

# RFID

## Radiofrequenz-Identifikation

# Was ist das?

Informationsbroschüre

Kaiser-Friedrich-Straße 1  
55116 Mainz

Poststelle@mufv.rlp.de  
www.mufv.rlp.de

Hintere Bleiche 34  
55116 Mainz

Poststelle@datenschutz.rlp.de  
www.datenschutz.rlp.de



# VORWORT

---

Intelligente Haushaltsgeräte, automatisches Bezahlen, Gesundheitsinformation am „Patientenarmband“ – all diese Anwendungen sind mit der Zukunftstechnologie RFID möglich. Was große Chancen bietet, kann aber auch Risiken mit sich bringen: Werden die auf RFID-Chips gespeicherten Daten mit Personen verknüpft, ist das Recht auf informationelle Selbstbestimmung in Gefahr. Bevor die Technologie flächendeckend eingeführt wird, muss daher der Schutz der persönlichen Daten gewährleistet sein. Umfragen ergeben zudem immer wieder einen großen Bedarf nach unabhängigen Informationen.

Wir möchten Ihnen in dieser Broschüre einen Überblick über die Funktionsweise, die Anwendungsbereiche sowie die Vor- und Nachteile von RFID geben. Sie sollen außerdem erfahren, welche Rechte Sie haben und wie Sie diese wahrnehmen können.

Die Broschüre ist ein Ergebnis des von uns ins Leben gerufenen „Verbraucherdialogs RFID“, einer Expertenrunde aus Vertreterinnen und Vertretern der Wirtschaft, der Wissenschaft und der Verbraucherverbände. Sie wäre ohne die Mitarbeit der Expertinnen und Experten nicht möglich gewesen. Ihnen gilt daher unser herzlicher Dank.



*Margri Colrad*



*Egon Woyt*

# INHALT

---

- 3 **Vorwort**
- 4 **Inhalt**
- 6 **RFID – Was ist das?**
- 8 Technische Grundlagen
- 12 Rechtliche Grundlagen
- 16 Weitere Grundlagen
- 18 **Wo gibt es RFID?**
- 19 **Wirtschaft**
- 19 Produktion, Logistik und RFID
- 21 Waren und RFID
- 22 Kunden- und Bezahlkarten und RFID
- 24 **Arbeit**
- 26 **Gesundheit**
- 26 RFID und Arzneimittel
- 27 Patientinnen und Patienten und RFID
- 29 **Mobilität**
- 29 RFID im Auto
- 30 RFID im Nahverkehr
- 31 Reisen mit RFID
- 34 **Prozessoptimierung im Alltag**
- 34 RFID in Bibliotheken und Büchereien
- 36 RFID bei Eintrittskarten und Veranstaltungen
- 37 Haus- und Nutztiere und RFID
- 39 **Vorteile und Nachteile auf einen Blick**
- 41 **Herausforderungen und Perspektiven**
- 42 **Gesundheitsbelastung durch RFID?**
- 44 **RFID contra Recycling?**
- 46 **Gläserne Kundinnen und Kunden dank RFID?**
- 48 **„Internet der Dinge“ – Was ist möglich?**
- 50 **Verbrauchertipps**
- 52 Glossar
- 54 Vorstellung der Herausgeber
- 56 Mitglieder des Verbraucherdialogs RFID
- 58 Ansprechpartnerinnen und Ansprechpartner
- 59 Links
- 60 Literaturtipps
- 62 Impressum

# RFID – Was ist das?

RFID steht für Radiofrequenz-Identifikation, was vereinfacht Identifizierung per Funk, also mit Hilfe von elektromagnetischen Wellen, heißt. Es ermöglicht das kontaktlose Speichern und Auslesen von Daten. Angewendet wird RFID für das automatische Identifizieren und bei besonderen Anwendungen auch für das Lokalisieren von Gegenständen und Lebewesen.

Im Unterschied zum bekannten System Barcode/Strichcode, bei dem zum Beispiel jedes Butterpaket einer Marke X mit einem bestimmten gleichen Barcode versehen wird und so an der Kasse einfach über den Scanner gezogen werden kann, ist es mit RFID technisch möglich, einzelne Objekte mit einer eindeutigen Nummer zu versehen und individuell zu verfolgen.

Die Entwicklung von RFID begann verstärkt in den 60er Jahren, nachdem bereits im 2. Weltkrieg ein Vorläufer des Systems zur „Freund-Feind-Erkennung“ eingesetzt worden war. Einfache RFID-Systeme wurden zur Diebstahlsicherung (englisch: Electronic Article Surveillance, EAS) verwendet. Die RFID-Technik konnte sich auf breiter Ebene jedoch nicht durchsetzen. Gründe dafür waren unter anderem die hohen Kosten der Chips und die noch nicht ausgereifte Technologie.

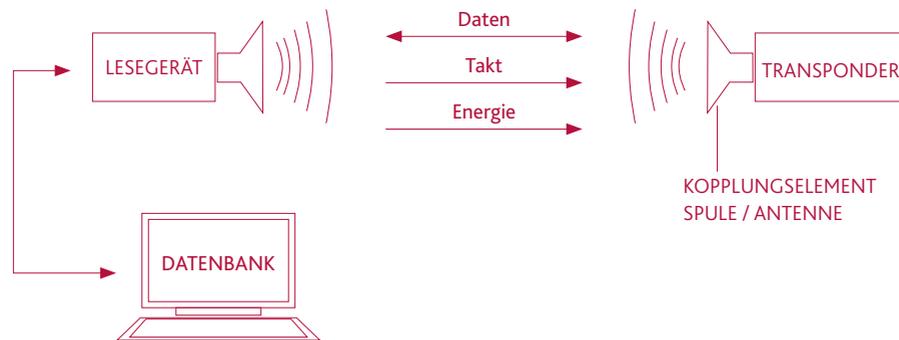
Seit den 90er Jahren des vergangenen Jahrhunderts wird die RFID-Technologie in den USA für Mautsysteme genutzt. In der Landwirtschaft wird RFID zur Tiererkennung eingesetzt.

Heute findet sich RFID an vielen Orten. Dank immer kostengünstigerer Transponder und massiver Investitionen in die Technologie durch die Wirtschaft wird das System in ganz unterschiedlichen Bereichen verwendet. Eingesetzt wird RFID mittlerweile zum Beispiel für elektronische Schlösser, Zutrittskontrollen, elektronische Wegfahrsperren, bargeldloses Zahlen und Skipässe, in Bibliotheken und in der Textilindustrie.



# TECHNISCHE GRUNDLAGEN

Alle RFID-Systeme bestehen aus einem **Transponder** und einem **Erfassungs- bzw. Lesegerät**. Der Transponder ist ein elektronischer Datenspeicher. Wenn der Transponder in den Empfangsbereich des Lesegerätes kommt, wird eine wechselseitige Kommunikation ausgelöst. Dazu verfügen beide Geräte über Kopplungselemente in Form von Antennen. Der Energie- bzw. Datenaustausch erfolgt durch magnetische oder elektromagnetische Wellen.



Die Funkwellen sind das Transportsystem für die Informationen, die von Transponder und Lesegerät ausgetauscht werden. Es gibt unterschiedliche Frequenzbereiche, die verwendet werden.

Frequenzbereich	Niedrigfrequenzbereich (LF)	Hochfrequenz (HF)	Ultrahochfrequenz (UHF)
	30 – 500 kHz	10 – 15 MHz	850 – 950 MHz
Reichweite	wenige Zentimeter bis zu 1,5 m	1 – 1,5 m	3 – 4 m
Beispiele	Wegfahrsperre Tieridentifikation	Bibliotheken Zutrittskontrolle Tickets	Palettenidentifikation Handelsgüter

Spezielle RFID-Systeme können noch höhere Frequenzen (im GHz-Bereich) verwenden und so eine Reichweite von mehreren hundert Metern erreichen. Ein einheitlicher Standard hat sich bisher noch nicht durchgesetzt. Verschiedene Organisationen, wie beispielsweise EPCglobal, befassen sich zur Zeit mit der Standardisierung.

Das Wort „**Transponder**“ ist ein Kunstwort und setzt sich aus den Bestandteilen „transmit“ und „response“ zusammen. Transmit bedeutet „übertragen, senden, funken“ und response „Antwort, Rückmeldung“. Der Transponder kann Informationen liefern oder aber mit Hilfe eines Speichers komplexe Daten aufnehmen. Er kann gelesen und in bestimmten Ausführungsarten auch beschrieben werden. Transponder werden auch als **(RFID-)Tags** bezeichnet.

Aufgebaut ist der Transponder folgendermaßen: Er besteht aus einem Mikrochip, der als Speicher dient und einem Kopplungselement, der Antenne. Durch den Speicher können Informationen über das Objekt, das getaggt (also mit einem Chip versehen) wurde, übermittelt werden. Das Objekt wird mit einer eindeutig identifizierbaren Nummer versehen. Derzeit reicht die übliche Größe des Speichers von wenigen Byte bis zu mehr als 100 Kilobyte. Zum Vergleich: 100 Kilobyte entsprechen ungefähr zwanzig voll geschriebenen Schreibmaschinenseiten. Die Speicher wiegen zwischen 200 Milligramm und 1 Gramm. Tags mit Kupferantenne wiegen rund 30 bis 40 Prozent mehr als gleich große Transponder mit Aluminium- bzw. Silberantenne.

Es wird zwischen aktiven und passiven Transpondern unterschieden. **Passive Transponder** beziehen ihre Energie aus dem elektromagnetischen Feld oder aus der elektromagnetischen Welle des Lesegerätes. **Aktive Transponder** verfügen über eine eigene Spannungsversorgung, eine Batterie. Der Nachteil der aktiven Transponder ist, dass sie meist größer und auch teurer sind als passive Transponder. Zudem ist ihre Lebensdauer kürzer als die der passiven Transponder.

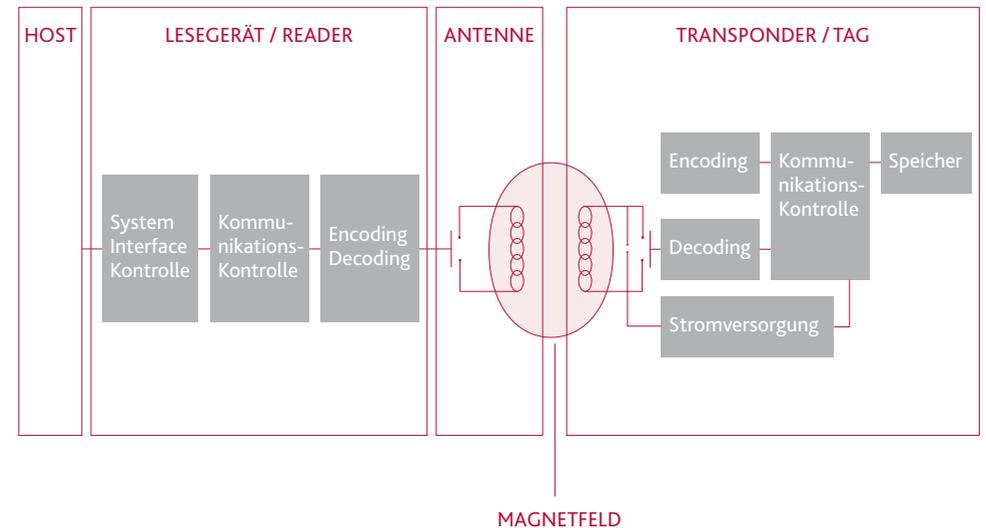
**Transponder** erhalten bei ihrer Produktion eine eindeutige Nummer. Darüber hinaus wird der Transponder vor seinem Einsatz mit einer Nummer beschrieben, die weltweit einmalig vergeben wird. Dabei kommen unterschiedliche Standards zum Einsatz. Ein Standard wurde von **EPCglobal** entwickelt und nennt sich **EPC (Electronic Product Code)**. Das Verfahren ist grundsätzlich gleich: Eine Nummer wird auf dem Transponder hinterlegt, durch das Lesegerät ausgelesen und dann an eine Datenbank weitergeleitet. Dort wird der Code mit Informationen, die in der Datenbank hinterlegt sind, verknüpft. Das Wissen liegt also in der Regel in der **Datenbank**, nicht im Transponder selbst, es sei denn, es handelt sich um einen Transponder, der selbst mit Informationen beschrieben worden ist. Diese Variante ist allerdings eher die Ausnahme.

