EINFÜHRUNG IN DIE ÖFFENTLICHE KONSULTATION ZUR RFID EMPFEHLUNG ZUR PRIVATSPHÄRE, ZUM DATENSCHUTZ UND ZUR SICHERHEIT

1. HINTERGRUND

Nach einer ersten öffentlichen Konsultation zur Rundfunkfrequenzidentifizierung (RFID) die im Jahre 2006 abgehalten wurde[1], hat sich die Kommission durch ihre Mitteilung vom 15. März 2007[2] verpflichtet, einige der Themen zu behandeln, die von den Beteiligten hinsichtlich der Risiken für Privatsphäre, Datenschutz und Sicherheit geäußert wurden und eine Empfehlung zu dieser Angelegenheit zu adoptieren.

Angesichts der Bedeutung dieser Sache hat die Kommission beschlossen, in einer öffentlichen Konsultation alle Artikel darzulegen, die im gegenwärtigen Empfehlungsentwurf berücksichtigt werden.

2. VORBEREITUNG DIESES EMPFEHLUNGSENTWURFS

Drei aufeinander folgende Konferenzen zu RFID in Brüssel[3], Berlin[4] und Lissabon[5] haben direkt zur Debatte und dem zugrunde liegenden Prozess zur Vorbereitung dieser Empfehlung beigetragen.

Darüber hinaus hat die Kommission eine Sachverständigengruppe[6], die *RFID Sachverständigengruppe,* eingerichtet, die unter anderem die Kommission zum Inhalt dieser Empfehlung berät.

Schließlich sind mehrere andere Beiträge zur Vorbereitung dieser Arbeit berücksichtigt worden. Hier sind beispielsweise die Beiträge des Europäische Wirtschafts- und Sozialausschusses (EWSA)[7], der Datenschutzarbeitsgruppe des Artikels 29[8,9], der Europäischen Datenschutzaufsichtskraft[10] und der OECD[11] zu nennen.

---

1 http://ec.europa.eu/information_society/policy/rfid/doc/rfidswp_en.pdf
2 COM/2007/96 - Rundfunkfrequenzidentifizierung (RFID) in Europa: Schritte hin zu einem Politikrahmen.
3 EU-Forum RFID, 13-14 März 2007.
4 http://www.nextgenerationmedia.de/Nextgenerationmedia/Navigation/de/rfid-conference.html
5 http://www.rfid-outlook.pt/
6 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:176:0025:01:DE:HTML und http://ec.europa.eu/information_society/policy/rfid/doc/reg.pdf
7 http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_256/c_25620071027en00660072.pdf
8 Stellungnahme 4/2007 vom 20. Juni 2007 - http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf
9 siehe Stellungnahme 105 und 136 (Schlussfolgerungen): http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm
10 siehe Stellungnahme vom 20. Dezember 2007: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/26
11 http://www.oecd.org/dataoecd/59/12/36069207.pdf

KALENDER UND NÄCHSTE SCHRITTE

Die öffentliche Konsultation wird für einen Zeitraum von acht Wochen verfügbar sein und wird am 25. April 2008 beendet werden. Eine Übersetzung dieser Konsultation im Französischen und Deutschen ist ebenfalls auf der Webseite verfügbar.

Es ist geplant, dass die Empfehlung vor Sommer 2008 angenommen wird.

VORGEHEN ZUM ANTWORTEN

Jede Frage entspricht einem Artikel des Empfehlungsentwurfs. Sie besteht aus einer kurzen Einführung gefolgt vom geplanten Text. Die Kommission sieht keine weiteren Artikel vor; in Abhängigkeit der Beiträge durch die Konsultation könnte sich dies jedoch ändern. Am Schluss haben Sie die Möglichkeit, in einer offenen Frage zusätzliche Anmerkungen, die nicht direkt im Zusammenhang mit einem vorgegebenen Artikel stehen, zu machen. Alle Fragen sind fakultativ, was bedeutet, dass Sie die Beantwortung einer Frage auslassen können, zu der Sie nicht Stellung nehmen wollen.

Respektieren Sie bitte die folgenden Regeln bei der Beantwortung der Fragen:

- Beantworten Sie jede Frage in dem dafür vorgesehenen Antwortfeld und beschränken Sie sich auf den zur Verfügung stehenden Umfang (d.h. verwenden Sie nicht beispielsweise das Feld für Antwort 4, um die Beantwortung von Frage 3 abzuschließen).

- Ihre Antworten müssen ohne das Lesen zusätzlicher Dokumente verstanden werden können. Referenzen auf zusätzliche Dokumente werden begrüßt, aber aus praktischen Gründen kann nicht garantiert werden, dass sie alle gelesen werden.

