EMPFEHLUNGEN

KOMMISSION

EMPFEHLUNG DER KOMMISSION

vom 12. Mai 2009

zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen

(Bekannt gegeben unter Aktenzeichen K(2009) 3200)

(2009/387/EG)

DIE KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 211,

nach Anhörung des Europäischen Datenschutzbeauftragten,

in Erwägung nachstehender Gründe:

(1) Die Funkwellenidentifikation (Radio Frequency Identification, RFID) markiert eine neue Entwicklung in der Informationsgesellschaft, in deren Verlauf Gegenstände mit mikroelektronischen Komponenten, die automatisch Daten verarbeiten können, zunehmend Einzug in den Lebensalltag halten werden.

(2) In dem Maße, wie sich die RFID-Technik verbreitet, wird sie in vielfältigen Bereichen wie Logistik ([1]), Gesundheitsfürsorge, öffentlicher Verkehr, Einzelhandel (insbesondere für eine höhere Produktsicherheit und den schnelleren Rückruf von Produkten), Unterhaltung, Arbeit, Mauterhebung, Gepäckabfertigung und Reisedokumente zum Teil des persönlichen Lebens der Menschen.

(3) Die RFID-Technik hat das Potenzial, zu einer wichtigen neuen Triebkraft für Wachstum und Beschäftigung zu werden und einen großen Beitrag zur Verwirklichung der Lissabonner Strategie zu leisten. Sie verspricht große wirtschaftliche Vorteile, denn sie kann neue Geschäftschancen eröffnen, zu Kostensenkungen und Effizienzsteigerungen führen, insbesondere in Bezug auf die Bekämpfung von Produktnachahmungen, die Bewirtschaftung von Elektronikabfällen und gefährlichen Stoffen und das Recycling von Altprodukten.

(4) Die RFID-Technik erlaubt die Verarbeitung von u. a. auch personenbezogenen Daten über kurze Entfernungen ohne physischen Kontakt oder sichtbare Wechselwirkung zwischen dem Lese- oder Schreibgerät und dem RFID-Tag, so dass eine solche Datenübertragung stattfinden kann, ohne dass die betroffene Person dies bemerkt.

(5) RFID-Anwendungen sind potenziell in der Lage, Daten zu verarbeiten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen, die dadurch direkt oder indirekt identifiziert werden kann. So können sie entweder direkt im RFID-Tag gespeicherte personenbezogene Daten wie Namen, Geburtsdatum und Anschrift oder biometrische Angaben einer Person oder aber Daten verarbeiten, durch die eine bestimmte RFID-Artikelnummer mit anderweitig im System gespeicherten personenbezogenen Daten verknüpft werden. Außerdem bietet die Technik die Möglichkeit, Personen anhand der in ihrem Besitz befindlichen Gegenstände, die eine RFID-Artikelnummer enthalten, zu überwachen.

(6) Da die RFID-Technik potenziell sowohl allgegenwärtig als auch praktisch unsichtbar ist, muss bei ihrer Einführung den Fragen der Privatsphäre und des Datenschutzes besondere Beachtung geschenkt werden. Funktionsmerkmale für die Wahrung der Privatsphäre und die Informationssicherheit sollten folglich in RFID-Anwendungen bereits integriert werden, bevor diese auf breiter Basis genutzt werden (Grundsatz der „eingebauten Sicherheit und Privatsphäre“).

(7) Die zahlreichen wirtschaftlichen und sozialen Vorteile der RFID-Technik werden nur dann zum Tragen kommen, wenn es wirksame Vorkehrungen für die Einhaltung des Datenschutzes, die Wahrung der Privatsphäre und die Achtung der damit zusammenhängenden ethischen Aspekte gibt, die im Mittelpunkt der Debatte um die öffentliche Akzeptanz der RFID-Technik stehen.

(8) Die Mitgliedstaaten und alle Beteiligten sollten insbesondere in dieser Anfangsphase der RFID-Einführung weitere Anstrengungen unternehmen, um sicherzustellen, dass RFID-Anwendungen überwacht und die Rechte und Freiheiten des Einzelnen geachtet werden.

([1]) KOM(2007) 607 endg.

(9) In ihrer Mitteilung vom 15. März 2007 „Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen“ ([1]) kündigte die Kommission an, dass sie Klarstellungen und Vorgaben in Bezug auf die Aspekte des Datenschutzes und der Wahrung der Privatsphäre in RFID-Anwendungen in Form von einer oder mehreren Empfehlungen der Kommission vorlegen würde.

