

**Position zum
Working Paper 105 der Art. 29 – Datenschutzgruppe**

**„Datenschutzfragen im Zusammenhang mit der RFID-
Technik“**

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) vertritt 1.300 Unternehmen, davon gut 700 als Direktmitglieder, mit ca. 120 Mrd. Euro Umsatz und etwa 700.000 Beschäftigten. Hierzu zählen Produzenten von Endgeräten und Infrastruktursystemen sowie Anbieter von Software, Dienstleistungen, neuen Medien und Content. Mehr als 500 Direktmitglieder gehören dem Mittelstand an. BITKOM setzt sich insbesondere für eine Verbesserung der ordnungsrechtlichen Rahmenbedingungen in Deutschland, für eine Modernisierung des Bildungssystems und für die Entwicklung der Informationsgesellschaft ein.

Eng verbunden mit dem Engagement von BITKOM für die Entwicklung der Informationsgesellschaft ist der Einsatz für einen modernen und technikadäquaten Datenschutz. Datenschutz ist ein unerlässlicher Akzeptanz- und Vertrauensfaktor der Informationsgesellschaft, der es ermöglicht, personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen. Er kann das notwendige Vertrauen in die elektronische Kommunikation schaffen und verbreiteten Befürchtungen vor Missbrauch entgegenwirken. Datenschutzrechtliche Anforderungen und Ausgestaltungen beeinflussen gleichzeitig die Entwicklung einer modernen Wirtschaft. Ein moderner und technikadäquater Datenschutz kann daher auch einen bedeutenden Wettbewerbsvorteil und positiven Standortfaktor darstellen.

BITKOM begrüßt vor diesem Hintergrund, dass sich die Art. 29 – Datenschutzgruppe in ihrem Arbeitspapier 105 eingehend mit dem aktuellen Stand der RFID – Technik, den Einsatzmöglichkeiten und der datenschutzrechtlichen Relevanz des Einsatzes auseinandersetzt. RFID ist eine innovative und zukunftsweisende Technologie mit beeindruckenden Fähigkeiten und Nutzenpotenzialen. Die Vorteile von RFID sind in vielen Anwendungsbereichen anerkannt; sie sollten nicht durch eine sachfremde und verzerrte Diskussion in der öffentlichen Wahrnehmung überlagert werden. Zu Recht stellt auch die Art. 29-Gruppe diese Vorteile an den Beginn ihrer Überlegungen und führt zutreffend aus, dass diese Vorteile nicht eine einzelne Gruppe betreffen, sondern die Wirtschaft, Privatpersonen und öffentliche Stellen (eingeschlossen Regierungen) gleichermaßen.

Vor dem Hintergrund der bauartbedingten Vielfalt und den breit gefächerten Einsatzmöglichkeiten der RFID-Technologie greift eine pauschale Diskussion datenschutzrechtlicher Belange zu kurz. Denn nur eine Einzelfallbetrachtung der verschiedenen technischen Möglichkeiten der Tags und des jeweiligen Einsatzes erlaubt die sachgerechte Bewertung der datenschutzrechtlichen Relevanz. Beiträge, die diese grundsätzliche Anforderung vernachlässigen oder sogar gänzlich ignorieren, erschweren und belasten die Diskussion in unnötiger Weise.

BITKOM begrüßt deshalb nachdrücklich, dass sich die Art. 29 -Gruppe mit ihrem Arbeitspapier zu der erforderlichen Differenzierung und Abschichtung klar bekennt und neben der abstrakten Schilderung möglicher Eingriffe in den Datenschutz auch Anwendungsbereiche aufzeigt, die von der rechtskonformen Tätigkeitsausübung durch Unternehmen und andere Stellen ausgehen. Das Arbeitspapier kann damit eine wichtige Grundlage für die aktuelle und zukünftige Diskussion bieten.