- Nur die ersten 20 Zeilen (30 Zeilen für Frage 12) einer Antwort werden vom System gespeichert. Längere Antworten werden abgeschnitten und sind deshalb nicht brauchbar.

- Antworten, die außerhalb des Geltungsbereichs einer Frage gegeben werden, werden nicht berücksichtig.

Wenn nicht anderweitig von der antwortenden Person gefordert, werden alle Beiträge nach Abschluss der Konsultation auf der Webseite der Kommission publik gemacht werden.

Abschnitt 1: Angaben zur Person

Dieser Fragebogen ist Teil eines öffentlichen Konsultationsverfahrens. Er ist Gegenstand der Regeln des Schutzes persönlicher Daten.

Bitte lesen Sie die VERTRAULICHKEITSERKLÄRUNG.

Nachname (optional)

Vorname (optional)

Geschlecht (optional)

Männlich Weiblich

E-mail-Adresse (erforderlich)

Welcher Typ von Stakeholder sind Sie? (erforderlich)

Interessierter Bürger

Regierungsorganisation

RFID-Industrie (Systeme)

Universität/Forschung

Verbraucherschutzgruppe

Kommerzieller RFID-Anwender

Nicht-Regierungs-Organisation

Telekommunikation

Arbeitnehmerorganisation

Berater für RFID-Anwendungen

Internationale Organisation

Sonstige

Bitte Geben Sie bitte Ihre Altersgruppe an (optional)

Unter 18

18 - 24

25 - 44

45 - 64

65 +

Sitz (Land) Ihrer Organisation (antworten Sie als Einzelperson, geben Sie bitte das Land Ihres Wohnsitzes an)

(erforderlich)

Algerien

Argentinien

Australien

Belgien

Bolivien

Brasilien

Bulgarien

Chile

China

Dänemark

Deutschland

Estland

Finnland

Frankreich

Griechenland

Hongkong

Indien

Irland

Island

Israel

Italien

Japan

Kanada

Kenia

Südkorea

Kroatien

Lettland

Liechtenstein

Litauen

Luxemburg

Mazedonien

Malta

Marokko

Mexiko

Neuseeland

Niederlande

Norwegen

Österreich

Polen

Portugal

Rumänien

Russland

Schweden

Schweiz

Singapur

Slowakische Republik

Slowenien

Spanien

Südafrika

Tschechische Republik

Tunesien

Türkei

Ukraine

Ungarn

Vereinigte Staaten

Vereinigtes Königreich

Zypern

Sonstige

Geographischer Tätigkeitsbereich Ihrer Organisation (geben Sie bitte Ihr geographisches Tätigkeitsgebiet an, wenn Sie als Einzelperson antworten)

(erforderlich)

Örtlich

Regional

National

Europäisch

International

EINZELNE FRAGEEINFÜHRUNG

Frage 1 – Geltungsbereich	
Die Empfehlung konzentriert sich auf die Aspekte der Vertraulichkeits- und Informationssicherheit des RFID-Technikeinsatzes und soll in dieser Hinsicht eine Anleitung an die EU-Mitgliedstaaten und an Beteiligte geben. Es ist nicht vorgesehen, andere wichtige politische Themen, die in der Mitteilung "RFID in *Europa: Schritte hin zu einem Politikrahmen*" angesprochen wurden, wie die Kontrolle von Ressourcen im Internet der Dingen, Technologieentwicklung und -Innovation, Rundfunkspektrum, Normen, Umwelt und Gesundheit zu behandeln. Die Empfehlung soll Auskunft geben über die praktische Durchführung der Grundsätze, wie sie die in der Datenschutzrichtlinie 95/46/EG, der Richtlinie über Rundfunkausrüstung und Datenendstationsgeräte für Telekommunikation 1999/5/EG und der Richtlinie über Vertraulichkeit und elektronische Kommunikationen 2002/58/EG definiert werden, deren Text hier eingesehen werden kann[12]. Die Empfehlung betrifft nicht die Gebiete der gemeinsamen Außen- und Sicherheitspolitik sowie polizeilicher und juristischer Zusammenarbeit in Strafsachen. Der vorgeschlagene Artikel über den Geltungsbereich lautet:	*Artikel 1* Anwendungsbereich 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 gesetzlichen 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

[12] http://eur-lex.europa.eu/RECH_naturel.do

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

Frage 2 – Definitionen	
Die Empfehlung verwendet die Definitionen der Datenschutzrichtlinie. Darüber hinaus werden RFID-spezifische Ausdrücke definiert und bestehende internationale technische Normen berücksichtigt. Der vorgeschlagene Artikel über die Definitionen lautet:	*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.