(10) Die Rechte und Pflichten in Bezug auf den Schutz personenbezogener Daten und den freien Datenverkehr, wie sie in der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ([2]) und in der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) ([3]) festgelegt sind, gelten uneingeschränkt für RFID-Anwendungen, in denen personenbezogene Daten verarbeitet werden.

(11) Die Grundsätze, die in der Richtlinie 1999/5/EG des Europäischen Parlaments und des Rates vom 9. März 1999 über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität ([4]) verankert sind, sollten auf die Entwicklung von RFID-Anwendungen angewandt werden.

(12) Der Europäische Datenschutzbeauftragte macht in seiner Stellungnahme ([5]) Vorgaben für den Umgang mit Produkten, die mit RFID-Tags versehen und für den Einzelnen bestimmt sind, und verlangt Datenschutz- und Sicherheitsfolgenabschätzungen zur Ermittlung und Weiterentwicklung der „besten verfügbaren Technik“ (BAT) für die Wahrung der Privatsphäre und die Sicherheit von RFID-Systemen.

(13) RFID-Anwendungsbetreiber sollten alle angemessenen Maßnahmen treffen, damit es nicht möglich ist, durch Mittel, die dem RFID-Anwendungsbetreiber oder einer sonstigen Person wahrscheinlich zur Verfügung stehen, die betreffenden Daten einer bestimmten oder bestimmbaren natürlichen Person zuzuordnen, sofern die Verarbeitung der Daten nicht in Übereinstimmung mit den geltenden Grundsätzen und Rechtsvorschriften über den Datenschutz erfolgt.

(14) In der Mitteilung der Kommission vom 2. Mai 2007 über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre ([6]) werden konkrete Maßnahmen dargelegt, um die Verarbeitung personenbezogener Daten auf das erforderliche Mindestmaß zu beschränken und nach Möglichkeit anonyme oder pseudonymisierte Daten zu verwenden, auch durch die Förderung der Entwicklung von Technologien zum Schutz der Privatsphäre und deren Nutzung durch die für die Datenverarbeitung Verantwortlichen und die Verbraucher.

(15) In der Mitteilung der Kommission vom 31. Mai 2006 „Eine Strategie für eine sichere Informationsgesellschaft — Dialog, Partnerschaft und Delegation der Verantwortung“ ([7]) werden Verschiedenartigkeit, Offenheit, Interoperabilität, Benutzerfreundlichkeit und Wettbewerb als Schlüsselfaktoren für eine sichere Informationsgesellschaft anerkannt, die Rolle der Mitgliedstaaten und öffentlichen Verwaltungen bei der Sensibilisierung und der Förderung bewährter Sicherheitsverfahren herausgestellt und die Akteure des Privatsektors aufgefordert, auf erschwingliche Sicherheits-Zertifizierungsprogramme für Produkte, Verfahren und Dienste hinzuarbeiten, die bestimmte EU-Anforderungen abdecken (insbesondere in Bezug auf die Privatsphäre).

(16) In der Entschließung des Rates vom 22. März 2007 zu einer Strategie für eine sichere Informationsgesellschaft in Europa ([8]) werden die Mitgliedstaaten aufgerufen, der notwendigen Prävention und Bekämpfung in Bezug auf neue und bestehende Bedrohungen der Sicherheit elektronischer Kommunikationsnetze gebührende Aufmerksamkeit zu schenken.

(17) Ein auf Gemeinschaftsebene aufgestellter Rahmen für die Durchführung von Datenschutzfolgenabschätzungen stellt sicher, dass den Bestimmungen dieser Empfehlung in den Mitgliedstaaten in einheitlicher Weise nachgekommen wird. Die Entwicklung eines solchen Rahmens sollte gestützt auf bestehende Praktiken und Erfahrungen in den Mitgliedstaaten und in Drittländern sowie auf die Arbeiten der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) ([9]) erfolgen.

(18) Die Kommission wird für die Aufstellung von gemeinschaftlichen Leitlinien für das Informationssicherheitsmanagementsystem bei RFID-Anwendungen sorgen und sich dabei auf bestehende Praktiken und Erfahrungen in den Mitgliedstaaten und in Drittländern stützen. Die Mitgliedstaaten sollten ihren Beitrag zu diesem Prozess leisten und private Einrichtungen wie auch Behörden zur Mitarbeit anhalten.

