

Kommentare und Antworten des FoeBuD e.V. für die EU-Konsultation zu RFID im April 2008

Die EU-Kommission arbeitet an einem Empfehlungsentwurf zu RFID. Die fertige Empfehlung soll sich an Mitgliedstaaten und an alle Beteiligten richten, die an Entwicklung und Betrieb von RFID-Anwendungen in der EG involviert sind. Es gab bis zum 24.04.2008 die Möglichkeit den Entwurfstext mit Hilfe einer Online-Umfrage zu kommentieren. Hier ist unser Gesamtkommentar:

Material:

- FoeBuD-Aufruf zur Teilnahme: <http://www.foebud.org/rfid/eu-umfrage-zu-rfid-2008>
- Die Umfrage: <http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=RFIDRec>
- Deutsche Übersetzung des Empfehlungstextes:
http://ec.europa.eu/information_society/policy/rfid/doc/consde.pdf

Frage / Artikel 1 – Geltungsbereich

1. Diese Empfehlung liefert eine Anleitung für die Mitgliedstaaten und Beteiligte zu Entwicklung und Betrieb von RFID-Anwendungen in gesetzmäßiger, ethisch zulässiger und sozial und politisch verträglicher Weise, wobei die Privatsphäre respektiert und der Schutz von personenbezogenen Daten sowie angemessene Informationssicherheit sichergestellt werden.
2. Diese Empfehlung betrifft Maßnahmen, die in Bezug auf den Einsatz von RFID-Anwendungen ergriffen werden sollen, wodurch garantiert wird, dass die nationalen Rechtsvorschriften zur Umsetzung der Richtlinien 95/46/EG, 1999/5/EG und 2002/58/EG beim Einsatz derartiger Anwendungen respektiert werden. Diese Empfehlung berührt nicht die Verpflichtungen, welche aus den nationalen Rechtsvorschriften zur Umsetzung des Gemeinschaftsrechts resultieren.
3. Diese Richtlinie gilt nicht für Tätigkeiten, die nicht in den Anwendungsbereich des Vertrags zur Gründung der Europäischen Gemeinschaft fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall für Tätigkeiten betreffend die öffentliche Sicherheit, die

Landesverteidigung, die Sicherheit des Staates und die Tätigkeiten des Staates im strafrechtlichen Bereich.

Die Antworten / Kommentare des FoeBuD zum Artikel 1

- Die Empfehlung darf nicht nur das Wie behandeln, sondern vor allem auch das Ob RFID überhaupt eingeführt werden darf.
- RFID darf nicht eingeführt werden, wenn die Gefahren für die Gesellschaft nicht ausgeräumt werden können: Es darf kein noch so kleines Restrisiko bleiben.
- In der bisherigen Diskussion rund um die erste EU-Konsultation zu RFID wurden Probleme und Risiken im Bereich RFID vor allem auf einzelne Personen bezogen. Daneben jedoch existieren Risiken auch auf einer gesellschaftlichen Ebene.
- Zu nennen ist hierbei vor allem die sich abzeichnende Machtkonzentration durch Information. RFID ist eine Informationssammeltechnologie. Information zu besitzen bedeutet in zunehmendem Maße Macht zu haben. Ein gesellschaftlicher Diskurs ist überfällig, ob derartige Macht überhaupt für die Gesellschaft wünschenswert ist oder nicht und ob derartige Macht zur Wahrung von Gleichgewicht und Rechten nicht vielleicht begrenzt werden muß und wenn ja an welcher Stelle und wie weit.
- Punkt 3 enthält eine doppelte Verneinung.
- Punkt 3: Dieser Bereich muß ebenfalls von der Empfehlung erfaßt werden, denn gerade der Bereich der sogenannten Sicherheit wird gerne als Hintertür zur Einführung unliebsamer Techniken mißbraucht.