Frage 3 – Vertraulichkeits- und Datenschutzmaßnahmen	
Dieser Artikel gibt Auskunft über die Implementierung von RFID-Anwendungen, damit die Umsetzung des Datenschutzes und der Gesetzgebung zum Schutz der Privatsphäre praktisch gewährleistet werden kann. Zunächst wird eine systematische Analyse der Datenschutzrisiken (Datenschutz-Folgeabschätzung (PIA) empfohlen, bevor eine Anwendung implementiert wird (Absatz 1). Die Ergebnisse sollten öffentlich in angemessener Form zur Verfügung gestellt werden (Absatz 5). Die Verwendung von PIAs ist eine festgelegte Methodologie; Beispiele zu Verwendungsmöglichkeiten sind hier zu finden[13]. Die Datenschutz-Folgeabschätzung liefert auch einen Input für den Entwurfsprozess einer RFID-Anwendung, so dass Risiken minimiert werden können. Die Umsetzung angemessener Maßnahmen für die Abschwächung der Risiken wird empfohlen (Absatz 2). Es ist wichtig, dass eine klare organisatorische Verantwortung für diese Maßnahmen zugewiesen wird (Absatz 3). Die Datenschutz-Folgeabschätzung sollte auch einen Input im Zusammenhang mit dem allgemeinen Risikomanagement der Informationssicherheit liefern und mit diesem koordiniert werden, wie dies in Artikel 6 der Empfehlung angeben ist (Absatz 4). Der vorgeschlagene Artikel über Maßnahmen zum Schutz der Privatsphäre und zum	*Artikel 3* Maßnahmen zum Schutz der Privatsphäre und zum Datenschutz 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

[13] http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html

Datenschutz lautet:	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.

Frage 4 – Verhaltensregeln	
Um der Vielfalt von RFID-Anwendungen und dem zukünftigen weit verbreiteten Gebrauch, welchen Organisationen von ihnen machen werden, gerecht zu werden, regt dieser Artikel die Entwicklung sektor- oder anwendungsspezifischer Verhaltensregeln, mit verpflichtenden Maßnahmen für die Unterzeichnenden, an. In ähnlicher Weise sieht Artikel 27 der Datenschutzrichtlinie die Entwicklung von Verhaltensregeln vor, um Datenschutzaspekte zu erfassen. Die Bestimmungen dieses Artikels empfehlen, dass derartige Verhaltensregeln den relevanten Datenschutzbehörden einschließlich auf EU-Ebene zur Zustimmung unterbreitet werden. Der vorgeschlagene Artikel über Verhaltensregeln lautet:	*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 Verhaltensregelns der Arbeitsgruppe „Artikel 29“ zur

	Stellungnahme auf Gemeinschaftsebene unterbreitet werden.

Frage 5 – Informationen zum Gebrauch von RFID	
RFID-Anwendungen können technisch ohne direkt sichtbare oder andere wahrnehmbare Aktionen funktionieren, so dass nicht alle Transaktionen direkt wahrnehmbar sind. Die Bestimmungen dieses Artikels zielen darauf ab, die minimalen Informationen festzusetzen, die von RFID-Betreibern an betroffene Personen in Form schriftlicher Form und durch Hinweiszeichen über das Vorhandensein von RFID-Lesegeräten in öffentlichen Plätzen geliefert werden sollen. Werden darüber hinaus Verhaltensregeln gemäß Artikel 4 der Empfehlung erlassen, so kann es erforderlich sein, weitaus detailliertere und umfassendere Informationen an den Verbraucher zu geben. Es ist anzumerken, das Artikel 7 (RFID Einsatz im Einzelhandel) zusätzliche Informationsanforderungen im Falle des Einzelhandelssektors vorsieht. Der vorgeschlagene Artikel für die Informationen zum Gebrauch von RFID lautet:	*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.

Frage 6 – Risikomanagement der Informationssicherheit	
RFID-Anwendungen müssen, wie jede andere Informationstechnologie, in sicherer Art betrieben werden. In Übereinstimmung mit der Mitteilung der Kommission "Eine *Strategie für eine sichere Informationsgesellschaft - Dialog, Partnerschaft und Bevollmächtigung"* (COM (2006) 251-entgültig) beschreibt dieser Artikel Maßnahmen, die in Bezug auf die Informationssicherheit von RFID-Anwendungen ergriffen werden sollen. Der vorgeschlagene Artikel über das Risikomanagement der Informationssicherheit lautet:	*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.

