BITKOM

Informationspapier

Radio Frequency Identification (RFID) in der Diskussion

Technik, Einsatzformen, Datenschutz

RFID: Ein Überblick

RFID kommt! Über verschiedene Einsatzfelder hinweg revolutioniert RFID nicht nur Geschäftsprozesse, sondern bringt dem privaten Nutzer wahrnehmbaren Mehrwert im täglichen Leben. Schon heute trägt fast jeder Autofahrer mit dem Autoschlüssel einen RFID-Tag in der Tasche und sichert damit sein Auto gegen unbefugten Zugriff. Auf dem Weg zum Büro öffnet er mit Hilfe von RFID-Technologie das Tor der Tiefgarage und erhält Zutritt zu seinem abgesicherten Arbeitsbereich. In vielen Fällen wird auch dort RFID kein Fremdwort sein, sondern RFID trägt zur höheren Produktivität des Unternehmens bei – und das in einer Vielzahl von Branchen. In der Freizeit schließlich trifft der Nutzer bald schon auf „sprechende Plakate". Diese beinhalten nicht nur Informationen zu Veranstaltungen, sondern ermöglichen auch gleich den entsprechenden Ticketkauf, zum Beispiel per RFID-fähigen Handys.

Das wirtschaftliche Potenzial von RFID geht über diese Beispiele weit hinaus: Allein für den europäischen Markt im Handelsbereich erwarten Analysten einen Umsatz von Euro 2,5 Mrd. bis 2008. Darin erfasst sind noch nicht die positiven indirekten wirtschaftlichen Auswirkungen, die der Einsatz von RFID mit sich bringt – zu denken ist auch an den Einsatz neuer Systeme im Bereich der Datensammlung, -haltung und -verarbeitung, an neuartige Softwareanwendungen usw.

Das alles ist mehr als eine bloße technische Fortentwicklung – RFID revolutioniert die Technologie. Vieles deutet bereits darauf hin, dass es Deutschland durch die Sicherung seines Vorsprungs auf diesem Gebiet mittelfristig zu einem Wachstums- und Beschäftigungssprung schaffen kann. Wohlgemerkt geht es dabei um veredelte, qualitativ hochwertige Arbeitsplätze am Standort Deutschland!

RFID schließt nicht nur an vorhandene Technologien an – als Beispiel sei der allseits bekannte Barcode im Handel genannt – sondern schafft neue, bisher unbekannte Einsatzfelder und Wertschöpfungsketten. Diese sind weit gefächert und reichen, um nur einen kleinen Ausschnitt zu benennen, von Anwendungen in der Logistik, Warenautomation und Archivierung über Systeme für Zugangskontrollen bis hin zur Tieridentifikation.

Vergleichbar breit sind die technischen Ausprägungen von RFID: Diese reichen von relativ einfachen Tags, die beispielsweise im Konsumgüterbereich eingesetzt werden können, bis hin zu hochgradig abgesicherten Varianten, die über einen eigenen Mikroprozessor und ein eigenes Betriebssystem verfügen; von RFID-Technologie im Nahbereich in Form von Smart Objects bis hin zum vorwiegend personenungebundenen Gebrauch im Umgebungsbereich.

Zur fundierten Diskussion von RFID gehört auch die Betrachtung datenschutzrechtlicher Aspekte. Angesichts der vielfältigen Bauformen und Anwendungsfelder sollte diese differenziert erfolgen. Entsprechend vielfältig sind die bereits vorhandenen rechtlichen Instrumentarien, die einem – wenn auch sehr unwahrscheinlichen – missbräuchlichen Einsatz der Technologie schon jetzt vollständig begegnen können.

1. Technische Gesichtspunkte und Funktion

RFID bezeichnet ein aus Lesegerät und RFID-Tag (bzw. Smartcard) bestehendes Gesamtsystem, das an weitere Systeme angebunden wird. Dabei können die Tags in Bauart (aktiv / passiv), Größe und Leistungsfähigkeit je nach Einsatzfeld variieren.

Der RFID-Tag als Sende- und Empfangseinheit umfasst einen digitalen Schaltkreis mit Speichermodul, eine Antenne und ggf. Software als wesentliche Funktionselemente.

1.1 Verschiedene Varianten für ein breites Einsatzspektrum

Abhängig vom Einsatzzweck ist der Tag in verschiedenen Ausführungsformen verfügbar:

- In der einfachsten und preisgünstigsten Version enthält der RFID-Tag eine fest kodierte, offen lesbare Kennung, welche auch nicht mehr überschrieben werden kann („Read-Only-Tag“).
- Etwas mehr Flexibilität ermöglichen RFID-Tags, die zusätzlich über einen beschreibbaren Speicher verfügen. Die Speichergröße reicht von wenigen Bits bis hin zu einigen hundert Kilobytes.
- Für Anwendungen mit hohem Sicherheitsbedarf (z. B. Ticketing) sind RFID-Tags verfügbar, welche zusätzlich über fest eingebaute Verschlüsselungsmechanismen verfügen. Das Mitlesen oder Beschreiben der Tags mit systemfremden Lesegeräten wird dadurch wirkungsvoll verhindert.
- Für Anwendungen mit erhöhtem Sicherheitsbedarf und/oder Flexibilitätsanspruch sind RFID-Tags mit Mikroprozessor und eigenem Betriebsystem verfügbar. Diese Tags werden meist in der Bauform einer Chipkarte hergestellt und verfügen daher häufig über zusätzliche Chipkartenkontakte (Dual-Interface-Karten).

