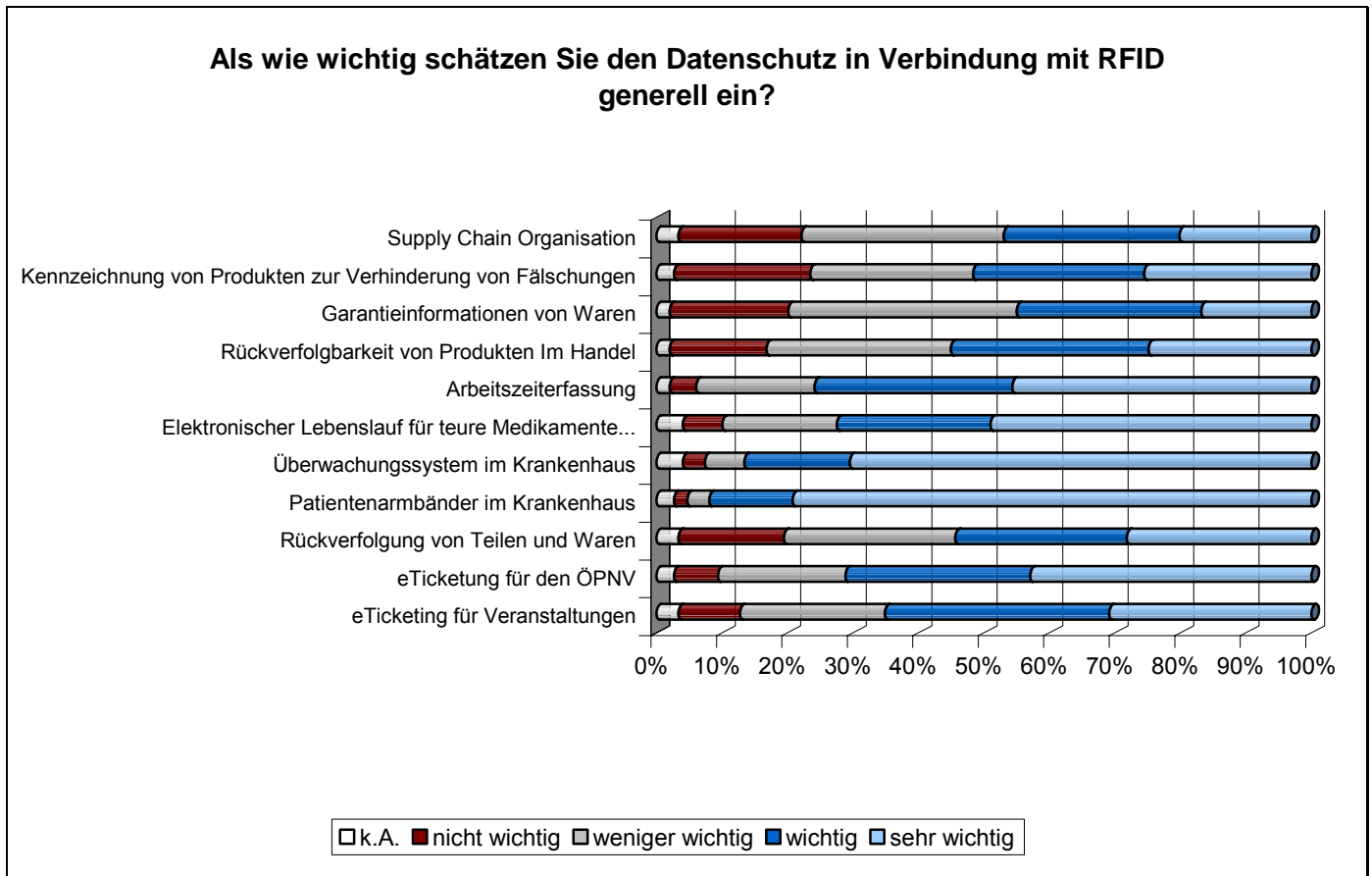
**Als wie wichtig schätzen Sie das Thema Datenschutz in Verbindung mit RFID generell ein?**



