ARTIKEL-29-DATENSCHUTZGRUPPE

10107/05/DE
WP 105

Arbeitspapier

Datenschutzfragen im Zusammenhang mit der RFID-Technik

19. Januar 2005

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN,

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995[1],

gestützt auf Artikel 29 und auf Artikel 30 Absatz 1 Buchstabe c und Absatz 3 der Richtlinie,

gestützt auf ihre Geschäftsordnung, insbesondere auf Artikel 12 und 14,

HAT DIESES ARBEITSPAPIER ANGENOMMEN:

1. Einführung

Der Einsatz von Radio Frequency Identification, gemeinhin bekannt als „RFID-Technik", für unterschiedliche Zwecke und Anwendungen kann für die Wirtschaft, für Privatpersonen und für öffentliche Stelle (Regierungen eingeschlossen) von Vorteil sein. Wie im Folgenden ausgeführt wird, kann RFID Einzelhändlern bei der Verwaltung ihrer Lagerbestände helfen, das Einkaufserlebnis des Verbrauchers verbessern, die Sicherheit von Arzneimitteln erhöhen und den Zugang zu Sperrbereichen überwachen helfen.

Die Vorteile, die mit dem Einsatz der RFID-Technik verbunden sind, liegen auf der Hand, doch eine breite Nutzung der Technik birgt auch Nachteile. Aus der Sicht des Datenschutzes befürchtet die „Datenschutzgruppe", dass einige Anwendungen der RFID-Technik die Menschenwürde und den Datenschutz verletzen könnten. Die Bedenken richten sich insbesondere auf die Möglichkeit für Unternehmen und Regierungen, mittels RFID in die Privatsphäre von Privatpersonen einzudringen. Die verdeckte Sammlung einer Vielzahl von Daten, die sich alle auf ein und dieselbe Person beziehen, die Lokalisierung von Personen, die sich an öffentlichen Plätzen (Flughäfen, Bahnhöfen, Geschäften) aufhalten, die Erstellung von Kundenprofilen durch Beobachtung des Verbraucherverhaltens in Geschäften, das Auslesen von Informationen über Kleidungsstücke und Accessoires, die gerade getragen, oder über Medikamente, die mitgeführt werden, sind Beispiele für das Nutzungspotenzial von RFID, das aus datenschutzrechtlicher Sicht Anlass zu Sorge gibt. Das Problem wird noch dadurch verschärft, dass die Technik aufgrund ihrer geringen Kosten nicht nur den großen Akteuren zur Verfügung stehen wird, sondern auch kleineren bis hin zum einzelnen Bürger.

Angesichts dieser neuen Risiken sah sich die Datenschutzgruppe veranlasst, die Auswirkungen der RFID-Technik auf die Persönlichkeitsrechte und andere Grundrechte

[1] ABl. L 281 vom 23.11.1995, S. 31, abrufbar unter: http://europa.eu.int/comm/internal_market/privacy/law_de.htm

näher zu untersuchen. Zu diesem Zweck hat sie die beteiligten Gruppen, darunter Hersteller und Anwender der Technik sowie Datenschützer befragt. Die sich daran anschließende Analyse mündete in das vorliegende Arbeitspapier, mit dem die Datenschutzgruppe im Wesentlichen zwei Ziele verfolgt: Zum einen will sie den Anwendern der RFID-Technik Leitlinien an die Hand geben für die Anwendung der Grundprinzipien der EG-Richtlinien, vornehmlich der Datenschutzrichtlinie[2] und der Datenschutzrichtlinie für elektronische Kommunikation[3], und zum zweiten möchte sie den Herstellern der technischen Bausteine, also der RFID-Tags, Lesegeräte und Anwendungen, sowie den RFID-Normungsstellen Empfehlungen geben im Hinblick auf ihre Verantwortung, eine datenschutzkonforme Technik zu entwickeln, damit die Anwender der Technik ihren Verpflichtungen aus der Datenschutzrichtlinie gerecht werden können.

Angesichts mangelnder Erfahrungen mit der RFID-Technik betrachtet die Datenschutzgruppe dieses Arbeitspapier als einen ersten Situationsbericht. Sie wird die Entwicklung weiter beobachten und mit zunehmender Erfahrung weitere Leitlinien vorschlagen. Dies wird umso wichtiger, als sich die RFID-Technik zu einem wesentlichen Baustein der künftigen „intelligenten Umgebung“ (Ambient Intelligence) entwickeln dürfte. Kurz gesagt, mit diesem Papier soll ein Anfang gemacht werden, und die Datenschutzgruppe wird ihre Arbeit zu diesem Thema fortsetzen.

2. Funk-Erkennung (Radio Frequency Identification, RFID): Einführung in die Technik und ihre Verwendung[4]

1. Grundlagen der RFID-Technik

Die wichtigsten Bestandteile der RFID-Technik bzw. Infrastruktur sind der RFID-Transponder (auch Tag oder Etikett genannt), also ein Mikrochip (engl. *tag*), und das Lesegerät (engl. *reader)*. Der Transponder besteht aus einem elektronischen Schaltkreis zur Datenspeicherung und einer Antenne zum Empfangen und Senden von Funkwellen. Das Lesegerät besitzt eine Antenne und einen Demodulator, der die ankommenden analogen Informationen in digitale Daten umwandelt, die dann von einem Rechner verarbeitet werden können.

Wie im Folgenden dargestellt, kann die RFID-Technik je nach Art des Tansponders und des Lesegerätes in unterschiedlicher Weise eingesetzt werden. Die Anwender der Technik können je nach Bedarf zwischen unterschiedlichen technischen Möglichkeiten wählen. Es gibt „aktive“ und „passive“ RFID-Transponder. „Passive“ Tags haben keine eigene Energieversorgung (Batterie) und bleiben daher jahrzehntelang funktionstüchtig. Sie beziehen ihre Energie aus den empfangenen Funkwellen. Ein RFID-

[2] Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

[3] Richtlinie 2002/58/EG vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

[4] Eine ausführlichere technische Beschreibung von RFID und der möglichen Einsatzbereiche ist diesem Papier als Anlage beigefügt.

Lesegerät sendet Funkwellen, die den Tag innerhalb einer bestimmten Reichweite aktivieren, damit er die auf ihm gespeicherten Daten überträgt. „Aktive“ Tags haben eine eigene Batterie, wodurch sich ihre Lebensdauer allerdings verringert. Sie senden ihre Informationen selbsttätig oder bleiben im Ruhezustand, bis sie von einem Lesegerät aktiviert werden.

2 Vielfältige Einsatzmöglichkeiten - Beispiele

Die RFID-Technik hält in zahlreichen *Gebieten* Einzug, z. B. im Gesundheitswesen, in der Luftfahrt oder im Verkehr. Darüber hinaus wächst auch die Zahl der spezifischen *Funktionen*, die RFID-Tags in den einzelnen Bereichen erfüllen können, und die Möglichkeiten sind noch lange nicht ausgeschöpft. In diesem Abschnitt sollen die wichtigsten Funktionen und Anwendungsbereiche der RFID-Technik, wie beispielsweise Verkehr oder Gesundheitswesen, veranschaulicht werden. Einige der beschriebenen RFID-Anwendungen befinden sich noch in der Erprobung, andere sind jedoch schon Realität, manchmal ohne dass es den Betroffenen bewusst ist.

Verkehr und Handel. RFID-Systeme eignen sich gut für einige verkehrstechnische Anwendungen. Bei entsprechender Verteilung von RFID-Lesegeräten können Fahrzeuge, die mit einem RFID-Transponder ausgerüstet sind, auf dem Weg zu ihrem Ziel lokalisiert werden. Bereits jetzt beruhen viele Fahrkarten auf der RFID-Technik. Nach Aussagen der Automobilindustrie sind außerdem bereits Millionen von Autoschlüsseln mit RFID-Technik ausgestattet.

Luftfahrt. Die RFID-Technik kann bei der Gepäckabfertigung eingesetzt werden. Beim Einchecken erhält jedes Gepäckstück einen Transponder, anschließend können Lesegeräte, die sich in verschiedenen Abschnitten der Flughäfen befinden, das Gepäckstück bei seiner Beförderung innerhalb eines Flughafens, aber auch zwischen verschiedenen Flughäfen verfolgen. Es gibt bereits Pläne, Bordkarten mit RFID-Tags zu versehen, um verspätete Passagiere ausfindig machen zu können.

