



00066/10/DE
WP 175

**Stellungnahme 5/2010 zum Vorschlag der Branche für einen Rahmen für
Datenschutzfolgenabschätzungen für RFID-Anwendungen**

Angenommen am 13. Juli 2010

Die Datenschutzgruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt. Sie ist das unabhängige Beratungsgremium der Europäischen Union in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 15 der Richtlinie 2002/58/EG festgelegt.

Die Sekretariatsgeschäfte werden wahrgenommen durch die Generaldirektion Justiz, Freiheit und Sicherheit, Direktion C (Grundrechte und Unionsbürgerschaft), der Europäischen Kommission, B-1049 Brüssel, Belgien, Büro LX-46 01/190.

Website: http://ec.europa.eu/justice/policies/privacy/index_en.htm

Inhalt

1	Hintergrund.....	3
1.1	Einleitung	3
1.2	RFID und Datenschutz	3
1.3	Ziele des Rahmens für Datenschutzfolgenabschätzungen	5
1.4	Zusammenfassung des vorgeschlagenen Rahmens	6
2	Analyse.....	7
2.1	Risikobewertung.....	7
2.2	Von Personen mitgeführte RFID-Tags	9
2.3	RFID im Einzelhandel.....	10
2.4	Weitere Anmerkungen	11
3	Fazit.....	12

1 Hintergrund

1.1 Einleitung

Am 12. Mai 2009 nahm die Kommission eine Empfehlung zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen¹ an.

In Nummer 4 dieser Empfehlung heißt es: *„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.“* (Hervorhebung hinzugefügt).

Sobald dieser Rahmen für die Datenschutzfolgenabschätzungen vorliegt, sollen die Mitgliedstaaten gemäß der Empfehlung dafür sorgen, dass RFID-Anwendungsbetreiber vor der Einführung von RFID-Anwendungen eine Datenschutzfolgenabschätzung durchführen und die dabei erstellten Berichte der zuständigen Behörde (d. h. der Datenschutzbehörde) zur Verfügung stellen.

Im Juli 2009 begann eine informelle RFID-Arbeitsgruppe unter Leitung von Branchenvertretern mit der Ausarbeitung eines Rahmens für Datenschutzfolgenabschätzungen. Sie kam dabei regelmäßig mit Beteiligten, darunter Vertretern von Verbraucherverbänden, Normungsgremien und Akademikern, zusammen. Am 31. März 2010 legten Branchenvertreter der Artikel-29-Datenschutzgruppe einen Vorschlag für einen Rahmen für Datenschutzfolgenabschätzungen zur Prüfung vor. **In dieser Stellungnahme sind die Ansichten der Datenschutzgruppe formell zusammengefasst.**

Nachfolgend bezieht sich „RFID-Empfehlung“ auf die am 12. Mai 2009 veröffentlichte Empfehlung der Kommission zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen. Der „vorgeschlagene Rahmen“ oder nur „Rahmen“ bezieht sich auf den der Datenschutzgruppe am 31. März 2010 übermittelten und im Anhang zu dieser Stellungnahme wiedergegebenen Rahmen für Datenschutzfolgenabschätzungen für RFID-Anwendungen (Originaltitel: *Industry Proposal – Privacy and Data Protection Impact Assessment Framework for RFID Applications*, deutsche Fassung liegt nicht vor – Anm. d. Ü.).

1.2 RFID und Datenschutz

Im Januar 2005 nahm die Datenschutzgruppe ein *Arbeitspapier*² zu *Datenschutzfragen im Zusammenhang mit der RFID-Technik* (WP 105) an, in dem sie die offensichtlichen Vorteile der RFID-Technik anerkannte, aber auch mögliche Bedenken aus Sicht des Datenschutzes hervorhob, die sich insbesondere auf *„die Möglichkeit für Unternehmen und Regierungen, mittels RFID in die Privatsphäre von Privatpersonen einzudringen“*, richten. Weiter heißt es darin: *„Die verdeckte Sammlung einer Vielzahl von Daten, die sich alle auf ein und dieselbe Person beziehen, die Lokalisierung von Personen, die sich an*