Bei der Frage nach der Relevanz des Datenschutzes im Hinblick auf die jeweiligen Anwendungsbereiche ergab sich ein deutlicher Schwerpunkt bei Anwendungen im Gesundheitswesen. Insgesamt 79 Prozent der Unternehmen halten den Datenschutz im Zusammenhang mit durch Transponder versehene Patientenarmbänder im Krankenhaus für sehr wichtig, weitere 13 Prozent für wichtig. Diese Ergebnisse gewinnen noch an Bedeutung, wenn man sie vor dem Hintergrund der positiven Markteinschätzungen für den Bereich Gesundheitswesen berücksichtigt. Glaubt man den Prognosen von IDTechEX, so werden die Ausgaben in dieser Branche von ca. 90 Millionen Dollar im Jahr 2006 auf ca. 2,1 Milliarden Dollar im Jahr 2016 steigen. Dieses starke Wachstum ist nicht zuletzt darauf zurück zu führen, dass das Gesundheitswesen ein Gebiet ist, in dem die RFID-Technologie in sehr vielen ganz unterschiedlichen Bereichen angewendet werden kann. Von der Identifizierung und Authentifizierung von Patienten über die Lokalisierung von medizinischen Geräten und eine Workflow-Optimierung im Sinne einer automatischen Übermittlung von Patientendaten, bis hin zur automatischen Überwachung von Messdaten wie Blutdruck oder Blutzucker gibt es zahlreiche Einsatzmöglichkeiten für RFID im Gesundheitswesen.

Anwender der Technologie tun gut daran, wenn sie den Datenschutz im Rahmen der zuvor genannten Lösungen entsprechend berücksichtigen. Der Umfrage zufolge halten insgesamt 70 Prozent der Befragten den Schutz der Patientendaten beim Einsatz von Überwachungssystemen im Krankenhaus, mit Hilfe derer zum Beispiel der Aufenthaltsort von Demenz-

Patienten beobachtet werden kann, für sehr wichtig und 16 Prozent für wichtig.

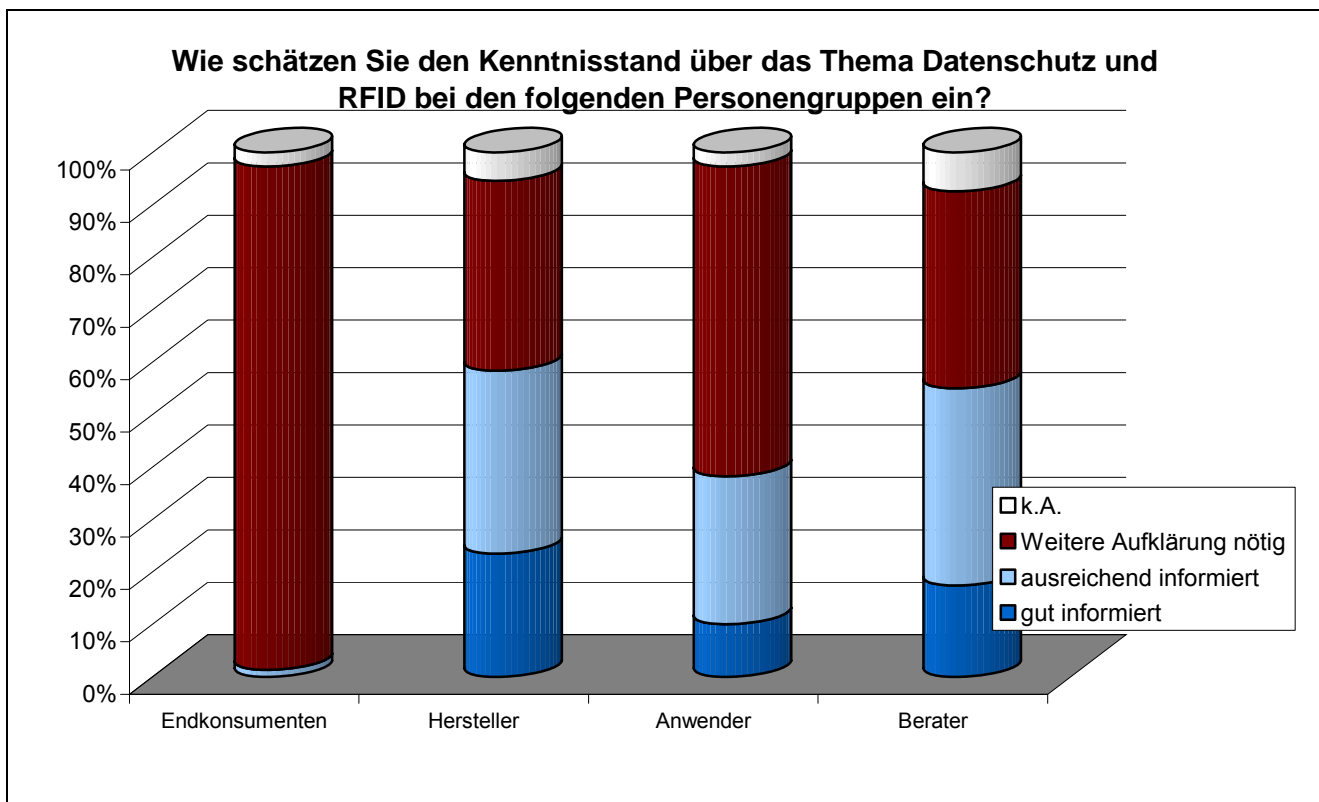


Neben Anwendungen aus dem Gesundheitswesen sind es vor allem Arbeitszeiterfassungssysteme für Mitarbeiter sowie die Nutzung von RFID-gestützten Ticketing-Systemen für Veranstaltungen sowie im ÖPNV, für die nach Meinung der befragten Personen der Schutz der verwendeten Daten sehr wichtig ist.