Zutreffend betont die Art. 29 – Gruppe, dass die Diskussion um die datenschutzrechtlichen Anforderungen bei RFID – Technologien erst am Anfang steht und daher auch das Arbeitspapier lediglich als ein erster Situationsbericht gesehen werden kann. BITKOM begrüßt, dass die Art. 29 –Gruppe die Arbeit und Diskussion zu diesem Thema fortsetzen wird. Erst im Laufe dieser Diskussion werden die Einzelheiten der praktischen Umsetzung datenschutzrechtlicher Anforderungen schrittweise geklärt werden können. BITKOM steht mit seinem Arbeitskreis Datenschutz in dieser Diskussion als Partner zur Verfügung.

Wichtig wird es sein bei der Diskussion darauf zu achten, dass keine überschießenden und praxisfremden Anforderungen zur datenschutzrechtlichen Einbettung der RFID-Technologie entstehen. Solche entstehen häufig, wo Datenschutz und Verbraucherschutz vermengt werden, so dass bei den Überschneidungen beider Bereiche mit besonderem Augenmaß vorzugehen ist.

Beispielhaft sollen an dieser Stelle aus der Vielfalt der Anforderungen zwei Aspekte kurz aufgegriffen werden, nämlich die Frage der Informationen des Betroffenen über die Aktivierung des Tags und die Frage der Löschung bzw. Deaktivierung.

- In dem Arbeitspapier führt die Art. 29 – Gruppe (unter 5.2) aus, der Anwender müsse (neben der Information über die Anwesenheit von RFID – Geräten) die betroffene Person „auch über die Aktivierbarkeit bzw. Echtzeitaktivierung von RFIDs“ informieren. Dies bedeute, dass einfache Verfahren zur Sichtbarmachung des Aktivierungszustands bzw. der Aktivierbarkeit gefunden werden müssten. Als Rechtsgrundlage für diese Anforderung nennt die Art. 29 – Gruppe die Datenschutzrichtlinie. Unabhängig von der tatsächlichen Frage, ob eine derartige Information dem Betroffenen zur Wahrnehmung seiner Rechte nützlich ist, kann nach Ansicht des BITKOM zumindest die Datenschutzrichtlinie nicht als Grundlage dieser Forderung herangezogen werden. Der Zusammenhang der Ausführungen im Arbeitspapier lässt erkennen, dass sich die Art. 29 – Gruppe auf Art. 10 der Richtlinie 95/46/EG bezieht. Die Reichweite und Inhalte dieses Artikels werden im Arbeitspapier an anderer Stelle zutreffend beschrieben (S. 11), für die Information über den Aktivierungszustand lässt sich dies nicht fruchtbar machen. Die Information über die Aktivierbarkeit bzw. Echtzeitaktivierung von RFIDs ist daher keine rechtlich begründbare Anforderung, sondern kann lediglich den Charakter einer Empfehlung haben.

Ein solcher Empfehlungscharakter wird in der Einleitung zum Abschnitt 5 (S.13) auch ausdrücklich klargestellt und nach üblichem systematischem Verständnis damit den folgenden Unterabschnitten beigelegt. Nicht nachzuvollziehen ist es daher, wenn gleichwohl auf den S.13 ff häufig von zwingenden Anforderungen gesprochen wird.

- In dem Arbeitspapier wird (unter 5.3 c und 5.4, Seiten 17 f) die Frage der Löschung von Inhalten bzw. der Deaktivierung der Transponder angesprochen. Diese Problematik wird in der zukünftigen Diskussion voraussichtlich eine wichtige Rolle spielen. Deshalb sollte sie besonders sorgfältig geprüft werden und genau differenziert werden, welchen Inhalt ein Anspruch auf Löschung bzw. Deaktivierung haben kann. So muss beispielsweise die Frage geklärt werden, ob der Betroffene einen Anspruch auf Löschung/Deaktivierung durch den Verantwortlichen hat oder ob der Betroffene immer die Möglichkeit haben muss, diese selbst vorzunehmen. Nicht zuletzt kommt es in diesem Zusammenhang auch entscheidend auf den Verwendungszweck des Tags an. Das Arbeitspapier scheint davon auszugehen, dass grundsätzlich letzteres

sicherzustellen ist, was allerdings nicht nur über Art. 12 der Richtlinie 95/46/EG als Rechtsgrundlage hinausgeht (der von einer Löschung der personenbezogenen Daten durch den Verantwortlichen ausgeht), sondern auch gegenüber der heutigen Praxis bei Lösungsansprüchen einen Paradigmenwechsel darstellen würde.