¹ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:DE:PDF>

² http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_de.pdf

öffentlichen Plätzen (Flughäfen, Bahnhöfen, Geschäften) aufhalten, die Erstellung von Kundenprofilen durch Beobachtung des Verbraucherverhaltens in Geschäften, das Auslesen von Informationen über Kleidungsstücke und Accessoires, die gerade getragen, oder über Medikamente, die mitgeführt werden, sind Beispiele für das Nutzungspotenzial von RFID, das aus datenschutzrechtlicher Sicht Anlass zu Sorge gibt.“

Zu diesem Arbeitspapier fand anschließend eine öffentliche Konsultation statt, deren Ergebnisse in einem von der Datenschutzgruppe im September 2005 veröffentlichten Dokument (WP 111)³ zusammengefasst wurden. Wie diese Ergebnisse zeigten, *„besteht nach Ansicht der meisten Hochschulen, Denkfabriken, Privatpersonen und Unternehmen der Sicherheitsbranche Bedarf für zusätzliche Leitlinien seitens der Datenschutzgruppe“*, während einige *„eine Ergänzung der Datenschutzrichtlinie durch spezifische RFID-Vorschriften“* anregen.

In diesem Gesamtzusammenhang wurde in Abstimmung mit den Beteiligten, darunter Vertretern der RFID-Branche, von Datenschutzorganisationen und Verbraucherverbänden, unter Federführung der Europäischen Kommission eine Empfehlung⁴ *„zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen“* erarbeitet, die *„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“* geben soll.

Diese im Mai 2009 veröffentlichte Empfehlung enthält etwas völlig Neues: Sie sieht vor, dass RFID-Anwendungsbetreiber vor der Einführung einer RFID-Anwendung eine *„Datenschutzfolgenabschätzung“* durchführen und deren Ergebnisse der zuständigen Behörde zur Verfügung stellen. Dieser neue Ansatz, der den durch die Datenschutzrichtlinie und die Datenschutzrichtlinie für elektronische Kommunikation gebildeten derzeitigen Regulierungsrahmen ergänzt, gibt der Branche angesichts des sich rasch verändernden technologischen Umfelds die Gelegenheit, ihr Potenzial zur Selbstregulierung als ergänzendes, flexibles und effizientes Instrument zum europäischen Rechtsrahmen zu demonstrieren. Die Datenschutzgruppe befürwortet *„die Durchführung von Datenschutz-Verträglichkeitsprüfungen, insbesondere für bestimmte Datenverarbeitungsvorgänge, von denen angenommen wird, dass sie [...] besondere Risiken für die Rechte und Freiheiten der Betroffenen darstellen.“*⁵ Sie ist außerdem der Auffassung, dass der Erfolg oder das Scheitern dieses Ansatzes entweder den Weg für die Durchführung von Datenschutzfolgenabschätzungen in anderen Bereichen ebnet oder aber zu einem strengeren Regulierungsansatz führen werden.

Die RFID-Empfehlung soll außerdem *„Informationen und Transparenz in Bezug auf die RFID-Nutzung“* fördern, insbesondere *„mit Hilfe eines europaweit einheitlichen Zeichens, das von den europäischen Normungsgremien mit Unterstützung der beteiligten Akteure entwickelt wird“*, *„um Einzelpersonen über die Präsenz von Lesegeräten zu informieren“*. Diese Initiative wird von der Datenschutzgruppe voll und ganz unterstützt.

³ *„Ergebnisse der öffentlichen Konsultation über Arbeitspapier WP 105 der Artikel-29-Datenschutzgruppe zu Datenschutzfragen im Zusammenhang mit der RFID-Technik“*,

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_de.pdf.