Je nach Art der Energieversorgung wird zwischen passiver und aktiver RFID unterschieden:

- Passive RFID-Tags besitzen keine eigene Stromquelle, sind daher sehr kompakt, wartungsfrei und lassen sich sehr kostengünstig herstellen. Da diese Variante der Tags über ihre integrierte Antenne nicht nur nach Aktivierung die gespeicherten Informationen überträgt, sondern darüber auch von dem Lesegerät mit Energie versorgt wird, ergeben sich Reichweiten von wenigen Zentimetern bis maximal 3 Metern, je nach Frequenz und Antennenkonfiguration.
- Aktive RFID-Tags haben im Gegensatz dazu eine eigene Stromquelle. Sie sind deutlich größer, weniger robust gegenüber Umweltbedingungen und kostenintensiver. Ihr Einsatzgebiet bezieht sich daher auf Anwendungen, bei denen zusätzliche Anforderungen den Nachteil der erforderlichen Stromversorgung und der höheren Kosten kompensieren, wie z. B. eine höhere Reichweite und integrierte Sensoren zur Temperaturüberwachung oder Positionsbestimmung (GPS). Derzeit werden aktive RFID-Tags üblicherweise in Kreislaufprozessen eingesetzt, bei denen sie über längere Zeit immer wieder Verwendung finden.

RFID bietet Funktionalitäten, die weit über die bekannter Technologien (beispielsweise Barcode-Systeme) hinausreichen. In Abhängigkeit vom Einsatzfeld werden RFID-Tags in unterschiedlichen Formen produziert:

- Als flexible Folien mit integrierter Elektronik und direkt als Leiterbahnen aufgetragener Antenne.
- Im Kreditkartenformat als kontaktlose Chipkarten.
- Als Glaskörper, insbesondere für Implantate.
- Integriert in Plastik-Chipgehäuse, beispielsweise für Anwendungen in Wegfahrsperren in der Automobilindustrie.
- Integriert in robuste Gehäuse, z. B. für Ohrmarken, Schlüsselanhänger oder in Logistikanwendungen.

1.2 Frequenzbereiche, Standards und Beispielanwendungen

Weltweit wird RFID aufgrund der Entwicklung und der Verfügbarkeit von freien Frequenzen in unterschiedlichen Frequenzbereichen eingesetzt. Damit wird klar, dass verschiedenen Anwendungen auch unterschiedliche Frequenzbereiche gegenüberstehen. Durch die weitgehende internationale Harmonisierung gewinnen insbesondere die folgenden Frequenzbereiche an Bedeutung:

Frequenzen	Standards	Beispiele	Reichweite	Eigenschaften
< 135 kHz	ISO/IEC 18000-2 ISO/IEC 11785 ISO/IEC 14223	- Elektronische Wegfahrsperre - Produktidentifizierung und allgemeine industrielle Anwendungen - Tieridentifikation	30 cm – 1,5 m 30 cm – 1,5 m 10 cm – 1,5 m 10 cm – 50 cm	Read Only Read + Write Sensors
13,56 MHz	Nahbereich (Proximity) gemäß ISO/IEC 14443 Umgebungs-bereich (Vicinity) gemäß ISO/IEC 15693, EPC global, ISO/IEC 18000-3	- E-Ticketing - E-Passport - Zutrittskontrollen - Counterfeit Protection - Mitarbeiterkarten - Diebstahlüberwachung - Warenwirtschaftssysteme - Fluggepäcklogistik - Bibliotheken -Counterfeit Protection	Bis zu 10 cm 0,5 m – 3 m	Einsatz von Prozessorchips mit dem Niveau kontaktbehafteter Smartcards möglich
433 MHz	ISO/IEC 18000-7	Produktidentifizierung und allgemeine industrielle Anwendungen	1 m – 50 m	Aktive Technik mit extrem geringer Leistungs-aufnahme
865 MHz – 868 MHz	ISO/IEC 18000-6 EPC global in Definition	Warenverfolgung bzw. Produktidentifikation im Logistik- und Handelsbereich	0,5 m – 5 m	
2,45 GHz	Zigbee (IEEE 802.15.4a) ISO/IEC 18000-4	- Logistik - Anwendungen mit hohen Datenraten - Warenverfolgung bzw. Produktidentifikation im Logistik- und Handelsbereich - EPC - Asset Management - Container- und Palettenverfolgung	10 m – 100 m Bis zu 1,5 m	Aktive Technik mit extrem geringer Leistungsauf-nahme Passive Technik
5,8 GHz	ISO/IEC 18000-5 (zurückgezogen)	- Verkehrstelematik - Mikrowellen-Mautportale	10 m – 50 m	

Neben der Realisierung von Lesegeräten für einzelne Frequenzbereiche bietet sich mit dem Einsatz von Multifrequenz-Chips die Möglichkeit, mehrere Frequenzbereiche in einem Lesegerät unterzubringen.

Genutzt wird diese Möglichkeit bereits von Wal-Mart, der amerikanischen Handelskette: Lieferanten des US-Handelsriesen müssen künftig nicht nur ihre Paletten und Transportverpackungen mit RFID-Tags ausstatten, sondern diese auch mehrfrequenzfähig gestalten, damit weltweit (USA, Japan, Europa) zwischen Tag und Lesegerät kommuniziert werden kann.

1.3 RFID-Sicherheitsanforderungen

RFID-Tags senden die auf ihnen gespeicherten Informationen nur nach Aktivierung durch das Lesegerät. Abhängig von den Sicherheitsanforderungen der jeweiligen Anwendung erfolgt hierzu eine gegenseitige Identifikation des RFID-Tags mit dem Lesegerät. So ist sichergestellt, dass Daten nur zwischen RFID-Tags und Lesegeräten einer Anwendung (eines technischen Systems) ausgetauscht werden.

Zusätzlich zur gegenseitigen Identifikation können weitere Sicherheitsfunktionen implementiert werden. Beim Systemdesign wird die notwendige Sicherheitsstufe mit den Sicherheitsfunktionen definiert; dementsprechend wird die Wahl des Tags (bzw. der Smartcard) und der Leistungsfähigkeit des Lesegerätes getroffen. Ein wichtiges Auswahlkriterium hierbei ist die Stromversorgung, um beispielsweise grundlegende kryptographische Funktionen zum Schutz von Daten und der Datenübertragung zu unterstützen. So muss das Lesegerät bei passiven RFID-Tags genügend Energie liefern. Dies wird in den meisten Fällen durch einen geringen Leseabstand sichergestellt. Bei aktiven RFID-Tags spielt dies eine geringere Rolle.

