Kommentare des FoeBuD e.V. zum WP 105 „Datenschutzfragen im Zusammenhang mit der RFID-Technik"

Von padeluun und Jan E. Hennig

Der FoeBuD e.V. in Bielefeld hat sich zur Aufgabe gemacht, die Menschheit auf Ihrem Weg in eine Kommunikationsgesellschaft zu begleiten. Das KnowHow des FoeBuD soll dazu dienen, dass Technik sinnvoll und ungefährlich für das Zusammenleben der Menschen eingesetzt wird. Da der FoeBuD hat kein Partikularinteresse am Thema. Durch kritisches Hinterfragen der Technik und das Herantragen des Themas an die Öffentlichkeit ist der FoeBuD weltweit bekannt geworden. Wir möchten der Arbeitsgruppe unsere Überlegungen zum Arbeitspapier WP105 vorlegen. Wir beziehen uns in der Regel auf die deutsche Übersetzung des Papiers.

Der FoeBuD besteht nicht aus Juristen und ist kein Datenschutzverein. Deswegen werden etliche Kommentare sich nicht ausschließlich auf Datenschutz beziehen, sondern auch sonstige Aspekte beleuchten. Dies ist unter anderem wichtig, weil sich einige der Auswirkungen (auch für den Bereich Datenschutz) fast nur aus interdisziplinären Kenntnissen herleiten lassen. RFID tangiert auch die Interessen vonMenschenrechtlern, engagierten Bürgerinnen und Bürgern, Umweltschützern und ArbeitnehmervertreterInnen.

Wir sehen es als unerläßlich an, dass gesetzliche Anpassungen bezüglich RFID vorgenommen werden. Dies ist auch für die beteiligten seriösen Firmen von Vorteil, weil dies Schutz vor der (vielleicht gewissenlosen) Konkurrenz und den eigenen Aktionären bietet, die das Management zwingen könnten, so „effizient“ wie möglich gegen Grundsätze des ethischen Umgang mit Daten zu verstoßen.

1.0 Übersicht über das WP105

Wir versuchen durch Abbilden der Struktur des WP105 die Navigation innerhalb des WP105-Dokuments zu ermöglichen. Ein genaues Strukturieren unserer Kommentare und ein formellerer Stil ist uns aus zeitlichen Gründen nicht möglich. Wir bitten uns dies nachzusehen.

1.1 Kapitel 1: Einführung

1.1.1 „Die Vorteile der RFID-Technik liegen auf der Hand“

An dieser Stelle möchten wir gleich darauf hinweisen, dass diese Vorteile nicht „auf der Hand“ liegen. Viele sogenannte Vorteile sind bei genauerem Hinschauen „Marketing-Blabla“ oder gar, von einer anderen Seite aus betrachtet, in Wirklichkeit massive Nachteile.

Aus Sicht des Datenschutzes birgt RFID-Technik vor allem Nachteile. Vorteile sind eher mit der Lupe zu suchen und mit der Pinzette herauszuklauben.

1.2 Kapitel 2 Funk-Erkennung (RFID): Einführung in die Technik und ihre Verwendung

1.2.1 Grundlagen der RFID-Technik

Wenn die RFID-Technik beschrieben wird, darf dieser nicht nur als Verbindung eines elektronischer Schaltkreis zur Datenspeicherung und eines Lesegerät beschrieben werden. Sondern es muss bereits an dieser Stelle herausgestellt werden, dass Drittens bereits beim Herstellungsprozeß eine Informationseinheit aufgebracht wird: Die eindeutige Nummer des Transponders.
Ein Tag an sich ist – auch ohne, dass weitere Daten aufgespielt werden –
potentiell gefährlich.

1.2.2 UID unnötig?

Warum werden RFID-Chips nicht ohne UID (eindeutige Seriennummer) hergestellt? Wenn nur der EPC aufgespielt werden soll, braucht's die UID nicht.

Gesetzesanpassungen können unterschiedlich sein, je nachdem RFID-Anwendungen mit Chips, die eine UID beinhalten oder nicht, arbeiten.

Bei einer Deaktivierung (Speicher mit Nullen überschreiben) sind uns bisher nur Implementationen bekannt, die die UID unangetastet lassen, womit der Chip nicht deaktiviert ist!