Frage / Artikel 2 – Definitionen

Für die Empfehlung gelten die Definitionen, die in der Richtlinie 95/46/EG dargelegt werden. Weiterhin gelten die folgenden Definitionen:

- (a) 'Funkidentifizierung' (RFID) bedeutet die Verwendung elektromagnetischer Funkwellen oder Nahfeldkopplung im Funkfrequenzbereich des Spektrums, die eine Kommunikation von oder zu einem Funkchip durch eine Vielfalt von Modulations- und Kodierungsschemata aufbauen, um eindeutig die Identität eines Funkchips zu bestimmen oder darauf gespeicherte Daten auslesen zu können.
- (b) 'RFID-Transponder' oder 'Funkchip' bedeutet entweder ein RFID-Gerät, welches die

Fähigkeit besitzt, ein entsprechendes Funksignal zu produzieren oder ein RFID-Gerät, welches ein Trägersignal, das von einem Lesegerät empfangen wird, moduliert zurückkoppelt, zurückstreut oder reflektiert (in Abhängigkeit der Art des Gerätes).

- (c) 'Lesegerät' bedeutet ein stationäres oder mobiles Datenerfassungs- und Identifizierungsgerät, das in der Lage ist, auf Basis elektromagnetischer Funkwellen oder einer Nahfeldkopplung die Aussendung eines modulierten Signals von einem Funkchip oder einer Gruppe von Funkchips zu induzieren.
- (d) 'RFID-Anwendung' bedeutet ein System zur Datenverarbeitung durch den Einsatz von Funkchips und/oder Lesegeräten, eines Hintergrundsystem und/oder einer vernetzten Kommunikationsinfrastruktur.
- (e) 'Betreiber der RFID-Anwendung' bedeutet eine natürliche oder juristische Person, die eine RFID-Anwendung entwickelt, einführt, benutzt oder wartet.
- (f) 'Informationssicherheit' bedeutet die Bewahrung von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen.
- (g) 'Überwachung' bedeutet jegliche Aktivität, die dem Zwecke der Feststellung, Beobachtung, Duplizierung oder Aufzeichnung von Standort, Bewegung, Aktivität, Bild, Text, Stimme, Geräusch oder Zustand einer Person dient.
- (h) 'Deaktivierung' eines Funkchips bedeutet einen Vorgang, welcher die Beendigung jeglicher Funktionalität bewirkt. Die Deaktivierung kann dauerhaft sein, wobei der Funkchip auf keinen weiteren Befehl hin mehr reagiert, oder temporär, wobei der Funkchip nur auf spezifische Befehle zum Zweck der teilweisen oder vollständigen Reaktivierung reagiert.
- (i) 'Öffentlicher Bereich' bedeutet jeder Ort einschließlich nichtstationärer Mittel für den öffentlichen Transport wie zum Beispiel Busse, Flugzeuge, Eisenbahnen oder Schiffe, der jederzeit oder zu bestimmten Zeiten für jedermann zugänglich ist.

Die Antworten / Kommentare des FoeBuD zum Artikel 2

- Zur Definition 'Überwachung' muß mit bedacht und aufgenommen werden, daß auch Aktivitäten, die nicht zum Zwecke der in (g) genannten Tätigkeiten durchgeführt werden, z.B. durch Datenaufzeichnung später dennoch zu ebenjenen Tätigkeiten herangezogen werden können (Zeitlicher Versatz der Begründung).

- Die Definition muss unterscheiden, ob ein RFID-Chip dauerhaft irreversible deaktiviert ("kill") ist, oder wieder eingeschaltet werden kann ("deactivate").
- "Öffentlicher Raum", "Öffentlicher Platz" im Text ist stets im Sinne der Definition von "Öffentlicher Bereich" zu verstehen.