Gesundheitswesen. Die Arzneimittelindustrie verwendet RFID-Systeme, um Arzneimittel leichter lokalisieren und Fälschungen und Diebstahlsverluste während des Transports vermeiden zu können. Bei der Herstellung erhält jedes Arzneimittel ein RFID-Tag, das seine Herkunft bescheinigt. Apotheken oder Geschäfte, die Arzneimittel verkaufen, erhalten Lesegeräte, die überprüfen, ob das Arzneimittel auch wirklich von dem angeblichen Hersteller stammt. Die amerikanische Gesundheitsbehörde (FDA) hat bereits Leitlinien für das Anbringen von RFID-Tags auf Arzneimittelverpackungen veröffentlicht, um die Medikamente lokalisieren und Fälschungen vermeiden zu können[5]. Auch in Krankenhäusern kann RFID-Technik die Sicherheit der Patienten erhöhen und den Kliniken helfen, Kosten zu sparen; so können Tags auf dem Operationsmaterial verhindern, dass am Ende einer Operation etwas im Körper des Patienten vergessen wird. Auch die Patienten selbst können mit RFID-Transpondern ausgerüstet werden, um ihre

[5] Radiofrequency Identification Feasibility Studies and Pilot Programs for Drugs; Guidance for FDA Staff and Industry; Compliance Policy Guide; Sec. 400.210; Radiofrequency Identification Feasibility Studies and Pilot Programs for Drugs; November 2004.

Identität, ihren Aufenthaltsort und den genauen Behandlungsverlauf feststellen zu können. Das Klinikpersonal kann ebenso mit Transpondern ausgestattet werden, damit es in Notfällen schneller ausfindig gemacht werden kann. Die amerikanische Gesundheitsbehörde hat vor kurzem einem Unternehmen die Genehmigung für den Einsatz von RFID im Menschen erteilt: unter die Haut injiziert oder eingepflanzt soll der VeriChip den Ärzten bei Notfällen Auskunft über die Krankengeschichte des Patienten geben[6].

Sicherheit und Zugangskontrolle. Mit RFID-Systemen können die Bewegungen und die Verwendung wertvoller Gegenstände verfolgt werden, da die Transponder Informationen über den Aufenthaltsort dieser Gegenstände an Lesegeräte in angemessener Reichweite senden. In der Automobilindustrie wird die RFID-Technik bereits als Bestandteil einer Wegfahrsperre genutzt. In der Konsumgüterindustrie kann mit speziellen RFID-Tags die Herkunft bestimmter Waren festgestellt werden. Auf diese Weise können hochwertige Produkte auf Fälschung überprüft werden. Seit einigen Jahren ist das Anbringen von RFID-Tags auf Banknoten ein Forschungsschwerpunkt.

Aus der Arbeit der ICAO[7] zu schließen, ist ein Einsatz von RFID auch für Pässe vorgesehen[8]. Der beschränkte Zugang von Personen zu bestimmten Bereichen kann ebenfalls mit Hilfe von RFID-Tags oder berührungslosen Smartcards kontrolliert werden, wie auf dem Weltgipfel Informationsgesellschaft oder bei einem Kongress der Kommunistischen Partei Chinas bereits geschehen.

Anwendungen im Einzelhandel. Einige Einzelhandelsketten haben die Hersteller ihrer Produkte bereits gebeten, die Waren mit RFID-Tags zu versehen. Solche „getaggten“ Produkte bieten dem Händler vielfältige Vorteile. So kann er mittels RFID-Technik seine Lagerverwaltung verbessern. Jedes einzelne Produkt kann in den verschiedenen Phasen, die es durchläuft, also bei der Anlieferung, im Regal oder beim Verkauf identifiziert werden; so bietet die RFID-Technik dem Händler ein flexibles Werkzeug, um die Verfügbarkeit seiner Waren im Laden und im Lager zu regeln und zu überwachen. RFID kann auch die Effizienz innerhalb der Verkaufsräume erhöhen, was sowohl dem Händler als auch möglicherweise den Kunden zugute kommt. Lesegeräte im Kassenbereich könnten die Wartezeiten und somit die Aufenthaltsdauer des Kunden im Geschäft verkürzen. RFID kann die Lokalisierung von Produkten vereinfachen und somit Rückrufaktionen für fehlerhafte, unsichere oder Produkte mit abgelaufenem Haltbarkeitsdatum erleichtern.

Im Zusammenhang mit der Anwendung von RFID-Technik im Einzelhandel sollten die Normungsarbeiten von EPCglobal nicht außer acht gelassen werden, die auf

---

6 Department of Health and Human Services; Food and Drug Administration; 21 CFR Part 880; Docket No. 2004N–0477]; veröffentlicht im Federal Register / Vol. 69, No. 237 / 10. Dezember 2004 / Rules and Regulations.

7 International Civil Aviation Organisation – Internationale Zivilluftfahrt-Organisation

8 Im Jahr 2003 legte die ICAO die technischen Anforderungen für RFID-Technik fest, mit der elektronische Pässe ausgestattet werden sollen. Die Spezifikationen wurden im ICAO-Papier 9303 veröffentlicht.

die Schaffung eines „Elektronischen Produktcodes“ abzielen, mit dem jedes einzelne Produkt gekennzeichnet wird[9].

3. Eingriffe in den Datenschutz und die Persönlichkeitsrechte

Während einige RFID-Anwendungen keine datenschutzrechtlichen Probleme aufwerfen, bieten viele, wie nachfolgend beschrieben, sehr wohl Anlass zu Sorge. Dieser Abschnitt gibt einen Überblick über die wichtigsten datenschutzrechtlichen Folgen, die sich aus den unterschiedlichen Anwendungen der RFID-Technik ergeben.

3.1. Erhebung von Informationen, die mit personenbezogenen Daten verknüpft sind

Datenschutzrechtliche Bedenken kommen auf, wenn die RFID-Technik zur Erhebung von Informationen eingesetzt wird, die mittelbar oder unmittelbar mit personenbezogenen Daten verknüpft werden. Vorstellbar wäre ein Fall, in dem die RFID-Nummer eines Produktes mit den Daten des Käufers verknüpft wird. So könnte beispielsweise ein Elektronikhändler seine Waren mit eindeutigen Produktcodes versehen, die dann systematisch mit dem bei der Kreditkartenzahlung erfassten Kundennamen kombiniert und später mit der Kundendatei des Händlers verknüpft werden, unter anderem für Garantiezwecke. Ferner ist eine Situation denkbar, in der ein Supermarkt Kundenkarten oder ähnliches, die die Kunden namentlich identifizieren, mit RFID-Transpondern versieht, um das Kundenverhalten in den Verkaufsräumen zu erfassen, z. B. die Zeit, die Kunden in bestimmten Abteilungen verbringen, die Zahl der Besuche ohne Einkauf usw.

In den oben genannten Fällen ist der Eingriff in die Persönlichkeitsrechte offensichtlich, da die mittels RFID-Technik erhobenen Informationen mit personenbezogenen Daten verknüpft werden. Mit Hilfe des Systems der Kundenkarten können schon heute Verbrauchergewohnheiten erfasst und individuelle Profile erstellt werden; die RFID-Technik erweitert diese Möglichkeiten noch: die Ausrüstung jedes einzelnen Produkts mit einem RFID-Tag („item-level tagging“) erhöht das Direktmarketingpotenzial, da die Kunden beim Betreten des Geschäftes identifiziert und ihr Verhaltensweisen im Geschäft beobachtet werden können. Darüber hinaus wird der großflächige Einsatz der Technik, sowohl was die Art als auch was die Zahl der Daten angeht, eine Datenflut auslösen, die von den unterschiedlichsten Verantwortlichen verarbeitet werden muss; auch dies gibt Anlass zu Sorge.

3.2. Speicherung personenbezogener Daten auf dem Transponder

Persönlichkeitsrechte werden aber auch verletzt, wenn personenbezogene Daten unmittelbar auf RFID-Tags gespeichert werden. Ein Beispiel für diese Nutzungsart sind Fahrkarten. Vorstellbar wäre der Fall eines Unternehmens, das beschließt, ein

[9] Weitere Informationen über EPCglobal sind in Abschnitt 5.2 nachzulesen.

berührungsloses RFID-basiertes Fahrkartensystem für Monatskarten aufzubauen, bei dem Name, Anschrift, Telefonnummer usw. des Fahrkarteninhabers auf dem Tag gespeichert sind. Auf diese Weise könnte das Unternehmen jederzeit die Fahrstrecken des einzelnen Kunden nachvollziehen. Dies stellt einen offensichtlichen Eingriff in die Privatsphäre der Betroffenen dar. Doch nicht nur das Verkehrsunternehmen könnte über diese Informationen verfügen; auch Dritte könnten sich die Informationen verdeckt beschaffen, da jedes Standard-Lesegerät die Existenz bestimmte RFID-Tags erkennen kann. Es sei darauf hingewiesen, dass RFID-Systeme sehr angriffsanfällig sind. Da sie unsichtbar und berührungslos arbeiten, kann ein Angriff aus der Entfernung erfolgen und das passive Auslesen eines Tags ist für den Betroffenen nicht feststellbar.

3.3. Personenverfolgung ohne „traditionelle“ Kenndaten

Eine dritte Art von Datenschutzverletzungen ergibt sich aus dem Einsatz von RFID zur Verfolgung („Tracking“) einzelner Personen und zur Gewinnung personenbezogener Daten. Die nachfolgenden Beispiele zeigen, wie die RFID-Technik in die Persönlichkeitsrechte eingreifen kann.