**Transponder** variieren insgesamt in Größe und Form. Es gibt flache oder sehr kleine Transponder, zum Beispiel in Stiftform oder in Kreditkartenformat für den Einsatz bei Zutrittskontrollsystemen.

Das **Lesegerät (Reader)** besteht aus einem **Sender** und einem **Empfänger (Hochfrequenzmodul)**, einem **Controller** und einem **Kopplungselement** in



Form einer Antenne. Häufig gibt es noch eine Schnittstelle zu einem Computer, um die empfangenen Daten weiterzuverarbeiten. Die Bauform wird meistens von der Größe der Antenne bestimmt. Es gibt stationäre und mobile Lesegeräte. Die **Reichweite** der Geräte reicht bei passiven Transpondern von wenigen Zentimetern bis zu vier Meter, was jeweils von der Leistung und der verwendeten Frequenz abhängt. Aktive Transponder können über deutlich größere Distanzen gelesen werden.



Aufgabe des Lesegeräts ist es, Informationen aus einem Transponder auszu-lesen und gegebenenfalls Daten auf einen Transponder zu schreiben. Dies funktioniert folgendermaßen:

Das Lesegerät sendet das **Sendesignal**, es „ruft“ also nach Transpondern in der Umgebung. Dann filtert es das Antwortsignal und bereitet gegebenenfalls die empfangenen Daten in einer definierten Form für eine Auswertung durch nachgelagerte Computer-Systeme auf, beispielsweise für ein Lagerverwaltungssystem.

Lesegeräte und Transponder bilden zusammen das RFID-System. Nimmt man auch die nachgelagerten IT-Systeme in einem bestimmten Einsatz in den Blick, spricht man von RFID-Anwendungen.

# RECHTLICHE GRUNDLAGEN

Die Rechte, die Verbraucherinnen und Verbraucher beim Einsatz von RFID zustehen können, werden aus den Vorschriften des **Bundesdatenschutzgesetzes (BDSG)** abgeleitet. Spezielle Gesetze zu RFID gibt es bisher nicht.



Im Bundesdatenschutzgesetz ist der Umgang mit personenbezogenen Daten geregelt. Die hieraus gewonnenen Informationen dürfen nur dann verwendet werden, wenn die Betroffenen eingewilligt haben oder dies durch eine Rechtsvorschrift erlaubt ist (§ 4 BDSG).

**Voraussetzung für die Anwendbarkeit des Bundesdatenschutzgesetzes** ist, dass personenbezogene Daten der Verbraucherinnen und Verbraucher betroffen sind.

Nach § 3 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten Person, wie zum Beispiel Name, Geburtsdatum oder Adresse. Die **Anwendbarkeit des BDSG** hat zur Folge, dass den Betroffenen Auskunftsrechte sowie gegebenenfalls Berichtigungs- oder Löschanträge zustehen.

Werden beispielsweise Joghurtbecher mit einem RFID-Transponder versehen, damit ihr Weg von der Produktion über das Lager in den Verkaufsraum kontrolliert werden kann, so betrifft dies die Endkundinnen und Endkunden nicht. Anders ist es hingegen, wenn Kundinnen und Kunden eine dieser Joghurtbecher kaufen und beim Kauf beispielsweise eine EC-Karte oder eine Kundenkarte verwenden. Nun ist eine **Verknüpfung mit den personenbezogenen Daten** der Kundinnen und Kunden möglich und damit sind auch ihre bzw. seine Rechte nach dem BDSG betroffen.

Es gibt drei Konstellationen, bei denen RFID mittels eines Transponders, der mit einem **elektronischen Produktcode (EPC)** versehen wurde, eingesetzt werden kann:

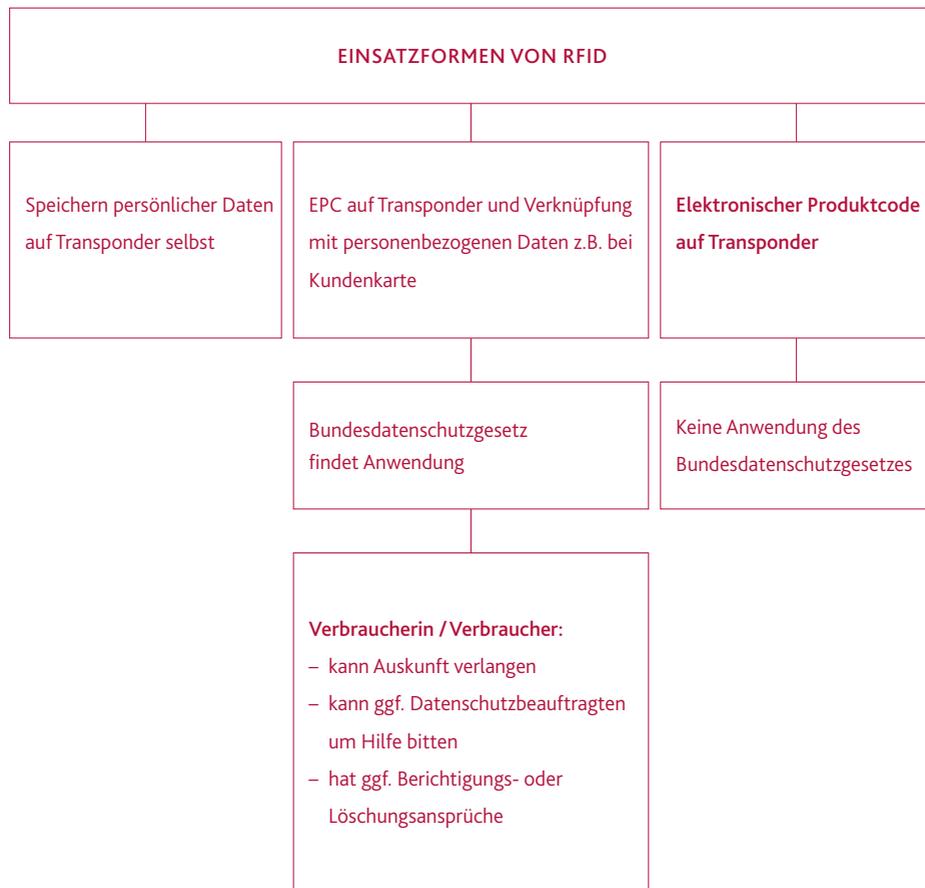
1. Ein EPC wurde auf einem Transponder gespeichert,
2. der EPC wurde mit Kundendaten verknüpft oder
3. persönliche Daten wurden direkt auf dem Tag gespeichert.

Im ersten Fall findet das Bundesdatenschutzgesetz keine Anwendung, da es sich nicht um personenbezogene Daten handelt. Auf dem Transponder sind keine persönlichen Daten gespeichert und es kann auch nicht aus dem Inhalt oder dem Zusammenhang auf eine Person geschlossen werden. Diese ist also im Sinne des Bundesdatenschutzgesetzes nicht bestimmbar.

Im Falle der **Verknüpfung mit Kundendaten** kann hingegen auf die Person geschlossen werden, die zum Beispiel ein getaggttes Produkt gekauft hat und dieses mit einer Kundenkarte bezahlt (vgl. oben genanntes Beispiel mit dem Joghurtbecher). Hier ist das Bundesdatenschutzgesetz einschlägig.

Im letzten Fall sind die Daten direkt auf dem Tag gespeichert, der zum Beispiel in einer Kundenkarte oder in einer Zugangsberechtigungskarte integriert ist. Dabei handelt es sich um personenbezogene Daten. Die Vorschriften des Bundesdatenschutzgesetzes sind somit anzuwenden.

Die Vorgaben des Bundesdatenschutzgesetzes sind immer dann anzuwenden, wenn es sich um **personenbezogene Daten** handelt oder wenn eine Verknüpfung mit solchen stattfindet.



Grundsätzlich ist die **Erhebung, Verarbeitung und Nutzung** personenbezogener Daten nach § 4 BDSG nur zulässig, wenn dies durch eine Rechtsvorschrift erlaubt oder angeordnet ist oder die Betroffenen eingewilligt haben. Wenn Einzelne ihre Daten zur Verfügung stellen, so muss die Transparenz insoweit gewährleistet sein, dass sie die Erhebungs- und Verarbeitungszusammenhänge kennen.

Aus diesem **Transparenzgebot** heraus folgt, dass die Betroffenen ein Recht auf Offenlegung der über sie gespeicherten Daten haben. Sie müssen informiert werden und verfügen über Auskunftsrechte, um ihre Löschungs- und Korrekturanträge wirksam geltend machen zu können.

Das BDSG legt vor diesem Hintergrund der verantwortlichen Stelle grundsätzlich die Pflicht auf, Betroffene über die **Datenverarbeitung** zu informieren (§§ 19a, 33 BDSG), wenn diese keine Kenntnis davon haben, dass ihre personenbezogenen Daten erhoben, gespeichert oder verarbeitet werden. Eine Pflicht zur Benachrichtigung besteht nicht, wenn die Speicherung oder Übermittlung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen ist. Verbraucherinnen und Verbraucher können sich in einem solchen Fall aber auch direkt an das betreffende Unternehmen wenden und gemäß § 34 BDSG Auskunft verlangen. Sie können **Aufklärung** darüber fordern, ob Daten über sie gespeichert werden, woher diese stammen und zu welchem Zweck sie gespeichert und an wen sie gegebenenfalls weitergegeben wurden oder werden.

Reagiert ein Unternehmen nicht, so können sich Verbraucherinnen und Verbraucher an jeweils zuständige **Datenschutzbeauftragte** wenden. Darüber hinaus stehen Verbraucherinnen und Verbrauchern nach § 35 Absatz 1 BDSG Berichtigungsansprüche zu, wenn falsche Daten gespeichert wurden. Nach § 35 Absatz 2 BDSG haben Verbraucherinnen und Verbraucher auch einen **Löschungsanspruch**, unter anderem wenn persönliche Daten unzulässig gespeichert oder für eigene Zwecke verarbeitet werden, obwohl deren Kenntnis nach der Erfüllung des ursprünglichen Zwecks der Speicherung nicht mehr erforderlich ist. Gegebenenfalls ist auch eine **Sperrung der Daten** möglich (§ 35 Absatz 3 BDSG).

Die verarbeitende Stelle hat zudem nach § 9 BDSG auch die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Einhaltung der datenschutzrechtlichen Anforderungen sicherzustellen.

# WEITERE GRUNDLAGEN

Neben den gesetzlichen Regelungen im BDSG gibt es Vereinbarungen und auch internationale Beschlüsse, die mittelbar Einfluss auf das Verhältnis zwischen Unternehmen und Verbraucherinnen und Verbrauchern im Zusammenhang mit RFID nehmen.

Ein Teil der Wirtschaft hat sich im Jahr 2006 auf eine **Selbstverpflichtung** geeinigt. Es handelt sich um die Mitglieder von EPCglobal, der weltweiten Standardisierungsinitiative zu RFID. Im Rahmen einer freiwilligen Selbstverpflichtung haben sie sich zu Transparenz und Aufklärung beim Einsatz von RFID im Einzelhandel verpflichtet. Sie haben festgelegt, dass mit Transpondern versehene Produkte und Verpackungen mit dem **EPC-global-Logo** zu kennzeichnen sind. Sie informieren Endkundinnen und Endkunden, wie man zum Beispiel



Transponder auf gekauften Produkten entfernen, ausschalten oder unbrauchbar machen kann. Indes sind nicht alle Unternehmen in Deutschland Mitglieder dieser Initiative.