Frage / Artikel 3 – Vertraulichkeits- und Datenschutzmaßnahmen

1. Bevor eine RFID-Anwendung implementiert wird, sollten die Betreiber der RFID-Anwendung allein oder zusammen innerhalb einer gemeinsamen Wertschöpfungskette eine Datenschutz-Folgeabschätzung (PIA) durchführen, um zu ermitteln, welche Auswirkungen der RFID-Einsatz für die Privatsphäre und den Schutz personenbezogener Daten bewirkt, und ob die Anwendung verwendet werden könnte, um eine Person zu überwachen.
2. Der Grad der Detailgenauigkeit der Datenschutz-Folgeabschätzung sollte in angemessenem Verhältnis zu den Risiken stehen, die mit einer speziellen RFID-Anwendung verbunden sind. Die Abschätzung sollte im Einklang mit guten Praktiken stehen, welche in transparenter Weise partnerschaftlich mit allen relevanten Beteiligten und in Beratung mit den zuständigen Datenschutzaufsichtsbehörden festgelegt werden.
3. Soweit nicht ausgeschlossen werden kann, dass Daten, die durch RFID-Anwendungen verarbeitet werden, von einem Betreiber der RFID-Anwendung oder Dritten auf eine identifizierbare natürliche Person bezogen werden können, sollten die Mitgliedstaaten garantieren, dass die Betreiber derartiger RFID-Anwendungen und die Anbieter von Teilkomponenten dieser Anwendungen angemessene technische und organisatorische Maßnahmen ergreifen, um die damit verbundenen Risiken für die Privatsphäre und den Datenschutz zu verringern.
4. Betreiber von RFID-Anwendungen sollten eine verantwortliche Person benennen, welche für die Durchführung, die Überprüfung und Folgemaßnahmen wie oben stehend beschrieben zuständig ist.
5. Der Betreiber der RFID-Anwendung sollte die Datenschutz-Folgeabschätzung an das globale Risikomanagement der Informationssicherheit gemäß Artikel 6 dieser Empfehlung anlehnen

Die Antworten / Kommentare des FoeBuD zum Artikel 3

- "sollten" und "sollte" müssen gegen "müssen" und "muß" ersetzt werden.
- Absatz 1: Eine derartige Abschätzung gehört zur Pflicht.
- Absatz 1, letzter Halbsatz muß ergänzt werden: " um eine oder mehrere Personen mittelbar oder unmittelbar zu überwachen."
- Absatz 2: Bereits die partnerschaftlich genannte Zusammenarbeit an einem runden Tisch beim BMWI in Deutschland hat gezeigt, daß offenbar nur wenig Interesse an einer transparenten Zusammenarbeit mit relevanten Beteiligten gegeben ist. So wie Selbstverpflichtungserklärungen der Industrie schon früher nur begrenzte Haltbarkeit hatten sehe ich im Entwurf nicht, wie dieser gut gemeinte Punkt tatsächlich durchgesetzt werden könnte - obschon er es muß.
- Absatz 3: Ein Verringern der Risiken ist ein guter Vorsatz, allein es fehlt an einer Bemessungsgrundlage die geeignet ist darüber auszusagen, ob die Risiken weit genug verringert werden können. Diese zu schaffen und auch gesellschaftlich relevant abzusichern wäre eine Aufgabe, die u.a. die EU wahrnehmen könnte. Risiken dürfen also nicht nur minimiert, sondern sie müssen ausgeschlossen werden.
- Es muß sichergestellt sein, daß auch in Kombination mit weiteren Merkmalen keine personenbezieharen Daten entstehen.
- Absatz 5 muß ergänzt werden: "... gemäß Artikel 6 dieser Empfehlung anlehnen oder darüber hinausgehen.
- Es fehlt ein Absatz: Folgeabschätzung und begleitende Dokumente müssen vor Einsatz der Anwendung mit genügender Frist zur öffentlichen Begutachtung frei verfügbar gemacht werden. Es muß Gelegenheit geben, Probleme und Unzulänglichkeiten auch nach Anwendungsbeginn zu korrigieren.