Eine Handelskette gibt an ihre Kunden beispielsweise mit RFID-Tags versehene Pfandmünzen für Einkaufswagen aus, die bei jedem Einkauf wiederverwendet werden können. Mit Hilfe der auf der Pfandmünze gespeicherten Identifikationsnummer könnte eine Datei erstellt werden, aus der ersichtlich wäre, welche Produkte eine durch die Pfandmünze identifizierte Person kauft, wie häufig sie diese Produkte kauft und welche Filialen der Handelskette sie aufsucht. Die Filialen könnten Rückschlüsse auf das Einkommen, den Gesundheitszustand, den Lebensstil, die Einkaufsgewohnheiten usw. des Kunden ziehen. Diese Informationen wiederum könnten bestimmte Verkäuferentscheidungen beeinflussen, z. B. die Marketingstrategie oder gar eine dynamische Preispolitik. Da der Kunde mit Hilfe der Pfandmünze jedes Mal identifiziert würde, wenn er die Verkaufsräume betritt, könnten seine gespeicherten Einkaufsgewohnheiten für individuelle Werbeaktionen genutzt werden. Neben den einzelnen Filialen könnten aber auch Dritte diese Angaben erhalten. Auf diese Weise könnten eine Reihe von Entscheidungen über die identifizierte Person getroffen werden, ohne dass diese hierzu in voller Kenntnis der Sachlage ihre Einwilligung gibt. Ähnlich wie bei der Verwendung von Cookies im Internetkontext lässt sich die betroffene Person, selbst wenn sie nicht sofort und unmittelbar anhand eines bestimmten Produkts identifiziert werden kann, auf der assoziativen Ebene problemlos identifizieren, und zwar über die Masse der sie umgebenden bzw. über sie gespeicherten Informationen. Die erhobenen Daten können sogar die Art beeinflussen, in der die betroffene Person behandelt oder beurteilt wird. Auch diese RFID-Anwendung löst schwerwiegende datenschutzrechtliche Befürchtungen aus.

Datenschutzrechtliche Bedenken ergeben sich auch in Situationen, in denen die Verwendung von RFID-Tags die Verarbeitung personenbezogener Daten nach sich zieht, selbst wenn keine weiteren eindeutigen Kenndaten verwendet werden. Angenommen die Person Z betritt das Geschäft C mit einer Tasche, in der sich „getaggte“ Produkte aus den Geschäften A und B befinden. Geschäft C scannt diese Tasche, und die darin

befindlichen Produkte (wahrscheinlich eher ein Wirrwarr an Zahlen) werden erfasst. Geschäft C speichert diese Zahlen. Kommt der Kunde Z am nächsten Tag wieder in das Geschäft, wird er wieder gescannt. Das Produkt Y, das bereits am Vortag gescannt wurde, wird wiedererkannt — die Nummer steht für die Armbanduhr, die der Kunde täglich trägt. Geschäft C erstellt eine Datei mit der Nummer des Produktes Y als „Schlüssel". Nun kann der Kunde beim Betreten des Geschäfts anhand der RFID-Nummer der Armbanduhr erkannt werden. Geschäft C kann jetzt für den Kunden Z (dessen Name ihm nicht bekannt ist) ein Profil erstellen und verfolgen, was der Kunde bei späteren Besuchen in seiner Einkaufstasche hat. Auf diese Weise verarbeitet Geschäft C personenbezogene Daten, folglich findet das Datenschutzrecht Anwendung.

Schließlich wären da noch RFID-Transponder auf bestimmten Gegenständen, die Auskunft über die Art des Gegenstandes geben. Eigentumsgegenstände einer Person sind etwas sehr Persönliches und beinhalten Informationen, deren Kenntnis durch Dritte einen Eingriff in die Privatsphäre dieser Person darstellen würde. Folgende Beispiele veranschaulichen diese Aussage. Angenommen jeder, der ein Lesegerät besitzt, kann Banknoten, Bücher, Arzneimittel oder Wertgegenstände von Passanten ausfindig machen. Erhalten Dritte Kenntnis von diesen Informationen, stellt dies einen Eingriff in die Persönlichkeitsrechte des Eigentümers. Bedenklich wäre auch, wenn Terroristen in der Lage wären, in einer Menschenmenge Personen bestimmter Nationalitäten ausfindig zu machen. Noch schwerwiegender wäre der hier beschriebene Eingriff, wenn der Gegenstand selbst wichtige personenbezogene Daten enthielte, beispielsweise Ausweisdaten oder hochsensible Daten.

Diese Beispiele veranschaulichen einige der größten Gefahren der RFID-Technik für den Datenschutz und die Persönlichkeitsrechte, die darin bestehen, dass Personen verdeckt und ohne ihre Einwilligung ausspioniert werden, und zwar durch den unautorisierten Zugriff auf die von den RFID-Tags übertragenen Informationen.

In den folgenden Abschnitten wird erläutert, wie wichtig es ist, die oben beschriebenen Datenverarbeitungsverfahren an Leitlinien für die Anwendung der in den EG-Richtlinien, insbesondere der Datenschutzrichtlinie, verankerten Grundprinzipien zu knüpfen.

4. Anwendung des EU—Datenschutzrechts auf die Datenerhebung mittels RFID-Technik

4.1. Leitlinien für die Anwendung der Datenschutzrichtlinie auf die Sammlung und Weiterverarbeitung von Daten mittels RFID-Technik

Der Geltungsbereich der Datenschutzrichtlinie umfasst die Verarbeitung aller personenbezogenen Daten. Die Richtlinie enthält eine sehr weitgefasste Definition für „personenbezogene Daten", die sich auf *„alle Informationen über eine bestimmte oder bestimmbare natürliche Person"* erstreckt. Somit stellt sich die Frage, ob die Datenschutzrichtlinie damit zwangsläufig für die Datenerhebung mittels RFID-Technik gilt. Die Antwort wird immer von der jeweiligen Anwendung abhängen, insbesondere

davon, ob die sie eine Verarbeitung personenbezogener Daten im Sinne der Datenschutzrichtlinie nach sich zieht.

Um zu beurteilen, ob die Erhebung personenbezogener Daten mittels einer bestimmten RFID-Anwendung unter die Datenschutzrichtlinie fällt, gilt es zu klären, a) inwieweit die verarbeiteten Daten sich auf eine betroffene Person *beziehen* und b) ob diese Daten eine Person betreffen, die *bestimmbar* oder bereits bestimmt ist. Daten beziehen sich auf eine Person, wenn sie die Identität, die Merkmale oder das Verhalten dieser Person betreffen oder wenn sie verwendet werden, um die Art festzulegen oder zu beeinflussen, in der die Person behandelt oder beurteilt wird. Um festzustellen, ob die Daten eine bestimmbare Person betreffen, ist Erwägungsgrund 26 der Datenschutzrichtlinie heranzuziehen; danach sollten *„alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen*".

Somit fällt nicht jede Datenerhebung mittels RFID-Technik unter die Datenschutzrichtlinie, es ist aber auch nicht von der Hand zu weisen, dass es viele Situation geben wird, in denen personenbezogene Daten mittels RFID-Technik erhoben werden, deren Verarbeitung sehr wohl richtlinienrelevant ist.

Jeder, der Informationen verwenden will, die mittels RFID-Technik erhoben wurden, wird vorher prüfen müssen, ob die Informationen als „personenbezogene Daten" im Sinne der Datenschutzrichtlinie anzusehen sind. Enthalten die RFID-Informationen keine personenbezogenen Daten und werden auch nicht, wie oben beschrieben, mit personenbezogenen Daten verknüpft, findet die Datenschutzrichtlinie keine Anwendung. Werden also die Informationen auf dem RFID-Tag nicht mit anderem „Identifizierungsmaterial" verknüpft, beispielsweise mit einem Foto, dem Namen und der Anschrift der betreffenden Person oder einer wiederkehrenden Kennnummer, dann kommt die Datenschutzrichtlinie nicht zur Anwendung.

In den drei in Abschnitt 3 beschriebenen Fällen würde die Datenschutzrichtlinie Anwendung finden. Im ersten Fall, weil die mittels RFID-Technik erhobene Produktinformation direkt mit den auf einer Kredit- oder Kundenkarte gespeicherten personenbezogenen Daten verknüpft wird. Im zweiten Fall gilt die Datenschutzrichtlinie ab dem Zeitpunkt, an dem personenbezogene Daten, wie ein Name, im RFID-Transponder gespeichert werden. Schließlich gilt die Datenschutzrichtlinie auch dann, wenn mittels RFID-Technik Bewegungen einzelner Personen verfolgt werden, die zwar nicht bestimmt werden, angesichts der massiven Datenaggregation, der Speicher- und Verarbeitungsmöglichkeiten, aber bestimmt werden könnten.