Auch die **Europäische Kommission** ist um eine einheitliche und transparente Anwendung im Zusammenhang mit RFID bemüht. Im Mai 2009 hat die Europäische Kommission die „Empfehlung zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen“ verabschiedet. Diese Empfehlung richtet sich an die Mitgliedstaaten der Europäischen Union. Wie das Wort „Empfehlung“ bereits zum Ausdruck bringt, kommt ihr keine unmittelbare Verbindlichkeit zu. Ziel

der **Empfehlung** ist es, gleiche Ausgangsbedingungen für die europäische Wirtschaft zu schaffen und gleichzeitig die Privatsphäre der Einzelnen zu schützen. Für Verbraucherinnen und Verbraucher sind besonders folgende Punkte der Empfehlung relevant:

## ■ Folgenabschätzung für den Datenschutz

Betreiberinnen und Betreiber sollen vor dem Einsatz der RFID-Technologie feststellen, ob eine Bedrohung für die **Privatsphäre** oder für den Schutz personenbezogener Daten wahrscheinlich ist. Diese Abschätzung soll spätestens sechs Wochen vor Einführung der Anwendung der zuständigen Stelle zugeleitet werden

## ■ Kennzeichnung der Produkte und der Standorte von Lesegeräten

Die Mitgliedstaaten sollen dafür Sorge tragen, dass die Verbraucherinnen und Verbraucher über die Nutzung von RFID durch die Betreiberinnen und Betreiber informiert werden. Betreiberinnen und Betreiber sollten Verbraucherinnen und Verbraucher auf **Standorte von Lesegeräten** durch ein europaweit einheitliches Zeichen hinweisen. Betreiberinnen und Betreiber im Einzelhandel sollten auch jedes Produkt, das mit einem RFID-Chip versehen wurde, mit einem solchen Zeichen versehen.

## ■ Kostenfreie Deaktivierung auf Wunsch der Kunden

Beim Kauf von Produkten mit RFID-Chips sollen die Chips noch im Geschäft sofort und kostenfrei **deaktiviert** werden, es sei denn die Käuferinnen und Käufer wünschen ausdrücklich, dass sie funktionsfähig bleiben (Opt-In-Prinzip). Von einer Deaktivierungspflicht soll abgesehen werden können, wenn die Folgenabschätzung ergeben hat, dass keine Beeinträchtigung für die Privatsphäre oder den Schutz personenbezogener Daten droht. In diesem Fall reicht es, eine **Deaktivierungsmöglichkeit** anzubieten.

# Wo gibt es RFID?

Der Einsatz von RFID-Systemen eignet sich grundsätzlich überall dort, wo automatisch gekennzeichnet, erkannt, registriert, gelagert, überwacht oder transportiert werden muss. Die Anwendungsbereiche sind dementsprechend vielfältig. Hauptsächliches Einsatzgebiet ist der Produktions- und Logistikbereich.

## WIRTSCHAFT

### PRODUKTION, LOGISTIK UND RFID

Das Haupteinsatzgebiet für RFID sind die Bereiche Produktion und Logistik. Handelt es sich um geschlossene Systeme, werden RFID-Chips oft mehrmals verwendet. Geschlossenes System bedeutet hierbei, dass zum Beispiel komplett in einer Firma produziert wird und so keine Rücksicht auf unterschiedliche Standards oder Schnittstellen genommen werden muss.

In der Produktion werden **RFID-Transponder** entweder auf Paletten oder auf Einzelteilen angebracht. Einzelteile können zum Beispiel Autozubehörteile oder kleine elektronische Bauteile sein. Die mit den Transpondern versehenen Gegenstände passieren an verschiedenen Punkten ihrer Herstellung oder Bearbeitung Lesegeräte. Damit soll ein geregelter Ablauf gesichert werden. Auf dem Chip und in einer verbundenen Datenbank können Daten über den Hersteller und die Materialzusammensetzung enthalten sein, aber auch weitere Informationen wie zum Beispiel beim Einsatz von Chargennummern oder dem Verfallsdatum. Diese Daten können entweder in der Datenbank oder, beim Einsatz wiederbeschreibbarer Transpondern mit einem großen Datenspeicher, direkt auf dem Chip fortwährend aktualisiert werden.



Mit Hilfe von RFID-Systemen können auch **Fließbandprozesse** automatisiert werden. Hierbei werden Roboter mit Lesegeräten versehen und können so mit den Gegenständen kommunizieren, was wiederum bestimmte Handlungen der Roboter auslöst.

Im Bereich der **Logistik** spielt RFID besonders bei der Bestandskontrolle eine Rolle. Alle Paletten oder Gegenstände werden mit RFID-Transpondern ausgestattet. Bei der Ankunft im Lager werden die Transponder mit Hilfe eines Lesegeräts automatisch erfasst – ebenso bei Verlassen des Lagers.



Auf dem Gebiet der **Standardisierung** wird versucht, innerhalb eines Netzwerks verschiedener Unternehmen die gleichen Lesegeräte und Frequenzen zu verwenden, um den Ablauf der Lieferkette zu vereinfachen. Dies wird auch Lieferkettenmanagement („Supply Chain Management“) genannt.

#### Vorteile

- Verluste durch Diebstahl werden gesenkt
- Durchlaufzeiten von Gütern werden verkürzt, Verbesserungen der Warenmanagementprozesse möglich
- Lieferungsqualität wird erhöht beispielsweise durch Erleichtern von Just-in-time-Lieferungen, dadurch erhöhte Wettbewerbsfähigkeit möglich

#### Nachteile

- Bislang haben sich nicht in allen Branchen einheitliche Standards durchgesetzt, das kann zu mehrfachem Taggen führen
- elektromagnetische Strahlungsbelastung für Waren, Arbeitnehmerinnen und Arbeitnehmer

## WAREN UND RFID

Im Bereich der Endkundinnen und Endkunden wird RFID zum Teil zur Diebstahlsicherung oder in Pilotprojekten als Warenetikett angewendet.

Einige der heute gebräuchlichen **Elektronischen Artikelsicherungssysteme (EAS-Systeme)** sind der RFID-Technologie verwandt. Allerdings speichern sie keine Nummer, mit der eindeutig identifiziert werden kann, sondern lediglich ob bezahlt wurde. In letzter Zeit wird erprobt, die EAS-Systeme durch RFID zu ersetzen. Werden alle Kleidungsstücke in einem Geschäft mit RFID versehen, kann der Transponder als Diebstahlsicherung genutzt werden. Die Etiketten lösen einen Alarm an den Lesegeräten am Ladenausgang aus, solange der Tag aktiv ist und nicht entfernt oder entwertet bzw. deaktiviert wurde. Die Transponder können entweder sichtbar oder unsichtbar an Artikeln angebracht werden. Dies kann auch schon direkt bei der Herstellung (Source Tagging) geschehen.

In einigen **Pilotprojekten** wird getestet, wie der Einsatz von RFID an jedem einzelnen Produkt in einem Geschäft gestaltet werden könnte. Dazu werden alle Produkte mit einem RFID-Tag versehen. An der Kasse werden Lesegeräte aufgestellt, die die Transponder an den jeweiligen Produkten im Einkaufswagen auslesen und erfassen.

Mit Hilfe dieser Systeme könnte gesichert werden, dass genug Ware vorhanden ist oder es könnten so Inventuren jederzeit durchgeführt werden. Auch eine Herkunftsgarantie für Lebensmittel wäre denkbar oder der Zugriff auf Produktinformation für die Verbraucherinnen und Verbraucher, die selbst mit Hilfe eines Lesegeräts durch den Einkaufsladen gehen. Durch ein Lesegerät am Ladenausgang werden alle Waren im Einkaufswagen erfasst und automatisch eine Rechnung erstellt. Im Anschluss wäre ein ordnungsgemäßes Recycling der Transponder vorstellbar, das an die Produktinformationen, die auf dem Tag gespeichert sind, anknüpft.

#### Vorteile

- Diebstahlsicherung
- Arbeitsentlastung, da Sicherungen nicht mehr von Hand angebracht werden müssen
- Einkaufen könnte auf diese Art vereinfacht werden

#### Nachteile

- Ggf. keine Deaktivierung des RFID-Chips bei Verlassen des Ladens, dadurch späteres illegales und unautorisiertes Auslesen denkbar/angeklagt
- Erstellung von Bewegungsprofilen der Kundinnen und Kunden und Sammlung von Informationen zu deren Vorlieben

## KUNDEN- UND BEZAHLKARTEN UND RFID

Viele Menschen besitzen eine, wenn nicht sogar mehrere Kundenkarten. In der Regel sollen diese Karten Rabatte sichern, entweder indem man als Karteninhaberin oder Karteninhaber Prozente auf die gekaufte Ware erhält oder indem über die Karte beim Einkaufen Punkte oder Ähnliches gesammelt werden können.

Die gesammelten Punkte können teilweise bei einer bestimmten Anzahl in eine Prämie eingetauscht werden.

Unternehmen sind sehr an dem Kaufverhalten ihrer Kundinnen und Kunden interessiert. So weiß das kartenausgebende Unternehmen in der Regel was wann gekauft beziehungsweise welche Dienstleistung in Anspruch genommen wurde, wenn die Kundenkarte beim Bezahlen vorgelegt wurde.



Unternehmen sind sehr an dem Kaufverhalten ihrer Kundinnen und Kunden interessiert. So weiß das kartenausgebende Unternehmen in der Regel was wann gekauft beziehungsweise welche Dienstleistung in Anspruch genommen wurde, wenn die Kundenkarte beim Bezahlen vorgelegt wurde.

Das erste Unternehmen, das in Deutschland eine Kundenkarte versuchsweise mit RFID ausstattete, war die **Metro-Gruppe**. Die Karte, die keinen Hinweis auf den RFID-Chip enthielt, wurde inzwischen wieder eingezogen und durch Karten ohne RFID-Chip ersetzt. In neueren Projekten setzt die Metro-AG auf umfangreiche Verbraucherinformationen bei RFID-Projekten.

Wenn RFID bei einer intelligenten Kundenkarte verwendet wird, können auf dieser die persönlichen Daten der Kundinnen und Kunden gespeichert werden. RFID-unterstützende Softwares für den Einzelhandel ersetzen hierbei zum Beispiel das Führen von Kundenstammkarteikartensystemen. So gibt es beispielsweise Kundenkarten mit RFID-Chips für den Kundenstamm von Frisörinnen und Frisören.

Als Bezahlkarte wird RFID vor allem in Kantinen und Mensen verwendet. In der Regel wird hierzu die sogenannte **Smart Card** benutzt, die von Nutzerinnen und Nutzern zunächst mit einem Geldbetrag „aufgeladen“ werden muss (Pre-Paid-System). An der Kasse wird die Karte mit dem Transponder vom Lesegerät erfasst und der Kaufpreis abgezogen. Im Normalfall befindet sich auf der Karte nur eine eindeutige Nummer, die im System mit dem Guthaben verknüpft wird. Auf der Karte selbst befinden sich also keine weiteren Informationen, auch nicht das Guthaben selbst. In einigen Schwimmbädern oder Diskotheken wird die Nummer der Karte im Laufe des Aufenthalts mit den jeweiligen Kaufpreisen belastet und erst beim Verlassen an der Kasse wird der Gesamtpreis bezahlt (Post-Paid-System).

#### Vorteile

- Rabatte / Prämien
- Schnelle, individuelle Beratung möglich
- Bei Bezahlkarten: Kürzere Wartezeiten an der Kasse

#### Nachteile

- Möglichkeit der Erstellung von Bewegungs- und Interessenprofilen
- Unbemerkttes Auslesen der auf der Kundenkarte gespeicherten Daten möglich

# ARBEIT

Im Arbeitsleben spielt RFID unter anderem bei der Zeiterfassung eine Rolle. Ebenfalls wird das System bei der Regelung der Zugangsberechtigungen oder auch beim Bezahlen in der Kantine eingesetzt.