⁴ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:DE:PDF>

⁵ Vgl. *„Die Zukunft des Datenschutzes: Gemeinsamer Beitrag zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz der personenbezogenen Daten“*, WP 168,

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_de.pdf

Obwohl sich die RFID-Empfehlung ausdrücklich auf die Richtlinie 95/46/EG bezieht, weicht sie in einigen Fällen von der üblicherweise in den Datenschutzvorschriften verwendeten Terminologie ab, insbesondere wenn es um „Personen“, „Einzelpersonen“ und „Nutzer“ geht. Um Missverständnisse zu vermeiden, bezeichnet in dieser Stellungnahme der Begriff „Person“ eine natürliche Person im Sinne von Artikel 2 der Richtlinie 95/46/EG, während die Begriffe „Benutzer“ und „Einzelperson“ die Bedeutung behalten, die sie in der RFID-Empfehlung haben. Insbesondere kann sich der Begriff „Person“ zusammenfassend auf „Nutzer“ und „Einzelpersonen“ beziehen, zwei Personengruppen, zwischen denen ansonsten gemäß den Definitionen in Nummer 3 der RFID-Empfehlung, die im vorgeschlagenen Rahmen wiederholt werden, unterschieden wird. Um die in der RFID-Empfehlung verwendete Terminologie beizubehalten, ist in dieser Stellungnahme von „RFID-Anwendungsbetreibern“ anstatt von „für die Verarbeitung Verantwortlichen“ die Rede, wenngleich die beiden Begriffe nicht exakt dasselbe bedeuten.

Im November 2009 änderte der europäische Gesetzgeber die Datenschutzrichtlinie für elektronische Kommunikation⁶ und bezog dabei ausdrücklich die RFID-Technik ein. In Erwägungsgrund 56 der Richtlinie 2009/136/EG heißt es: *„Die breite Nutzung solcher Technologien kann erhebliche wirtschaftliche und soziale Vorteile bringen und damit einen großen Beitrag zum Binnenmarkt leisten, wenn ihr Einsatz von den Bürgern akzeptiert wird.“* Dann wird zu bedenken gegeben: *„Um dieses Ziel zu erreichen, muss gewährleistet werden, dass sämtliche Grundrechte des Einzelnen, einschließlich des Rechts auf Privatsphäre und Datenschutz, gewahrt bleiben.“* Anschließend wird ausgeführt: *„Werden solche Geräte an öffentlich zugängliche elektronische Kommunikationsnetze angeschlossen oder werden elektronische Kommunikationsdienste als Grundinfrastruktur genutzt, so sollten die einschlägigen Bestimmungen der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation), einschließlich der Vorschriften über Sicherheit, Datenverkehr, Standortdaten und Vertraulichkeit, zur Anwendung kommen.“* Dementsprechend wurde der Geltungsbereich der Datenschutzrichtlinie für elektronische Kommunikation (Artikel 3) um *„öffentliche[r] Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen“*, erweitert.

1.3 Ziele des Rahmens für Datenschutzfolgenabschätzungen

Mit der RFID-Empfehlung leitete die Europäische Kommission einen auf Datenschutzfolgenabschätzungen gerichteten Prozess ein, mit dem mehrere Ziele erreicht werden sollen:

- Ersten sollte eine Datenschutzfolgenabschätzung dem Grundsatz des „eingebauten Datenschutzes“ („Privacy by Design“) Rechnung tragen, indem sie den für die Verarbeitung Verantwortlichen hilft, sich vor der Einführung eines Produktes oder einer Dienstleistung um die damit verbundenen Datenschutzbelange zu kümmern. Dies nützt nicht nur dem Einzelnen, sondern auch den für die Verarbeitung Verantwortlichen, werden doch die hohen Kosten (und oft unbefriedigenden Lösungen) vermieden, zu denen es häufig kommt, wenn ein bereits eingeführtes Produkt auf Datenschutz „getrimmt“ werden muss.