4.2 Leitlinien für die Konformität mit den Datenschutzerfordernissen

Die Verantwortlichen für die Verarbeitung von mittels RFID-Technik erhobenen Daten sind an die Datenschutzrichtlinie gebunden (in dem vorliegenden Papier werden sie häufig als „Anwender der Technik" bezeichnet). Es kann zwar unmöglich festgelegt, wie diese Anforderungen in jedem einzelnen RFID-Szenario zu erfüllen sind, es ist aber

möglich, einige allgemeine Leitlinien zu entwerfen, an die sich die für die Datenverarbeitung Verantwortlichen halten und die sie an die jeweiligen Umstände der Datenverarbeitung anpassen können. Wie in Abschnitt 5 näher erläutert wird, sind die Hersteller für die Bereitstellung einer datenschutzkonformen Technik direkt verantwortlich; diese soll dazu beitragen, dass die Verarbeiter ihren Verpflichtungen aus der Datenschutzrichtlinie nachkommen und dass die betroffenen Personen ihre Rechte wahrnehmen können.

Grundsätze:

Die Datenschutzgruppe weist darauf hin, dass Erwägungsgrund 2 der Datenschutzrichtlinie den Rahmen für die Anwendung der RFID-Technik, wie für jede andere Technik bildet: „*Die Datenverarbeitungssysteme stehen im Dienste des Menschen; sie haben, ungeachtet der Staatsangehörigkeit oder des Wohnortes der natürlichen Personen, deren Grundrechte und –freiheiten und insbesondere deren Privatsphäre zu achten und zum wirtschaftlichen und sozialen Fortschritt, zur Entwicklung des Handels sowie zum Wohlergehen der Menschen beizutragen*."

Grundsätze der Datenqualität: Die für die Datenverarbeitung Verantwortlichen, die im Zuge von RFID-Anwendungen Daten erheben, müssen u. a. folgende **Datenschutzgrundsätze** einhalten:

Grundsatz der begrenzten Verwendung (Zweckbestimmung): Dieser Grundsatz, der teilweise in Artikel 6 Absatz 1 Buchstabe b der Datenschutzrichtlinie verankert ist, verhindert unter anderem eine Weiterverarbeitung, die mit dem Zweck (den Zwecken) der Datenerhebung unvereinbar ist.

Grundsatz der Datenqualität: Dieser ebenfalls in der Richtlinie festgeschriebene Grundsatz fordert, dass die personenbezogenen Daten für die Zwecke, für die sie erhoben werden, erheblich sind und nicht darüber hinausgehen. Demzufolge dürfen keine unerheblichen Daten erhoben werden; falls dies dennoch geschehen ist, müssen sie gelöscht werden (Artikel 6 Absatz 1 Buchstabe c). Darüber hinaus müssen die Daten sachlich richtig und auf dem neuesten Stand sein.

Aufbewahrungsgrundsatz: Diesem Grundsatz zufolge dürfen personenbezogene Daten nicht länger aufbewahrt werden, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist.

Rechtsgrundlage für die Verarbeitung: Gemäß Artikel 7 der Datenschutzrichtlinie dürfen personenbezogene Daten nur verarbeitet werden, wenn eine der Voraussetzungen für eine rechtmäßige Datenverarbeitung erfüllt ist[10].

[10] Artikel 7 listet die folgenden Voraussetzungen auf, die eine Datenverarbeitung rechtfertigen: i) die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben, ii) die Verarbeitung ist erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, iii) die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche

In der Mehrzahl der Fälle, in denen RFID-Technik eingesetzt wird, werden sich die für die Verarbeitung Verantwortlichen lediglich auf die Einwilligung der betroffenen Person als rechtmäßige Voraussetzung für die Datenerhebung mittels RFID stützen können. So wird ein Supermarkt, der seine Kundenkarten mit RFID-Tags versieht, entweder ausdrückliche vertragliche Vereinbarungen oder die Einwilligung der betroffenen Person benötigen, um die personenbezogenen Informationen, die er bei der Ausstellung der Kundenkarte erhalten hat, mit den Daten verknüpfen zu dürfen, die das RFID-Tag übermittelt. Die Einwilligung der betroffenen Person ist jedoch nicht immer die adäquate rechtliche Voraussetzung, um die Verarbeitung personenbezogener Daten, die im Rahmen von RFID-Systemen erhoben wurden, zu rechtfertigen. So bräuchte beispielsweise eine Klinik, die RFID in Operationsbestecken verwendet, um zu vermeiden, dass bei Beendigung einer Operation Instrumente im Körper des Patienten vergessen werden, nicht unbedingt das Einverständnis des Patienten, da diese Form der Verarbeitung mit den lebenswichtigen Interessen der betroffenen Person gerechtfertigt werden könnte, die gemäß Artikel 7 der Datenschutzrichtlinie[11]) einen anderen Rechtfertigungsgrund darstellen.

Basiert die Verarbeitung auf der Einwilligung der betroffenen Person, sind gemäß Artikel 2 und Artikel 7 Buchstabe a der Richtlinie bestimmte Erfordernisse zu erfüllen. (i) Die Einwilligung muss freiwillig gegeben werden, d. h. ohne „Täuschung oder Zwang“. (ii) Sie muss spezifisch sein, d. h. sie muss sich auf einen bestimmten Zweck beziehen. (iii) Die Einwilligung muss Ausdruck des tatsächlichen Willens der betroffenen Person sein. (iv) Die Einwilligung muss in voller Kenntnis der Sachlage erfolgen. Schließlich muss sie „*ohne jeden Zweifel*“ gegeben werden, d. h. eine Einwilligung, die mehr als eine Interpretation zulässt, gilt nicht als Einwilligung.

Informationserfordernisse: Gemäß Artikel 10 der Datenschutzrichtlinie müssen die für die Datenverarbeitung Verantwortlichen, die mittels RFID-Technik Daten verarbeiten, den betroffenen Personen folgende Informationen mitteilen: die Identität des für die Verarbeitung Verantwortlichen, die Zweckbestimmungen der Verarbeitung sowie unter anderem Informationen über die Empfänger der Daten und das Bestehen eines Auskunftsrechts[12]. In dem in Abschnitt 4 geschilderten Szenario müsste der Einzelhändler in Erfüllung dieser Verpflichtungen die betroffenen Personen mindestens über Folgendes informieren:

---

unterliegt, iv) die Verarbeitung ist erforderlich für die Wahrung lebenswichtiger Interessen der betroffenen Person, v) die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, vi) die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von der für die Verarbeitung verantwortlichen Partei wahrgenommen wird, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

[11] Die Datenschutzgruppe weist darauf hin, dass die in Artikel 7 der Datenschutzrichtlinie aufgestellten rechtlichen Voraussetzungen, die eine bestimmte Datenverarbeitung rechtfertigen, letztlich von den besonderen Umständen dieser Verarbeitung abhängig sind.

[12] Informationen über die Empfänger der Daten, über die Antwortpflicht und über das Bestehen von Auskunfts- und Berichtigungsrechten müssen unter Berücksichtigung der jeweiligen Umstände, unter denen die Daten erhoben werden, bereitgestellt werden, sofern sie notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.

(i) die Existenz von RFID-Tags auf Produkten oder auf ihren Verpackungen und die Existenz von Lesegeräten;

(ii) die Folgen im Hinblick auf die Datenerhebung; insbesondere sollten die für die Verarbeitung Verantwortlichen die Betroffenen sehr genau darüber informieren, dass die RFID-Tags von den Lesegeräten zur Übertragung von Daten veranlasst werden können, ohne dass hierfür die betroffenen Personen in irgendeiner Weise tätig werden müssen.

(iii) die Zwecke, für die die Informationen bestimmt sind, einschließlich Angaben darüber a) mit welchen Daten die RFID-Informationen verknüpft werden und b) ob die Informationen Dritten verfügbar gemacht werden; ferner

(iv) die Identität des für die Verarbeitung Verantwortlichen.

Darüber hinaus muss der für die Verarbeitung Verantwortliche je nach Art der RFID-Anwendung die betroffenen Personen darüber informieren, (v) wie die Tags gelöscht, deaktiviert oder von den Produkten entfernt werden können, um zu verhindern, dass sie weitere Informationen übermitteln, und (vi) wie die Betroffenen ihr Auskunftsrecht wahrnehmen können. Diese Auskünfte wären in den in Abschnitt 3.1 beschriebenen Szenarios erforderlich. Hinweise bei Gebrauchsgütern, wie z. B. die für EPCglobal vorgeschlagenen, dienen zwar der Bereitstellung der unter i) genannten Informationen; diese sollten aber um die oben aufgeführten Informationen ergänzt werden[13].

Gemäß dem in Artikel 6 Buchstabe a der Datenschutzrichtlinie verankerten Prinzip der Verarbeitung nach Treu und Glauben, müssen die Informationen für die betroffene Person klar und verständlich sein.

Schließlich möchte die Datenschutzgruppe darauf hinweisen, dass die betroffene Person durch die Bereitstellung der obigen Informationen in der Lage sein sollte, ohne Weiteres die Folgen der RFID-Anwendung zu verstehen.

Das Auskunftsrecht der betroffenen Person: Artikel 12 der Datenschutzrichtlinie gibt den betroffenen Personen die Möglichkeit, die Richtigkeit der Daten zu überprüfen und sicherzustellen, dass die Daten auf dem neuesten Stand sind. Diese Rechte gelten in vollem Umfang auch bei der Erhebung personenbezogener Daten mittels RFID-Technik. Für den Supermarkt, der Kundenkarten „taggt“, bedeutet dies z. B., dass er im Rahmen des Auskunftsrechts *alle* Informationen offenlegen muss, die mit der betroffenen Person verknüpft sind, beispielsweise die Anzahl der Besuche in dem Geschäft, die Art der Einkäufe usw.