Frage / Artikel 4 – Verhaltensregeln

1. Die Mitgliedstaaten sollten Handels- oder Berufsverbände oder Organisationen, die in die RFID-Wertschöpfungskette involviert sind, anregen, ausführliche Anleitungen über den praktischen Einsatz der RFID- Technologie zu geben, indem spezifische Verhaltensregeln zum RFID- Einsatz ausgearbeitet werden. Gegebenenfalls sollte

dies gemeinsam mit den betroffenen zivilgesellschaftlichen Organisationen, z. B. Verbraucherschutzverbänden oder Gewerkschaften, unternommen werden. Verhaltensregeln sollten spezifische Maßnahmen enthalten, die garantieren, dass die Unterzeichnenden sich an ihre Grundsätze halten. Sie sollten im Hinblick darauf die betroffenen Personen zu informieren weit verbreitet werden.

2. In Bezug auf Datenschutzaspekte sollten die Mitgliedstaaten die Ausarbeitung von Verhaltensregeln anregen, die zu einer richtigen Durchführung der nationalen Bestimmungen gemäß der Richtlinie 95/46/EG beitragen sollen, die spezifische Merkmale der verschiedenen Sektoren berücksichtigen.
3. In Übereinstimmung mit der Richtlinie 95/46/EG sollten nationale Verhaltensregeln den relevanten nationalen Datenschutzbehörden zur Stellungnahme unterbreitet werden; darüber hinaus sollten gemeinschaftliche Verhaltensregeln der Arbeitsgruppe „Artikel 29“ zur Stellungnahme auf Gemeinschaftsebene unterbreitet werden.

Die Antworten / Kommentare des FoeBuD zum Artikel 4

- Auch hier: "Sollen" gegen "müssen" ersetzen.
- Absatz 1: Es sind relevante Strafmaßnahmen für Verfehlungen gegenüber den erstellten Verhaltensregeln vorzusehen.
- Absatz 2: statt "anregen" muss hier "vorgaben" stehen. Das zweite "sollten" muß wegfallen.
- Absatz 3: Datenschutzbehörden und -gruppen müssen personell wie finanziell ausreichend für ihre Aufgaben ausgestattet werden und unabhängig sein. Ihnen muß die Möglichkeit gegeben werden, Anwendern bei Fehlverhalten geeignete spürbare Strafen aufzuerlegen.

Frage / Artikel 5 – Informationen zum Gebrauch von RFID

1. Wo RFID-Anwendungen in öffentlichen Plätzen implementiert werden, sollten Betreiber von RFID-Anwendungen öffentlich schriftliche und verständliche Leitlinien zur Verfügung stellen, die die Nutzung ihrer RFID- Anwendung regelt. Unbeschadet der Verpflichtungen von für die Verarbeitung personenbezogener Daten

Verantwortlicher gemäß den Richtlinien 95/46/EG und 2002/58/EG sollte die Leitlinie festlegen:

- (a) die Identität und Adresse des Betreibers der RFID-Anwendung
- (b) den Zweck der RFID-Anwendung,
- (c) welche Daten durch die RFID-Anwendung verarbeitet werden, insbesondere ob die Position von Funkchips überwacht wird,
- (d) welche Verbindung, wenn überhaupt, zu personenbezogenen Daten hergestellt wird,
- (e) welche Leitlinie zur Datenspeicherung vom Betreiber verfolgt wird,
- (f) ob Dritte auf die Daten zugreifen oder diese erhalten können.

Die Leitlinie sollte prägnant und allgemein verständlich sein.

2. Wo RFID-Anwendungen in öffentlichen Plätzen implementiert werden, sollten die Betreiber von RFID-Anwendungen mindestens durch ein eindeutiges, für alle zugängliches Zeichen über die Anwesenheit von RFID-Lesegeräten informieren. Die Hinweise sollten, wo angemessen, beinhalten, dass Funkchips und Lesegeräte Informationen ohne aktives Zutun einzelner Personen übertragen können und einen Verweis auf die Leitlinie enthalten, welche den RFID-Einsatz regelt, sowie einen Ansprechpartner/Kontaktperson ausweisen, durch den Einzelne zusätzliche Informationen erhalten können.