⁶ Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

- Zweitens sollte eine Datenschutzfolgenabschätzung den für die Verarbeitung Verantwortlichen dabei helfen, Datenschutzrisiken auf umfassende Weise in Angriff zu nehmen, denn die Datenschutzfolgenabschätzung zählt zu den Instrumenten, mit deren Hilfe Datenschutzrisiken beurteilt sowie technische und organisatorische Lösungen zum Schutz personenbezogener Daten gegen unbefugte Weitergabe und unbefugten Zugang gefunden und die anderen Sicherheitspflichten nach Artikel 17 der Datenschutzrichtlinie und Artikel 4 der geänderten Richtlinie 2002/58/EG erfüllt werden können. Dieser Prozess bietet auch die Gelegenheit, für mehr Rechtssicherheit zu sorgen und dem Vertrauensverlust in der Öffentlichkeit vorzubeugen, dem der für die Verarbeitung Verantwortliche bei Vernachlässigung von Datenschutzaspekten möglicherweise ausgesetzt wäre.
- Schließlich können Datenschutzfolgenabschätzungen dazu beitragen, dass sowohl die für die Verarbeitung Verantwortlichen als auch die Datenschutzbehörden tiefere Einblicke in die Datenschutzaspekte von RFID-Anwendungen gewinnen. Die Durchführung einer Datenschutzfolgenabschätzung sollte den für die Verarbeitung Verantwortlichen dabei helfen, die in der Richtlinie 95/46/EG, der geänderten Richtlinie 2002/58/EG und der RFID-Empfehlung dargelegten Grundsätze zu verstehen und umzusetzen. Informationen aus Datenschutzfolgenabschätzungen können den Datenschutzbehörden dabei helfen, bewährte Verfahren zur Umsetzung der Datenschutzvorschriften in der Branche zu ermitteln, und in denjenigen Mitgliedstaaten, die eine Vorabprüfung (einiger oder aller) RFID-Anwendungen vorschreiben, den Prozess für die Datenschutzbehörden und die für die Verarbeitung Verantwortlichen vereinfachen⁷.

Außerdem ist die Datenschutzgruppe davon überzeugt, dass die Entwicklung von Datenschutzfolgenabschätzungen zur Stärkung der Wettbewerbsfähigkeit der europäischen RFID-Branche beiträgt, weil dadurch innovative Konzepte zur Bekämpfung von Datenschutzproblemen durch Technologien wie die Anonymisierung von Daten, die Teildeaktivierung von Tags, leichtgewichtige Kryptographie usw. gefördert werden.

Wenngleich der in der Empfehlung vorgesehene Rahmen für Datenschutzfolgenabschätzungen den Grundsatz der „eingebauten Sicherheit und Privatsphäre“ durch Prüfung von RFID-Anwendungen vor ihrer Einführung unterstützen soll, werden bereits heute viele RFID-Anwendungen eingesetzt. Die Datenschutzgruppe hofft, dass die Beteiligten diese Erfahrungen nutzen und die Gelegenheit ergreifen werden, um Bewertungsinstrumente für bestehende RFID-Anwendungen zu entwickeln.

1.4 Zusammenfassung des vorgeschlagenen Rahmens

Im vorgeschlagenen Rahmen erfolgt zunächst eine Klassifizierung von RFID-Anwendungen in vier möglichen Stufen. Für Anwendungen der Stufe 0, die hauptsächlich RFID-Anwendungen umfassen, die

⁷ In diesem Zusammenhang sieht Nummer 5 Buchstabe d der RFID-Empfehlung vor, dass die Betreiber ungeachtet ihrer sonstigen Verpflichtungen aus der Richtlinie 95/46/EG die Folgenabschätzung spätestens sechs Wochen vor Einführung der Anwendung der zuständigen Behörde zur Verfügung stellen. Auf welche Weise die Datenschutzfolgenabschätzung zur Verfügung zu stellen ist (z. B. auf Verlangen oder unaufgefordert), legen die Datenschutzbehörden der Mitgliedstaaten fest. Auf diese Weise können insbesondere die mit der Anwendung verbundenen Risiken sowie auch andere Faktoren, etwa ob ein Datenschutzbeauftragter bestellt ist oder nicht, berücksichtigt werden.