Enthalten RFID-Transponder personenbezogene Daten wie in Abschnitt 3.2 beschrieben, sollten die betroffenen Personen erfahren dürfen, welche Informationen auf den Transpondern gespeichert sind, und das Recht haben, mit einfachen Mitteln Berichtigungen vorzunehmen.

[13] Abschnitt 5.1 enthält einen Überblick über die Tätigkeiten von EPCglobal.

Sicherheitserfordernisse: Artikel 17 der Datenschutzrichtlinie verpflichtet die für die Verarbeitung Verantwortlichen, geeignete Maßnahmen zum Schutz gegen zufällige oder unrechtmäßige Zerstörung oder unberechtigte Offenlegung zu ergreifen. Die Maßnahmen können organisatorischer oder technischer Art sein. Auf dieses Erfordernis wird in Abschnitt 5 näher eingegangen, der sich mit der RFID-Technik und dem notwendigen Einsatz datenschutzfreundlicher Technik beschäftigt.

5. Technische und organisatorische Erfordernisse, die eine angemessene Verwirklichung der Datenschutzgrundsätze gewährleisten

Die Anwender von RFID-Technik müssen die oben genannten Grundsätze sowie das in Artikel 6 Absatz 1 der Datenschutzrichtlinie verankerte Prinzip der Datensparsamkeit einhalten.

Nach Auffassung der Datenschutzgruppe kann die Technik eine Schlüsselrolle übernehmen, wenn bei der Verarbeitung personenbezogener Daten, die mittels RFID erhoben wurden, die Einhaltung der Datenschutzgrundsätze gewährleistet werden soll. So könnte beispielsweise mit der Normung des Aufbaus von RFID-Tag, -Lesegeräten und -Anwendungen erreicht werden, dass personenbezogene Daten sparsam erhoben und verwendet werden, und dass jedwede unrechtmäßige Verarbeitung verhindert wird, indem ein unautorisierter Zugriff auf personenbezogene Daten technisch vereitelt wird.

In diesem Zusammenhang möchte die Datenschutzgruppe betonen, dass zwar die Anwender letztlich für die mittels einer RFID-Anwendung erhobenen personenbezogenen Daten verantwortlich sind, dass es aber Aufgabe der Hersteller und der Normungsgremien ist, den Anwendern eine datenschutzkonforme Technik zur Verfügung zu stellen, die Eingriffe in die Persönlichkeitsrechte verhindert. Es sollten Mechanismen entwickelt werden, die sicherstellen, dass solche Normen bei der praktischen Anwendung weitgehend eingehalten werden. Datenschutzkonforme RFID-Normen müssen insbesondere gewährleisten, dass Verantwortliche, die personenbezogene Daten mittels RFID-Technik verarbeiten, über die Instrumente verfügen, die zur Einhaltung der Datenschutzrichtlinie erforderlich sind. Die Datenschutzgruppe ruft daher die Hersteller von RFID-Tags, -Lesegeräten und -Anwendungen sowie die Normungsgremien auf, die folgenden Empfehlungen bei ihrer Arbeit zu berücksichtigen.

5.1 Einfluss von Normung und Interoperabilität auf die Verwirklichung der Datenschutzgrundsätze

Bei jeder Technik ist die Normung normalerweise die wichtigste Voraussetzung für Interoperabilität, die wiederum für eine erfolgreiche Akzeptanz und Umsetzung neuer Techniken wichtig ist. Normung kann auch den Erlass von Bestimmungen zum Datenschutz und zum Schutz der Privatsphäre erleichtern.

Alle Bestandteile eines RFID-Systems sind oder werden genormt, beispielsweise der Aufbau des Transponders und des Lesegeräts, die auf dem Tag gespeicherten Daten, das Kommunikationsprotokoll (Luftschnittstelle) zwischen Lesegerät und Transponder, die Verwaltung der vom Lesegerät ausgelesenen Daten usw. Die Normungsgremien und auch andere Stellen sind bereits im RFID-Bereich tätig geworden. Die RFID-Normung wird sich auf zahlreiche Märkte auswirken, insbesondere auf den Warenhandel.

Ursprünglich als Reaktion auf die BSE-Krise hat die Internationale Normungsorganisation (ISO) sektorspezifische Normen (Frachtbehälter, Transporteinheiten, Tiere usw.) für RFID-Transponder entwickelt, außerdem allgemeinere Normen für die Luftschnittstelle (ISO-Reihe 18000) und für das Artikelmanagement (ISO/EIC/15963:2004).

EPCglobal Inc.[14], ein Joint Venture zwischen EAN International und dem Uniform Code Council (UCC), wird geleitet von dem EPCglobal-Direktorium, in dem führende Unternehmen vertreten sind. Das Unternehmen arbeitet an einem „elektronischen Produkt-Code (EPC)“, mit dem jeder einzelne Artikel identifiziert werden kann. Jedes Produkt erhält einen Transponder auf dem die jeweilige Artikelnummer verzeichnet ist. Vorläufer dieses Systems ist der „Universal Product Code (UPC)“ oder Barcode, den der EPC ersetzen soll. Der Unterschied zwischen den beiden Systemen besteht darin, dass der UPC einen Produkttyp identifiziert, ohne dass jeder Artikel individuell nummeriert wird. Daneben entwickelt das EPCglobal-Netzwerk Normen für die Verbindung von Servern, die Informationen über mit EPC-Nummern identifizierte Artikel enthalten. Diese Server, auch EPC Information Services oder EPCIS genannt, sind über das Internet zugänglich und über eine Reihe von Netzwerkdiensten verknüpft, autorisiert und zugänglich[15].

Bei den meisten RFID-Normungsinitiativen können Datenschutzmerkmale in die technischen Spezifikationen aufgenommen werden. So wurde beispielsweise kürzlich vorgeschlagen[16], die ISO-Norm für das Reader-to-Tag-Protokoll zu verändern, um die von der OECD ausgearbeiteten Fair Information Practices[17] mit einzubeziehen.

Vor kurzem hat das Europäische Institut für Telekommunikationsstandards (ETSI) eine neue europäische Norm für den Einsatz von RFID-Systemen angenommen, die die zulässige Leistung des Lesegerätes und die Zahl der verfügbaren Kanäle auf dem UHF-Band erhöht, dem vielversprechendsten Band für die Artikelidentifizierung im Bereich

---

14 http://www.epcglobalinc.org/

15 Bis heute sind die Interessen der EU bei diesen Normungsinitiativen unterrepräsentiert, da dort im Wesentlichen Interessenträger der US-Industrie vertreten sind. Ferner steht noch nicht fest, ob die chinesische Seite eine der genannten Normen übernehmen oder möglicherweise eigene Normen entwickeln wird.

16 Christian Floerkemeier, Roland Schneider, Marc Langheinrich: Scanning with a Purpose - Supporting the Fair Information Principles in RFID protocols. 2nd International Symposium on Ubiquitous Computing Systems (UCS 2004), 8.-9. November 2004, Tokio, Japan.

17 ISO 18000 Teil 6 Typ A

des Einzelhandels. Diese Entwicklung wird insbesondere die Reichweite zwischen Lesegerät und RFID-Transponder vergrößern[18].

Die Interoperabilität von RFID-Systemen (Hardware, Software und erzeugte Daten) ergibt sich logischerweise aus der Normung. Die Unternehmen sehen die Interoperabilität von RFID-Systemen positiv. Natürlich sollte ein Einzelhändler im Hinblick auf ein nachhaltiges Geschäftsmodell nicht gezwungen sein, unterschiedliche Lesegeräte zu installieren, um die Transponder unterschiedlicher Hersteller auslesen zu können. Aus Sicht des Datenschutzes kann die Interoperabilität zwar die technische Qualität der Daten erhöhen und zur Einhaltung von Artikel 6 Absatz 1 Buchstabe d der Datenschutzrichtlinie beitragen, gleichzeitig kann sie aber auch negative Nebeneffekte auf den Datenschutz haben, sofern keine entsprechenden Maßnahmen ergriffen werden. So ist beispielsweise das Prinzip der Zweckbegrenzung schwieriger anzuwenden und zu kontrollieren. Wenn die Zahl der Akteure ansteigt, die die Daten verarbeiten, könnte darüber hinaus auch die Verwaltung der Zugriffsrechte aus datenschutzrechtlicher Sicht problematischer werden.