1.2.3 Analogie zum Personalausweisgesetz

Wenn mit RFID ausgestattete Systeme eine Identifizierung eines Menschen erlauben (z.B. Bahncard), dürfen diese RFID-Systeme nicht für andere Identifizierungszwecke eingesetzt werden.

Hier müssen dann ähnliche Bestimmungen wie z.B. im deutschen Personalausweisgesetz niedergelegt sind, gelten.

1.2.4 „Bitte“ oder „Zwang“

Der Einzelhandel hat Hersteller „gebeten“, ihre Waren zu taggen. Diese Bitte ist eher ein Zwang, den Hersteller mehr zähneknirschend mitmachen, weil sie aus den Sortimenten nicht ausgelistet werden wollen.

1.2.5 Keine RFID im Verkaufsraum!

Wir denken, dass Kunden auch im Verkaufsraum nicht mit RFID in Berührung kommen sollen.

1.2.6 EPC-Code darf keine Seriennummer enthalten

Aus dem Standard EPC-Code soll die Seriennummer entfernt werden. Bei Gefahrgütern mag eine Seriennummer in Ordnung sein. Nicht aber schon in Medikamenten etc.

1.3 Kapitel 3: Eingriffe in den Datenschutz und die Persönlichkeitsrechte

1.3.1 personenbezogene Daten / personenbeziehbare Daten

Alles was für personenbezogene Daten gilt, gilt auch für (potentiell) personenbeziehbare Daten.

Zur Erklärung: Daten sind

personenbezogene Daten (linked), wenn Daten wie z.B. Name, Anschrift, Geburtsdatum, direkt auf dem Chip gespeichert sind

personenbeziehbare Daten (linkable), wenn auf dem Chip nur eine Nummer (z.B. die UID) gespeichert ist, die mit den personenbezogenen Daten in einer externen Datenbank verknüpft werden können

potentiell personenbeziehbare Daten (possibly linkable), wenn Daten zwar gesammelt, vorerst aber noch keiner Person zugeordnet werden können, sondern diese Zuordnung z.T. sehr viel später erfolgen kann (eine Person X ist unbekannt, jedoch ist bekannt, dass eine Person mit den RFID-Tags A, B und C bestimmte Produkte G, H, I gekauft oder angeschaut hat und bestimmte Wegstrecken K-L, O-P zurückgelegt hat. Diese Person bezahlt einmal etwas mit einer Kreditkarte und ist somit als Person X identifiziert. Alle Ereignisse (A,B,C, G, H, I und den Wegstrecken K-L und O-P) sind Person X zuzuordnen (siehe WP105, 4.1 „bestimmbare natürliche Person“).

An allen Stellen des WP105 sollte „personenbezogen“ in „(potentiell) personenbeziehbar“ geändert werden.

Nebenbei bemerkt genießt auch eine mir gegenüber anonyme Person, Schutz vor Datengebrauch- und mißbrauch.

1.3.2 Cryptalgorithmen und Authentifizierung des Lesegerätes

Siehe auch: 1.5.16 Keine Security by Obscurity

Monatskarten etc. müssen mit Cryptalgorithmen und Authentifizierung arbeiten. Das Lesegerät muß sich der Karte (mit dem Chip) gegenüber ausweisen. EC-Geldautomaten müssen sich der EC-Karte gegenüber z.B. nicht authentifizieren – was dazu führt, dass viele Karten und PIN-Nummern hier von Betrügern abgefischt werden. Die Kommunikation zwischen Lesegerät und Tag muß verschlüsselt ablaufen. (Hinweis: Die Kommunikation zwischen Tag und Lesegreät ist auf weite Strecken hin abhörbar!)

1.4 Kapitel 4: Anwendung des EU-Datenschutzrechtes auf die Datenerhebung mittels RFID-Technik

1.4.1 Grundsatz Datensparsamkeit / Datenvermeidung

Im WP105, 4.2 werden drei Grundsätze aufgelistet. Der zweite Punkt ist mit „Grundsatz der Datenqualität“ bezeichnet. Muss das nicht „Grundsatz der Datensparsamkeit/-Vermeidung“ heißen (Artikel 6 Absatz 1 Buchstabe c)?