keine personenbezogenen Daten verarbeiten und deren RFID-Tags nur von Nutzern bearbeitet werden, sind keine Datenschutzfolgenabschätzungen vorgesehen. Obwohl der Begriff „Nutzer“ unter Umständen auch Mitarbeiter einschließen kann, lässt sich die Definition der Stufe 0 nur so verstehen, dass keine der Überwachung von Mitarbeitern dienenden Anwendungen darunter fallen, weil eine solche Überwachung irgendwo in der Anwendung die Speicherung von personenbezogenen Daten erfordern würde. Daher teilt die Datenschutzgruppe die Auffassung, dass es den Datenschutzzielen vermutlich nicht schadet, wenn Anwendungen der Stufe 0 von der Durchführung von Datenschutzfolgenabschätzungen ausgenommen werden.

Anwendungen der Stufe 1 sind Anwendungen, die keine personenbezogenen Daten verarbeiten, deren RFID-Tags jedoch von Einzelpersonen mitgeführt werden. Anwendungen der Stufe 2 sind Anwendungen, die personenbezogene Daten verarbeiten, deren RFID-Tags jedoch keine personenbezogenen Daten enthalten. Anwendungen der Stufe 3 sind schließlich Anwendungen, deren RFID-Tags personenbezogene Daten enthalten. Wie in Abschnitt 2.4 hervorgehoben wird, ist die Verwendung des Begriffs „personenbezogene Daten“ im vorgeschlagenen Rahmen missverständlich, soweit es um die im RFID-Tag enthaltenen Informationen geht.

Wird eine RFID-Anwendung in Stufe 1 oder höher eingestuft, muss der RFID-Anwendungsbetreiber eine aus vier Teilen bestehende Analyse der Anwendung durchführen, deren Detailtiefe im Verhältnis zu den erkannten Datenschutzfolgen steht. Im ersten Teil wird die RFID-Anwendung beschrieben. Im zweiten Teil können Kontroll- und Sicherheitsmaßnahmen hervorgehoben werden. Der dritte Teil befasst sich mit Informationen für Nutzer und deren Rechten. Im letzten Teil des vorgeschlagenen Rahmens für Datenschutzfolgenabschätzungen muss der RFID-Anwendungsbetreiber einschätzen, ob die RFID-Anwendung eingeführt werden kann oder nicht. Das Ergebnis der Datenschutzfolgenabschätzung ist ein Bericht, der der zuständigen Behörde vorgelegt wird.

Die Verfasser des vorgeschlagenen Rahmens für Datenschutzfolgenabschätzungen sehen zur Erleichterung seiner Anwendung vor, dass die Branche den Rahmen in sektorspezifischen Vorlagen umsetzen kann. In diesem Fall soll der Bericht zur Datenschutzfolgenabschätzung nicht auf dem allgemeinen Rahmen, sondern auf der sektorspezifischen Vorlage beruhen.

2 Analyse

Die Datenschutzgruppe erkennt die von den Verfassern des vorgeschlagenen Rahmens geleistete umfangreiche Arbeit an und pflichtet den in den einleitenden Abschnitten hervorgehobenen grundlegenden Zielen bei.

Während der vorgeschlagene Rahmen an sich keine speziellen Fragen aufwirft, hat die Datenschutzgruppe zu drei inhaltlichen Aspekten erhebliche Bedenken sowie einige Anmerkungen, die nachfolgend dargelegt werden.