(19) Eine Datenschutzfolgenabschätzung, die der Betreiber vor der Einführung einer RFID-Anwendung durchgeführt, liefert die für angemessene Schutzmaßnahmen erforderlichen Informationen. Solche Maßnahmen müssen über die gesamte Lebensdauer der RFID-Anwendung überwacht und überprüft werden.

(20) Im Einzelhandel sollten anhand einer Datenschutzfolgenabschätzung für an Verbraucher verkaufte Produkte, an denen RFID-Tags angebracht sind, die erforderlichen Informationen ermittelt werden, um festzustellen, ob eine Bedrohung für die Privatsphäre oder den Schutz personenbezogener Daten wahrscheinlich ist.

([1]) KOM(2007) 96 endg.
([2]) ABl. L 281 vom 23.11.1995, S. 31.
([3]) ABl. L 201 vom 31.7.2002, S. 37.
([4]) ABl. L 91 vom 7.4.1999, S. 10.
([5]) ABl. C 101 vom 23.4.2008, S. 1.
([6]) KOM(2007) 228 endg.
([7]) KOM(2006) 251 endg.
([8]) ABl. C 68 vom 24.3.2007, S. 1.
([9]) Artikel 2 Absatz 1 der Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates (ABl. L 77 vom 13.3.2004, S. 1).

(21) Die Anwendung von internationalen Normen, wie sie z. B. von der Internationalen Organisation für Normung (ISO) entwickelt werden, sowie von Verhaltenskodizes und bewährten Praktiken, die mit dem EU-Rechtsrahmen vereinbar sind, kann helfen, die Maßnahmen zur Gewährleistung der Informationssicherheit und der Privatsphäre über den gesamten RFID-gestützten Geschäftsablauf zu verwalten.

(22) RFID-Anwendungen, die sich auf die allgemeine Öffentlichkeit auswirken, z. B. elektronische Fahrscheine im öffentlichen Verkehr, müssen angemessen geschützt werden. RFID-Anwendungen, die den Einzelnen berühren, weil beispielsweise biometrische Identifikationsdaten oder Gesundheitsdaten verarbeitet werden, sind im Hinblick auf die Informationssicherheit und die Wahrung der Privatsphäre besonders problematisch und müssen daher besondere Berücksichtigung finden.

(23) Die Gesellschaft als Ganzes muss sich der im Zusammenhang mit dem Einsatz von RFID-Anwendungen geltenden Rechte und Pflichten bewusst sein. Diejenigen, die solche Technik einführen, sind deshalb auch dafür verantwortlich, dass dem Einzelnen Informationen über die Nutzung dieser Anwendungen gegeben werden.

(24) Die Sensibilisierung der Öffentlichkeit sowie der kleinen und mittleren Unternehmen (KMU) für die Funktionsmerkmale und Fähigkeiten der RFID-Technik wird dazu beitragen, dass die Technik ihr wirtschaftliches Potenzial entfalten kann und gleichzeitig die Risiken einer Nutzung zum Nachteil öffentlicher Interessen mindern, wodurch ihre Akzeptanz gesteigert wird.

(25) Die Kommission wird an der Umsetzung dieser Empfehlung sowohl direkt als auch indirekt mitwirken, indem sie den Dialog und die Zusammenarbeit der Beteiligten fördert, und zwar insbesondere über das Rahmenprogramm für Wettbewerbsfähigkeit und Innovation (CIP), das mit dem Beschluss Nr. 1639/2006/EG des Europäischen Parlaments und des Rates [1] eingerichtet wurde, und das Siebte Forschungsrahmenprogramm (7. RP), das mit dem Beschluss Nr. 1982/2006/EG des Europäischen Parlaments und des Rates [2] eingerichtet wurde.

(26) Die Forschung und Entwicklung auf dem Gebiet der preisgünstigen Technologien für einen besseren Schutz der Privatsphäre und die Erhöhung der Informationssicherheit sind auf Gemeinschaftsebene unverzichtbar, wenn eine breitere Einführung dieser Technologien unter annehmbaren Bedingungen erreicht werden soll.