### Noch kein ausreichender Kenntnisstand

Ein Aspekt, der im Rahmen der allgemeinen Diskussion um den Datenschutz häufig beklagt wird ist der, dass häufig die Unkenntnis der technischen Möglichkeiten sowie der rechtlichen Rahmenbedingungen zu unsachlichen Argumenten und falschen Annahmen führe.

Die Einschätzung der Befragten nach dem Kenntnisstand über das Thema Datenschutz und RFID spiegeln dies wieder:

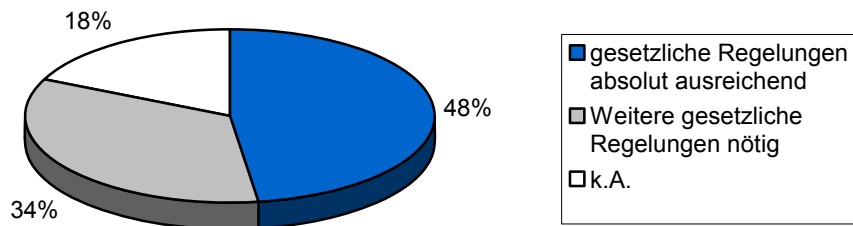


96 Prozent der befragten Personen halten es für notwendig, weitere Aufklärungsarbeit für Endkonsumenten zu leisten und 59 Prozent sind der Meinung, dass dies auch für Anwender der Technologie notwendig sei. 23,5 Prozent halten die Hersteller der Technologie für gut informiert und gut ein Drittel schätzen sie immerhin als ausreichend informiert ein. Bei beratenden Unternehmen zeigt sich ein etwas anderes Bild: 37,5 Prozent dieser Unternehmen wird nicht zugetraut, ausreichend mit dem Thema Datenschutz vertraut zu sein. In Ergänzung hierzu wurde von mehreren an der Umfrage Beteiligten geäußert, dass auch bei Politikern, Gesetzgebern sowie den Medien Aufklärung über den Datenschutz notwendig sei. 43,6 Prozent halten es dabei für dringend notwendig, dass eine verstärkte Aufklärung über RFID und speziell über das Thema Datenschutz stattfindet.

### **Ist die vorhandene Rechtslage ausreichend?**

Der Einsatz von RFID-Technologie bietet zwar vielfältige Vorteile, birgt jedoch im selben Maß datenschutzrechtliche Risiken. Für RFID-Tags gelten – wie für alle Technologien und Anwendungen – die allgemeinen Grundsätze des Bundesdatenschutzgesetzes (BDSG). Diese müssen bei der Entwicklung, der Einführung und der Verwendung von RFID-Technologien berücksichtigt werden.