5.2 Technische und organisatorische Maßnahmen zur Information der Betroffenen über die Anwesenheit, Erkennbarkeit und Aktivierbarkeit von RFID-Geräten

Wie in Abschnitt 4 bereits erwähnt, müssen die Anwender der RFID-Technik die betroffenen Personen nicht nur über die Zweckbestimmungen der Datenverarbeitung informieren, sondern *auch* über die Anwesenheit von RFID-Geräten; dabei müssen sie folgende Anforderungen erfüllen:

Erstens müssen die Betroffenen über die Anwesenheit RFID-ähnlicher Geräte bzw. aktivierter RFID-Lesegeräte informiert werden. Zu diesem Zweck sind Piktogramme unerlässlich, wobei hier eine weltweite Norm erstrebenswert wäre, ferner weitere sachdienliche Informationsmittel, die diesen Zweck erfüllen. Die Bereitstellung dieser Information ist unverzichtbar, damit die unautorisierte und verdeckte Sammlung personenbezogener Daten mittels RFID-Technik verhindert werden kann. Gibt es beispielsweise in einem Geschäft oder in einer Klinik aktivierte Lesegeräte, sollten die betroffenen Personen darüber informiert werden.

Zweitens ist es aus den gleichen Gründen (Vermeidung verdeckter Datensammlung) wichtig, dass die betroffenen Personen *RFID-Tags in ihrer Umgebung* (beispielsweise in der Kleidung) erkennen können, da diese aufgrund ihrer Größe möglicherweise fast unsichtbar sind. Hier bieten sich vielfältige Möglichkeiten an, z. B. Standardhinweise oder auch technische Lösungen.

Drittens werden die Informationen über die bloße Anwesenheit von RFID in der Praxis nicht ausreichen; auch über die Aktivierbarkeit bzw. die *Echtzeitaktivierung* von RFIDs sollten die betroffenen Personen gemäß Datenschutzrichtlinie informiert werden. Dies bedeutet, dass einfache Verfahren zur Sichtbarmachung des Aktivierungszustands

[18] Die Reichweite des Lesegeräts und seine Leistung können darüber entscheiden, inwieweit eine bestimmte RFID-Anwendung in die Privatsphäre betroffener Personen eindringt.

bzw. der Aktivierbarkeit benötigt werden. Für die Betroffenen leicht zugänglich sein sollten auch Informationen über die Existenz und die Art datenschutzfreundlicher Techniken, wie die Möglichkeit der vorübergehenden Deaktivierung oder physischen Entfernung des Tags, ferner Informationen über organisatorische Maßnahmen in einer bestimmten Umgebung.

Die Datenschutzgruppe betont, dass weitere Forschungs- und Entwicklungsanstrengungen zur Erfüllung dieser drei Erfordernisse für alle Beteiligten unabdingbar sind.

5.3 Technische und organisatorische Maßnahmen zur Wahrnehmung des Rechts auf Auskunft, Berichtigung und Löschung

Wie im Folgenden beschrieben, kann der Aufbau der RFID-Technik einen großen Einfluss darauf haben, inwieweit die Wahrnehmung des Rechts auf Auskunft, Berichtigung und Löschung im Sinne des Artikels 12 Datenschutzrichtlinie tatsächlich gewährleistet ist.

(a) Auskunft über den Inhalt des RFID-Tags (Artikel 12 Buchstabe a Datenschutzrichtlinie)

Technisch bedingt ist der Zugriff auf den Inhalt eines RFID-Transponders nur mit einem Lesegerät, das mit dem Tag über ein Protokoll kommuniziert, und einem Anzeigegerät möglich. In vielen Anwendungen enthält der Tag Aber lediglich eine ID-Nummer, deren Bedeutung nur über eine komplette IT-Anwendungsumgebung ermittelt werden kann. Unserer Kenntnis nach enthalten nur wenige RFID-Tags aussagekräftige Informationen (Beschreibung des Artikels, Kennung des für die Verarbeitung Verantwortlichen, Zweck der Datenerhebung usw.), aber selbst dann ist es für die betroffenen Personen schwierig, Auskunft über den Inhalt zu erhalten.

Eine Möglichkeit, diesen Informationen Aussagekraft zu verleihen, besteht darin, semantische Normen zu definieren, z.B. mit XML. Gleichwohl werfen diese semantischen Beschreibungen unabhängig von ihrer Form noch das Problem des Zugriffs durch unberechtigte Dritte auf (vgl. Abschnitt 3).

(b) Berichtigung des Inhalts (Artikel 12 Buchstabe b Datenschutzrichtlinie)

Im Gegensatz zum bloßen Zugriff auf den Inhalt sind für die Berichtigung ein Lesegerät, das mit dem Transponder-Protokoll kommunizieren kann, und ein interaktives IT-System erforderlich; auf diese Weise hat die betroffene Person die Möglichkeit, sowohl das Auslesen des Inhalts als auch seine Berichtigung zu überwachen.

Vorgeschlagen wurde bereits, in den Transponder eine Vorrichtung einzubauen, die die Artikelseriennummer löscht oder verschlüsselt, so dass lediglich die

Objektklassenbeschreibung ganz oder teilweise lesbar ist; vorstellbar wäre auch die umgekehrte Möglichkeit, allerdings mit anderen Implikationen für die Privatsphäre.

(c) Löschen des Inhalts (Artikel 12 Buchstabe b Datenschutzrichtlinie)

Die Entscheidung, ob Vorrichtungen zur Deaktivierung der Tags eingeführt werden sollten oder nicht, mit denen die betroffenen Personen die Verarbeitung ihrer personenbezogenen Daten unterbinden können, wenn der Transponder in die Reichweite eines Lesegerätes kommt, hängt von der Rechtsgrundlage ab, auf der im jeweiligen Fall die Verarbeitung personenbezogener Daten beruht. Nicht sinnvoll wäre es beispielsweise bei RFID-Tags in Ausweisen, wohingegen es aus Datenschutzgründen bei RFID-Tags auf Konsumgütern durchaus erforderlich wäre. Diese Frage wurde auch auf der Konferenz der Datenschutzbeauftragten in Sydney erörtert und fand ihren Niederschlag in einer Erklärung zu RFID[19].

In den letzten Jahren wurden verschiedene Lösungen vorgeschlagen. Ein Vorschlag betraf die Einführung eines „Kill"-Befehls. Dies bedeutet, dass der Transponder dauerhaft oder vorübergehend über einen „Kill"-Befehl deaktiviert werden kann. Die permanente Deaktivierung kann mittels Durchbrennen einer Sicherung im Tag (fuse effect), Verschlüsselung des Speichers oder Entfernen des Transponders erfolgen. Die vorübergehende Deaktivierung kann mechanisch erfolgen oder mit Hilfe einer Softwaresperre. Allerdings geht bei diesem Ansatz der Vorteil eines Wiedereinsatzes der RFID-Geräte außerhalb des Geschäftes verloren. Daher wurden andere Varianten vorgeschlagen.

Eine besteht darin, die auf einem RFID-Tag gespeicherten Daten mit Nullen zu überschreiben. Der Transponder bleibt aktiv, sendet aber, wenn er „angefunkt" wird, nur Nullen anstatt einer Nummer. Mit diesem System wird der Transponder nicht wirklich deaktiviert. Er antwortet und sendet die Information, dass die betroffene Person einen „getaggten" Artikel bei sich trägt. Das kann mehrere Konsequenzen haben: Da erstens RFID-Tags, die lediglich Nullen übertragen, nicht sehr verbreitet sind, besteht die verwertbare Information in der reinen Existenz eines solchen Tags. Es zeigt, dass die betroffene Person in einem Geschäft eingekauft hat, das seine Artikel mit RFID-Tags versieht. Ein gut informiertes Unternehmen kann damit fundierte Vermutungen anstellen. Zweitens hat es den Anschein, als ob zunächst nur wertvolle Gegenstände mit RFID-Transpondern ausgestattet werden. Einige Jahre lang werden sich Diebe an der reinen Existenz eines RFID-Tags orientieren können (selbst wenn es lediglich Nullen oder unverständliche Daten überträgt), um wertvolle Gegenstände aus Garderoben oder Parkhäusern zu stehlen. Schließlich werden die Händler mit zunehmender Verbreitung der RFID-Tags, nicht unbedingt von Tags begeistert sein, die zwar antworten, dabei aber nur wertlose Daten übermitteln.

---

[19] Entschließung zur Radio-Frequency Identification, 25. Konferenz der Datenschutzbeauftragen, Sydney 2003, http://www.privacyconference2003.org : „...soweit RFID-Etiketten im Besitz von Personen sind, sollten diese die Möglichkeit zur Löschung der gespeicherten Daten oder zur Deaktivierung oder Zerstörung der Etiketten haben".

Eine andere Möglichkeit ist die physische Abschirmung des Transponders, die von der betroffenen Person bewusst eingesetzt werden kann. So können beispielsweise „getaggte“ Banknoten in abgeschirmten Geldbörsen nicht lokalisiert werden. Eine Alufolie in der Hülle eines RFID-Ausweises kann ausreichen, um den Inhalt zu schützen, es sei denn der Ausweis wird geöffnet. Eine Abschirmung eignet sich jedoch nicht für alle Anwendungen. So können beispielsweise Kleidungsstücke mit eingenähten RFID-Tags nicht in abschirmendes Material eingepackt werden, wenn sie getragen werden. Ferner dürfte ein solcher Ansatz einen unverhältnismäßigen Aufwand für die betroffenen Personen bedeuten, da sie letztlich allein dafür sorgen müssen, dass der Transponder keine Informationen preisgibt.