(27) Diese Empfehlung steht im Einklang mit den Grundrechten und Grundsätzen, die insbesondere mit der Charta der Grundrechte der Europäischen Union anerkannt wurden. Sie dient insbesondere der uneingeschränkten Wahrung des Privat- und Familienlebens und dem Schutz personenbezogener Daten —

[1] ABl. L 310 vom 9.11.2006, S. 15.
[2] ABl. L 412 vom 30.12.2006, S. 1.

EMPFIEHLT:

Anwendungsbereich

1. Diese Empfehlung gibt den Mitgliedstaaten Orientierungshilfen für die Gestaltung und den Betrieb von RFID-Anwendungen in einer rechtmäßigen und gesellschaftlich wie politisch annehmbaren Weise und unter Wahrung der Privatsphäre und Gewährleistung des Schutzes personenbezogener Daten.

2. Diese Empfehlung enthält Orientierungshilfen für Maßnahmen, die bei der Einführung von RFID-Anwendungen getroffen werden müssen, um sicherzustellen, dass die in Umsetzung der Richtlinien 95/46/EG, 1999/5/EG und 2002/58/EG erlassenen nationalen Rechtsvorschriften bei dieser Einführung, soweit zutreffend, eingehalten werden.

Begriffsbestimmungen

3. Für die Zwecke dieser Empfehlung gelten die Begriffsbestimmungen der Richtlinie 95/46/EG. Ferner gelten folgende Begriffsbestimmungen:

a) „Funkwellenidentifikation“ (RFID) ist die Nutzung elektromagnetischer Wellen oder der elektromagnetischen Nachfeldkopplung im Funkbereich des Frequenzspektrums für die Kommunikation von oder zu einem RFID-Tag mit Hilfe verschiedener Modulations- oder Kodierungstechniken oder nur für das Auslesen der Kennung eines RFID-Tags oder anderer darin gespeicherter Daten;

b) „RFID-Tag“ oder „RFID-Transponder“ oder RFID-Etikett ist entweder ein RFID-Gerät, dass in der Lage ist, ein Funksignal zu erzeugen, oder ein RFID-Gerät, das ein von einem Lese- oder Schreibgerät empfangenes Trägersignal rückkoppelt, rückwärtsstreut oder reflektiert (je nach Art des Geräts) und moduliert;

c) „RFID-Lese- oder Schreibgerät“ oder „Lesegerät“ ist ein festes oder mobiles Datenerfassungs- und Identifizierungsgerät, das durch eine elektromagnetische Welle oder durch elektromagnetische Nachfeldkopplung im Funkfrequenzbereich von einem oder mehreren RFID-Tags eine Antwort in Form modulierter Daten anregt und bewirkt;

d) „RFID-Anwendung“ oder „Anwendung“ ist eine Anwendung, die Daten unter Einsatz von RFID-Tags und Lesegeräten verarbeitet und dabei von einem Back-End-System oder einer vernetzten Kommunikationsinfrastruktur unterstützt wird;

e) „RFID-Anwendungsbetreiber“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über Zweck und Mittel des Betriebs einer Anwendung entscheidet, einschließlich der für die Verarbeitung personenbezogener Daten unter Einsatz einer RFID-Anwendung Verantwortlichen;

f) „Informationssicherheit“ ist die Wahrung der Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Informationen;

g) „Überwachung“ ist jede Tätigkeit zur Ermittlung, Beobachtung, Kopie oder Aufzeichnung des Aufenthaltsorts, der Bewegung, der Tätigkeiten oder des Zustands einer Person.

Datenschutzfolgenabschätzungen

4. Die Mitgliedstaaten sollten dafür sorgen, dass die Branche in Zusammenarbeit mit den jeweiligen Beteiligten aus der Zivilgesellschaft einen Rahmen für Datenschutzfolgenabschätzungen aufstellt. Dieser Rahmen sollte der Artikel-29-Datenschutzgruppe innerhalb von 12 Monaten nach Veröffentlichung dieser Empfehlung im *Amtsblatt der Europäischen Union* zur Prüfung vorgelegt werden.