**Wie schätzen Sie die geltende Rechtslage zum Datenschutz in Bezug auf die Technologie ein?**

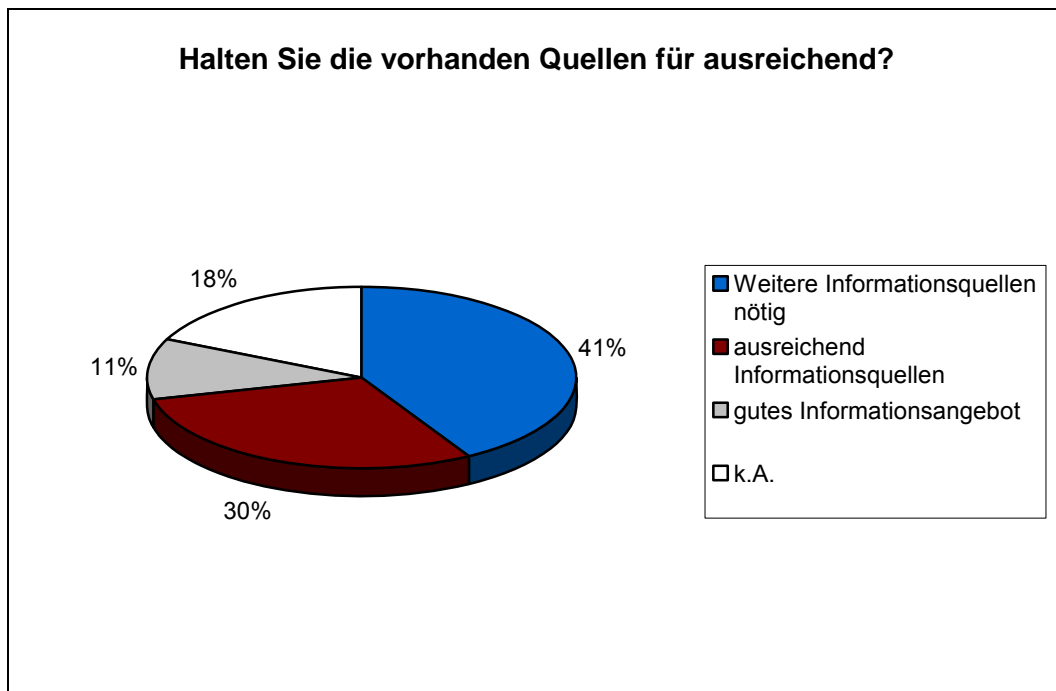


Die Ergebnisse zu der Frage, wie die geltende Rechtslage zum Datenschutz in Bezug auf die Technologie betrachtet werde, zeigen sich zwei Meinungslager. Den 48 Prozent, die die gesetzlichen Regelungen für absolut ausreichend halten, stehen 34 Prozent gegenüber, die weitere gesetzliche Regelungen für nötig halten. Im Übrigen haben 18 Prozent der Beteiligten zu dieser Frage keine Angaben gemacht.

**Hochwertige Informationsquellen sind verfügbar**

Über die Thematik RFID und Datenschutz sind in der Vergangenheit verschiedene Studien, Leitfäden und Orientierungshilfen veröffentlicht worden, die eine breite Informationsbasis bieten. Aber kennen die Akteure aus dem RFID-Umfeld dieses Informationsangebot überhaupt? Um das herauszufinden wurde im Rahmen der Befragung der Kenntnisstand über fünf einschlägige Informationsquellen abgefragt. Rund die Hälfte der befragten Personen kennt die Studie "Risiken und Chancen des Einsatzes von RFID-Systemen", die das Bundesamt für Informationssicherheit (BSI) im Jahr 2004 herausgegeben hat. Der Leitfaden "RFID und Datenschutz" der Eicar Task Force RFID ist 37,5 Prozent der Teilnehmer bekannt. Die in 2007 erschienene und vom Bundesministerium für Bildung und Forschung geförderte Studie "Technologieintegrierte Datensicherheit bei RFID-Systemen" ist einem knappen Viertel der Beteiligten ein Begriff. Einen Bekanntheitsgrad von 16 Prozent kann das Rechtsgutachten "Rechtliche Dimensionen der Radiofrequenz-Identifikation" verzeichnen, das vom Informationsforum RFID in Berlin veröffentlicht wurde. Den gleichen Wert erreichte die Orientierungshilfe des Arbeitskreises Technische und organisatorische Datenschutzfragen mit dem Titel "Datenschutzgerechter Einsatz von RFID", die im Rahmen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet wurde.

Es bleibt festzuhalten, dass hochwertige Informationsquellen über Datenschutz und RFID - meist kostenlos - verfügbar sind, aber noch nicht alle der genannten Informationsquellen ausreichend bekannt sind. Eine Auflistung zu den genannten Veröffentlichungen mit Download-Hinweisen wird auf Seite 35 zur Verfügung gestellt. 41 Prozent der Befragten waren allerdings der Meinung, dass noch weitere Informationsquellen nötig sind, um sich über das Thema informieren zu können.