Frage 7 – RFID Einsatz im Einzelhandel	
Die Empfehlungen hinsichtlich der Vertraulichkeitsmaßnahmen, der Selbstregulierung (Verhaltensregeln), der Information zum Gebrauch von RFID und des Risikomanagements der Informationssicherheit sind auf *alle* RFID-Anwendungen und auf *alle* wirtschaftlichen und auf *alle* sozialen Sektoren anzuwenden. Jedoch wird davon ausgegangen, dass der *Einzelhandelssektor* auf Grund spezifischer Gegebenheiten im Zusammenhang mit der potentiell großen Verbreitung von Konsumgütern, die mit RFID-Transpondern ausgestattet sind, einer zusätzlichen Anleitung bedarf. Der Artikel empfiehlt, die Verbraucher durch Zeichen und weitere Hinweise zu informieren, damit sie in die Lage versetzt werden, eine „informierte Wahl“ treffen zu können (Absatz 2). In Übereinstimmung mit der Anwendung der Kriterien der Richtlinie 95/46EG empfiehlt der Artikel bei der Verarbeitung personenbezogener Daten in RFID-Anwendungen die Anwendung des ”Opt-in” Prinzips an der Stelle des Verkaufs. Dies bedeutet standardmäßig eine Deaktivierung des RFID-Transponders, es sei denn, der Verbraucher entschließt sich, den Funkchip betriebsbereit zu belassen (Absatz 3a). Werden keine personenbezogenen Daten verwendet, legt der Artikel fest, dass der Einzelhändler eine Vorrichtung zur Abschaltung oder Entfernung des RFID-Transponders bereitstellen muss, wenn die Kunden dies fordern (”Opt-out” Prinzip) (Absatz 3b). Die Europäische Kommission wird in den kommenden drei Jahren die	*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

Effizienz and Effektivität der Systeme zur Transponderentfernung und –deaktivierung analysieren. Es wird angestrebt, dass durch die Ergebnisse einer zielgerichteten Forschung und Entwicklung eine Deaktivierung oder Entfernung des Transponders automatisch und einfach erfolgen kann; es sei denn, der Verbraucher wünscht, dass ein Transponder funktionsfähig verbleibt. Der vorgeschlagene Artikel über den RFID Einsatz im Einzelhandel lautet:	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 personenbezogene 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.

Frage 8 – Maßnahmen zur Sensibilisierung	
Wie sich bereits in der öffentlichen Konsultation von 2006 gezeigt hat und regelmäßig von allen Beteiligten bestätigt wird, sind die wirklichen Vorteile und Risiken der RFID-Technik sowohl in der breiten Öffentlichkeit als auch in vielen Unternehmen, insbesondere KMU nicht bekannt. Die folgenden Maßnahmen zielen darauf ab, das Bewusstsein für die RFID-Technik zu wecken, um die weitere Entwicklung zu fördern, während gleichzeitig auf die Bedenken aller Benutzer eingegangen wird. Der vorgeschlagene Artikel über Maßnahmen zur Sensibilisierung lautet:	*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.

Frage 9 – Forschung und Entwicklung	
Dieser Artikel empfiehlt, ein spezielles Augenmerk auf Forschung und Entwicklung von wirksamen Sicherheits– und Privatsphärenschutz-Funktionen für dennoch erschwingliche RFID-Komponenten und –systeme zu richten. Vorgeschlagen wird im Folgenden:	*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.

Frage 10 – Folgemaßnahmen	
RFID-Techniken und ihre Anwendungen entwickeln sich sehr schnell. Da nicht alle Auswirkungen von zukünftigen Anwendungen vorhersehbar sind, sieht sich die Kommission verpflichtet, ihre Arbeit auf diesem Gebiet jenseits der Annahme dieser Empfehlung fortzusetzen und tut dies, indem sie folgende Bestimmungen zu Folgemaßnahmen vorschlägt:	*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.

Frage 11 – Empfänger	
Da der erfolgreiche und groß angelegte Einsatz der RFID-Technik nicht nur in den Händen von Behörden sondern ebenfalls der anderer Beteiligter liegt, schlägt die Kommission vor, die Empfehlung an beide mit der folgenden Bestimmung zu richten:	*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.

Frage 12 – zusätzliche Bemerkungen	
Teilnehmer an dieser Konsultation, die es wünschen, zusätzliche Anmerkungen zu machen, die nicht direkt mit einem der vorstehenden Artikel verbunden sind, sondern vielmehr die gesamte Empfehlung umfassen oder die außerhalb der vorgeschlagenen Artikel fallen, können dies hier tun.	