Wenn Normungsgremien, Hersteller und Anwender der RFID-Technik Verfahren zur Deaktivierung von Tags festlegen, sollten sie neben dem oben Gesagten auch berücksichtigen, dass betroffene Personen, die sich für das Entfernen des Transponders entscheiden, nicht bestraft werden sollten.

Auch in Bezug auf die oben angesprochene Problematik betont die Datenschutzgruppe, dass weitere Forschungs- und Entwicklungsanstrengungen zu diesen Problemen für alle Beteiligten unabdingbar sind.

5.4. Rechtsgrundlagen für die Verarbeitung

Deaktivierung der Transponder: Neben den in Abschnitt 5.3 genannten Gründen verlangen auch andere Bestimmungen der Datenschutzrichtlinie nach dieser Option. Wenn gemäß der Datenschutzrichtlinie die Einwilligung die einzige Rechtsgrundlage darstellt, die die Erhebung personenbezogener Daten mittels RFID-Technik rechtfertigt (vgl. Abschnitt 4.2), haben betroffene Personen natürlich immer die Möglichkeit, ihre Einwilligung zur Datenverarbeitung zu widerrufen (früher Artikel 7 Buchstabe a). Gibt es kein Gerät, mit dem eine betroffene Person den Transponder deaktivieren kann, wird sie, wenn sie die weitere Übermittlung ihrer Daten durch das Tag unterbinden will, an der Wahrnehmung ihres Rechts gehindert. Wenn auf RFID-Tags gespeicherte personenbezogene Daten auf einer anderen Rechtsgrundlage als der Einwilligung erhoben wurden, müssen diese Tags nicht unbedingt deaktivierbar sein. So wären beispielsweise für personenbezogene Daten auf Transpondern, die zur Überwachung des Zugangs zum Arbeitsplatz verwendet werden, keine Deaktivierungsvorrichtungen nötig, da die Datenverarbeitung aufgrund des Arbeitsverhältnisses gerechtfertigt ist.

Bei einigen RFID-Anwendungen, beispielsweise wenn die betroffene Person das Recht hat, ihre Einwilligung zu widerrufen oder Widerspruch gegen die Verarbeitung einzulegen (früher Artikel 14 Buchstabe a) und dementsprechend den Transponder zu deaktivieren, sollten Hersteller und Anwender der RFID-Technik sicherstellen, dass die Deaktivierung einfach durchzuführen ist. Mit anderen Worten: die betroffenen Personen sollte diese Aufgabe problemlos bewältigen können.

5.5 Datensicherheit

Verschlüsselung (Tags und Anwendungen): Enthalten RFID-Tags personenbezogene Daten müssen sie gemäß Artikel 17 Datenschutzrichtlinie über technische Maßnahmen verfügen, die eine unbefugte Offenlegung der Daten verhindern. Sonst könnte jeder, der über ein Lesegerät verfügt, einen Transponder aktivieren und die darin gespeicherten Informationen auslesen. Gemäß Datenschutzrichtlinie (früher Artikel 6 Absatz 1 Buchstabe d) sind solche Maßnahmen auch erforderlich, um die Integrität der auf dem Tag gespeicherten Daten zu gewährleisten und unautorisierte Veränderungen an den Daten zu verhindern.

Die Art der technischen Maßnahmen richtet sich nach der Art der Daten. Wie im Folgenden näher erläutert, dürfte es in den meisten Fällen genügen, dass die Daten *verschlüsselt* werden und das Lesegerät authentifiziert wird, um zu verhindern, dass Dritte mit Hilfe von Lesegeräten die Informationen auslesen. Das Beispiel der Patienten-Tags, auf denen die Identität des Patienten, des behandelnden Arztes und der vom Klinikpersonal durchzuführenden Behandlungsmethoden gespeichert sind, macht deutlich, dass die Klinik sicherstellen muss, dass diese Angaben nicht von Dritten ausgelesen werden. Daraus ergibt sich zwangsläufig die Notwendigkeit des Einsatzes technischer Maßnahmen wie der Verschlüsselung.

Die am weitesten verbreitete und sicherste Methode besteht in der Verwendung von Standard-Authentifizierungsprotokollen (z. B. ISO/IEC 9798). Sie finden bereits breite Verwendung in Netzwerken und bei Smartcards. In diesen Standardprotokollen werden kryptografische Grundelemente verwendet. Bei symmetrischen Authentifizierungsverfahren, bei denen die Schlüssel für Sender und Empfänger gleich sind, werden MACs (message authentication codes) oder symmetrische Verschlüsselungsalgorithmen wie DES oder AES verwendet. Bei den asymmetrischen Verfahren verfügt jede Partei über einen privaten (geheimen) und einen öffentlichen Schlüssel. Zum Einsatz kommen asymmetrische Verschlüsselungsalgorithmen, wie RSA oder ECC, oder Signaturen.

Einige kryptografische Authentifizierungsverfahren sind bereits in Wegfahrsperren oder bei Zugangskontrollsystemen implementiert. Sie beruhen jedoch häufig auf proprietären Algorithmen, da diese häufig einfacher und kostengünstiger zu implementieren sind als Standardalgorithmen. Gleichwohl sollten in Fällen, in denen eine erhöhte Sicherheit erforderlich ist, wie beim Schutz sensibler Daten, Standardalgorithmen und -protokolle verwendet werden. Der Vorteil dieser Protokolle und Algorithmen besteht darin, dass sie weitverbreitet sind und von vielen Akteuren bereits getestet und erprobt wurden. Sie stoßen also in puncto Sicherheit auf breite Akzeptanz.

Einige Veröffentlichungen verweisen bereits auf symmetrische Algorithmen, wie AES, als geeignete Verschlüsselung für RFID-Etiketten[20]. Das Problem bei der

[20] Feldhofer M., Dominikus S., Wolkerstorfer J., "Strong Authentication for RFID Systems using the AES Algorithm", In the Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004, 11.-13. August 2004, Boston, USA), Lecture Notes in Computer Science (LNCS) Vol. 3156, Springer Verlag, 2004, ISBN 3-540-22666-4, S. 357ff.
http://www.iaik.tugraz.ac.at/research/publications/2004/CHES2004_AES.htm

Verwendung symmetrischer Authentifizierungsalgorithmen besteht darin, dass die Erzeugung und die Verwaltung des Schlüssels kompliziert sind. Asymmetrische Verfahren kennen dieses Problem nicht, sind aber teurer.

6. Fazit

Angesichts des zunehmenden Einsatzes von RFID für eine Vielzahl von Zwecken und Anwendungen von teilweise enormer Datenschutzrelevanz wählte die Datenschutzgruppe bewusst diesen Zeitpunkt, um mit diesem Arbeitspapier in die laufende Diskussion über die RFID-Problematik einzugreifen. Sie hofft, dass das Papier einen nützlichen Beitrag zu der Debatte um RFID leistet und fordert alle Interessenträger auf, sich den hier genannten Grundsätzen anzuschließen.

Das Arbeitspapier beruht auf den verfügbaren Informationen und berücksichtigt den aktuellen Stand der Technik, insbesondere die derzeitigen Einsatzgebiete in den verschiedensten Bereichen. Die Datenschutzgruppe ist sich jedoch darüber im Klaren, dass der Einsatz von RFID kontinuierlich weiterentwickelt wird: Es gibt immer wieder neue Entwicklungen und mit zunehmender Erfahrung nimmt auch das Wissen um die problematischen Aspekte zu. Aus diesem Grund wird die Datenschutzgruppe zusammen mit interessierten Gruppen die technischen Entwicklungen in diesem Bereich weiter beobachten. Einige der in dem Arbeitspapier angesprochenen Fragen müssen vielleicht im Lichte der Erfahrungen noch einmal diskutiert werden. Im Übrigen schließt die Datenschutzgruppe nicht aus, dass sie sich im Zuge der Entwicklung der RFID-Technik und ihrer Anwendungen zu einem späteren Zeitpunkt ausführlich mit spezifischen Bereichen oder Anwendungen beschäftigen und ergänzende Leitlinien zu bestimmten Anwendungen veröffentlichen wird.

ANHANG

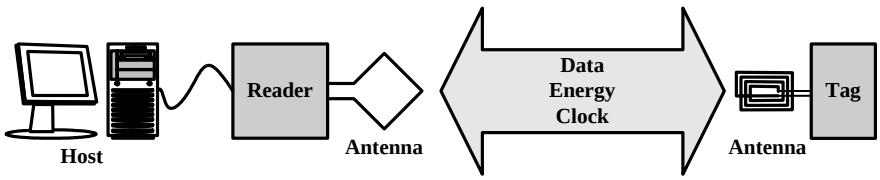
DIE RFID-TECHNIK

Die drahtlose Kommunikation schreitet immer weiter voran und ist bereits jetzt in einer Vielzahl von Anwendungen zu finden. Dazu gehören der Aufbau drahtloser lokaler Netze (WLAN) oder drahtlose Verbindungen niedriger Bandbreite zwischen einzelnen Geräten wie Laptops, PDAs, Handys usw. (Bluetooth).