2. Einsatzfelder

Schon vor mehreren Jahren wurden die Vorläufer der RFID-Technologie in Systemen zur Tieridentifikation, zum Diebstahlschutz oder in Zugangskontrollsystemen eingesetzt. Neu ist allerdings das durch die nun erwartete preiswertere Herstellung von RFID-Tags rapide angewachsene Einsatzspektrum. Die nachfolgende Aufzählung kann daher nur einen kleinen Ausschnitt aus der Vielzahl von Anwendungsmöglichkeiten aufzeigen.

■ **Beispiel Bibliothekslösungen**

Wer hat sich noch nicht über endlose Schlangen bei der Buch-Ausleihe geärgert? Wem ist es noch nicht so gegangen, dass die gesuchte Medieneinheit nicht an ihrem angestammten Platz stand?

Schluss damit! Die Nutzung von RFID in Bibliotheken ermöglicht es, schnell und unkompliziert Bücher zu entleihen (und unbefugte Entnahmen genau zu identifizieren). Mit Hilfe handlicher Scanner kann das Bibliothekspersonal zudem seine Medienbestände auf deren richtige Platzierung im Regal überprüfen.

Durch RFID-basiertes Medienmanagement und erweiterte Sicherheitseigenschaften werden Abläufe effizienter gestaltet und ein nutzerfreundlicheres Umfeld geschaffen. Die gewonnene Zeit und die freigewordenen Ressourcen landen dort, wo sie hingehören: Beim Nutzer der Bibliothek.

Zukunftsmusik? Keinesfalls, sondern heute schon Realität in den Bibliotheksverwaltungen von Stuttgart und Wien.

■ **Beispiel Automation und Logistik**

RFID erschließt neue Anwendungsfelder im Automations- und Logistikbereich. Zusätzlicher Nutzen ergibt sich beispielsweise daraus, dass nicht nur wie bisher Informationen von

der Ware zum Nutzer fließen (Erfassung bzw. Identifikation von Waren), sondern darüber hinaus nun auch der umgekehrte Weg beschritten werden kann. Durch das Hinzufügen von Informationen an Waren ist es beispielsweise möglich, komplexe Systeme zur Qualitätsüberwachung und Fertigungskontrolle aufzubauen.

Das heißt: Durch den Einsatz von RFID in der Logistikkette und in den Fertigungsprozessen werden die Durchlaufzeiten von Gütern verkürzt, Warenmanagementprozesse optimiert, die Lieferungsqualität verbessert und die Nutzungsgrade von Lagerraum erhöht.

■ **Beispiel Öffentlicher Personennahverkehr**

Die hektische Suche nach Kleingeld beim Einsteigen in den Bus wird vielleicht schon bald der Vergangenheit angehören.

Fahrscheine mit RFID-Technologie, wie sie beispielsweise derzeit in Helsinki verwendet werden, sind an vielen Stellen aufladbar und werden beim Einsteigen einfach vor das Lesegerät gehalten. Denkbar ist auch, diese Anwendung mit weiteren Mehrwertdiensten zu verbinden. Bezahlungsprozesse werden dadurch schneller, einfacher und kundenfreundlicher.

■ **Beispiel Reisepass**

Spätestens seit dem 11. September 2001 ist allen bewusst, dass in unserer zunehmend mobilen und vernetzten Welt „Papier"-Dokumente ohne zusätzliche Sicherheitsmerkmale kein ausreichendes Maß an Fälschungssicherheit aufweisen. Durch den Rückgriff auf RFID-Technologien kann diese Sicherheitslücke entscheidend verringert werden.

So sollen nach Plänen der Internationalen Behörde für zivile Luftfahrt Reisedokumente künftig mit RFID-Technologie ausgestattet werden. Damit wird der Reisepass zu einem kontaktlos überprüfbaren, hochgradig sicheren Dokument. Die Personendaten werden im RFID-Chip fälschungssicher gespeichert und können ausschließlich an den amtlichen Kontrollstellen komfortabel ausgelesen werden.

■ **Beispiel Zugangskontrolle**

Bei der 75. Oscar-Verleihung in Los Angeles wurde RFID-Technologie eingesetzt, um während der Veranstaltung für die Sicherheit von mehreren tausend Prominenten zu sorgen. Dazu wurden an strategischen Standorten die Identität der Anwesenden und deren Zugangsberechtigung überprüft.

Auch im Rahmen sportlicher Großveranstaltungen birgt RFID entscheidende Vorteile: Schluss mit langen Schlangen am Eingang, denn RFID-Nahbereichstechnologie an Stadieneingängen trägt dazu bei, Menschenmassen durch berührungsloses Abfragen der Zugangsdaten auf dem Ticket zum Ort des Geschehens zu lotsen. Schluss auch mit dem Ärger über gefälschte Eintrittskarten. Schluss auch mit überfüllten Rängen im Stadion, denn RFID kann die Zuschauer sicher in den für sie zutreffenden Stadionabschnitt leiten.

■ **Beispiel gesetzliche Auflagen**

Durch die Verwendung von RFID-Technologie wird die Erfüllung gesetzlicher Anforderungen in einigen Bereichen erheblich erleichtert. Dies ist z. B. bei der EU-Verordnung 178/2002 (Artikel 18) der Fall, die die globale Rückverfolgung von Lebensmitteln über alle Produktions-, Verarbeitungs- und Vertriebsstufen ab Januar 2005 fordert. Mit RFID-Technologie wird dies nicht nur ermöglicht, sondern auch eine artgerechte Tierhaltung, die computergestützt

die selbständige Hinführung von Tieren zum Fütterungsbereich und die Verabreichung/ Dokumentation der jeweils angemessenen Futtermischung garantiert.

Damit ist die Liste der Beispiele noch nicht erschöpft: Im Umsetzungsbereich der Elektro- und Elektronik-Altgeräte-Richtlinie wird im Auftrag der Europäischen Kommission derzeit untersucht, wie mit Hilfe von RFID eine eindeutige Herstellerzuordnung möglich ist. Das Verantwortungsbewußtsein von Herstellern und Verbrauchern wird geschärft, die Umwelt profitiert.