5. Die Mitgliedstaaten sollten dafür sorgen, dass Betreiber ungeachtet ihrer sonstigen Verpflichtungen aus der Richtlinie 95/46/EG

a) eine Abschätzung der Folgen der Anwendungseinführung auf den Schutz personenbezogener Daten und die Wahrung der Privatsphäre durchführen und dabei auch klären, ob die Anwendung zur Überwachung einer Person verwendet werden könnte; die Ausführlichkeit der Folgenabschätzung sollte den möglichen Datenschutzrisiken, die mit der Anwendung verbunden sind, angemessen sein;

b) geeignete technische und organisatorische Maßnahmen treffen, um den Schutz personenbezogener Daten und die Wahrung der Privatsphäre zu gewährleisten;

c) eine Person oder Personengruppe benennen, die für die Prüfung der Folgenabschätzungen und der dauerhaften Eignung der technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten und zur Wahrung der Privatsphäre verantwortlich ist;

d) die Folgenabschätzung spätestens sechs Wochen vor Einführung der Anwendung der zuständigen Behörde zur Verfügung stellen;

e) die obigen Bestimmungen im Einklang mit dem in Nummer 4 genannten Rahmen für Datenschutzfolgenabschätzungen umsetzen, sobald dieser vorliegt.

Informationssicherheit

6. Die Mitgliedstaaten sollten die Kommission bei der Ermittlung jener Anwendungen unterstützen, aus denen sich Bedrohungen der Informationssicherheit mit Folgen für die Allgemeinheit ergeben könnten. Bei solchen Anwendungen sollten die Mitgliedstaaten dafür sorgen, dass die Betreiber gemeinsam mit den zuständigen nationalen Behörden und den Organisationen der Zivilgesellschaft neue Programme entwickeln oder bestehende Programme anwenden, z. B. für die Zertifizierung oder Selbstbewertung der Betreiber, um nachzuweisen, dass in Bezug auf die festgestellten Risiken ein angemessenes Niveau der Informationssicherheit und des Schutzes der Privatsphäre besteht.

Informationen und Transparenz in Bezug auf die RFID-Nutzung

7. Unbeschadet der aus den Richtlinien 95/46/EG und 2002/58/EG erwachsenen Pflichten der für die Datenverarbeitung Verantwortlichen sollten die Mitgliedstaaten dafür sorgen, dass die Betreiber für jede ihrer Anwendungen eine kurze, genaue und leicht verständliche Information ausarbeiten und veröffentlichen. Diese Information sollte mindestens folgende Angaben enthalten:

a) Name und Anschrift des Anbieters,

b) Zweck der Anwendung,

c) Art der Daten, die durch die Anwendung verarbeitet werden, anzugeben ist insbesondere, ob personenbezogene Daten verarbeitet werden und ob der Standort der RFID-Tags überwacht wird,

d) Zusammenfassung der Datenschutzfolgenabschätzung,

e) wahrscheinliche Risiken, die sich aus dem Einsatz von RFID-Tags in der Anwendung ergeben können, und Maßnahmen, die der Einzelne treffen kann, um diese Risiken zu mindern.

8. Die Mitgliedstaaten sollten dafür sorgen, dass die Betreiber Schritte unternehmen, um Einzelpersonen über die Präsenz von Lesegeräten zu informieren, und zwar mit Hilfe eines europaweit einheitlichen Zeichens, das von den europäischen Normungsgremien mit Unterstützung der beteiligten Akteure entwickelt wird. Das Zeichen sollte den Namen des Betreibers und eine Anlaufstelle enthalten, bei der Einzelpersonen die oben genannte Information über die Anwendung erhalten können.

RFID-Anwendungen im Einzelhandel

9. Die Betreiber sollten Einzelpersonen anhand eines europaweit einheitlichen Zeichens, das von den europäischen Normungsgremien mit Unterstützung der beteiligten Akteure entwickelt wird, über die Präsenz von RFID-Tags informieren, die an Produkten angebracht oder darin eingebettet sind.

10. Bei der Durchführung der in Nummer 4 und 5 genannten Datenschutzfolgenabschätzung sollte der Betreiber einer Anwendung besonders feststellen, ob RFID-Tags, die an oder in Produkten angebracht sind, welche von Einzelhändlern, die nicht Betreiber dieser Anwendung sind, an Verbraucher verkauft werden, wahrscheinlich eine Bedrohung für die Privatsphäre oder den Schutz personenbezogener Daten darstellen.