Bei der **Zeiterfassung** werden Chipkarte oder Schlüsselanhänger der Mitarbeiterin oder des Mitarbeiters mit einem RFID-Tag ausgestattet. Auf diesem ist eine Nummer gespeichert, die beim Auslesen durch Verknüpfen mit der Datenbank einer Benutzerin

oder einem Benutzer zugeordnet werden kann. Bei Betreten und Verlassen des Gebäudes, und je nach Dienstvereinbarung auch für die Pausen, wird am Lesegerät „ausgestochen“. Dies wird zum Beispiel beim Zweiten Deutschen Fernsehen (ZDF) in Mainz so gehandhabt. Es werden in der Regel Tags mit einer geringen Reichweite verwendet. Chipkarten oder Schlüssel können auch an Besucherinnen und Besucher des jeweiligen Unternehmens ausgegeben werden.

Besondere Sicherheitszonen eines Betriebes können durch **Zutrittssysteme** gesichert werden. Diese Zonen können nur solche Mitarbeiterinnen, Mitarbeiter, Besucherinnen oder Besucher betreten, deren Zugangskarten den entsprechenden Code aufweisen. Lesegeräte an Zugangssperren, zum Beispiel Schließzylinder mit Leseoption an Türen, hindern Unbefugte am Betreten. So erhalten Personen nur Zutritt zu den Räumen, in denen sie sich aufhalten dürfen. Das System mit dem Zutritt eines Schließzylinders mit Leseoption wird so beispielsweise in der Kreisverwaltung Mainz-Bingen eingesetzt. Es gibt dort keine herkömmlichen Schlüssel, sondern es werden Chips mit den jeweiligen Zugangsberechtigungen ausgegeben.

Chipkarten, die mit RFID-Tags versehen wurden, werden auch für Parksysteme am Arbeitsplatz oder zum Bezahlen in der Kantine (Pre-Paid-System) genutzt.

## Vorteile

- Besonders sensible Bereiche können sicher geschützt und Gefahrenbereiche überwacht und im Notfall schnell evakuiert werden
- Zuverlässigkeit der Systeme, geringe Störanfälligkeit, Karten sind wartungsärmer als Magnetstreifenkarten

## Nachteile

- Mitarbeiterinnen und Mitarbeiter könnten überwacht werden, indem gezielt verfolgt wird, wann welche Mitarbeiterinnen und Mitarbeiter sich wo aufgehalten haben; dadurch Eingriff in Persönlichkeitsrechte möglich
- Misstrauen zwischen Arbeitnehmerinnen, Arbeitnehmern, Arbeitgeberinnen und Arbeitgebern könnte durch RFID-Einsatz verstärkt werden, da Mitarbeiterinnen und Mitarbeiter Spionage befürchten könnten

# GESUNDHEIT

## RFID UND ARZNEIMITTEL

Im Bereich der Arzneimittel dient RFID dazu, Medikamente zu identifizieren und zu lokalisieren, zur Qualitätsüberwachung sowie zur Dokumentationsicherheit. Dies gilt auch für Blutkonserven.

Der Einsatz von RFID soll vor **Arzneimittelfälschungen** schützen, die immer mehr auf den deutschen Markt drängen. Dabei handelt es sich vor allem um Fälschungen, in denen der benötigte Wirkstoff entweder überhaupt nicht oder



in zu geringer Menge enthalten ist. Ebenfalls steigen die gesetzlichen Anforderungen an die Rückverfolgbarkeit pharmazeutischer Produkte. Mit RFID wollen die Hersteller pharmazeutischer Produkte diesen Anforderungen gerecht werden.

Der Transponder wird entweder auf der Umverpackung oder beispielsweise bei Tabletten direkt am Blister

angebracht. Er kann über eine Verbindung mit einer Datenbank Informationen zu Herstellerinnen und Herstellern bieten und das Medikament als Original ausweisen. So sollen jederzeit eine **Rückverfolgbarkeit** der Lieferkette sowie eine eindeutige **Identifikation** möglich sein. Fälschungen sollen unterbunden oder zumindest aufgedeckt werden können. Die einfache Lokalisierung der Medikamente durch RFID soll die Kontrollmöglichkeiten und damit auch die Dokumentationsicherheit erleichtern.

Bei vielen Arzneimitteln sowie bei Blutkonserven ist die Dokumentation des Transports von größter Wichtigkeit. Temperaturempfindliche Arzneimittel dür-

fen, um ihre Wirksamkeit nicht zu verlieren, nur bei bestimmten Temperaturen gelagert und transportiert werden. Vor allem **Blutkonserven** benötigen eine ununterbrochene Kühlkette, um nicht zu verderben. Ein auf dem Medikament oder auf der Blutkonserve angebrachter spezieller Transponder kann neben den Identifikationsdaten Auskunft über die Haltbarkeit, Lagerzeit und die auf dem Transport gemessenen Temperaturdaten geben. Wird eine Unterbrechung der Kühlkette festgestellt, können die betreffenden Medikamente und Blutkonserven sofort aussortiert werden.

### Vorteile

- Geringeres Fälschungsrisiko von Medikamenten
- Qualitätskontrolle von Arzneimitteln und Blutkonserven durch bessere Kontrollmöglichkeiten
- Sicherung der Kühlkette

### Nachteile

- Mögliche Preissteigerung von Medikamenten durch aufwändigere Schutzmaßnahmen
- In Zukunft evtl. Möglichkeit des illegalen Auslesens der Medikamente mit RFID-Chip, die jemand bei sich trägt

## PATIENTINNEN UND PATIENTEN UND RFID

Patientinnen, Patienten und pflegebedürftige Menschen könnten in Zukunft verstärkt mit RFID in Berührung kommen. Wie bereits in einigen Krankenhäusern eingesetzt, soll RFID bei der Identifizierung und Lokalisierung von Patientinnen und Patienten, sowie im Qualitätsmanagement helfen.

Patientinnen und Patienten können an ihren Armbändern, die mit einem Transponder versehen sind, identifiziert werden. Der Chip enthält eine **individuelle Patientennummer**, unter welcher auf einem Server die Patientendaten gespeichert sind. Die behandelnden Ärztinnen und Ärzte können die Patientennummer durch ein mobiles Lesegerät auslesen und sodann über einen

Computer alle auf dem Server vorhandenen Daten einsehen. Zu den gespeicherten Patientendaten können beispielsweise der Krankheitsverlauf, Arzneimittelunverträglichkeiten, die Blutgruppe und eventuell vorhandene Implantate als auch aktuelle Befunde wie Blutbilder und derzeitige Medikation gehören. Das Klinikpersonal kann auf diese Daten zugreifen und falls nötig Änderungen vornehmen.



In einigen Pflegeeinrichtungen werden RFID-Armbänder eingesetzt, um den Zugang einzelner Personenkreise zu bestimmten Bereichen

einzuschränken. Dies soll vor allem der **Sicherheit** demenzkranker oder desorientierter Menschen dienen. Hierzu werden Lesegeräte in den Durchgängen angebracht, die überprüfen, welche Personen durchgelassen werden dürfen und welche nicht. So kann beispielsweise verhindert werden, dass ein Demenzpatient ohne Wissen des Pflegepersonals das Gebäude verlässt.

RFID kann auch zur **Lokalisierung** von Instrumenten und Untersuchungsgeräten in Krankenhäusern oder Pflegeeinrichtungen eingesetzt werden. Mittels RFID kann festgestellt werden, wo sich ein für eine Untersuchung benötigtes Gerät im Gebäude befindet. Dies wird durch einen Chip am jeweiligen Gerät und durch im Gebäude verteilte Lesegeräte erreicht.

#### Vorteile

- Keine Patientenverwechslung durch Vertauschen der Patientenakten möglich
- Schutz von Patientinnen und Patienten
- Effizientere Nutzung vorhandener Kapazitäten in Krankenhäusern durch RFID-Chips an Betten und Geräten

#### Nachteile

- Je nach Sicherheitsstandard Missbrauchsgefahr der sensiblen Daten

# MOBILITÄT

## RFID IM AUTO

RFID-Systeme werden genutzt, um Autos diebstahlsicherer zu machen. Wegfahrsperrern sollen verhindern, dass sich Unbefugte ohne Schlüssel Zugang zu einem Fahrzeug verschaffen.

Der Transponder befindet sich dabei im Autoschlüssel, während das Lesegerät am Zündschloss montiert ist. Wird der Schlüssel in das Zündschloss gesteckt, werden die Daten gelesen. Der Transponder ist mit einer festen **Seriennummer** beschrieben und kann so zugeordnet werden. Werden die korrekten Daten ausgelesen, startet das Auto; bei falschen Daten, wird die Wegfahrsperrre aktiviert. Diese kann ein eigenständiges Steuergerät oder auch ein in den Bordcomputer integriertes Steuergerät sein. Der Austausch zwischen dem RFID-Transponder und dem Lesegerät sowie die Kommunikation zwischen Lesegerät und Motorsteuergerät zur Freigabe des Fahrzeugs sind bei aufwendigeren Wegfahrsperrern durch Verschlüsselungen abgesichert. Bei einfacheren Fabrikaten genügt die Übereinstimmung der Seriennummer zum Starten des Motors.

RFID wird auch in der Automobilproduktion eingesetzt. Die Systeme werden dazu benutzt, Informationen von Montageanleitungen an die Roboter im Fertigungsbereich weiterzugeben. Die verwendeten aktiven Transponder sind hitzebeständig bis zu 250 °C und können aus einer Entfernung von bis zu zehn Metern ausgelesen werden. Über den Einsatz von RFID kann dokumentiert werden, welche Schritte mit welchem Autoteil durchgeführt wurden. Damit soll die **Produktionssicherheit** erhöht werden und Verbraucherinnen und Verbrauchern Regressansprüchen erleichtert werden.

Autos werden zum Beispiel in den USA mit einem Transponder an der Windschutzscheibe versehen, um so mit Hilfe der RFID-Technik Mautstellen mit Erfassungssystemen zu passieren.

#### Vorteile

- Schutz vor Diebstahl
- Bei lizenzierten Werkstätten einfaches Zuordnen von Autos zu Besitzerinnen und Besitzern durch Verwenden einer Datenbank, welche die Nummer mit der jeweiligen Besitzerin oder dem Besitzer verknüpft
- Dokumentation von Produktion, dadurch Verbesserungen möglich

#### Nachteile

- Tag kann mit hohem Aufwand unbemerkt ausgelesen werden, und so die Wegfahrsperre überwunden werden kann

### RFID IM NAHVERKEHR

In großen Städten wie London, Istanbul und vielen asiatischen Städten wird RFID im öffentlichen Nahverkehr mittels **Smart Card** beziehungsweise **Smart Ticket** genutzt. Dabei kauft man ein Ticket, das mit einem RFID-Transponder ausgestattet ist. Die Art des Einsatzes ist unterschiedlich. Zum Teil wird beim Kauf statt eines Fahrscheins eine Plastikkarte ausgegeben, die ausgelesen wird.



Es gibt jedoch schon Testläufe mit Karten, die einen Chip enthalten und wie eine Kreditkarte des Verkehrs funktionieren. Dort wird am Ende des Monats abgerechnet.

Das gängige **Zeitkartensystem** wird teilweise mit RFID kombiniert. Dabei werden keine Papiermarken mehr ausgegeben, sondern Plastikkarten mit einem RFID-Chip. Auf diesem befinden sich

meist eindeutige Nummerncodes, die im Abgleich mit dem System die Gültigkeit des Tickets belegen. In einigen Fällen befinden sich Daten zur räumlichen und zeitlichen Gültigkeit der Karte sowie Namen und Geburtsdaten der Karteninhaberinnen und Karteninhaber auf dem Ticket. Das Auslesen der Daten beziehungsweise die Kontrolle über die Fahrberechtigung erfolgt beim Einsteigen durch Lesegeräte oder durch Kontrolleurinnen und Kontrolleure.

In Deutschland ist ein sogenanntes **eTicket** geplant. Bislang wird es nur in einigen Pilotregionen eingesetzt, es sollen jedoch bald weitere Regionen folgen. Statt eines Fahrscheins oder einer Zeitfahrkarte wird ein **Smart Ticket** gekauft. Dieses ist mit einem Transponder ausgestattet. Beim Ein- und Aussteigen wird der Transponder im Ticket von den Lesegeräten in den Verkehrsmitteln erfasst. Damit wird die getätigte Fahrt gebucht. Am Ende des Monats erhält der Kunde eine Rechnung über seine Fahrten. Die genaue Erfassung des jeweils benutzten Verkehrsmittels soll auch für die Abrechnung der verschiedenen Verkehrsbetriebe untereinander genutzt werden.