Künftige Einsatzmöglichkeiten

Darüber hinaus ist eine nicht enden wollende Vielzahl von künftigen Anwendungsfeldern vorstellbar. Vorstellbar (und teilweise bereits implementiert) sind zum Beispiel folgende Optionen:

- **Tree-tagging.** Wertvolle Naturhölzer aus den Tropen können mit RFID-Tags versehen werden. Die darin enthaltenen Informationen geben Aufschluss über Herkunft, Transport und Fertigungskette des Holzes. Raubbau an der Natur kann wirksam vorgebeugt werden, indem die Herkunft des Endproduktes bis an seine Quelle nachverfolgt wird. Damit werden nur die Hölzer der Natur entnommen, für die eine Nutzungsgenehmigung vorliegt.

- **Verkehrstelematik.** Während wir uns heute noch in kilometerlangen Staus über die Autobahnen quälen, könnte in Zukunft der Einsatz von RFID-Technologie dazu beitragen, den Verkehrsfluss zu optimieren und moderne Verkehrsleitsysteme flächendeckend einzuführen. Einsatzmöglichkeiten beschränken sich nicht auf die Straße: Die Schweizer Staatsbahn hat vorgemacht, wie mit der RFID-Kennzeichnung von Transporteinheiten Haltezeiten an Stationen verkürzt und Fahrpläne optimiert werden können.

- **Gepäcklogistik.** Vorstellbar wäre, RFID auf Gepäckstücken am Flughafen anzubringen. Wie Tests von Delta Airlines auf Inlandsflügen zeigen, fällt die Erkennungsrate von derart gekennzeichneten Gepäckstücken höher aus als die Markierung mit traditionellen Barcode-Systemen. Damit sollte das Warten auf ein versehentlich falsch eingechecktes Gepäckstück am Zielflughafen bald der Vergangenheit angehören.

3. Wirtschaftliches Potenzial

Wenn regional marktbeherrschende Ketten wie Wal-Mart bereits ab 2005 ihren Top-Lieferanten die RFID-Kennzeichnung von Paletten und Verpackungen vorschreiben, stellt sich die Frage nach dem „Ob“ beim Einsatz der Technologie nicht mehr. Zentraler Punkt ist vielmehr, wie Deutschland und deutsche Firmen ihren technologischen Vorsprung durch und mit RFID sichern können, um Pioniergewinne zu realisieren und international wettbewerbsfähig zu bleiben.

Die Nutzengewinne durch RFID sind vielfältig. Für deutsche Firmen – und insbesondere für den qualifizierten deutschen Mittelstand – ist RFID ein Mittel zur Optimierung, Dynamisierung und Automatisierung bestehender Prozesse. Über die gesamte Prozesskette hinweg können bisher mühselig, zeit- und kostenaufwendig manuell durchgeführte Prozesse automatisiert werden. Im Unternehmen entstehen Effizienzgewinne nicht nur durch die Technologie selbst; sondern die Technologie ist gleichzeitig Katalysator des Wandels im

Prozessmanagement des Unternehmens. Damit werden die Transparenz in der Prozesskette erhöht, Arbeitskosten verringert und die Entscheidungsbasis für die Unternehmensführung verbessert.

Kosten- und Effizienzgewinne entstehen dabei nicht allein auf Unternehmensebene, sondern branchenübergreifend: Technology-Push und Demand-Pull verstärken sich gegenseitig, so dass auch nachgelagerte Wirtschaftszweige profitieren.

Beispiel Logistik: Während bisher Warenfluss und Informationsfluss „manuell" miteinander verknüpft werden mussten (beispielsweise beim Wareneingang im Lager), verbindet nun RFID diese beiden Ströme automatisch, sicher und schnell. Informationslogistik optimiert nicht nur die Verwaltung bestehender Stocks und Flows, sondern generiert auch neue Informationen. Neu ist, dass bestimmte RFID-Systeme nicht nur Informationen erhalten, sondern auch die Güter mit entsprechenden Informationen versehen, d. h. mit dem Tag kommunizieren. Dabei können zum Beispiel Daten zum Lebenszyklus einer Ware im Produktions- und Distributionsprozess gesendet und empfangen werden. Deren Auswertung stellt zusätzliche Anforderungen an Systeme zu Datensammlung, -haltung und -verarbeitung, die wiederum zu mehr Innovation in der ITK-Branche beitragen.

Ein zentraler Punkt, gerade mit Blick auf den Mittelstand: RFID „senkt die Zugangsbarrieren" zur modernen Logistik. Die Technik eröffnet auch dem Mittelstand, wirtschaftliches Rückgrat der Bundesrepublik, den Zugang zu leistungsfähigen Logistikprozessen. Diese waren bisher , bedingt durch die damit verbundenen kostenintensiven Investitionen, lediglich Großunternehmen vorbehalten.

Wie eine Studie von Booz Allen Hamilton und der Universität St. Gallen zeigt, ist die interne Prozessoptimierung also nur ein Grund für den Einsatz von RFID. Neben äußeren Einflüssen (z. B. Anforderungen wie im Falle Wal-Marts) geht es also auch um die Erweiterung bestehender Technologien und die Durchsetzung neuer Produkte und Leistungen.

Welcher Handlungsbedarf lässt sich daraus konkret für Deutschland ableiten? Solange andere Staaten den Einsatz dieser innovativen Technologie unterstützen und forcieren, werden auch Standards und technische Spezifikationen an anderer Stelle , als bei diesen festgelegt. In der deutschen Öffentlichkeit muss nachhaltig das Bewusstsein dafür verankert werden, dass wir es hier mit einem Technologiesprung zu tun haben. Behäbiges Bedenkenträgertum ist an dieser Stelle fehl am Platze: Gefragt ist der Mut zur Veränderung, zur Innovation. Gefragt sind Politik und Wirtschaft, RFID-Technologien zu fördern und deutsche Beiträge zu einer weltweiten Standardisierung zu unterstützen.