2.1 Risikobewertung

In der Einleitung des vorgeschlagenen Rahmens heißt es unmissverständlich, dass der Prozess der Datenschutzfolgenabschätzung dazu dient, die mit einer RFID-Anwendung verbundenen

Datenschutzrisiken aufzudecken und die zur Bewältigung dieser Risiken unternommenen Schritte zu bewerten. **Doch dieser zentrale Grundsatz fehlt im Inhalt des vorgeschlagenen Rahmens.**

Während der vorgeschlagene Rahmen zwar vereinzelt Hinweise auf die Risikobewertung enthält (vornehmlich in den einleitenden Abschnitten), ist in keinem Abschnitt ausdrücklich vorgesehen, dass der RFID-Anwendungsbetreiber die mit einer RFID-Anwendung verbundenen Datenschutzrisiken ermitteln oder aufdecken muss. Daraus folgt, dass es nicht möglich ist, die zur Bewältigung dieser Risiken unternommenen Schritte zu bewerten. Stattdessen sieht der vorgeschlagene Rahmen lediglich vor, dass der RFID-Anwendungsbetreiber die verschiedenen zum Schutz der Privatsphäre und personenbezogener Daten in der RFID-Anwendung getroffenen Schutz- und Kontrollmaßnahmen auflistet. Dies kann nicht genügen, um dem RFID-Anwendungsbetreiber oder der zuständigen Behörde hinreichend zu gewährleisten, dass die vorgeschlagenen Maßnahmen angemessen sind bzw. im Verhältnis zu den Risiken stehen, weil diese Risiken gar nicht erst ermittelt worden sind.

Die Datenschutzgruppe bedauert zutiefst, dass die Verfasser des vorgeschlagenen Rahmens diesen Aspekt nicht berücksichtigt haben.

Ein Rahmen für Datenschutzfolgenabschätzungen sollte per definitionem eine allgemeine Methodik vorschlagen, die als wesentlichen Bestandteil eine Risikobewertungsphase enthält. In der RFID-Branche werden sicherlich bereits Risikobewertungen als Teil eines methodischen Ansatzes im Rahmen des Informationssicherheitsmanagements, wie etwa in ISO/IEC 27005⁸ und anderen nationalen oder internationalen Normen beschrieben, durchgeführt. Die Datenschutzgruppe ist davon überzeugt, dass die RFID-Branche auf diesem Erfahrungsschatz im herkömmlichen Informationssicherheitsmanagement aufbauen und den vorgeschlagenen Rahmen mit einem entsprechenden Risikobewertungskonzept bereichern könnte. Dies würde sich auch auf andere spezifische Elemente des vorgeschlagenen Rahmens auswirken, die insbesondere in den Abschnitten 2.2, 2.3 und 2.4 dieser Stellungnahme hervorgehoben werden.

Zudem wird in Erwägungsgrund 17 der RFID-Empfehlung ausgeführt, dass die Entwicklung des Rahmens für Datenschutzfolgenabschätzungen „gestützt auf bestehende Praktiken und Erfahrungen in den Mitgliedstaaten und in Drittländern sowie auf die Arbeiten der Europäischen Agentur für Netz- und Informationssicherheit (ENISA)“ erfolgen sollte. Damit sind die Autoren des vorgeschlagenen Rahmens zu Recht aufgefordert, die kürzlich von der ENISA angenommene Stellungnahme zum Rahmen für Datenschutzfolgenabschätzungen⁹ ernsthaft zu berücksichtigen und von der europäischen Agentur weitere Orientierungshilfen zur Umsetzung eines Risikobewertungskonzepts im RFID-Kontext anzufordern. Die ENISA hat sich insbesondere vorgenommen¹⁰, neu aufkommende und künftige Risiken eines besonderen IoT/RFID-Szenarios vor allem im Zusammenhang mit der diesbezüglichen Rolle der

⁸ Vgl. ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements

⁹ ENISA Opinion on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, Juli 2010, <http://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia> [deutsche Fassung liegt nicht vor – Anm. d. Ü.]

¹⁰ Siehe beispielsweise den ENISA-Bericht „Flying 2.0 – Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology“ [deutsche Fassung liegt nicht vor – Anm. d. Ü.]