In den vergangenen Jahren hat eine neue Technik immer mehr an Boden gewonnen: RFID - Radio Frequency Identification, übersetzt etwa: Funk-Erkennung. Dahinter steht vor allem die Idee, jedem Objekt, das mit einem RFID-Tag ausgestattet ist, eine eindeutige Kennung zu geben, die über Funkwellen an ein Lesegerät übermittelt werden kann. Damit ergeben sich vielfältige Anwendungsmöglichkeiten in der Lieferkette und in anderen gewerblichen Bereichen. Zunächst waren die RFID-Etiketten als Ersatz für Barcodes gedacht. Die Vorteile liegen auf der Hand: Da sie ohne Sichtkontakt funktionieren, ist eine automatische Erfassung möglich. Mit fortschreitender Entwicklung sind inzwischen noch andere, differenziertere Anwendungen denkbar. Vor der Diskussion möglicher Anwendungen soll ein Überblick über die Technik gegeben werden:

Das einfachste RFID-System besteht aus zwei Komponenten: einem Transponder (auch *Tag* oder *Etikett*), der an einem Objekt befestigt ist, und einem Lesegerät, das die Daten aus dem Transponder auslesen kann. Die beiden Komponenten kommunizieren miteinander über eine Funkverbindung. Transponder und Lesegerät besitzen eine Antenne und einen Demodulator (analoges Frontend). Dieses Frontend „übersetzt“ die per Funk ankommenden analogen Informationen in digitale Daten, die vom digitalen Teil des Lesegerätes oder des Transponders weiterverarbeitet werden können.

Im Transponder erfolgt die digitale Verarbeitung entweder mittels gezielt entwickelter Hardware oder mittels eines Mikroprozessors. Zur Verarbeitung der aus den Tags ausgelesenen Daten kann ein an das Lesegerät angeschlossener Server verwendet werden. Dieser Server muss unter Verwendung der Tag-Daten besondere Anwendungen ausführen können. Das Schaubild zeigt ein gängiges RFID-System:



Aufbau eines RFID-Systems

Ein RFID-System kann durch verschiedene technische Parameter beschrieben werden. Diese Parameter bestimmen die unterschiedlichen Anwendungsmöglichkeiten von RFID-Systemen.

Aktive/passive RFID-Tags. Einfache passive Tags beziehen ihre Energie und das Taktsignal zur Verarbeitung und Übermittlung der Daten über das elektromagnetische Feld des Lesegerätes. Die Stärke dieses Feldes ist durch nationale und internationale Vorschriften

begrenzt. Daher muss der Energieverbrauch des Tags begrenzt werden, um ein einwandfreies Funktionieren zu gewährleisten. Die Feldstärke nimmt mit der Entfernung zum Lesegerät ab. Kommt der Tag mit weniger Energie aus, hat das Lesegerät folglich eine größere Reichweite, sprich: Lesegerät und Tag können über eine größere Entfernung miteinander kommunizieren. Aktive Tags übermitteln Daten, auch wenn kein Lesegerät vorhanden oder in Reichweite ist. Aus diesem Grund besitzen sie eine Batterie. Der Vollständigkeit halber sollte erwähnt sein, dass einige Tags Prüf- oder Messschaltungen enthalten können, die bestimmte Werte aufnehmen; das kann beispielsweise ein Thermometer sein, das die Unterbrechung der Kühlkette feststellen soll; in diesen Fällen ist ebenfalls eine Batterie erforderlich, die allerdings unabhängig von der Art des Tags (aktiv oder passiv) ist.

Betriebsfrequenz: RFID-Systeme können mit unterschiedlichen Frequenzen, Reichweiten und Kopplungsarten arbeiten. Diese Parameter hängen stark voneinander ab. Die Frequenzen reichen von 135 kHz bis 5,8 GHz. Hier sind internationale Beschränkungen sowie physikalische Erfordernisse zu berücksichtigen. Die Kopplungsverfahren können elektrisch, magnetisch oder elektromagnetisch sein. Die Kopplung beeinflusst die Reichweite, die sich zwischen wenigen Millimetern bis zu 15 Metern und mehr bewegen kann. Insbesondere können unterschieden werden:

- ✓ So genannte „Close-Coupling-Systeme“ mit einer kurzen Reichweite von maximal einem Zentimeter. Ihre Arbeitsfrequenz reicht vom Niederfrequenzbereich bis 30 MHz. Tags dieser Art müssen in oder auf das Lesegerät gelegt werden, damit sie kommunizieren können. Diese Systeme können mit hohem Energieverbrauch und hoher Datenübertragungsrate arbeiten.

- ✓ „Remote-Coupling-Systeme“ mit einer Reichweite von bis zu einem Meter. Die meisten RFID-Systeme arbeiten mit Remote-Coupling auf Frequenzen zwischen 135 kHz und 13,56 MHz.

- ✓ „Long-Range-Systeme“ mit einer Reichweite von mehr als einem Meter. Sie arbeiten auf Frequenzen zwischen 868 MHz und 5,8 GHz.

RFID-Systeme können andere Funkeinrichtungen stören. Daher müssen sie auf anderen Frequenzen arbeiten als Hörfunk, Fernsehen oder mobile Funkstationen. Vorwiegend arbeiten RFID-Systeme auf Frequenzen zwischen 0 und 135 kHz, ferner auf den ISM-Frequenzen (Industrial, Scientific, Medical) von 6,78 MHz, 13,56 MHz, 27,125 MHz, 40,68 MHz, 869,0 MHz, 2,45 GHz, 5,8 GHz und 24,125 GHz.

- *Lese-/Schreibfunktion*: Die Komplexität von RFID-Systemen variiert und ist häufig begrenzt durch die Leistungsfähigkeit des Tags.

- ✓ So genannte „Low-end-Systeme“ haben lediglich lesbare Tags. Das Lesegerät kann nur den Inhalt des Tags auslesen, der normalerweise aus einer Seriennummer mit wenigen Bytes besteht. Diese Tags werden häufig eingesetzt, weil sie kostengünstig sind und nur einen kleinen Chip benötigen. Sie können Barcode-Systeme ersetzen, wo immer Objekte lokalisiert werden müssen, üblicherweise bei der Lagerlogistik oder beim Produkt-Routing in einem Produktionsprozess. Auch die Lokalisierung von Tieren ist mit solchen Tags möglich.

- ✓ RFID-Systeme mittlerer Leistungsfähigkeit können Tags mit wieder beschreibbarem Speicher haben. Die Speicherkapazität schwankt derzeit zwischen wenigen Bytes und einigen zehn oder hundert Kilobyte EEPROM[21] für passive und SRAM[22] für aktive Transponder. In diesem Leistungsspektrum können auch (Temperatur-, Druck- usw.) Sensoren in die Transponder integriert werden, die dann Umweltunfälle erfassen, die der Transponder aufzeichnet. Darüber hinaus können solche Tags für Zugangskontrollen eingesetzt werden. Ein weiteres, bereits erprobtes Einsatzgebiet ist das Gepäck-Routing auf Flughäfen. Der Bestimmungsort des Gepäckstückes wird auf dem Tag gespeichert und das Gepäckstück wird automatisch weitergeleitet. Auch im Gesundheitswesen ist der Einsatz von Transpondern vorstellbar. Im Klinikbetrieb können Einzelheiten der Behandlung oder bestimmte Werte über den Gesundheitszustand des Patienten auf dem Tag gespeichert werden.

- ✓ Berührungslose Smartcards mit einem Mikroprozessor und einem Betriebssystem bilden so genannte High-End-Systeme. Sie verfügen über eine gewisse Speicherkapazität, die im Allgemeinen höher ist als bei RFID-Transpondern des mittleren Leistungsspektrums. Auf der Karte können komplexe Funktionen implementiert werden. Im Transponder können Programme gespeichert und dann vom Mikroprozessor ausgeführt werden. Aufgrund des hohen Energieverbrauchs dieser Karten ist die Reichweite solcher Systeme derzeit noch auf wenige Zentimeter begrenzt. Mit diesen Karten können komplexere Anwendungen realisiert werden. Eine typische Smartcard-Anwendung ist beispielsweise die Zugangskontrolle. Ferner können Sie als Ausweis oder als Krankenversicherungskarte verwendet werden. Diskutiert wird auch der Einsatz solcher High-End-RFID-Systeme in Reisepässen mit IC-Chip[23], wie von der Internationalen Zivilluftfahrtorganisation (ICAO) definiert, oder als Visa und Aufenthaltsgenehmigungen mit IC-Chip.

Brüssel, 19. Januar 2005
Für die Datenschutzgruppe
Der Vorsitzende
Peter SCHAAR

[21] Electrically Erasable Programmable Read Only Memory (digitaler Festwertspeicher, in dem Daten gelöscht und neu geschrieben werden können).
[22] Static Random Access Memory (statischer Speicher mit wahlfreiem Zugriff).
[23] Integrated Circuit Chip