#### Vorteile

- Senken des Fälschungsrisikos
- Ein verlorenes Zeitkartenticket kann gesperrt und durch ein neues ersetzt werden
- Kostenersparnis durch Wegfall von Wartung und Reparatur von Fahrkartenautomaten
- Teilweise automatische Erfassung der Auslastung des jeweiligen Verkehrsmittels

#### Nachteile

- Personalabbau durch weitere Automatisierung
- Je nach Art des Tickets Gefahr des illegalen Erstellens von Bewegungsprofilen ohne Einwilligung des Betroffenen
- Kein anonymes Fahren möglich durch ständiges Erfassen der Verbindungsdaten beim Nutzen der Verkehrsmittel

### REISEN MIT RFID

Wer einen **elektronischen Reisepass (ePass)** hat, verreist bereits mit RFID. Der Transponder befindet sich in der Passdecke.

Im November 2005 wurde der **ePass** in Deutschland eingeführt. Der Reisepass enthält einen Chip, auf dem Daten zur Person (Name, Geburtsdatum, Ge-

schlecht, Staatsangehörigkeit) sowie zum Dokument (Seriennummer, ausstellender Staat, Gültigkeitsdatum) gespeichert sind. Zudem enthält der Chip einige biometrische Daten, die von jeder Person bei Antragstellung erhoben werden. Bei Reisepässen, die bis zum 31.10.2007 beantragt wurden, ist es das Passfoto, bei späterer Antragstellung das Passfoto sowie zwei Fingerabdrücke. Ohne diese Daten wird ein neuer Reisepass nicht ausgestellt.

Ein Zugriff auf die gespeicherten Daten soll nur möglich sein, wenn Passinhaberinnen und Passinhaber den Beamtinnen und Beamten den ePass aushändigen

und diese über ein entsprechendes Lesegerät verfügen. Ein Auslesen der Daten ohne Aushändigung des Dokuments soll durch **Verschlüsselung** verhindert werden. Dennoch ist es einem Spezialisten kurz nach Einführung des Reisepasses gelungen, durch die vorherige Beschaffung der Passdaten die Zugangssperre des Funkchips zu überwinden und die auf dem Pass sichtbaren Daten auszulesen. Gespeicherte Fingerabdrücke sind durch eine weitere Codierung geschützt.

Ab November 2010 wird auch der **neue Personalausweis** im Scheckkartenformat mit einem Chip versehen. Auf diesem werden

alle Daten gespeichert, die heute auf dem Personalausweis zu sehen sind. Das bedeutet, dass auch das Lichtbild gespeichert wird. Freiwillig ist, ob auch zusätzlich Fingerabdrücke gespeichert werden. Die biometrischen Daten sollen nur für Kontrollen an Grenzen und im Inland abgefragt werden dürfen.

Der neue Ausweis soll aber nicht nur für mehr Sicherheit sorgen, sondern auch für die Inhaberinnen und Inhaber Vorteile bringen. Immer mehr Aktionen des täglichen Lebens werden ins Internet verschoben, sei es das Online-Banking oder das Einkaufen im Internet. Auch Behörden bieten mehr und mehr Funk-

tionen und Dienstleistungen über das Internet an. Schwierig ist, dass dabei die Identität des Nutzers oftmals nicht zweifelsfrei festgestellt werden kann. Dies kann zum **Missbrauch** fremder Daten führen. Durch den elektronischen Personalausweis soll die Identität im Internet genauso sicher und einfach nachgewiesen werden können wie sonst auch.

Die Ausweisinhaberinnen und Ausweisinhaber sollen zudem durch ein **Zertifikat** die Sicherheit haben, dass die von ihnen aufgerufene Webseite auch zur Datenabfrage seines elektronischen Personalausweises berechtigt ist. Nur Anbieterinnen und Anbieter, die eine staatliche Berechtigung haben, erhalten technischen Zugang zu den Ausweisdaten.

Im Luftverkehr soll RFID zukünftig den **Gepäcktransport** erleichtern. Anstelle des Barcodes am Koffer soll ein Transponder dafür sorgen, dass kein Gepäckstück verloren geht oder an einem anderen Flughafen ankommt als der Fluggast. Der Einsatz dieses RFID-Systems wird bereits an mehreren Flughäfen mit Erfolg getestet.

#### Vorteile

Bei Ausweisdokumenten:

- Geringeres Fälschungsrisiko
- Höherer Schutz vor Dokumentenmissbrauch
- Sichere Identitätsfeststellung im Internet zur Vermeidung von Datenmissbrauch

Bei Einsatz im Luftverkehr:

- Kostenersparnis bei Fluggesellschaften durch geringere Sortier- und Zustellungsfehler
- Reduzieren von Gepäckverlusten

#### Nachteile

Bei Ausweisdokumenten:

- Mögliche Gefahr der Datenabfrage ohne Kenntnis der Ausweisinhaberinnen und Ausweisinhaber
- Mögliche Gefahr der illegalen Datenabfrage durch Unberechtigte

# PROZESSOPTIMIERUNG IM ALLTAG

## RFID IN BIBLIOTHEKEN UND BÜCHEREIEN

Bislang musste bei der **Ausleihe** in Bibliotheken und Büchereien jedes Medium einzeln von einer Mitarbeiterin oder einem Mitarbeiter erfasst werden, damit es als „verliehen“ verbucht war. In vielen Bibliotheken und Büchereien wird heute



bereits mit RFID gearbeitet, so auch in der Universitätsbibliothek der Johannes Gutenberg Universität Mainz.

Alle Medien (wie Bücher, DVDs, CDs, Zeitschriften) werden mit einem Etikett versehen, welches den Transponder enthält. Über den Chip können eine Vielzahl von medienrelevanten Informationen wie Autorin

oder Autor, Titel, Auflage, Altersbeschränkung etc., die in einer Datenbank gespeichert sind, mit dem Buch verknüpft werden. Bei der Verleihausgabe werden die Transponder dann von einem Lesegerät erfasst und ausgelesen.

Unabhängig davon, ob auch der Bibliotheks- oder Büchereiausweis mit einem Transponder ausgestattet ist, muss die Identität der Nutzerin oder des Nutzers durch Vorlage des Ausweises und gegebenenfalls durch Eingabe eines Passwortes oder einer PIN sichergestellt werden. Danach wird auf dem Nutzerkonto gespeichert, dass die erfassten Medien von ihm entliehen wurden.

Die Lesegeräte werden meist bei der Ausleihe sowie an den Ein- und Ausgängen aufgestellt. Dies liegt daran, dass auf dem Chip auch ein so genanntes Siche-

rungsbit gespeichert werden kann, welches bei ordnungsgemäßer Ausleihe gelöscht wird. Ist das Bit hingegen „aktiv“, wird beim Passieren der Lesegeräte ein Alarm ausgelöst.

### Vorteile

- Entlastung des Personals durch Automatisierung von Routinearbeiten
- Kürzere Wartezeiten, schnelleres Ausbuchen
- Sichern der Medien gegen Diebstahl
- Erleichterung beim Auffinden von Medien, die falsch einsortiert wurden und bei der Inventur
- Einsparpotential für Kommunen

### Nachteile

- Bei RFID-Einsatz im Bibliotheks- bzw. Büchereiausweis besteht bei spezieller Ausrüstung der Bibliotheken die Möglichkeit Bewegungsprofile zu erstellen
- Bei Medienrückgabe allein mittels RFID erfolgt in der Regel keine Kontrolle des Mediums auf Beschädigung
- Stellenabbau durch Automatisierung

## RFID BEI EINTRITTSKARTEN UND VERANSTALTUNGEN

Bei größeren Veranstaltungen oder Events wird vermehrt mit RFID gearbeitet, zum Beispiel bei Sportveranstaltungen, Musikkonzerten und Messen.

Unterschieden wird zwischen **Eintrittskarten aus Papier (Smart Tickets)** und Eintritts- beziehungsweise **Berechtigungskarten aus Kunststoff (Smart Cards)**. Die herkömmliche und kostengünstigere Eintrittskarte aus Papier wird meist bei einmaligem Gebrauch verwendet. Der Transponder wird hierbei zwischen zwei Papierlagen angebracht. Die Lesegeräte, meist bei den Ein- und Ausgängen der Veranstaltung angebracht, erfassen die eventuell auf dem Transponder gespeicherten Daten. Äußerlich unterscheidet sich die Eintrittskarte nicht von einer Eintrittskarte ohne Chip.

Bei mehrfacher Verwendung einer Karte wird meist eine stabilere Smart Card eingesetzt, die für die Eintritts- und Zutrittskontrolle sowie häufig auch zum Bezahlen genutzt wird. Eingesetzt wird diese unter anderem bei Dauerkarten für Sportvereine und Messen sowie bei Skipässen. Der Transponder ist hierbei direkt in der Kunststoffkarte integriert.

Bei der **Einlasskontrolle** mittels RFID kann beispielsweise das Ergebnis der Überprüfung per Software direkt mit einem Drehkreuz verbunden werden, das so nur Besucherinnen und Besucher mit gültiger Eintrittskarte einlässt. Allerdings ist von Fall zu Fall verschieden, welche Daten gespeichert werden. Manche Veranstalter nutzen die RFID-Technik „nur“ für eine automatisierte Einlasskontrolle oder zur späteren Analyse der Besucherströme. Teilweise werden lediglich die für die Nutzung relevanten Daten gespeichert (zum Beispiel das Gebiet und der Zeitraum für die Nutzungsberechtigung der Skilifte



auf Skipässen). Es gibt jedoch auch Einsätze, bei denen bereits beim Kauf der Karte Personendaten erhoben werden, die dann auf dem Chip gespeichert werden. Dies wird häufig bei Dauerkarten gemacht, die nicht auf andere Personen übertragen werden sollen. Auch die WM-Tickets zur Fußball-WM 2006 wurden personalisiert, indem auf dem Chip des Tickets eine Kundennummer gespeichert wurde, die in der Datenbank mit den Daten der Käuferin oder des Käufers verknüpft war.

#### Vorteile

- Senken des Fälschungsrisikos
- Kürzere Wartezeiten durch automatisierte Einlasskontrolle und bargeldlose Bezahlung
- Höhere Sicherheit durch Identifikation der Besucherinnen und Besucher

#### Nachteile

- Gefahr des Auslesens der Daten durch unbefugte Dritte
- Gefahr der Erstellung von Bewegungsprofilen zu Marketingzwecken der Unternehmen ohne Einwilligung der Betroffenen

### HAUS- UND NUTZTIERE UND RFID

RFID wird nicht nur bei Gegenständen verwendet, sondern auch bei Lebewesen. Dabei werden sowohl Wild- und Nutztiere als auch Haus- und Zootiere mit einem Chip versehen. Der Zweck bei Nutztieren ist es, Bestand und Logistik zu kontrollieren. Bei Haustieren dient es dem eindeutigen Zuordnen eines Tieres zu seiner Besitzerin oder seinem Besitzer.

Praktisch jedes Tier kann getaggt werden. Zu Forschungszwecken wurden schon Bienen mit winzigen Transpondern ausgestattet, um unter anderem ihr Flugverhalten verfolgen zu können.

Bei Haustieren wird der etwa reiskorngroße Chip von einer Tierärztin oder einem Tierarzt mit einer Spezialkanüle ins Bindegewebe eingesetzt (so genanntes Chippen). Jeder Chip enthält eine einmalige Nummer mit 15 Stellen, wobei die ersten drei Ziffern einen Ländercode (zum Beispiel 276 für Deutschland) darstellen.



Mit Hilfe eines Lesegeräts wird die Nummer ausgelesen. Durch Abgleichen mit einer Datenbank, bei der die jeweilige Besitzerin oder der Besitzer mit Nummer hinterlegt ist, kann die Besitzerin oder der Besitzer ermittelt werden.