4. Datenschutz

Vor dem Hintergrund der bauartbedingten Vielfalt und den breit gefächerten Einsatzmöglichkeiten der RFID-Technologie wäre eine pauschale Diskussion datenschutzrechtlicher Belange in Zusammenhang mit dem Einsatz von RFID-Technologie zu kurz gegriffen. Den beeindruckenden Fähigkeiten und Nutzenpotenzialen von RFID steht bereits heute eine ausgewogene und ausreichende Gesetzgebung gegenüber. Verbunden mit einem verantwortungsbewussten Nutzerverhalten spielen datenschutzrechtliche Fragen bei RFID also keine größere oder kleinere Rolle als dies auch bei anderen technologischen Innovationen der Fall ist.

5. Ausblick

In Zukunft wird die Spannbreite der Anwendungsfelder von RFID potenziell zunehmen. Dies ist zum einen auf die langjährigen Erfahrungen mit dieser Technologie zurückzuführen, zum anderen auf den in den nächsten 5 – 10 Jahren zu erwartenden geringeren Preis dieser Technologie. Dazu wird nicht zuletzt die weiter ansteigende Nachfrage der Nutzer beitragen.

Die künftige Verbreitung von RFID wird unter anderem auch davon abhängen, inwieweit es gelingt, einheitliche Standards für diese Technologie festzulegen. Was RFID-Anwendungen betrifft, muss daher sowohl auf technischer als auch auf logischer Ebene zuvor das exakt gleiche Verständnis über die ausgetauschten Daten bei allen beteiligten Partnern vorliegen bzw. geschaffen werden, um die Interoperabilität zu gewährleisten.

Datenschutzbedenken und Sicherheitsfragen wird man, wie oben im Überblick erwähnt, auch künftig angemessen begegnen können. Die Wahrung der Interessen aller Beteiligten kann somit (auch weiterhin) in vollem Umfang gewährleistet werden.

BITKOM unterstützt den Einsatz von RFID, begleitet sie im Rahmen entsprechender Projekte und versteht sich als die geeignete Instanz, die die Plattform zur Bündelung von Expertenwissen und zum Austausch von Erfahrungen über Pionieraktivitäten gewährleistet. Politik, Wirtschaft und Gesellschaft sind dazu aufgefordert, den Einsatz dieser innovativen Technologie zu unterstützen und voranzutreiben.

Anlage

Rechtliche Betrachtungen zur datenschutzrechtlichen Relevanz von RFID

Viele der in der aktuellen Diskussion um RFID geäußerten Bedenken sind datenschutzrechtlicher Natur. Häufig wird befürchtet, dass die informationelle Selbstbestimmung des Bürgers in Frage gestellt oder allgemein seine Privatsphäre gefährdet würden.

Dabei werden Gefahrenszenarien entworfen, in denen Bürger durch die heimliche Anbringung von RFID-Tags minutiös überwacht werden, Konsumenten im Warenhaus von Kleidungsetiketten bis zum Inhalt der Brieftasche ausgelesen werden und anschließend individuelle Waren und Preise angeboten bekommen. Befürchtet werden die Erstellung von Einkaufs-, Nutzungs-, Verhaltens- und Bewegungsprofilen. Angeführt wird zudem, der Schutz, den das Bundesdatenschutzgesetz biete, reiche nicht aus, es müssten daher neue, ergänzende Gesetze geschaffen werden. BITKOM hält diesen Ruf nach neuen gesetzlichen Instrumentarien für vorschnell und nicht zielführend.

Eine generelle Diskussion über Datenschutz im Zusammenhang mit dem Einsatz von RFID erscheint wenig hilfreich. Wie bereits dargelegt, unterscheiden sich die RFID-Tags erheblich hinsichtlich Gesamtkonzept, Bauart und Einsatzfeld. Insofern sollten datenschutzrechtliche Aspekte stets unter Berücksichtigung der jeweiligen Bauart und Zielanwendung erörtert werden.

Bei der Diskussion über den beim Einsatz von RFID erforderlichen Datenschutz sind zunächst die zahlreichen Anwendungen auszublenden, bei denen überhaupt keine natürlichen Personen involviert sind, per se stellt sich damit die Frage nach Datenschutz nicht. Das betrifft zum Beispiel

- Industrieautomation (Management von Transportbehältern, Steuerung von Fertigungsprozessen),
- Reine Logistikanwendungen (Supply Chain Management, Inventarisierung, Frachtgutmanagement, elektronische Plombe),
- Archivierung (Akten- und Dokumentenerfassung, Lagersysteme und Bibliotheken),
- Tieridentifikation (Züchtung und Seuchenkontrolle (Seuchengesetz ab 2007), Standortlokalisierung bei Tieren),
- Diebstahlsicherung (KFZ-Wegfahrsperre) / Schutz vor Verlust oder Fälschung,
- After Sales Unterstützung (Kontrolle von Mehrwegbehältnissen).

Die Vorteile von RFID sind bei diesen Anwendungsbereichen anerkannt und unkritisch. Sie sollten daher auf keinen Fall durch eine sachfremde und verzerrte Diskussion um datenschutzrechtliche Anforderungen in der öffentlichen Wahrnehmung überlagert werden.

Jedoch auch dort, wo natürliche Personen in die Anwendung von RFID einbezogen sind, ist eine differenzierte Betrachtung geboten: Wo durch die Identifikation mit Hilfe von Funkwellen personenbezogene Daten erhoben oder verarbeitet werden, greift das Bundesdatenschutzgesetz (BDSG). Mit den Rechten, die es dem Betroffenen gibt (beispielsweise Auskunfts- und Löschungsansprüche), und den Pflichten, die es dem Verantwortlichen auferlegt (zum Beispiel Unterrichtungs- und Löschungspflichten), bietet es einen ausgewogenen und umfassenden Schutz.

In vielen Bereichen kommt das BDSG aber nicht zur Anwendung, und zwar deshalb, weil trotz der Einbeziehung natürlicher Personen überhaupt keine personenbezogenen Daten betroffen sind. Diese Sachverhalte bewegen sich gleichermaßen im Vorfeld des gesetzlich geforderten Schutzes. Eben deswegen liegen aber in diesem Vorfeld auch keinesfalls Schutzlücken vor. Das Grundrecht auf informationelle Selbstbestimmung sieht nicht den Schutz des Einzelnen vor der Kenntnisnahme beliebiger Umstände vor, sondern gewährleistet die Befugnis des Einzelnen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen, hinsichtlich persönlicher, also personenbezogener Daten. Ein solches personenbezogenes Datum liegt (nur) bei Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person vor (vgl. § 3 Abs. 1 BDSG).