Als Anlage ist diesem Positionspapier ein eigenes Positionspapier des BITKOM zum Thema RFID beigelegt, das u. a. ausführlich auf weitere datenschutzrechtliche Fragen (orientiert an der Rechtslage in Deutschland) eingeht. BITKOM würde es begrüßen, wenn die in diesem Papier dargelegten Ansätze auch in die Diskussion auf europäischer Ebene Eingang finden.

Dem Vernehmen ist auf europäischer Ebene (zunächst) eine Mitteilung der EU – Kommission geplant; die Inter -Service –Konsultationen könnten in naher Zukunft stattfinden. Unbedingt sichergestellt werden sollte die umfassende und frühzeitige EU -interne Kooperation und Abstimmung aller zuständigen Gremien, damit keine Widersprüchlichkeiten und Reibungsverluste auftreten.

Anlage: Positionspapier des BITKOM zu RFID, 23.07. 2004

Berlin, den 21. März 2005

Anlage

RFID und personenbezogene Daten (Datenschutzrechtliche Relevanz von RFID)

BITKOM setzt sich für die Entwicklung, die Herstellung und den Einsatz innovativer Technologien ein. Den Befürchtungen, mit RFID werde eine Technik entfesselt, die dem Missbrauch (z. B. durch Kontrollverluste über persönliche Daten oder eine Überwachung einzelner Personen bzw. Bevölkerungskreise) Tür und Tor öffnet, möchte BITKOM daher durch eine differenzierte Betrachtung des Status Quo und die sachkundige Begleitung des weiteren Einsatzes entgegentreten. Die erheblichen Vorteile, die der Einsatz von RFID -Technik in vielen Bereichen bietet, können nur zur Geltung kommen, wenn dieser Einsatz auch von den Betroffenen akzeptiert wird. Hierfür ist es erforderlich, zum einen die Diskussion zu versachlichen und zum anderen weg von der Expertenebene hin zu einer breiten Diskussion zu kommen.

1. Datenschutz

Viele der in der aktuellen Diskussion um RFID geäußerten Bedenken sind datenschutzrechtlicher Natur. Häufig wird befürchtet, dass die Privatsphäre gefährdet und bürgerliche Freiheiten bedroht werden.

Gefahrenszenarien werden entworfen, in denen Bürger durch die heimliche Anbringung von RFID -Tags minutiös überwacht werden, Konsumenten im Warenhaus von Kleidungsetiketten bis zum Inhalt der Briefftasche ausgelesen werden und anschließend individuelle Waren und Preise angeboten bekommen. Befürchtet werden Einkaufs-, Nutzungs-, Verhaltens- und Bewegungsprofile; beklagt wird, 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.

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 und daher per se kein Datenschutz erforderlich ist. Das betrifft z. B.

- Industrieautomation (Management von Transportbehältern, Steuerung von Fertigungsprozessen, z.B. Infinion Wafer Produktion)
- 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 - Wegfahrsperrung) / Schutz vor Verlust oder Fälschung
- After Sales Unterstützung (Kontrolle von Mehrwegbehältnissen)

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

Zudem besteht (nicht nur in diesen Bereichen) eine erhebliche Notwendigkeit der technologischen Innovation. Denn der herkömmliche Bar Code ist ein Auslaufmodell, er ist demnächst überaltert und kann für neue Anforderungen, z. B. in Supply Chain und Handel, nicht ausreichend genutzt werden. Darüber hinaus darf nicht übersehen werden, dass durch die Verwendung von RFID -Technik die Erfüllung gesetzlicher Anforderungen in manchen Bereichen erst ermöglicht wird, so z. B. bei der EU -Verordnung 178/2002 (Artikel 18), die die globale Rückverfolgung von Lebensmitteln über alle Produktions-, Verarbeitungs- und Vertriebsstufen hin ab 1.1. 2005 fordert.