Bei Nutztieren findet das RFID-System bereits breite Anwendung, auch aufgrund des frühen flächendeckenden Einsatzes in den USA. Bei Haustieren gibt es in der Schweiz eine gesetzliche Pflicht, jedes Tier bereits mit drei Monaten zu chippen, in Deutschland

ist es bisher bundesgesetzlich nicht geregelt. Einige Hunde-Verordnungen der Länder (Nordrhein-Westfalen, Hamburg, Berlin) legen eine Pflicht zum Chippen fest. Will man in den EU-Ländern reisen, muss man einen Heimtierausweis mitführen, der eine Kennzeichnung des jeweiligen Tieres enthält. Bis Juli 2011 ist als Tierkennzeichnung eine Tätowierung anerkannt, danach nur noch implantierte Transponder.

#### Vorteile

Bei Haustieren:

- Tiere können schneller ihrem Besitzer zugeordnet werden
- Weniger Tiere werden ausgesetzt, da Tiere nun eindeutig zugeordnet werden können
- Beim Einsetzen keine Vollnarkose erforderlich

Bei Nutztieren:

- Herkunft der Tiere lässt sich verifizieren
- Erleichtert die Logistik mit Tieren

#### Nachteile

Bei Haustieren:

- Gechipptes Tier ist nicht als solches erkennbar
- Durch Fehler beim Einsetzen ist ein „Wandern“ des Chips im Körper möglich

Bei Nutztieren:

- Gefahr der Manipulation von außen, zum Beispiel wenn Name der Eigentümerin oder des Eigentümers verändert wird

# VORTEILE UND NACHTEILE – AUF EINEN BLICK

Auf den vorangegangenen Seiten wurde gezeigt, wo RFID beispielsweise eingesetzt wird. Die jeweiligen Vor- und Nachteile sind hier noch einmal gesammelt dargestellt:

## VORTEILE

- Steigerung der Effizienz von logistischen Prozessen
- Arbeitserleichterung
- Kostensenkung durch effiziente Nutzung von Ressourcen möglich
- Produktionssteuerung
- Zugangsmanagement
- Verbesserte Erkenntnisgewinnungsmöglichkeiten für Forschung (Verhalten von Tieren)
- Diebstahlsicherung
- Inventarkontrolle
- Senkung von Personalkosten
- Sicherheit durch bessere Personenidentifikation
- Kürzere Wartezeiten
- Sicherung durch bessere Identifikation von Originalen und damit Schutz vor Plagiaten

## NACHTEILE

---

- Möglichkeit, Bewegungsprofile zu erstellen  
– so genannte Tracking-Maßnahmen
- Die oder der Einzelne hat keine Kenntnis darüber,  
wann und wer ihre oder seine mitgeführten RFID-Chips ausliest
- Stellenabbau durch Automatisierung
- Durch elektromagnetische Strahlungsbelastung sind Risiken  
für die Gesundheit möglich
- Begrenzte Reichweite
- Problem der Entsorgung bei massenhaftem Einsatz von RFID-Transpondern
- Unklar, was mit gesammelten Daten und Datenbanken später passieren soll
- Gefahr des Datenmissbrauchs
- Gefahr der Manipulation der Daten durch Dritte
- Bei flächendeckendem Einsatz von RFID, droht Gefahr der einseitigen  
Abhängigkeit von einer Technologie, die von außen angreifbar wird  
(Worst-case-Szenario)

# Herausforderungen und Perspektiven



# GESUNDHEITSBELASTUNG DURCH RFID?

Wie bereits auf den Seiten 8 bis 11 dargestellt, findet bei einem **RFID-System** ein Informationsaustausch zwischen Transponder und Lesegerät statt. Die Informationen werden durch elektromagnetische Felder (EMF) transportiert. Erzeugt werden elektromagnetische Felder durch Lesegeräte und aktive Transponder. Passive Transponder erzeugen keine eigenen Felder, sondern beziehen ihre Energie aus den Feldern der Lesegeräte. Bislang werden im verbraucher-nahen Bereich nur passive Transponder eingesetzt. Die elektromagnetischen



Felder, die hier zur Anwendung kommen, sind dem Bereich der nichtionisierenden Strahlung zuzuordnen.

Bei der Vielfalt der Einsatzmöglichkeiten von **RFID-Systemen** variieren die verwendeten Frequenzen und Sendeleistungen. Dadurch unterscheidet sich auch die Intensität der durch elektromagnetische Felder erzeugten Strahlung, der man möglicherweise ausgesetzt ist. Für die

Verbraucherinnen und Verbraucher sind dabei insbesondere die Elektronischen Artikelsicherungssysteme (EAS) in Ausgangsbereichen der Geschäfte, dem sogenannten Schleusenbereich, von Bedeutung.

Bei Untersuchungen im Schleusenbereich von einigen EAS-Systemen (vgl. zu EAS-Systemen Seite 21) wurden zum Teil, bei einem Abstand von unter 0,5 Metern, sehr starke elektromagnetische Felder gemessen. Deshalb sollten

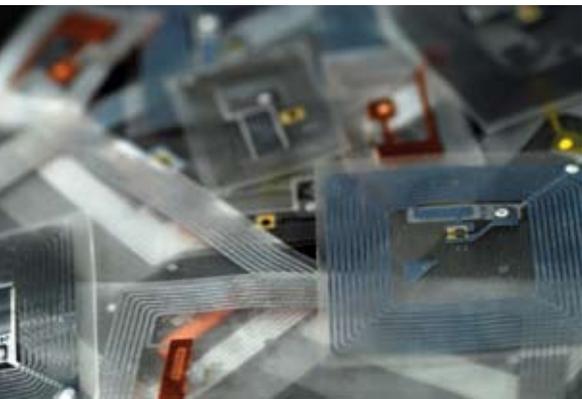
sich Trägerinnen und Träger von **aktiven elektronischen Implantaten** wie zum Beispiel Herzschrittmachern oder implantierten Defibrillatoren informieren, ob die Implantate auf **Verträglichkeit mit elektromagnetischen Feldern** hin überprüft wurden. Bei früheren Studien wurde festgestellt, dass gewisse EAS-Systeme Fehlfunktionen bei Implantaten auslösen können. International und national, so auch vom Bundesamt für Strahlenschutz, wird Trägern von Implantaten empfohlen sich nicht länger als nötig in der Nähe von EAS-Systemen im Schleusenbereich aufzuhalten. Die Verbraucherinnen und Verbraucher sollten im Übrigen im Schleusenbereich mit großen und übersichtlichen Hinweisschildern auf das Vorhandensein eines Artikelüberwachungssystems aufmerksam gemacht werden.

# RFID CONTRA RECYCLING?

RFID-Systeme werden heute beispielsweise im Rahmen von Forschungsprojekten zur Trennung von Stahlschrott oder für die Wiederaufbereitung von Stahlfässern eingesetzt. Mit Hilfe von RFID-Systemen könnte **Abfallverwertung** kostengünstiger und umweltschonender gestaltet werden.

RFID kann das **Recycling** aber auch erschweren, da die einzelnen Komponenten schwer voneinander trennbar sind. Recycling bedeutet, dass durch stoffliche Verwertung Abfallstoffströme aufbereitet werden können, um vermarktungsfähige Sekundärrohstoffe wieder zu gewinnen oder dass durch energetische Verwertung (zum Beispiel Verbrennung) Energie gewonnen wird.

Häufig werden RFID-Chips nur einmal verwendet und dann entsorgt. Laut einem Umweltforschungsplan des Bundesumweltamtes aus dem Jahr 2009 kann der derzeit durch den Einsatz von RFID anfallende Müll mit den herkömmlichen Entsorgungssystemen bewältigt werden. Ungewiss ist, welche Auswirkungen wachsende RFID-Märkte auf das Recycling haben werden.



Ein einzelner passiver RFID-Chip, so wie er heute bereits in Produktion und Logistik Einsatz findet, besteht hauptsächlich aus Silizium, Nickel, Polyurethan, Kupfer bzw. Aluminium

oder Silber. Diese Bestandteile sind beim Recycling schwer voneinander zu trennen, besonders, wenn der Chip fest mit der Verpackung verbunden ist. Sortenreines Verpackungsmaterial wie Altglas, Altpapier oder Kunststoff kann durch die RFID-Chips verunreinigt werden. **Mögliche Risiken** können aufwendigeres Recycling oder mindere Qualität der entstehenden Rohstoffe sein.

Besondere **Schwierigkeiten** würde das Trennen von Glas und Transpondern, die hauptsächlich aus Kupfer bestehen, bereiten. Einer Untersuchung zufolge können bereits geringe Mengen Metall das Glas verfärben, das üblicherweise nach dem Zersplittern geschmolzen wird. Die Grenzwerte für Kupfer würden überschritten, wenn nur 2,5 Prozent der Flaschen mit einem Kupfer-RFID-Chip versehen wären.



Eine Lösung, wie sie auch das Bundesumweltamt in seiner Analyse vorschlägt, ist es, dass Tags selbst so intelligent gestaltet werden (Eco-design), dass sie leicht trennbar werden. Vorstellbar wäre es, wenn bereits von vornherein ein automatisches Abtrennen der Transponder bei Passieren der Lesegeräte am Eingang der Entsorgungsstellen vorgesehen werden würde.

# GLÄSERNE KUNDINNEN UND KUNDEN DANK RFID?

Die in dieser Broschüre beschriebenen Beispiele stellen lediglich einen Teil der Einsatzmöglichkeiten für die noch neue Technologie RFID dar. Der Einsatz von RFID beschränkt sich derzeit vornehmlich auf die Logistik und auf die Automatisierung einfacher Arbeitsabläufe. Doch je mehr RFID eingesetzt wird, desto höher ist die Gefahr, dass Daten gesammelt und auch genutzt werden.

Sollte es zukünftig zu einer **flächendeckenden Anwendung** von RFID in und an Produkten, in Kundenkarten sowie in Ausweisen und Tickets kommen, besteht die Möglichkeit Kauf- und Bewegungsprofile zu erstellen. Supermarktbetreiberinnen und -betreiber könnten dann über den Chip

auf der Rabattkarte und die im Eingangsbereich aufgestellten Lesegeräte wissen, welche Kundinnen und Kunden den Geschäftsraum gerade betreten haben und könnten das Kaufverhalten jedes Einzelnen durch Transponder an den Produkten sowie aufgestellter Lesegeräte im ganzen Geschäft erfassen. Wie lange bleiben welche Kundinnen

und Kunden vor welchem Regal stehen? Wie reagieren Kundinnen und Kunden auf die individuell auf sie eingestellte Werbung an ihren Einkaufswagen? Wird tatsächlich das beworbene Produkt gekauft? Mag das dem einen oder anderen bis hierhin noch recht praktisch erscheinen, so endet diese Einstellung in dem Moment, in dem man dank seines Kaufverhaltens als „schlechte Kundin“ oder „schlechter Kunde“ eingestuft wurde und Nachteile erleidet.

Unerfreulich könnte es auch werden, wenn die eben in der Apotheke gekauften Medikamente mit Transpondern ausgestattet sind und Lesegeräte im Supermarkt, Kaufhaus, Arbeitgeberin oder Arbeitgeber in der Lage sind, diese Me-

dikamente in der Tasche der Kundinnen und Kunden zu identifizieren. Sollten sich Betreiberinnen und Betreiber nicht an die gesetzlichen Vorgaben halten, könnten diese im **Zusammenhang mit der Kundenkarte** Kenntnis über mögliche Krankheiten ihrer Kundinnen und Kunden erhalten.

Das Bundesdatenschutzgesetz sieht vor, dass ein Unternehmen nur dann **personenbezogene Daten** erheben, nutzen oder verwenden darf, wenn es dafür eine Rechtsgrundlage gibt oder wenn Verbraucherinnen und Verbraucher ihre **Einwilligung** dazu erteilen. Es gibt generell keine Rechtsgrundlage dafür, Daten des persönlichen Kaufverhaltens analysieren und speichern zu dürfen. Die Betreiberinnen und Betreiber nutzen jedoch die Möglichkeit, sich die Einwilligung hierfür geben zu lassen. Diese kann zum Beispiel beim Ausstellen einer Kundenkarte im „Kleingedruckten“ zu finden sein.