ENISA gemäß der Mitteilung der Kommission „Internet der Dinge – ein Aktionsplan für Europa“¹¹ zu ermitteln und zu bewerten. **Die Datenschutzgruppe fordert die Branche nachdrücklich auf, diese Gelegenheit wahrzunehmen.**

2.2 Von Personen mitgeführte RFID-Tags

Eine der drei im *Arbeitspapier zu Datenschutzfragen im Zusammenhang mit der RFID-Technik* (WP 105)¹² geäußerten Befürchtungen „*ergibt sich aus dem Einsatz von RFID zur Verfolgung („Tracking“) einzelner Personen und zur Gewinnung personenbezogener Daten*“. Tatsächlich enthalten mit RFID-Tags versehene Gegenstände, die von Personen mitgeführt werden, eindeutige Kennungen, die mit entfernten Lesegeräten ausgelesen werden können. Diese eindeutigen Kennungen können wiederum dazu verwendet werden, die betreffende Person mit der Zeit zu erkennen und somit „identifizierbar“ zu machen. In machen Fällen kann dies wünschenswert sein, insbesondere wenn der mit einem RFID-Tag versehene Gegenstand ausdrücklich als Zugangskontrollmechanismus dienen soll (z. B. ein Mitarbeiterausweis). In anderen Fällen bietet dies jedoch die Möglichkeit, eine Person ohne ihr Wissen zu verfolgen¹³. Wie in der *Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“* (WP 136)¹⁴ hervorgehoben wird, fällt eine eindeutige Kennung, wenn sie mit einer Person verbunden ist, unter die Definition des Begriffs „personenbezogene Daten“ im Sinne der Richtlinie 95/46/EG, auch wenn die „soziale Identität“ der Person (Name, Anschrift usw.) unbekannt bleibt (sie ist also „identifizierbar“, muss aber nicht notwendigerweise „identifiziert“ werden).

Zudem kann die in einem RFID-Tag gespeicherte eindeutige Nummer auch dazu dienen, die Art der von einer Person mitgeführten Gegenstände mit entfernten Lesegeräten zu bestimmen, woraus sich wiederum Informationen über die soziale Stellung, die Gesundheit usw. ableiten lassen. Somit ist es also selbst in den Fällen, in denen ein RFID-Tag lediglich eine in einem bestimmten Kontext eindeutige Nummer und keine weiteren personenbezogenen Daten enthält, geboten, mögliche Datenschutz- und Sicherheitsaspekte sorgfältig zu erwägen, wenn der RFID-Tag von Personen mitgeführt werden soll.

Die Datenschutzgruppe begrüßt es, dass die Branche diesen Aspekt im Rahmen für Datenschutzfolgenabschätzungen berücksichtigt hat, indem sie eine Datenschutzfolgenabschätzung vorsieht, wenn sich mit RFID-Tags versehene Gegenstände im Besitz von Einzelpersonen befinden sollen (Anwendungen der Stufe 1).

Bedauerlicherweise verfolgt **der vorgeschlagene Rahmen** trotz dieser Prämisse dieses Anliegen nicht weiter und **versäumt es, den RFID-Anwendungsbetreiber ausdrücklich aufzufordern, Datenschutzprobleme, die auftreten können, wenn Einzelpersonen RFID-Tags täglich mit sich führen, zu beurteilen.** Es reicht nicht aus zu bedenken, ob der Aufenthaltsort von Einzelpersonen oder Nutzern durch die RFID-Anwendung überwacht wird¹⁵. **Es ist ebenfalls äußerst wichtig, das Risiko einer unbefugten Überwachung außerhalb der Anwendung zu analysieren.** Ferner versäumt es der Rahmen, die

¹¹ Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Internet der Dinge – ein Aktionsplan für Europa, KOM(2009) 278, Brüssel, 18.6.2009.

¹² Siehe Fußnote 2.

¹³ Vgl. die Beispiele in WP 105, Abschnitt 3.3.

¹⁴ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_de.pdf

¹⁵ Vgl. Abschnitt 2.3.4 des vorgeschlagenen Rahmens.