1. Arten der Datenerhebung

Beim Einsatz von RFID muss (nach der Ausblendung von Anwendungen, bei denen natürliche Personen gar nicht betroffen sind, vgl. oben) zwischen drei Konstellationen unterschieden werden:

1. **Konstellation:** Der RFID-Tag enthält bzw. erhebt personenbezogene/personenbeziehbare Daten.
2. **Konstellation:** Der RFID-Tag enthält bzw. erhebt keinerlei personenbezogene/personenbeziehbare Daten.
3. **Konstellation:** Der RFID-Tag enthält oder erhebt keinerlei personenbezogene/personenbeziehbare Daten, solche werden jedoch später, zum Beispiel durch Zusammenführung mit anderen Daten bzw. Anreicherung, generiert.

Bei allen drei Konstellationen sollten allgemeine Grundsätze des BDSG wie Datenvermeidung und Datensparsamkeit (vgl. § 3 a BDSG) analoge Anwendung finden. Ebenso sollte der allgemeine Transparenzgedanke, wie er etwa in Erwägungsgrund 38 der EG-Datenschutzrichtlinie Ausdruck gefunden hat, durchgängig beachtet werden:

„Datenverarbeitung nach Treu und Glauben setzt voraus, dass die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei ihnen erhoben werden."

Im Übrigen zeigen sich aber erhebliche Unterschiede.

1. Konstellation: Der RFID-Tag enthält bzw. erhebt personenbezogene Daten

Solche Anwendungen sind bisher die Ausnahme. Anzutreffen sind sie aber, wo die Integration personenbezogener Daten Voraussetzung der Funktionalität ist, nämlich dort, wo es um Identifikation und Sicherheit geht. Aktuelle Beispiele sind der Einsatz kontaktloser Smartcards bei der Zugangskontrolle für Gebäude, Signaturkarten oder Karten mit besonderen Schutzmechanismen.

Als datenschutzrechtliche Sicherung wird regelmäßig § 6c BDSG Anwendung finden (mobile personenbezogene Speicher- und Verarbeitungsmedien). Diese Vorschrift legt der ausgebenden Stelle umfangreiche Pflichten auf: So muss die ausgebende Stelle z. B. unterrichten über ihre Identität und Anschrift, die Funktionsweise des Mediums einschließlich der

Art der zu verarbeitenden Daten sowie die Möglichkeit zur Ausübung von Auskunfts- und Löschungsrechten. Darüber hinaus muss sie dafür Sorge tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen. Darüber hinaus müssen die Vorgänge, die auf dem Medium eine Datenverarbeitung auslösen, für den Betroffenen eindeutig erkennbar sein. Beim Einsatz mobiler Speicher- und Verarbeitungsmedien ist zudem der Datenschutzbeauftragte einzuschalten (§ 4g BDSG), in Arbeitsverhältnissen sind die Mitbestimmungsrechte der Mitarbeitervertretung zu beachten. Iin Betracht kommen zum Beispiel § 87 Abs. 1 Nr. 6 BetrVG, Leistungs- und Verhaltenskontrolle, sofern Reader-ID, Staplernummer und Zeitstempel erfasst werden; § 89 BetrVG, Arbeits- und Umweltschutz; § 90 Abs. 1 Nr. 4 BetrVG, Gestaltung Arbeitsplatz, wenn Reader im direkten Arbeitsumfeld angebracht werden.

Die häufig erhobenen Forderungen nach Transparenz und Kontrolle werden durch diese Bestimmung also schon umfassend erfüllt.

2. Konstellation: Der RFID-Tag enthält bzw. erhebt keinerlei personenbezogene Daten

In der überwiegenden Anzahl der Anwendungen werden auf dem RFID-Tag keinerlei personenbezogene Daten gespeichert oder durch den Chip erhoben, sondern der Chip enthält lediglich sach- bzw. objektbezogene Informationen. Beispiele hierfür sind Fluggepäckverfolgung, die Nutzung von Mehrwegverpackungen, die elektronische Wegfahrsperre beim Auto und insbesondere die Kennzeichnung von Waren zur automatischen Erfassung im Kassenbereich.

Da das letzte Beispiel die Darstellung und Diskussion in den Medien stark geprägt hat, soll es im Folgenden zur näheren Erläuterung der 2. Konstellation dienen. Wird ein Produkt oder Artikel im Handel mit einem RFID-Tag ausgestattet (Lebensmittel, Kleidungsstücke etc.), so enthält dieser ausschließlich Informationen zu diesem Produkt wie beispielsweise Produktnummer, Hersteller, Größe, Gewicht, Füllmenge etc., sowie eventuell Herstellungs- und Verfallsdatum sowie den Preis. Wird der RFID-Tag an der Kasse ausgelesen, dienen diese Informationen zum einen der Erfassung des Einzel- oder Gesamtpreises des Kundeneinkaufs, zum anderen wird dem Handel durch nachgelagerte Systeme ein aktueller Überblick über die eigenen Bestände, eine optimierte Bestellbearbeitung und die Reduzierung von Lagerengpässen ermöglicht.

Diese sach- bzw. objektbezogenen Informationen sind datenschutzrechtlich irrelevant, gleichsam neutral. Sie werden auch nicht dadurch zum geschützten, personenbezogenen Datum, dass eine natürliche Person den Artikel und damit auch den RFID-Tag samt der Informationen in Besitz nimmt. Denn der Käufer ist regelmäßig anonym, so dass die Produktinformationen keiner bestimmten oder bestimmbaren Person zugeordnet werden kann (vgl. § 3 Abs.1 BDSG). Nicht anders wäre es, wenn der Käufer nach seinem Einkauf einen weiteren Laden betritt und dort durch die Lesegeräte sein bisheriger Einkauf „erkannt“ werden könnte (was im Übrigen zunächst eine umfassende Standardisierung von Chips, verwendeten Codes und Lesegeräten erfordert). Auch diese Konstellation bewegt sich im Vorfeld des gesetzlich geforderten Datenschutzes (vgl. oben).