11. Einzelhändler sollten die in ihrer Anwendung genutzten RFID-Tags am Verkaufsort deaktivieren oder entfernen, es sei denn, die Verbraucher stimmen nach Aufklärung anhand der in Nummer 7 genannten Informationen der weiteren Betriebsfähigkeit der RFID-Tags zu. Unter Deaktivierung der RFID-Tags sollte jedes Verfahren verstanden werden, durch das ohne aktive Beteiligung des Verbrauchers jede Wechselwirkung zwischen dem RFID-Tag und seiner Umgebung beendet wird. Die Deaktivierung oder Entfernung der RFID-Tags durch den Einzelhändler sollte sofort und für den Verbraucher kostenlos erfolgen. Die Verbraucher sollten überprüfen können, ob die Deaktivierung oder Entfernung tatsächlich erfolgt ist.

12. Nummer 11 sollte keine Anwendung finden, wenn die Datenschutzfolgenabschätzung ergeben hat, dass die RFID-Tags, die in einer Einzelhandelsanwendung genutzt werden und nach Verlassen des Verkaufsorts betriebsfähig bleiben, wahrscheinlich keine Bedrohung für die Privatsphäre oder den Schutz personenbezogener Daten darstellen. Dennoch sollten Einzelhändler ein einfaches Mittel zur sofortigen oder späteren Deaktivierung oder Entfernung dieser RFID-Tags kostenlos zur Verfügung stellen.

13. Die Rechtspflichten des Einzelhändlers oder Herstellers gegenüber dem Verbraucher sollten durch Deaktivierung oder Entfernung von RFID-Tags keinesfalls verringert oder aufgehoben werden.

14. Die Nummern 11 und 12 sollten nur für Einzelhändler gelten, die auch Betreiber sind.

Sensibilisierungsmaßnahmen

15. Die Mitgliedstaaten sollten in Zusammenarbeit mit der Branche, der Kommission und anderen Beteiligten geeignete Maßnahmen treffen, um die Behörden und Unternehmen, insbesondere KMU, über die potenziellen Vorteile und Risiken im Zusammenhang mit der Nutzung der RFID-Technik zu informieren und dafür zu sensibilisieren. Besondere Aufmerksamkeit sollte dabei den Aspekten der Informationssicherheit und der Privatsphäre gewidmet werden.

16. Die Mitgliedstaaten sollten in Zusammenarbeit mit der Branche, den Organisationen der Zivilgesellschaft, der Kommission und anderen Beteiligten Beispiele für die gute Praxis bei der Einführung von RFID-Anwendungen ermitteln und bekannt machen, um die Allgemeinheit zu informieren und dafür zu sensibilisieren. Sie sollten außerdem geeignete Maßnahmen ergreifen, z. B. groß angelegte Pilotprojekte durchführen, um die RFID-Technik mit ihren Vorteilen, Risiken und Auswirkungen der Nutzung in das öffentliche Bewusstsein zu rücken und dadurch die Voraussetzungen für eine breitere Übernahme dieser Technik zu schaffen.

Forschung und Entwicklung

17. Die Mitgliedstaaten sollten mit der Branche, den Beteiligten aus der Zivilgesellschaft und der Kommission zusammenarbeiten, um schon frühzeitig in der Entwicklung der RFID-Anwendungen die Einführung des Grundsatzes der „eingebauten Sicherheit und Privatsphäre“ anzuregen und zu unterstützen.

Folgemaßnahmen

18. Die Mitgliedstaaten sollten alle notwendigen Maßnahmen treffen, um allen am Entwurf und Betrieb von RFID-Anwendungen in der Gemeinschaft Beteiligten diese Mitteilung zur Kenntnis zu bringen.

19. Die Mitgliedstaaten sollten der Kommission spätestens 24 Monate nach der Veröffentlichung dieser Empfehlung im *Amtsblatt der Europäischen Union* mitteilen, welche Maßnahmen sie eingeleitet haben, um dieser Empfehlung nachzukommen.

20. Innerhalb von drei Jahren nach der Veröffentlichung dieser Empfehlung im *Amtsblatt der Europäischen Union* wird die Kommission einen Bericht über die Umsetzung dieser Empfehlung, ihre Wirksamkeit und ihre Auswirkungen auf die Wirtschaftsteilnehmer und Verbraucher, insbesondere über die in Nummern 9 bis 12 empfohlenen Maßnahmen, vorlegen.

Adressaten

21. Diese Empfehlung ist an die Mitgliedstaaten gerichtet.

Brüssel, den 12. Mai 2009

Für die Kommission
Viviane REDING
Mitglied der Kommission