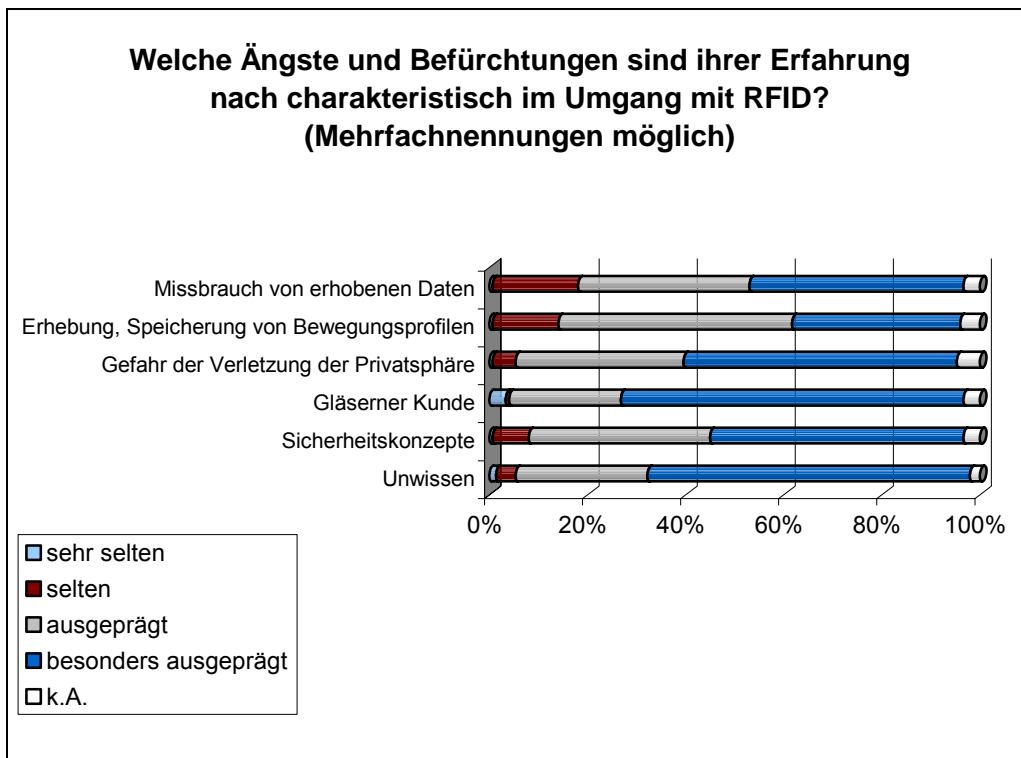


### Ängste vor RFID

Experten und Praktiker sind sich darüber einig, dass in weiten Teilen der Gesellschaft Ängste und Skepsis gegenüber der Radiofrequenz-Identifikation bestehen. Ein häufig genannter Grund dafür ist die unzureichende Auseinandersetzung mit der Technologie. Um herauszufinden, an welcher Stelle angesetzt werden muss, um diese Ängste zu beseitigen wurde in der Umfrage ermittelt, welche Ängste und Befürchtungen charakteristisch im Umgang mit RFID sind.

Als besonders ausgeprägt bezeichnen 70 Prozent der Teilnehmer der Befragung die Angst der Konsumenten, zum "gläsernen Kunden" zu werden, zum Beispiel durch die Erhebung und Speicherung von Kaufverhaltensprofilen. Diese Angst ist vor dem Hintergrund der allgemeinen Diskussion über das Thema Datenschutz nicht verwunderlich. Sie ist nach Meinung von 66 Prozent der Befragten vor allem darin begründet, dass kaum jemand weiß, welche personenbezogenen Daten überhaupt gespeichert werden und wer

einen Zugriff darauf hat. Eine weitere große Befürchtung ist nach Einschätzung der Befragten die Gefahr einer Verletzung der Privatsphäre durch die Erfassung personenbezogener Daten. Einen Datenmissbrauch, der etwa dadurch entsteht, dass die erfassten Daten nach der Nutzung nicht wieder gelöscht werden, sehen 43,6 Prozent als sehr charakteristisch für die Entstehung von Ängsten. Immerhin hält aber auch ein Teil der Personen (17,5 Prozent) diese Befürchtungen für selten.



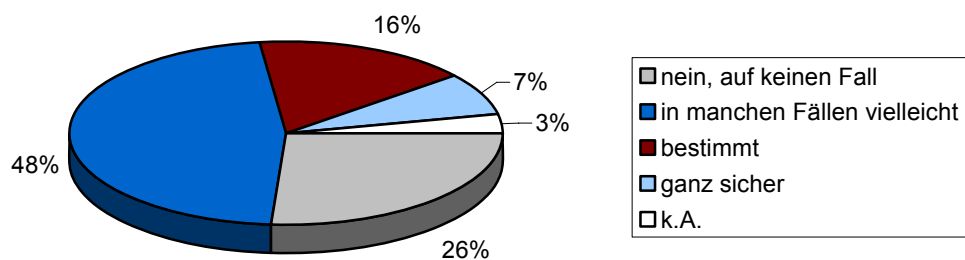
Zum Abbau der zuvor genannten Ängste können verschiedene Maßnahmen durchgeführt werden. Darüber waren sich auch die Teilnehmer an der Umfrage relativ einig und hielten es beispielsweise für wichtig bzw. sehr wichtig, dass innerhalb von Unternehmen eine umfassende Aufklärung von Mitarbeitern und Kunden erfolgt, wenn RFID-Technologie zum Einsatz kommt. Weitere wichtige Maßnahmen sind der Befragung zu Folge die Schaffung möglichst großer Transparenz bezüglich der erhobenen Daten und deren Speicherung sowie die Erarbeitung vertrauensbildender Maßnahmen bei den relevanten Zielgruppen. Hierzu hält ein Großteil der Befragten die Durchführung von Mitarbeiterschulungen für geeignet. Ebenfalls gut bis sehr gut geeignet sei die Kommunikation vorhandener Sicherheitskonzepte sowie Demonstrationen der Funktionsweisen von RFID-Anwendungen.