Die Antworten / Kommentare des FoeBuD zum Artikel 5

- Auch hier müssen "sollten" und "soll" gegen "müssen" und "muß"; "personenbezogene" gegen "personenbeziehbare" ersetzt werden.
- Absatz 1: Vor der Erfassung und Speicherung von Daten muß schriftlich die explizite Erlaubnis eingeholt werden.
- Es muß auf die Besonderheiten durch nicht Sichtverbindung benötigende Datenerfassung hingewiesen werden.
- Es muß auf alternative Möglichkeiten sowie auf Schutzmaßnahmen hingewiesen werden.
- Die Leitlinie muß neutral (nicht beschönigend) und in gut wahrnehmbarer Art

verfaßt und dargestellt sein.

- zu Punkt (a): Die E-Mail-Anschrift muß mit angegeben werden.
- Ergänzung zu (c): Welche Verbindung zu personenbeziehbaren Daten durch Kombination mit anderweitig gesammelten Daten hergestellt werden kann
- zu Punkt (f): Es muß ebenfalls alle Identitäten, Adressen und E-Mail von Weiterverarbeitern und Dienstleistern angegeben werden.
- neuer Punkt (g): wie lange die Daten gespeichert werden.
- Absatz 2: Nicht nur der Datenaustausch ohne Zutun einzelner Personen, auch auf die nicht sichtbare Art muß hingewiesen werden.
- Die Worte "wo angemessen" sind ersatzlos zu streichen.
- Das eindeutige Zeichen darf nicht beschönigend sein, sondern muß dem Standard eines Gefahrenwarnzeichens entsprechen.
- Das in 1 a bis g Gesagte gilt auch hier.

Frage / Artikel 6 – Risikomanagement der Informationssicherheit

1. Die Mitgliedstaaten sollten Betreiber von RFID-Anwendungen anregen, ein Informationssicherheitsmanagement nach dem Stand der Technik einzurichten, das auf einem wirksamen Risikomanagement beruht, um angemessene technische und organisatorische Maßnahmen bezogen auf die bewerteten Risiken sicherzustellen. Die Sicherheitsbedrohungen und die entsprechenden Sicherheitsmaßnahmen sollten in dem Sinne verstanden werden, dass sie alle Komponenten und Schnittstellen der RFID-Anwendung abdecken.
2. Die Mitgliedstaaten sollten eine Anleitung für die Bestimmung jener RFID-Anwendungen liefern, deren Informationssicherheitsbedrohungen Auswirkungen auf die breite Öffentlichkeit haben. Die Mitgliedstaaten sollten ebenfalls die Betreiber von RFID-Anwendungen, die diese Anwendungen bereitstellen, anregen, anwendungsspezifische Richtlinien partnerschaftlich mit allen Betroffenen zu entwickeln. Organisationen des öffentlichen und privaten Sektors sollten danach streben, sicherzustellen, dass ihre Mitglieder diese Richtlinien einhalten. Im Hinblick auf einen einheitlichen Binnenmarktansatz zur Informationssicherheit sollte die Verbreitung von besten verfügbaren Techniken für diese Anwendungen auf

europäischer Ebene angeregt werden.

3. Die Mitgliedstaaten sollten die Betreiber von RFID-Anwendungen ermutigen, zusammen mit den zuständigen staatlichen Behörden und Organisationen der Zivilgesellschaft Schemata wie Zertifizierung oder Betreiber-Selbsterklärung neu zu entwickeln oder bestehende anzuwenden, um aufzuzeigen, dass ein angemessenes Niveau des Schutzes der Privatsphäre und der Informationssicherheit bezogen auf die bewerteten Risiken von RFID-Anwendungen gegeben ist.