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 und bietet mit den Rechten, die es dem Betroffenen gibt (z. B. Auskunfts- und Löschungsansprüche), und den Pflichten, die es dem Verantwortlichen auferlegt (z. B. Unterrichts- und Löschungspflichten), 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, denn 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 *persönlichen, also personenbezogenen Daten*. Ein solches personenbezogenes Datum liegt (nur) vor bei Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (vgl. § 3 Abs. 1 BDSG).

Im Einzelnen

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 bzw. erhebt keinerlei personenbezogene/ personenbeziehbare Daten, solche werden jedoch später, z.B. 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 z. B. 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 die Zugangskontrolle für Gebäude, die oft mit einem Zeiterfassungssystem gekoppelt ist, Signaturkarten, Karten mit besonderen Schutzmechanismen (z. B. Patientenkarte), Massennutzungen erscheinen auch denkbar im Bereich des Ticketing, wo zunehmend die herkömmlichen Berechtigungsscheine durch RFIDs ersetzt werden (Skipässe, Konzert, Theater, Öffentlicher Personennahverkehr).

Als datenschutzrechtliche Sicherung wird regelmäßig § 6 c 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 die ausgebende Stelle dafür Sorge tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Vergütung stellen; schließlich 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 (in Betracht kommen z. B. § 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 Wegfahrsperrung beim Auto und insbesondere die Kennzeichnung von Waren zur automatischen Erfassung im Kassensbereich.

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 bzw. Artikel im Handel mit einem RFID – Tag ausgestattet (Lebensmittel, Kleidungsstücke etc.), so enthält dieser naturgemäß ausschließlich Informationen zu diesem Produkt wie z. B. Produktnummer, Hersteller, Größe (oder Gewicht, Füllmenge etc.), ein evtl. Herstellungs- und Verfallsdatum und 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 werden dem Handel durch nachgelagerte Systeme ein aktueller Überblick über die eigenen Bestände, die Optimierung des Orderprocessing und die Reduzierung von Out of Stock - Situationen 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 bestimmbarer 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 § 6 b BDSG waren- bzw. anwendungs-basierte Hinweis- und Transparenzpflichten für die Verwender von RFID – Tags geschaffen werden. § 6 b 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 § 6 b BDSG fruchtbar gemacht werden. 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 §§ 19 a 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, unter 3. behandelten Konstellation.

Schließlich kann auch § 6 a 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). 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. Denn Nach dem Kauf einer Ware hat der Kunde regelmäßig Besitz und Eigentum an der Ware, die Verfügungsgewalt über den dazugehörigen RFID –Tag liegt damit ausschließlich bei ihm. 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 Selbst Datenschutzes durch den Betroffenen hingewiesen werden. Selbstschutz ist ein Kern der informationellen Selbstbestimmung und wird als gestaltender Faktor der persönlichen Freiheit häufig unterschätzt. Selbstschutz meint dabei, dass „jeder Betroffene in Bezug auf die Offenlegung seiner personenbezogenen Daten sein eigener Datenschützer ist“ (vgl. zur Rolle des Selbst Datenschutzes 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 unterstricht 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 mit anderen Daten bzw. Anreicherung, 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.“*

Für Referenzsysteme (Savant Datenbank, ONS Server und PML Server) gilt zudem § 4 Abs. 1 und Abs. 3 BDSG (Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung) und u. U. kommen auch die Anforderungen aus § 9 BDSG zur Anwendung (Übermittlungskontrolle sowie die Zugriffskontrolle bei mehreren speichernden Stellen, vgl. Anlage zu § 9 S. 1 BDSG).

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 Relation 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 Relation Management sich auch schon heute 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 gesetzgeberischer Handlungsbedarf ist daher insoweit nicht zusätzlich erforderlich.

2. Schutz der Betroffenen 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 (§ 3 Nr. 22 TKG n. F.) stattfindet, indem Informationen ohne Verbindungsleitungen (vgl. § 3 Nr.4 TKG a. F.) als Nachricht ausgesandt und empfangen werden, aus der –je nach Umfang der auf dem RFID - Chip gespeicherten Informationen- sich 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 Dritte) verboten ist und einem möglichen Missbrauchspotential durch das strafbewehrte Verbot (Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe, § 148 Abs. 1 Nr. 1 TKG n. F.) entgegengetreten wird.