### Sind datenschutzrechtliche Fragen ein Hindernis für RFID-Projekte?

Die Berücksichtigung datenschutzrechtlicher Aspekte stellt für Unternehmen bei der Einführung von RFID-Lösungen eine gewisse Herausforderung dar. In diesem Zusammenhang erscheint die Frage interessant, ob sie sich hierdurch von ihren Vorhaben abhalten lassen würden. Insgesamt 18 Prozent antworteten, dass dies auf keinen Fall geschehen würde, wohingegen 15 Prozent das „bestimmt für möglich“ hielten. Der überwiegende Teil der Befragten, nämlich 61 Prozent, ist der Überzeugung, dass sich Unternehmen „vielleicht in manchen Fällen“ von ihren Vorhaben zur Einführung der Technologie abhalten lassen, wenn es um die Berücksichtigung datenschutzrechtlicher Fragestellungen geht.

Ob datenschutzrechtliche Fragen im Zusammenhang mit der Realisierung von RFID-Projekten für kleine und mittelständische Unternehmen eher ein Hindernis darstellen würden als für große Unternehmen, war für ein Viertel der Antwortenden klar zu verneinen. Jedoch war sich rund die Hälfte der Befragten in diesem Zusammenhang nicht ganz sicher und gab an, dass dies in manchen Fällen vielleicht möglich sei.

**Denken Sie, dass datenschutzrechtliche Fragen für kleine und mittelständische Unternehmen eher ein Hindernis darstellen als für große Unternehmen?**



## Handlungsempfehlungen der Befragungsteilnehmer

Der letzte Punkt der Befragung bot den Teilnehmern der Online-Umfrage die Gelegenheit, sich in einer offenen Frage darüber zu äußern, welche generellen Handlungsempfehlungen sie in Bezug auf den Datenschutz geben würden, um eine möglichst reibungslose Einführung der Technologie zu gewährleisten. 44 Prozent der Teilnehmer haben diese Möglichkeit genutzt und ihre Empfehlungen eingebracht. Die zentralen Ergebnisse dieser letzten Frage werden im Folgenden vorgestellt.

Ein Hinweis, der in den Ausführungen mehrfach auftauchte war der, dass die Konzeption einer RFID-Anwendung unter Berücksichtigung der unterschiedlichen Interessen und Mitwirkung der betroffenen Unternehmensbereiche stattfinden sollte. In diesem Zusammenhang müsse eine Integration der Anwendungen in die bestehende Security Policy des Unternehmens angestrebt werden und es müssten jeweils firmenspezifische Schutzszenarien geplant und umgesetzt werden. Dabei sei es sinnvoll, die Durchführung relevanter datenschutzrechtlicher Maßnahmen zunächst innerhalb von Pilotprojekten zu verifizieren.

Von Endverbrauchern wurde bei diesen „Handlungsempfehlungen“ darauf hingewiesen, dass die von Unternehmen bereitgestellten Informationen häufig schwierig zu verstehen sind. Es besteht der Wunsch nach einfach verständlichen Texten über RFID ohne Fremdworte und englischsprachige Begriffe, damit sie für die allgemeine Bevölkerung zu verstehen sind. Durch das aus dem Unverständnis entstehende mangelhafte Wissen entstehen Ängste, die eine Akzeptanz der Technologie verhindern und letztlich die Ablehnung verstärken.