Es sollte verpflichtend sein, keine Anwendungen zu installieren, die Daten sammeln, wenn ein ähnliches Ergebnis auch ohne das Ansammeln von Daten erreicht werden könnte.

1.4.2 Zweckbindung

Die Zweckbindung von erhobenen Daten muss klarer werden. Daten, die z.B. für die Rabattgewährung erhoben werden, dürfen nie für andere Zwecke verwendet werden. Abonnentendaten von TV-Zeitungen dürften nicht an die GEZ (Gebühreneinzugszentrale) weiter verkauft werden.

1.4.3 Erschleichung des Einverständnisses

Das Einverständnis in die Datensammlung darf nicht erschlichen werden (z.B. wurden und werden die Payback-Kundenkarten in Deutschland statt „Datensammel-“ immer noch „Kundenkarten“ genannt).

1.4.4 Informationserfordernisse

Siehe auch: 1.5.6 Daten-Kontoauszug, 1.5.10 Bekanntgabe des Datenflusses

Es muss auch mitgeteilt werden, von wem und wo die Daten verarbeitet werden. Lesbare Schriftgrößen und kontrastreiche Ausführung müssen vorgeschrieben sein.

1.4.5 Recht auf Änderung

Betroffene sollen nicht nur das Recht auf Berichtigung, sondern allgemeiner ein Recht auf Änderung der Informationen haben.

1.4.6 Sanktionsmöglichkeiten

Zuwiderhandlungen müssen spürbare Sanktionen nach sich ziehen.

1.4.7 Schnelligkeit der Datenerhebung

Wir haben es mit neuen Qualitäten in der Schnelligkeit der Datenerhebung zu tun. Die Datenschutzgesetzgebung und die Abwehrtechnik (Privacy Enhancement Technic PET) muss entsprechend angepaßt werden.

War vordem die Datenspeicherung oft auch zum Vorteil des Betroffenen (bequemere Lieferung einer Zeitung direkt nach Hause, also Abo), kann heute jede Kleinigkeit gespeichert werden (Wie lange stand der Kunde vor dem Regal?). Diese Speicherungen dienen ausschließlich den Interessen der Unternehmen. Dies muss in neuer Datenschutzgesetzgebung berücksichtigt werden.

1.4.8 Datenverarbeitung aufgrund von Arbeitsverhältnissen

Jeder Chip muß außerhalb des Arbeitsplatzes abschaltbar sein. Auch hier gilt: Keine Chips in der Arbeitskleidung.

1.5 Kapitel 5: Technische und organisatorische Erfordernisse, die eine angemessene Verwirklichung der Datenschutzgrundsätze gewährleisten

Die Kapitelüberschrift sollte geändert werden in: „Technische, organisatorische und gesetzliche Erfordernisse, die eine angemessene Verwirklichung der Datenschutzgrundsätze gewährleisten“

1.5.1 RFID abschaltbar

RFIDs (Schlüsselkarten, Autoschlüssel, Kundenkarten etc.) müssen so gestaltet sein, dass der Besitzer des RFID das Senden des Chips abschalten kann. Der Zustand, ob das Chip-System aktiv ist muß optisch (für blinde Menschen möglichst auch haptisch) erkennbar sein. Zum Beispiel kann eine Chipkarte ähnlich einem Reedrelais abgestellt werden. Der Zustand kann durch ähnliche Funktionen wie sie elektronisches Papier beinhalten angezeigt werden. Karten müssen in abgeschaltetem Zustand übergeben werden. Der Kunde muss die Karte selbst einschalten (so kann er von der Schaltfunktion Kenntnis erlangen).

1.5.2 RFID nötig?

Es sollte immer geprüft werden, ob eine Lösung mit Strichcode nicht einfacher, besser und weniger gefährlich ist.

1.5.3 Vorsicht RFID -Warnsymbol

Siehe auch: 1.5.10 Bekanntgabe des Datenflusses

Es muss ein eindeutiges Gefahrensymbol entwickelt werden, das auch als Gefahrensymbol zu erkennen ist. Beispiele finden sich hier. Begleitende / erklärende Texte dürfen nicht euphemistisch sein. Das Zeichen muss ausreichend groß sein. Ggf. muß es weitere Symbole oder Kennummern oder Klartext geben, der weitere Infos über jenen RFID-Tag oder jenes Lesegerät gibt (Frequenz, Norm, ggf. zusammengefaßt in Klassen, Betreiber des Geräts, Gerätenummer, Wo gibt’s weitere Informationen über Betreiber und Gerät im Internet?).