Die Antworten / Kommentare des FoeBuD zum Artikel 6

- Auch hier müssen "sollten" und "soll" gegen "müssen" und "muß" ersetzt werden.
- Absatz 1: Die Sicherheitsmaßnahmen müssen in geeigneten Abständen an die technische und gesellschaftliche Fortentwicklung angepaßt werden.
- Absatz 2: Bereits die partnerschaftlich genannte Zusammenarbeit an einem runden Tisch beim BMWI in Deutschland hat gezeigt, daß offenbar nur wenig Interesse an einer transparenten Zusammenarbeit mit relevanten Beteiligten gegeben ist. So wie Selbstverpflichtungserklärungen der Industrie schon früher nur begrenzte Haltbarkeit hatten sehe ich im Entwurf nicht, wie dieser gut gemeinte Punkt tatsächlich durchgesetzt werden könnte - obschon er es muß. Es müssen daher relevante Sanktionsmöglichkeiten geschaffen werden.
- Absatz 3: Ein "Ermutigen" ist zu wenig. Ein "angemessenes Niveau des Schutzes" muß vom Betreiber nachgewiesen werden, sowohl vor Beginn der jeweiligen Anwendung als auch während und nach der Anwendung (letzteres z.B. durch qualifizierten Nachweis der Datenlöschung). Datenschutzbehörden müssen jederzeit in die Lage versetzt und verpflichtet werden, das Schutzniveau auch unangemeldet zu überprüfen (Datenschutz-TÜV).
- "danach streben" eratzlos streichen.
- Hinzufügen: "Es sollte ein Ausstiegsszenario vorgehalten werden (Strichcode / 2D/3D-Strichcode etc.)."

Frage / Artikel 7 – RFID Einsatz im Einzelhandel

1. Betreiber von RFID-Anwendungen sollten auf jeder Stufe einer Wertschöpfungskette garantieren, dass sie in ausreichender Weise Informationen und Mittel an in der Wertschöpfungskette folgenden Betreiber liefern, so dass die Bestimmungen dieser Empfehlung umgesetzt werden können.
2. Betreiber von RFID-Anwendungen sollten, wo angemessen, in Zusammenarbeit mit Einzelhändlern ein harmonisiertes Zeichen festlegen, das auf den Einsatz von Funkchips in Einzelhandelsprodukten hinweisen und sicherstellt, dass Verbraucher informiert sind:
 - über das Vorhandensein eines Funkchips in einem Einzelhandelsprodukt;
 - ob dieser Funkchip einen spezifizierten, ausdrücklichen und legitimen Zweck nach dem Verkauf hat;
 - über die wahrscheinlich realistischen Risiken für den Schutz der Privatsphäre aufgrund des Vorhandenseins des Funkchips und über die Maßnahmen, welche von den Verbrauchern getroffen werden können, um diese Risiken zu verringern.
3.
 - (a) Falls eine RFID-Anwendung personenbezogene Daten verarbeitet oder die Datenschutz-Folgeabschätzung (die in Übereinstimmung mit Art. 3.1 unternommen wird) eine erhebliche Wahrscheinlichkeit der Erzeugung personenbezogener Daten durch die Nutzung der Anwendung aufzeigt, muss der Einzelhändler gemäß den in der Richtlinie 95/46 für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten festgelegten Kriterien vorgehen, und den Funkchip an der Stelle des Verkaufs deaktivieren; es sei denn, der Verbraucher entschließt sich, den Funkchips betriebsbereit zu belassen.
 - (b) Falls eine RFID-Anwendung die Speicherung oder Verarbeitung personenbezogener Daten nicht beinhaltet, und wo die Datenschutz-Folgeabschätzung aufgezeigt hat, dass das Risiko der Erzeugung personenbezogener Daten durch die RFID-Anwendung vernachlässigbar ist, muss der Einzelhändler dem Verbraucher eine leicht zugängliche Möglichkeit zur Deaktivierung oder Entfernung des Funkchips anbieten.
4. Eine Deaktivierung oder Entfernung von Funkchips sollte keine Einschränkung oder

Beendigung der gesetzlichen Verpflichtungen des Einzelhändlers oder Herstellers in Bezug auf den Verbraucher mit sich bringen. Die Deaktivierung oder Entfernung von Funkchips durch den Einzelhändler sollte sofort und kostenlos für den Verbraucher durchgeführt werden. Die Verbraucher sollten überprüfen können, dass die Aktion wirksam gewesen ist.