### *Personenbezogene Daten*

Ein großer Handlungsbedarf besteht nach Meinung der Mehrheit der Befragungsteilnehmer im Zusammenhang mit der möglichen Speicherung personenbezogener Daten. Viele Teilnehmer fordern, dass beim Einsatz von RFID gar keine persönlichen Daten gespeichert werden dürfen. Gerade in Bezug auf den Handel bestehen hier Befürchtungen. Es wird zum Beispiel gefordert, dass auf Transpondern gespeicherte Produktdaten, die an Kleidung oder anderen Produkten angebracht sind, nach einem Einkauf nicht mit Personendaten verknüpft und in einer Datenbank abgespeichert werden dürfen. Unternehmen sollten sich demnach öfter die Frage stellen, ob eine Verknüpfung von Personendaten mit Produktdaten überhaupt notwendig sei. In diesem Kontext wurde zum Beispiel vorgeschlagen, über den Einsatz von Transpondern durch einen Aufdruck auf dem Produkt hinzuweisen und eine Deaktivierung durch den Endverbraucher zu ermöglichen, wie es zum Beispiel im METRO Group Future Store praktiziert wird. Darüber hinaus müsse sich an gesetzliche Regelungen gehalten werden, nach denen eine Freigabe von personenbezogenen Daten nicht automati-

sichert werden darf und die Speicherung nur mit ausdrücklicher Genehmigung des Betroffenen erfolgen darf.

Von Seiten der Umfrageteilnehmer wurde empfohlen, dass besser darüber aufgeklärt werden sollte, in welchen Anwendungen überhaupt personenbezogene Daten genutzt werden. Bei vielen Anwendungen, bei denen Kunden befürchten, dass persönliche Daten gespeichert würden, ist das nämlich gar nicht der Fall. Es wurde auch darauf hingewiesen, dass RFID nicht die einzige Möglichkeit darstellt, Kundendaten zu speichern und Kundenprofile zu erstellen. Mit den seit einigen Jahren existierenden Kunden- oder Bonuskarten würden ebenfalls personenbezogene Daten gespeichert und von den Unternehmen genutzt.

Insgesamt erwecken die Äußerungen der Befragungsteilnehmer den Eindruck, dass Datenschutz vorwiegend in Zusammenhang mit dem Umgang mit personenbezogenen Daten von Interesse ist.

Vor diesem Hintergrund wurde von einem Befragten darauf hingewiesen, dass ein Großteil aller RFID-Anwendungen, etwa in der Logistik und in der Materialwirtschaft, gar nicht oder nur selten mit derartigen Daten in Berührung kämen. In solchen Fällen müsse das ausreichend kommuniziert werden, um eine unnötige Behinderung der Einführung von RFID in solchen Bereichen zu vermeiden.

#### *Transparenz und Aufklärung*

Transparenz ist ein Aspekt, der in den Augen eines großen Teils der befragten Personen sehr wichtig ist. Das Wissensniveau sollte bei allen an der Diskussion um den Einsatz von RFID Beteiligten, wie zum Beispiel Herstellern und Anwendern sowie Datenschutzorganisationen und kritischen Endverbrauchern, möglichst gleich sein. Demnach ist die Schaffung von Transparenz und Aufklärung erforderlich, um das Entstehen unsachlicher Datenmissbrauchs-Szenarien zu vermeiden, so dass man sich auf die tatsächlich regulierungsbedürftigen Missbrauchsmöglichkeiten konzentrieren kann.

Im Zuge der Einführung einer RFID-Anwendung kann die frühzeitige Kommunikation und Aufklärung der Beteiligten Vertrauen aufbauen und mögliche Einwände frühzeitig ausräumen, so die Meinung mehrerer Umfrageteilnehmer. Dazu gehört auch eine umfassende Auskunft über die gesetzlichen Rahmenbedingungen. Auch die Offenlegung des Prozesses der Datenerhaltung und Datenverwendung ist für viele Befragte ein wichtiger Schritt, um Vertrauen zu schaffen. Grundsätzlich sind Anwendungen, bei denen ein Bezug zum Konsumenten hergestellt werden kann von solchen zu unterscheiden, bei denen Güter ohne Personenbezug betroffen sind. Man müsse klar kommunizieren, dass es eine Vielzahl von RFID-Anwendungen gibt, bei denen der Datenschutz nicht relevant ist.

Ein weiterer Aspekt, auf den eine Vielzahl der an der Umfrage beteiligten Personen hinweist, ist die Notwendigkeit einer breiten Aufklärung über die Möglichkeiten und auch die Grenzen der RFID-Technologie. Die Akteure im RFID-Umfeld sollten beispielsweise versuchen, den generellen Nutzen der Technologie herauszustellen, dabei aber gleichzeitig auch die möglichen Nachteile klarstellen.

#### *Sachliche Diskussion*

Sehr viele Befragungsteilnehmer waren der Überzeugung, dass die Diskussion um RFID und Datenschutz zu einem großen Teil nicht sachlich geführt wird. Um diesen Mangel zu beheben, sei beispielsweise eine stärkere Differenzierung zwischen den jeweiligen Anwendungen und dem nötigen Datenschutz angebracht. Die bisherigen Szenarien und damit verbundenen Ängste seien oft zu pauschal bzw. zu unspezifisch. Einige RFID-Anwendungen würden überhaupt nicht diskutiert, andere wiederum sehr ausgeprägt. Notwendig sei eine klare Unterscheidung und Abgrenzung von Realität und Vision.