1.5.4 Datenschutz muss Default sein

Standard muss das Entfernen des RFID durch den Händler oder Hersteller sein. Nur auf ausdrücklichen Wunsch des Kunden darf der RFID-Chip aktiviert und am Objekt bleiben. Auf gar keinen Fall darf die Wahrung des Rechtes auf Privatsphäre einen größeren Aufwand, Geld, oder Kommunikation notwendig machen, als wenn der Datenschutz aufgegeben wird.

1.5.5 Zustimmungspflicht zum Speichern von Daten

Das Abspeichern von Daten muss zustimmungspflichtig sein.

1.5.6 Daten-Kontoauszug

Über jeden Datenspeicherungsvorgang (neu anlegen, verändern, löschen) muss ein Kontoauszug angefertigt und versendet werden. Dieser regelmäßige Kontoauszug kann abbestellt werden. Am Jahresende wird aber auf jeden Fall ein Jahreskontoauszug mit der kompletten Auflistung aller Vorgänge zugesandt.

1.5.7 Kein RFID-Zwang

Eine Leistung darf nicht davon abhängig gemacht werden, dass der Kunde einen RFID-Chip akzeptieren muss. Gewähr- und Garantieleistungen müssen weiterhin in vollem Umfang in Anspruch genommen werden können, wenn das fehlerhafte Produkt und der Kaufbeleg vorgelegt werden kann.

1.5.8 Verbot der Preisdiskriminierung

Das unbemerkte Ausspionieren von Kundinnen und Kunden und das Verwerten der Erkenntnisse ermöglicht, dass Preise auf Kundinnen und Kunden individuell angepaßt werden. Sprich: Alle Kundinnen und Kunden zahlen den höchstmöglichen Preis, von dem das dahinter liegende Computersystem meint, den sie zahlen werden.

Zitat aus der Laudatio der BigBrotherAwards 2003:

„Startup-Unternehmer Lars H. ist krank. Er bittet seine Nachbarin Nina S., für ihn einkaufen zu gehen. Als sie ihm den Kassenbon präsentiert, ist er verwundert, dass Nina S. für viele Produkte das doppelte bezahlt hat. Sie stellen fest, dass zum Beispiel Toilettenartikel für sie teurer sind als für ihn. Beim Vergleich mit Freunden stellen sie fest, dass alle Frauen mehr für Toilettenartikel bezahlen als Männer, dass Familien mehr für Videos bezahlen als Singles usw.“

1.5.9 Löschen von Daten

Es muss feste Vorgaben für das physische Löschen der gesammelten Daten geben. Dabei müssen auch Höchstspeichergrenzen definiert werden (z.B. drei Monate). Daten von RFID-Fahrscheinen müssen sofort nach erfolgter Fahrt und Zahlung gelöscht werden. Rabattierungen dürfen nicht vom Sammeln von Daten abhängig gemacht werden. Beispiel: Bei einer „Mobilitätskarte“ brauchen nicht alle Fahrten gesammelt werden, um nachträglich die günstigste Preisstufe und ggf. Erstattungen vorzunehmen. Es reicht ggf. der Gesamtbetrag aller Fahrten in einem bestimmten Zeitraum.

1.5.10 Bekanntgabe des Datenflusses

Es muss durch Aushang im Geschäftsraum und auf derWebsite des Unternehmens, eine genaueste Beschreibung des Datenverarbeitungsprozesses geben. Dabei sind alle beteiligten Firmen, physischer Standort der Rechenzentren, Beteiligungen, Datenleitungen etc. anzugeben.

1.5.11 Dezentrale Datenhaltung

Dezentraler Datenhaltung muss Vorrang eingeräumt werden. Zentrale Datensammlungen müssen vermieden werden.

1.5.12 Monopolisierungen vermeiden

Im B2B-Bereich werden RFID eingesetzt (z.B. in Pfandsystemen – Fässer, Gemüsekisten), um herauszufinden, welche Kunden der Zwischenhändler beliefert. Wenn diese Informationen an den Konzern gegangen sind, kann der Zwischenhandel ausgeschaltet werden. Informationen sind dadurch zentralisierter und können eine größere Gefahr für den Datenschutz bedeuten.