5. Innerhalb von drei Jahren nach dem Inkrafttreten dieser Empfehlung wird die Europäische Kommission diese Bestimmungen überprüfen, um die Wirksamkeit und Wirtschaftlichkeit von Systemen zur Beseitigung oder Abschaltung von Funkchips zu bewerten; dies im Hinblick auf die Bereitstellung einer automatischen Deaktivierung aller Objekte an der Stelle des Verkaufs außer in Fällen, in denen der Verbraucher ausdrücklich der weiteren Nutzung der RFID-Anwendung zugestimmt hat.

Die Antworten / Kommentare des FoeBuD zum Artikel 7

- Auch hier müssen "sollten" und "soll" gegen "müssen" und "muß"; "personenbezogene" gegen "personenbeziehbar" ersetzt werden. Im Absatz 4 muß das "sollte" gegen ein "darf" ersetzt werden.
- Absatz 2: Das Zeichen muß das Risiko angemessen darstellen und darf nicht beschönigend sein. Es muß begleitend auf alternative Möglichkeiten hingewiesen werden; diese sind vom Betreiber dem Bürger leicht zur Verfügung zu stellen oder automatisch anzuwenden.
- Statt "harmonisiertes Zeichen" muß es heißen: "standardisiertes Zeichen".
- Dritter Spiegelstrich: "wahrscheinlich realistischen" ist zu streichen.
- Absatz 3a (ans Ende hinzufügen): "Dieser Entschluß kann nie vorausgesetzt werden."
- Absatz 3b ist zu streichen. Dafür ist Absatz 3a zu ergänzen: Der Betreiber ist dafür zuständig das Deaktivieren vor Erreichen öffentlichen Raumes wie z.B. der Verkaufsfläche eines Supermarktes automatisch und prüfbar durchzuführen.
- Absatz 4: "sollte keine Einschränkung" in "darf keine Einschränkung" ändern.
- Absatz 5: Es darf für einen Bürger keinen Mehraufwand (z.B. durch längere Warteschlangen durch Vorhandensein nur einer Nicht-RFID-Kasse) entstehen RFID nicht zu verwenden.

Frage / Artikel 8 – Maßnahmen zur Sensibilisierung

1. Die Mitgliedstaaten sollten gemeinsam mit der Industrie und anderen Interessenvertretern angemessene Maßnahmen ergreifen, um Unternehmen, insbesondere KMU über die potenziellen Vorteile im Zusammenhang mit der Nutzung von RFID-Technik zu informieren und ihre Bekanntheit zu erweitern. Besondere Aufmerksamkeit sollte den Aspekten der Informationssicherheit und der Privatsphäre gewidmet werden.
2. Die Mitgliedstaaten sollten gemeinsam mit der Industrie, Verbraucherschutzverbänden und anderen relevanten Interessenvertreter Beispiele guter Praktiken zum Einsatz von RFID-Anwendungen identifizieren. Sie sollten auch geeignete Maßnahmen wie zum Beispiel groß angelegte Pilotprojekte initiieren, um das öffentliche Bewusstsein über die RFID-Technik sowie über Vorteile und Auswirkungen ihres Gebrauchs als Voraussetzung eines breiteren Einsatzes zu erweitern.

Die Antworten / Kommentare des FoeBuD zum Artikel 8

- Absatz 1: Es darf nicht einseitig nur über die potentiellen Vorteile informiert werden, auch die potentiellen Nachteile sind gleichberechtigt und nicht beschönigend darzustellen. Demnach muß der Terminus "potentielle Vorteile" gegen "potentielle Risiken" ausgetauscht werden.
- Absatz 2 muß wegfallen.