Trotzdem bezieht sich ein großer Teil der in der öffentlichen Diskussion geäußerten Bedenken auf die Ausstattung von Alltags- und Verbrauchsgegenständen mit RFID-Etiketten. Um diesen Bedenken Rechnung zu tragen, könnten in Anlehnung an § 6b BDSG waren- bzw.

anwendungsbasierte Hinweis- und Transparenzpflichten für die Verwender von RFID-Tags geschaffen werden. § 6b des BDSG betrifft die Videoüberwachung im öffentlich zugänglichen Raum und ist im System des Bundesdatenschutzgesetzes, das dem Schutz personenbezogener Daten dient, ein Fremdkörper. Denn bei der Videoüberwachung öffentlich zugänglicher Räume (Bahnsteige, Verkaufsräume, Krankenhäuser, etc.) werden aufgrund der Anonymität der gefilmten Personen keinerlei Daten mit Personenbezug im Sinne des § 3 Abs. 1 BDSG aufgezeichnet. Das BDSG gibt dem Betroffenen durch Transparenzpflichten und eine Zweckbindung der ausführenden Stelle gleichwohl ein gewisses Maß an Schutz.

Für die ganz ähnlich gelagerte Konstellation 2 der Verwendung von RFID-Tags könnte daher insbesondere Absatz 2 von § 6b BDSG Anwendung finden. Absatz 2 bestimmt nämlich, dass der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen sind. Denkbar wäre insoweit eine Kennzeichnung von Verkaufsräumen etc. mit Hinweisschildern, die auf die Verwendung von RFID-Tags an der Ware hinweisen. Als Vorbild könnten die schon heute bei der Videoüberwachung verbreitet benutzten und insgesamt wegen der hohen Verständlichkeit bewährten Piktogramme (Video-Infozeichen DIN Norm 33450) dienen. Ergänzt werden könnten diese Hinweisschilder durch Aushänge/ Informationstafeln im Eingangs- und Kassenbereich mit näheren Erläuterungen zu Ablauf und Zweck der Verwendung.

Neben Absatz 2 könnte auch Absatz 4 von § 6 BDSG einen sachgerechten Ansatz darstellen, um die Bedenken der betroffenen Konsumenten aufzufangen. Nach dieser Vorschrift ist der Betroffene einer Videoüberwachung entsprechend §§ 19a und 33 BDSG zu benachrichtigen, wenn die durch die Überwachung zunächst anonym erhobenen Daten seiner Person zugeordnet werden, also ein geschütztes, personenbezogenes Datum i. S. d. BDSG entsteht. Dieser Sachverhalt gehört jedoch zur dritten behandelten Konstellation (siehe unten).

Schließlich kann auch § 6a BDSG relevant werden (automatisierte Einzelentscheidung). Diese Vorschrift findet Anwendung, wenn ausschließlich auf Basis automatisierter Entscheidungen persönliche Bewertungsmerkmale erstellt werden. Hierunter fallen auch Kreditwürdigkeit, (Kauf-) Verhalten oder Scoring-Werte. Diese Bewertungsmerkmale dienen nämlich als Basis für die Kopplung von Produkten und Services im Handel oder neuen Geschäftsmodellen, bei denen Gegenstände und deren Nutzung identifiziert und abgerechnet werden.

Eine automatische Deaktivierung bzw. Zerstörung des RFID-Tags, wie sie gelegentlich vorgeschlagen wird, hat den Nachteil, dass auch Informationen, die dem Käufer/Verbraucher auch nach dem Kauf nützlich sind (z. B. Informationen über das Produkt und den Kauf, die für die Geltendmachung von Kundenansprüchen im Gewährleistungsfall wichtig sind oder auch Pflege bzw. Bedienungsanleitungen, die zum Produkt gehören) verloren gehen. Es sollte jedoch überlegt werden, dem Kunden einen Anspruch gegen den Verwender auf Deaktivierung oder aber die Möglichkeit zur eigenen Entscheidung und selbständigen Deaktivierung der RFID-Tags zu geben. Schließlich hat der Kunde nach dem Kauf der Ware regelmäßig Besitz und Eigentum an der Ware, auch die Verfügungsgewalt über den dazugehörigen RFID-Tag liegt damit ausschließlich bei ihm (vgl. §§ 93, 903, 1004 BGB). Die Deaktivierung darf dabei nicht mit Restriktionen wie z. B. dem Verlust eines Rücktrittsrechts oder dem Wegfall der Gewährleistung verbunden werden.

In diesem Zusammenhang muss auf die vielfachen Möglichkeiten des Selbstdatenschutzes durch den Betroffenen hingewiesen werden. Selbstdatenschutz ist ein Kern der informa-

tionellen Selbstbestimmung und wird als gestaltender Faktor der persönlichen Freiheit häufig unterschätzt. Selbstdatenschutz meint dabei, dass „jeder Betroffene in Bezug auf die Offenlegung seiner personenbezogenen Daten sein eigener Datenschützer ist“ (vgl. zur Rolle des Selbstdatenschutzes auch das Gutachten von Rossnagel, Pfitzmann und Garstka zur Modernisierung des Datenschutzrechts). Der Betroffene sollte verstärkt in die Lage versetzt werden, die Erfassung seiner Daten und die Nutzung von technischen und organisatorischen Schutzinstrumenten selbst zu bestimmen. Regelmäßig liegt die Entscheidung, ob und welche Daten preisgegeben werden (z. B. durch bewusste Zustimmung zu Handlungen) beim Betroffenen. Grundlage seiner Entscheidung, welche Daten er wem anvertraut, muss aber die sachgerechte Information sein. Im Zusammenhang mit RFID unterstreicht das die Notwendigkeit für den Betroffenen zu erkennen, wo RFID zur Anwendung kommt.