1.5.13 Genehmigungsverfahren

Vorstellbar sind Genehmigungsverfahren für RFID-Anwendungen.

1.5.14 Datenschutzkonforme Technik erstellen

Nicht nur Hersteller und Normungsgremien sind gehalten, Datenschutzfreundliche Technik bereit zu stellen. Auch Anwender und Anwendnungsentwickler haben einen großen Einfluß auf die eigentlich Implementation und die entsprechende Datenschutz„freundliche“ Umsetzung.

1.5.15 Auskunft am POS

Betroffene müssen Ausdrucke am Point of Sale über ihre (potentiell) personenbeziehbare Daten verlangen können. Mittels PIN-Nummer sollte der Betroffene die Daten freischalten können (die sonst die Kassiererin nicht aufrufen könnte). Auf Anforderung muss der PIN per Brief mitgeteilt werden z.B. wenn er vergessen worden ist). Wenn Kürzel, Symbole oder ähnliches abgespeichert sind, müssen diese im Klartext ausgegeben oder zumindest in einer Legende erklärt werden.

1.5.16 Keine Security by Obscurity

Siehe auch: 1.5.13 Genehmigungsverfahren

Verschlüsselungsverfahren und Datenstrukturen müssen offengelegt sein. Es dürfen kein undokumentierten Codes verwendet oder in auf dem Chip abgelegten Schlüsseln verborgen werden. „Schlüssel mit gerader Bitanzahl bezeichnet Männer ...“ etc. Dies wird ggf. Teil des Genehmigungsverfahrens.

1.5.17 Recht auf Entfernung von RFID-Tags

Händler müssen Tags, soweit sie im Laden am oder im Produkt sein sollten, entfernen. Nur auf ausdrücklichen Wunsch eines Kunden, darf das Tag am Produkt verbleiben.

1.5.18 Besitzverhältnisse

Das Eigentum an einem RFID-Tag geht auf den Besitzer über. Der Besitzer darf Chip und Inhalte Ändern, Zerstören, Verfälschen.

1.5.19 Unterschied zwischen EPC und UPC

Der Unterschied zwischen UPC und EPC sollte im Text des WP105 so dargestellt sein, dass der qualitative deutlich herausgestellt, statt heruntergespielt, wird: „Der Unterschied zwischen den beiden Systemen besteht darin, dass im EPC im Gegensatz zum UPC nun eine eindeutige Seriennummer enthalten ist.“

1.5.20 EPCIS / ONS

Zu den Datenbanken mit den Produkt-Tag-Informationen darf es keine Standardzugänge geben. Es muss verhindert werden, dass von einer Stelle aus, alle Datenbanken im Zugriff sind (Zentralisierungsvermeidung). Auch für Bedarfsträger darf dieser Zugang nur nach Überwindung von Schwellwerten (Richterbeschluss, verteilte Datenbanken) passierbar sein. Zugangscodes müssen mindestens vierteljährlich geändert werden. Berechtigung der Nachfrage muss nachgewiesen und dokumentiert werden.

1.5.21 Logdatei auf Chip

Jeder Schreibvorgang wird auf dem Chip in einer Datei vermerkt (mit Lokalisierungsdaten des Lesegerätes). Auf Wunsch des Betroffenen kann das abgeschaltet werden. Logdaten müssen jederzeit vom Betroffenen gelöscht werden können.

1.5.22 Detektionsservice

In jeder Stadt muss es eine Stelle geben, wo ich meine Sachen hinbringen und kostenlos auf RFID-Tags untersuchen lassen kann.

1.5.23 Keine Tags in Kleidung

Keine Tags in Kleidung, auch Arbeitskleidung, Uniformen, Schuhen.

1.5.24 Weitere Forschung- und Entwicklungsanstrengungen

Bei der Forschung müssen auch Menschen- und Bürgerrechtler, Umwelt- und Verbraucherschützer mit einbezogen werden. Dafür sind Finanzen bereit zu stellen.

1.6 Kapitel 6: Fazit

Kein Kommentar

1.7 Anhang

Alle notwendigen Kommentare bereits abgegeben