Ob das **Bundesdatenschutzgesetz** beim Einsatz von RFID in verbraucherrelevanten Bereichen ausreichend Schutz bietet oder weitere Regeln notwendig sind, ist umstritten. Zurzeit verhandeln Politik und Wirtschaft über eine Selbstverpflichtung der Wirtschaft, um das Vertrauen in die Technologie bei Verbraucherinnen und Verbrauchern zu stärken. Der Landesbeauftragte für den Datenschutz in Rheinland-Pfalz fordert zum Schutz der Verbraucherinnen und Verbraucher gesetzliche Regelungen, mit denen den Gefahren, die mit RFID verbunden sind, besser begegnet werden kann.

Einigen mag es gleichgültig sein, ob ihr Kaufverhalten analysiert und Bewegungsprofile erstellt werden. Den Meisten wird es jedoch unangenehm sein, auch wenn sie an sich nichts zu verbergen haben. Es macht einen Unterschied, ob um Informationen gebeten wird oder ob heimlich analysiert wird.



# „INTERNET DER DINGE“ – WAS IST MÖGLICH?

Als „Internet der Dinge“ („Internet of Things“) wird die Vorstellung von einer Welt bezeichnet, in der alle Gegenstände und Menschen miteinander vernetzt sind. Bereits bestehende Netzwerke sollen mit der physischen Welt verknüpft werden. Gegenstände können „intelligent“ miteinander kommunizieren.

Im Zusammenhang mit RFID bedeutet „Internet der Dinge“ dass jeder einzelne Gegenstand über die jeweiligen Datenbanken, die wiederum mit einem großen System verbunden werden sollen, mit anderen kommunizieren kann. Die



Transponder an den Gegenständen geben dann nicht nur Auskunft über sich und ihren Status, sondern kommunizieren miteinander und mit ihrer Umwelt. Vorstellbar ist es, die Transponder mit Sensoren auszustatten, die zum Beispiel Temperatur, Feuchtigkeit, Vibrationen und Helligkeit messen können. Mit Hilfe einer GPS-Funktion könnten Gegenstände erkennen, wo sie sind und dies mitteilen. Sie könnten sich

so selbst steuern, statt zentral gesteuert zu werden. Ein Joghurtbecher könnte zum Beispiel selbständig seinen Weg zu Adressatin oder Adressat finden, wenn sein Transponder entsprechende Informationen enthält. Er wählt dann von Knotenpunkt zu Knotenpunkt eigenständig jeweils den Weg, der gerade frei oder am kürzesten ist.

Die Vorstellung einer **globalen Vernetzung** aller Dinge passt zu dem Gedanken des Ubiquitous Computing, der Anfang der 90er Jahre entwickelt wurde. Ubiquitous Computing bedeutet, dass rechnergestützte Informationsverarbeitung allgegenwärtig sein wird. Der Computer als Gerät soll verschwinden und stattdessen durch intelligente Geräte ersetzt werden, die den Menschen bei seinen Tätigkeiten unmerklich unterstützen.

Um beim Bild des Joghurtbechers zu bleiben, stelle man sich vor, dass dieser beim Verbraucher oder Verbraucher im Kühlschrank steht. Der intelligente Kühlschrank registriert, wenn der Chip auf dem Joghurtbecher, der ja das Abfülldatum und die Lagertemperatur kennt, meldet, dass der Joghurt demnächst zu verderben droht und gibt diese Information weiter an den Menschen.

Vorstellbar ist auch eine mit einem Chip versehene Waschmaschine, die den Strompreis beobachtet. Sie wäscht erst dann, wenn es preisgünstig ist. Ist die Wäsche ebenfalls mit RFID-Chips versehen, prüft die Maschine, welches Reinigungsprogramm richtig für die Wäsche ist.

Diese Szenarien klingen nach einer für den Menschen immer einfacheren Welt. Er muss sich nicht mehr um die alltäglichen Dinge kümmern. Maschinen denken für ihn mit. Die Gefahr bei einem solchen „Internet der Dinge“ besteht jedoch darin, dass die RFID-Technik mühelos dazu missbraucht werden könnte, unauffällig und gesetzeswidrig Menschen zu überwachen.

Bei solchen Zukunftsaussichten müssen Unternehmen und Politik eng zusammenarbeiten, um verbindliche Regeln aufzustellen, die die Rechte des Einzelnen schützen und die widerstreitenden Interessen miteinander in Ausgleich bringen.

# VERBRAUCHERTIPPS



## ■ Aufmerksamkeit

Welche Technologie auch zum Einsatz kommt: Der beste Datenschutz ist, dass Sie selbst sparsam mit Ihren Daten umgehen. Bleiben Sie wachsam, wem Sie Ihre Daten überlassen. Lesen Sie bei Verträgen das Kleingedruckte und die Allgemeinen Geschäftsbedingungen.

## ■ Zweckbindung klären

Wenn Sie Daten überlassen, achten Sie darauf, dass vorher eine Zweckbindung dieser Daten festgelegt wird. Fehlt es an einer vorher festgelegten Zweckbindung, besteht die Gefahr, dass die Daten später für andere Zwecke benutzt werden oder an andere Unternehmen weitergegeben werden.

## ■ Nachfragen

Fragen Sie nach, ob RFID verwendet wird. Wenn ja, erkundigen Sie sich genau, welche Daten gespeichert wurden und wer Zugriff auf diese Daten hat. Darüber hinaus sollten Sie sich erkundigen, wie im Vorfeld über den Einsatz von RFID aufgeklärt wurde. Erteilt man Ihnen keine Auskunft, machen Sie Gebrauch von Ihren Rechten aus dem Bundesdatenschutzgesetz, fragen Sie noch mal nach unter Hinweis auf Ihr Auskunftsrecht aus § 34 Bundesdatenschutzgesetz.

## ■ Transponder entfernen

Achten Sie auf mit EPC-Global versehene Produkte und lassen Sie die Transponder beim Kauf ausschalten oder entfernen.

## ■ Hilfe

Sollten Sie auf Ihr Auskunftsverlangen hin keine Antwort erhalten, wenden Sie sich an die zuständigen Datenschutzbeauftragten oder an die Verbraucherzentralen.

Je mehr Aufmerksamkeit dem Einsatz von RFID geschenkt wird und die Wirtschaft das Bedürfnis der Verbraucherinnen und Verbraucher und die Politik das Bedürfnis der Bürgerinnen und Bürger nach Aufklärung wahrnimmt, desto eher wird ein offener Dialog über Chancen und Risiken dieser Technologie möglich sein.

**aktiver Transponder** Transponder mit eigener Batterie

**Ecodesign** Ziel ist es, mit intelligentem Einsatz verfügbarer Ressourcen einen möglichst großen Nutzen für alle Beteiligten bei minimaler Umweltbelastung und unter sozial fairen Bedingungen zu erreichen

**Elektromagnetische Felder (EMF)** Durch bewegte elektrische Ladung entstehende Bereiche

**Elektromagnetische Wellen** Welle aus gekoppelten elektrischen und magnetischen Feldern z.B. Radiowellen; benötigt kein Medium um sich auszubreiten ( $\neq$  Schallwellen)

**Electronic Article Surveillance** EAS = Einsatz einfacher Transponder zur Diebstahlsicherung

**Electronic Product Code** EPC = weltweit eindeutigen 24-stellige Nummerncode, entwickelt von der Non-Profit-Organisation EPCglobal

**„Internet der Dinge“** Internet und reale Welt wird so miteinander verknüpft, dass intelligente Gegenstände entstehen

**Lesegerät/Reader** Gerät, das die Transponder mit seiner Antenne anfunkelt und deren Daten liest

**Opt-in-Prinzip** Person muss aktiv einwilligen  $\neq$  Opt-out-Prinzip

**passiver Transponder** Transponder, der seine Energie aus dem elektromagnetischen Feld des Lesegeräts bezieht

**Pre-Paid-System** Aufladen einer Karte, mit der so lange bezahlt werden kann, bis das Guthaben verbraucht ist

**Post-Paid-System** Karte wird im Laufe des Aufenthalts mit den jeweiligen Kaufpreisen belastet, bezahlt wird beim Verlassen an der Kasse

**Radio Frequency Identification** zu dt.: Identifizierung per Funk/mit Hilfe von elektromagnetischen Wellen; es ermöglicht kontaktloses Speichern und Auslesen von Daten

**Smart Card** Plastikkarte, die einen kontaktlosen Chip enthält; Nutzung meist als Ausweis oder Kundenkarte

**Smart Ticket** Papierticket, das einen kontaktlosen Chip enthält; meist für einmalige Verwendung als Fahrschein oder Eintrittskarte genutzt

**Source Tagging** Produkte werden bereits bei der Herstellung mit Tags versehen

**Strichcode / Barcode** optischelektronisch lesbare Schrift, die aus verschiedenen breiten, parallelen Strichen und Lücken besteht; Daten werden in binären Symbolen abgebildet und von optischen Lesegeräten maschinell eingelesen und elektronisch weiterverarbeitet

**Tag** Transponder/RFID-Chip

**Transponder** Kunstwort der Begriffe „transmit“ und „response“; bezeichnet den Chip inklusive Antenne, der an/in Gegenständen oder Lebewesen platziert wird um diese mit Hilfe des Readers zu identifizieren und zu orten

**Ubiquitous Computing** Vorstellung davon, dass rechnergestützte Informationsverarbeitung allgegenwärtig sein wird

### **Ministerium für Umwelt, Forsten und Verbraucherschutz**

Das Ministerium für Umwelt, Forsten und Verbraucherschutz Rheinland Pfalz ist innerhalb der Landesregierung zuständig für die Bereiche Umwelt, Naturschutz, nachhaltige Entwicklung, Wasserwirtschaft, Forsten, Gewerbeaufsicht, Immissionsschutz, Chemikalienrecht, Gentechnik, Abfall- und Rohstoffwirtschaft, Bodenschutz, Energie, Atomaufsicht, Strahlenschutz, Veterinärwesen, Tierschutz, gesundheitlicher und wirtschaftlicher Verbraucherschutz.

Richtschnur der Arbeit des Ministeriums ist das Leitbild der nachhaltigen Entwicklung. Nachhaltig heißt hierbei, die ökonomischen und ökologischen Lebensgrundlagen, Gesundheit, Ressourcen, Natur und Umwelt zu erhalten und zu verbessern sowie den sozialen Ausgleich sicherzustellen.

Seit dem 20. September 2001 ist Margit Conrad Staatsministerin für Umwelt, Forsten und Verbraucherschutz Rheinland-Pfalz.

Beim Einsatz von RFID müssen aus Sicht der Ministerin vor allem Information, Transparenz und Wahlfreiheit gewährleistet sein. Diese Faktoren sind notwendig, damit Verbraucherinnen und Verbraucher Vertrauen in die RFID-Technologie entwickeln können. Conrad: „Unser Leitbild sind informierte Verbraucherinnen und Verbraucher, die ihre Kaufentscheidung bewusst treffen.“

### **Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz**

Der Landesbeauftragte für den Datenschutz ist in Rheinland-Pfalz als Kontrollinstanz für den öffentlichen Bereich und als Datenschutzaufsichtsbehörde für die privaten Stellen (Unternehmen) tätig.

Er ist als unabhängige oberste Landesbehörde beim Landtag Rheinland-Pfalz eingerichtet.

In Bezug auf die öffentlichen und die privaten Stellen überwacht er die Einhaltung der Datenschutzgesetze und anderer Vorschriften über den Datenschutz. Er berät den Landtag, die Landesregierung und ihre Mitglieder sowie die datenverarbeitenden Stellen in Fragen des Datenschutzes und führt örtliche Kontrollen durch. Bedeutsam ist auch seine Aufgabe, Beschwerden von Bürgern nachzugehen.

Seit 15. April 2007 ist Edgar Wagner Landesbeauftragter für den Datenschutz in Rheinland-Pfalz.