3. Konstellation: Der RFID-Tag enthält bzw. erhebt keinerlei personenbezogene Daten, solche können jedoch später, z. B. durch Zusammenführung bzw. Anreicherung mit anderen Daten generiert werden

In der dritten Konstellation entsteht ein personenbezogenes Datum dadurch, dass eine auf dem RFID-Chip gespeicherte, sachbezogene Information in Bezug zu einer bestimmten, natürlichen Person gesetzt wird. Mögliche Beispiele hierfür sind der Einsatz von RFID-Tags bei Paketdiensten und Verleihsystemen. In diesen und ähnlichen Fällen (vgl. oben: Gepäckermittlung bei Flugreisen) wird die Erhebung bzw. Verarbeitung persönlicher Daten vielfach schon durch § 28 Abs.1 Nr. 1 BDSG erlaubt sein. Denn § 28 Abs. 1 Nr. 1 BDSG bestimmt: „Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig, wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.“

Darüber hinaus kann diese Konstellation aber auch im Zusammenhang mit der Kennzeichnung von Waren entstehen, nämlich dann, wenn der Kunde nicht anonym einkauft, sondern beim Einkauf eine Kundenkarte benutzt (Rabattkarte, Bonuspunkte etc.) und die auf dieser Karte gespeicherten, persönlichen Daten mit den Daten der gekauften Ware in Verbindung gebracht werden. Erst die Benutzung der persönlichen Karte durch den Kunden ermöglicht es dabei, aus dem schlichten Kauf einer Ware personenbezogene Daten zu generieren. Das ein Kunde aufgrund von materiellen Anreizen einem Unternehmen Einblick in sein Einkaufsverhalten gewährt, ist allerdings kein neuartiges Phänomen, sondern wird unter dem Stichwort Customer Relationship Management (CRM) schon seit langem diskutiert, vor allem auch unter datenschutzrechtlichen Aspekten. Klargestellt werden muss daher an dieser Stelle, dass die Ausstattung von Waren mit RFID-Etiketten die Erfassung von Kundendaten keinesfalls erstmalig ermöglicht, sondern lediglich zu einer weiteren Erscheinungsform von CRM führen könnte.

Ebenso sollte bei der Diskussion beachtet werden, dass Customer Relationship Management sich auch heute schon nicht im rechtsfreien Raum bewegt, im Gegenteil: Aus den Bestimmungen des BDSG ergeben sich für die Erhebung und Verarbeitung von Kundendaten strenge Anforderungen (Einwilligung des Betroffenen, Widerrufsrecht, Informationspflichten etc.). Diese Anforderungen sind technikneutral, sie gelten in gleicher Weise bei allen denkbaren Formen der Datenerfassung, also auch dann, wenn RFID-Tags in Verbindung mit dem Einsatz einer personalisierten Karte zur Generierung von Kundendaten genutzt werden. Ein zusätzlicher gesetzgeberischer Handlungsbedarf ist daher nicht vorhanden.

2. Schutz der Nutzer durch weitere Gesetze

Die Vorschriften des Strafgesetzbuches (StGB) kommen beim Einsatz von RFID-Tags nicht zum Tragen. Zwar sieht das StGB in seinem fünfzehnten Abschnitt den Schutz des persönlichen Lebens- und Geheimbereichs vor, die einzelnen dort aufgeführten Straftatbestände erfassen jedoch die unterschiedlichen Konstellationen beim RFID-Einsatz nicht.

Einen weiteren gesetzlichen Schutz kann jedoch das Telekommunikationsgesetz (TKG) bieten. Der RFID-Chip und das Lesegerät kann als TK-Anlage im Sinne des § 3 Nr. 23 TKG (n. F.) verstanden werden, zwischen denen Telekommunikation stattfindet (§ 3 Nr. 22 TKG n. F.), indem Informationen ohne Verbindungsleitungen (vgl. § 3 Nr.4 TKG a. F.) als Nachricht ausgesandt und empfangen werden, aus der sich je nach Umfang der auf dem RFID-Chip gespeicherten Informationen Zeichen und Bilder generieren lassen.

Zwar kommen weder die Meldepflicht (§ 6 TKG n. F.) noch das Fernmeldegeheimnis (§ 88 TKG n. F.) in Betracht, da diese die Erbringung von gewerblichen TK-Dienstleistungen (§ 3 Nr. 24 TKG n. F.) zur Voraussetzung haben. Zur Anwendung dürfte jedoch § 89 TKG (Abhörverbot, Geheimhaltung, § 86 TKG a. F.), kommen, der es nur bestimmten Personen erlaubt, die durch eine Funkanlage gesendeten Nachrichten abzuhören.

Zu unterscheiden ist dabei zwischen dem Senden der Transponder-ID und dem eigentlichen Transponder-Inhalt: § 89 Satz 1 TKG erfasst den Transponder-Inhalt, es greift ein Nachsorgeschutz, nämlich wenn zu erwarten ist, dass ein Personenbezug hergestellt werden kann. § 89 Satz 2 TKG erfasst hingegen den einmaligen Code des Hersteller des Tags (UID, Unique Identifier, vergleichbar mit dem GUID, Global Unique Identifier, bei Software Produkten). Dieser Code wird von allen Tags gesendet, die im Bereich des Datenschattens liegen.

In der Konsequenz führt die Anwendung von § 89 TKG dazu, dass ein unbefugtes Auslesen (also nicht durch den Verwender, sondern durch Dritte) verboten ist und einem möglichen Missbrauchspotenzial durch das strafbewehrte Verbot (Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe, § 148 Abs. 1 Nr. 1 TKG n. F.) entgegengetreten wird.

Über den BITKOM

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt 1.300 Unternehmen, davon 700 Direktmitglieder mit etwa 120 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Produzenten von Endgeräten und Infrastruktursystemen sowie Anbieter von Software, Dienstleistungen, neuen Medien und Content. Der BITKOM setzt sich insbesondere für bessere ordnungsrechtliche Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstr. 10
10117 Berlin

Tel.: 030/27576-0
Fax: 030/27576-400

bitkom@bitkom.org
www.bitkom.org

Stand: 16. November 2004