### **7. Checkliste für RFID-Projekte**

Die folgende Checkliste beinhaltet eine Übersicht von häufig genannten Empfehlungen der Befragungsteilnehmer, die im Zusammenhang mit einer möglichst reibungslosen Einführung der Technologie genannt wurden. Unternehmen können die folgenden Punkte im Rahmen der Planung und Umsetzung von RFID-Projekten als Orientierungshilfe nutzen, um möglichen Problemen im Zusammenhang mit dem Thema Datenschutz vorzubeugen.

- Veröffentlichung transparenter Praxisbeispiele aus verschiedenen Branchen.
- Durchführung von Praxisworkshops und Besuchen bei Unternehmen, die RFID bereits mit vorbildlichem Datensicherheits- und Datenschutzstandard umgesetzt haben.
- Herausstellen positiver Anwendungsfälle, bei denen RFID das tägliche Leben des Anwenders erleichtert (z.B. Skipass, ÖPNV, Zentralverriegelung etc.).
- Bereitstellung von ausreichend Informationamaterial, das dem technischen Verständnis der Endverbraucher gerecht wird.

- Abgrenzung von b2b- und b2c-Anwendungen, um Diskussionen über Anwendungen zu vermeiden, bei denen der Endkonsument nicht betroffen ist.
- Demonstration der Deaktivierungsmöglichkeit von RFID-Systemen im Einzelhandel.
- Schaffung von Möglichkeiten, die Deaktivierung von Transpondern zu kontrollieren.
- Möglichkeit der Long-Distance-Nutzung im Endverbraucher-Bereich technisch unterbinden.
- Kennzeichnung von Produkten mit einem Aufkleber (ähnlich wie Gesundheits-Warnhinweise auf Zigarettenpackungen), der auf das Vorhandensein eines Transponders hinweist.
- Medien, insbesondere Redaktionen von reichweitenstarken Zeitungen und Magazinen sowie Fernsehsendungen präzise informieren und eng in die Kommunikationsstrategie einbinden.
- Einbindung einer vertrauenswürdigen dritten Partei in RFID-Projekte (z.B. Verbraucherschutzorganisation oder Datenschutzbeauftragter).
- Auf vorhandene Datenschutzregelungen hinweisen und aufzeigen, wie diese innerhalb der RFID-Lösungen angewendet werden.

## 8. Weiterführende Informationen

Die folgenden Informationsquellen empfehlen sich zur weiteren Vertiefung des Wissens über das Themengebiet des Datenschutzes in Verbindung mit der Radiofrequenztechnologie. Die Informationen sind im Internet verfügbar und können durch Eingabe der entsprechenden Links

### **Bundesdatenschutzgesetz**

[http://bundesrecht.juris.de/bdsg\\_1990/index.html](http://bundesrecht.juris.de/bdsg_1990/index.html)

### **Europäische Datenschutzrichtlinie**

<http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML>

### **Leitfaden:** "RFID und Datenschutz", Eicar Task Force on RFID

<http://www.eicar.org/rfid/infomaterial/RFID-Leitfaden-100406.pdf>

**Orientierungshilfe:** Datenschutzgerechter Einsatz von RFID, Arbeitskreis "Technische und organisatorische Datenschutzfragen", Konferenz der Datenschutzbeauftragten des Bundes und der Länder

[http://www.datenschutz-bayern.de/technik/orient/oh\\_rfid.html](http://www.datenschutz-bayern.de/technik/orient/oh_rfid.html)

**Studie:** "Risiken und Chancen des Einsatzes von RFID-Systemen", Bundesamt für Sicherheit in der Informationstechnik (BSI)

<http://www.bsi.de/fachthem/rfid/RIKCHA.pdf>

**Studie:** "Technologieintegrierte Datensicherheit bei RFID-Systemen", Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Fachgebiet Mikroelektronische Systeme (MES) der Technischen Universität Darmstadt, Technologie-Zentrum Informatik (TZI) der Universität Bremen

<http://www.sit.fraunhofer.de/rfidstudie2007/RFID-Studie2007.pdf>

**Rechtsgutachten:** "Rechtliche Dimensionen der Radiofrequenz-Identifikation", Informationsforum RFID

[http://www.info-rfid.de/downloads/rfid\\_rechtsgutachten.pdf](http://www.info-rfid.de/downloads/rfid_rechtsgutachten.pdf)