Besonders wichtig ist dem Landesbeauftragten für den Datenschutz, dass die Bürgerinnen und Bürger in Hinblick auf den Einsatz von RFID ein Bewusstsein dafür entwickeln, was dies für ihre Daten bedeuten kann und wie sie sich schützen können. Dazu Wagner: „Es ist wichtig, die Bürger aufzuklären und ihnen so ein Bewusstsein dafür zu vermitteln, was Datenschutz bedeutet.“

## MITGLIEDER DES VERBRAUCHERDIALOGS RFID

---

Ziel des Verbraucherdialogs RFID ist es, sich vor einer großflächigen Einführung der Technologie auf Maßnahmen zu verständigen, die die Interessen der Verbraucherinnen und Verbraucher hinreichend berücksichtigen. Hierzu fanden sich am 25.08.2008 erstmals die Mitglieder unter der Schirmherrschaft des Ministerium für Umwelt, Forsten und Verbraucherschutz und des Landesbeauftragten für den Datenschutz Rheinland-Pfalz zusammen.

Der Verbraucherdialog RFID hat folgende Mitglieder:

### **Arbeitsgemeinschaft der Landfrauenverbände**

in Rheinland-Pfalz  
Burgenlandstraße 7  
55543 Bad Kreuznach  
[www.landfrau-rlp.de](http://www.landfrau-rlp.de)

### **Arbeitsgemeinschaft ev. Haushaltsführungskräfte des deutschen ev. Frauenbundes e.V. (DEF) Landesverband Rheinland-Pfalz (AEH)**

Keltenstraße 7  
67598 Gundersheim  
[www.evangelische-frauen.de](http://www.evangelische-frauen.de)

### **Bluhm Systeme**

Maarweg 33  
53619 Rheinbreitbach  
<http://www.bluhmsysteme.com/>

### **Bundesamt für Sicherheit in der Informationstechnik**

Godesberger Allee 185 – 189  
53175 Bonn  
<https://www.bsi.bund.de>

### **Bundesverband Informationswirtschaft, Telekommunikation und neue Medien**

Albrechtstraße 10a  
10117 Berlin-Mitte  
<http://www.bitkom.org/>

### **Deutsche Vereinigung für Datenschutz**

Bonner Talweg 33 – 35  
53113 Bonn

### **Ministerium für Arbeit, Soziales, Gesundheit, Familie und Frauen**

Bauhofstraße 9  
55116 Mainz  
<http://www.masfg.rlp.de>

### **Ministerium für Umwelt, Forsten und Verbraucherschutz**

Kaiser-Friedrich-Straße 1  
55116 Mainz  
[www.mufv.rlp.de](http://www.mufv.rlp.de)

### **Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau**

Stiftsstraße 9  
55116 Mainz  
[www.mwvlw.rlp.de](http://www.mwvlw.rlp.de)

### **SONTAG THE TAG-MAKER**

Ingelheimer Straße 7  
55268 Nieder-Olm  
<http://www.sontag.biz/>

### **Verband Deutscher Verkehrsunternehmen, Landesgruppe Südwest**

Mozartstraße 8  
55118 Mainz  
[www.vdv.de](http://www.vdv.de)

### **Deutscher Bibliothekenverband, Landesverband Rheinland-Pfalz**

Bahnhofplatz 14  
56068 Koblenz

### **Industrie- und Handelskammer Koblenz**

Schlossstraße 2  
56068 Koblenz  
<http://www.pfalz.ihk24.de>

### **Kompetenzstelle RFID**

Technische Universität Kaiserslautern  
Paul Ehrlich Straße Gebäude 34  
67653 Kaiserslautern

### **Landesapothekerkammer**

Rheinland-Pfalz  
Am Gautor 15  
55131 Mainz  
<http://www.lak-rlp.de/>

### **Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz**

Hinterer Bleiche 34  
55116 Mainz  
<http://www.datenschutz.rlp.de>

### **Ministerium des Innern und für Sport**

Wallstraße 3  
55122 Mainz  
[www.ism.rlp.de](http://www.ism.rlp.de)

### **Verband für Automatische Identifikation, Datenerfassung und Mobile Datenkommunikation**

Richard-Weber-Straße 29  
68623 Lampertheim  
<http://www.aim-d.de/>

### **Verband für den IT-Mittelstand**

Augustastrasse 78-80  
52070 Aachen  
<http://www.bitmi.de>

### **Verbraucherservice im Katholischen**

**Deutschen Frauenbund**  
Schützenheimweg 23b  
93049 Regensburg  
<http://www.frauenbund.de>

### **Verbraucherzentrale Rheinland-Pfalz**

Seppel-Glückert-Passage 10  
55116 Mainz  
<http://www.verbraucherzentrale-rlp.de>

### **Verkehrsclub Deutschland, Landesverband Rheinland-Pfalz**

Eltzerhofstraße 10  
56068 Koblenz  
<http://www.vcd.org/>

### **Ansprechpartnerinnen und Ansprechpartner**

#### **Verbraucherzentrale Rheinland-Pfalz**

Seppel-Glückert-Passage 10  
55116 Mainz  
Tel.: 06131 / 2848 - 0

E-Mail: [info@vz-rlp.de](mailto:info@vz-rlp.de).

Internet: <http://www.verbraucherzentrale-rlp.de>

#### **Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz**

Hintere Bleiche 34  
55116 Mainz  
Tel.: 06131 208 - 2449  
Fax: 06131 208 - 2497

E-Mail: [poststelle@datenschutz.rlp.de](mailto:poststelle@datenschutz.rlp.de)

Internet: <http://www.dateschutz.rlp.de>

#### **Ministerium für Umwelt, Forsten und Verbraucherschutz**

Kaiser-Friedrich-Straße 1  
55116 Mainz

Tel.: 06131 16 - 0  
Fax: 06131 16 - 4649

E-Mail: [poststelle@mufv.rlp.de](mailto:poststelle@mufv.rlp.de)

Internet: [www.mufv.de](http://www.mufv.de)

### **Links**

[www.discoverrfid.org](http://www.discoverrfid.org)  
[www.foebud.org/rfid](http://www.foebud.org/rfid)  
[www.info-rfid.de](http://www.info-rfid.de)  
[www.rfidatlas.de](http://www.rfidatlas.de)  
[www.rfid-basis.de](http://www.rfid-basis.de)  
[www.rfid-im-blick.de](http://www.rfid-im-blick.de)  
[www.rfid-informationen.de](http://www.rfid-informationen.de)  
[www.rfid-journal.de](http://www.rfid-journal.de)  
[www.aim-d.de](http://www.aim-d.de)  
[www.kompetenzzentrum-autoid.de](http://www.kompetenzzentrum-autoid.de)  
[www.foebud.org/rfid](http://www.foebud.org/rfid)  
[www.rfid-journal.de](http://www.rfid-journal.de)

Bundesdatenschutzgesetz:

[http://www.gesetze-im-internet.de/bdsg\\_1990/index.html](http://www.gesetze-im-internet.de/bdsg_1990/index.html)

Empfehlung der Kommission:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:DE:PDF>

Selbstverpflichtung der EPCglobal:

[http://www.epcglobalinc.org/public/ppsc\\_guide/](http://www.epcglobalinc.org/public/ppsc_guide/)  
[http://www.gs1-germany.de/internet/common/downloads/epc\\_rfid/3001\\_daten\\_verbraucherschutz.pdf](http://www.gs1-germany.de/internet/common/downloads/epc_rfid/3001_daten_verbraucherschutz.pdf)

Internetseite des Bundesamtes für Sicherheit in der Informationstechnik:  
[https://www.bsi.bund.de/cln\\_165/DE/Themen/ElektronischeAusweise/Radio-FrequencyIdentification/radiofrequencyidentification\\_node.html](https://www.bsi.bund.de/cln_165/DE/Themen/ElektronischeAusweise/Radio-FrequencyIdentification/radiofrequencyidentification_node.html)

Studie des Bundesamtes für Sicherheit in der Informationstechnik:  
[https://www.bsi.bund.de/cln\\_165/sid\\_8444741D3AE3C3C5556056270F7DAE38/DE/Themen/ElektronischeAusweise/RadioFrequencyIdentification/RFIDStudie/rfidstudie\\_node.html](https://www.bsi.bund.de/cln_165/sid_8444741D3AE3C3C5556056270F7DAE38/DE/Themen/ElektronischeAusweise/RadioFrequencyIdentification/RFIDStudie/rfidstudie_node.html)

### **Literaturtipps**

**Finkenzeller, Klaus**

RFID-Handbuch, Grundlagen und praktische Anwendungen von Transpondern, kontaktloser Chipkarten und NFC, 5. Aufl., München 2003

**Hasen, Marit / Wiese, Markus**

RFID-Radio Frequency Identification, in: Datenschutz und Datensicherung 2004, 109

**Kelter, Harald / Wittmann, Stefan**

Radio Frequency Identification – RFID, Chancen und Risiken des RFID-Einsatzes, in: Datenschutz und Datensicherung 2004, 331 f.

**Salditt, Thomas C.**

Netzwerkmanagement im Handel, Prozessinnovationen im Handel am Beispiel der RFID-Technologie, 1. Aufl., Wiesbaden 2008

**Straube, Frank / Bensel, Philipp / Spiegel, Timo / Vogeler, Stefan**

Themenfeld: Supply Chain Management: Aktuelle Situation der RFID-Standardisierung, Digitale Schriftenreihe Logistik der Technischen Universität Berlin

**Dirk Henrici**

RFID Security and Privacy– Concepts, Protocols and Architectures; Lecture Notes in Electrical Engineering, Nr. 17; Springer-Verlag; 2008; +

**Henrici, D. / Kabzeva, A. / Fleuren, T. / Müller, P.**

Data Storage in RFID Systems

In Radio Frequency Identification Fundamentals and Applications Bringing Research to Practice INTECH., February 2010

**Fleuren, T. / Müller, P.**

RFID und Datenschutz – Noch wird nicht auf derselben Wellenlänge gefunkt

In WIK-Zeitschrift für die Sicherheit der Wirtschaft (5/2009) (p. 72). SecuMedia Verlags-GmbH, May 2009

## Impressum

### Herausgeber:

Ministerium für Umwelt, Forsten und Verbraucherschutz

Kaiser-Friedrich-Straße 1

55116 Mainz

Tel.: 06131 16-0

Fax: 06131 16-4649

E-Mail: [poststelle@mufv.rlp.de](mailto:poststelle@mufv.rlp.de)

Internet: [www.mufv.de](http://www.mufv.de)

Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz

Hintere Bleiche 34

55116 Mainz

Tel.: 06131 208-2449

Fax: 06131 208-2497

E-Mail: [poststelle@datenschutz.rlp.de](mailto:poststelle@datenschutz.rlp.de)

Internet: <http://www.dateschutz.rlp.de>

**Text:** Gabriele Wolff, Jule Marie Schätzel

**Bildnachweis:** Fotolia: Ideeah Studio (Titelseite), Albert Lozano-Nieto S. 6, S. 41, S. 44,

Fineas S. 12, Stas Perov S. 18, seen S. 18, Frank-Peter Funke S. 18, Eisenhans S. 18, Stiefi S. 22,

shocky S. 24, Gina Sanders S. 26, Teodor Ostojic S. 28, eyeami S. 30, 313 S. 32, Robert Kneschke

S. 34, DWP S. 36, mbs S. 37, Herbie S. 41, S. 45, Benjamin Haas S. 41, rotoGraphics S. 41, Volker

Werner S. 41, Pavel Losevsky S. 48, ISO K°-photography S. 50 / Metro Group Future Store Ini-

tiative: S. 10, S. 16, S. 20, S. 42, S. 46 / Der Landesbeauftragte für den Datenschutz Rheinland-

Pfalz: S. 3 / Ministerium für Umwelt, Forsten und Verbraucherschutz Rheinland-Pfalz: S. 3

**Redaktion:** Ministerium für Umwelt, Forsten und Verbraucherschutz

Christiane Schäfer, Funda Römer, Julius Rohn

**Layout:** [design.buero.schneider](http://design.buero.schneider.de), [www.debusc.de](http://www.debusc.de)

**Druck:** Druckerei Schwalm, Mainz

Auflage: 8000

Stand: August 2010