Frage / Artikel 9 – Forschung und Entwicklung

Die Mitgliedstaaten sollten mit der Industrie und der Kommission zusammenarbeiten, um technologieintegrierte(n) Sicherheit und Datenschutz ("security und privacy by design") im Frühstadium der Entwicklung von RFID-Anwendungen anzuregen und zu unterstützen, insbesondere durch die Entwicklung leistungsfähiger und preiswerter Lösungen.

Die Antworten / Kommentare des FoeBuD zum Artikel 9

- Nicht nur Industrie und Kommission, sondern auch NGOs, resp. Betroffenengruppen, muss die Zusammenarbeit ermöglicht werden. Dazu gehört

auch die Finanzierung für notwendige Honorare und Spesen, die in den entsprechenden Budgets vorgesehen werden müssen.

- Es ist auch Augenmerk auf PET (Privacy Enhancing Technologies) zu legen sowie auf Möglichkeiten, Anwendungen auch ohne Funktechnik leistungsfähig und preiswert zu erstellen.
- Förderhin ist die Entwicklung von geeigneten Prüf- und Auditmaßnahmen sowie von Technologie- und Datenschutzfolgeabschätzungen anzuregen.

Frage / Artikel 10 – Folgemaßnahmen

1. Die Mitgliedstaaten sollten die Kommission 18 Monate nach der Veröffentlichung dieser Empfehlung im Amtsblatt der Europäischen Union zu den Aktionen, die als eine Reaktion auf diese Empfehlung ausgeführt werden, unterrichten.
2. Innerhalb von drei Jahren nach der Annahme dieser Empfehlung wird die Kommission einen Bericht über die Durchführung dieser Empfehlung und ihre Auswirkung auf Wirtschaftsunternehmen und Verbraucher insbesondere im Hinblick auf die Maßnahmen liefern, die in Artikel 7 empfohlen werden. Wo angemessen soll die Kommission diese Empfehlung ändern oder einen anderen Vorschlag vorlegen, den sie einschließlich verpflichtender Maßnahmen für erforderlich hält, um die Ziele dieser Empfehlung in höherem Maße zu erreichen.

Die Antworten / Kommentare des FoeBuD zum Artikel 10

- An dem Prozeß sind wiederum alle Beteiligten aus Industrie und Gesellschaft zu hören.
- Es bleibt weiterhin zu klären, nicht nur wie sondern auch ob RFID überhaupt eingeführt werden darf.
- RFID darf nicht eingeführt werden, wenn die Gefahren für die Gesellschaft nicht ausgeräumt werden können: Es darf kein noch so kleines Restrisiko bleiben.

Frage / Artikel 11 – Empfänger

Diese Empfehlung ist an die Mitgliedstaaten und an alle Beteiligten gerichtet, die an Entwicklung und Betrieb von RFID-Anwendungen in der Gemeinschaft involviert sind.

Die Antworten / Kommentare des FoeBuD zum Artikel 11

Als Empfänger sind auch all diejenigen zu nennen, die als Beteiligte beim Revisionsprozeß (laut Artikel 10 in 18 Monaten) infrage kommen.

Zusätzliche Bemerkungen des FoeBuD (Frage 12)

- Maßnahmen sind nicht nur durch den Gesetzgeber, sondern vor allem durch das Verursacherprinzip von RFID-Betreibern und solchen, die dies anstreben zu finanzieren.
- Alle "sollten" und "soll" müssen gegen "müssen" und "muß" ausgetauscht werden.
- Alle "personenbezogenen" müssen durch "personenbeziehbar" ersetzt werden (das ist zwar mit dem Wort "personenbezogen" gemeint, wird aber für die meisten Menschen anscheinend nicht deutlich genug).