Schritte zur Bewältigung dieser Risiken zu beschreiben. **Die Datenschutzgruppe fordert die Branche nachdrücklich auf, diesem Aspekt Rechnung zu tragen, indem sie ihn im Rahmen als Teil eines überarbeiteten Risikobewertungskonzepts unmissverständlich aufgreift.**

2.3 RFID im Einzelhandel

Einer der wichtigsten Anwendungsbereiche, in denen es dazu kommen kann, dass RFID-Tags von Einzelpersonen mitgeführt werden, ist der Einzelhandel. Die RFID-Empfehlung stuft diesen Sektor als kritisch ein und befasst sich in einzelnen Punkten damit.

In Nummer 11 der RFID-Empfehlung heißt es ausdrücklich: *„Einzelhändler sollten die in ihrer Anwendung genutzten RFID-Tags am Verkaufsort deaktivieren oder entfernen, es sei denn, die Verbraucher stimmen [...] der weiteren Betriebsfähigkeit der RFID-Tags zu.“*

Nummer 12 gestattet folgende Ausnahme zu dieser Regel: *„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.“* Das bedeutet, dass die Deaktivierung am Verkaufsort die Regel ist, es sei denn, die Datenschutzfolgenabschätzung ergibt etwas anderes.

Nach Abschnitt D des vorgeschlagenen Rahmens sind bei einer Datenschutzfolgenabschätzung jedoch nur zwei Schlussfolgerungen möglich: Die RFID-Anwendung ist entweder einsatzreif („*Ready for deployment*“) oder nicht einsatzreif („*Not ready for deployment*“). Der RFID-Anwendungsbetreiber hat nicht die Möglichkeit, wie in der RFID-Empfehlung gefordert, bei Einzelhandelsanwendungen eine Schlussfolgerung zum Einsatz von RFID-Tags außerhalb des Verkaufsorts zu ziehen. Die Datenschutzgruppe weist darauf hin, dass es bei manchen Anwendungen gerechtfertigt oder erforderlich sein kann, dass einige RFID-Tags aus bestimmten Gründen auch außerhalb des Einzelhandelsverkaufsorts betriebsfähig bleiben. Da dies im vorgeschlagenen Rahmen nicht berücksichtigt wurde, ist jedoch offenbar vorgesehen, dass alle RFID-Tags am Verkaufsort deaktiviert werden sollen.

Allgemeiner ausgedrückt hat die Datenschutzgruppe den Eindruck, dass die in Abschnitt D des vorgeschlagenen Rahmens vorgegebene Wahl zwischen zwei Möglichkeiten den RFID-Anwendungsbetreiber und die RFID-Branche insgesamt unnötig einschränkt. Manche Anwendungen könnten etwa als „einsatzreif unter bestimmten Bedingungen“, die in den Schlussfolgerungen der Datenschutzfolgenabschätzungen zu erläutern wären, eingestuft werden.

Die Datenschutzgruppe fordert die Verfasser des vorgeschlagenen Rahmens auf, die Frage der Deaktivierung von RFID-Tags im Einzelhandel klarzustellen. Der vorgeschlagene Rahmen muss (bei Anwendungen im Einzelhandel) ausdrücklich vorsehen, dass der RFID-Anwendungsbetreiber im Bericht zur Datenschutzfolgenabschätzung auf Nummer 12 der RFID-Empfehlung eingeht. **Ein überarbeitetes Risikobewertungskonzept sollte also, allgemeiner ausgedrückt, die richtigen Instrumente vorsehen, die eine Schlussfolgerung zu den Bedingungen oder zum Einsatz einer RFID-Anwendung ermöglichen.**

2.4 Weitere Anmerkungen

Wie bereits in Abschnitt 2.2 hervorgehoben, enthält ein RFID-Tag, der von einer Person (einem Nutzer oder einer Einzelperson) mitgeführt wird und eine eindeutige Kennung¹⁶ enthält, per definitionem personenbezogene Daten. Streng genommen führen daher die in Abschnitt 1.5 des vorgeschlagenen Rahmens gegebenen Definitionen für Anwendungen der Stufen 1 und 0 in den meisten Fällen zu einem Widerspruch, denn man kann nicht sagen, dass die RFID-Anwendung *keine* personenbezogenen Daten verarbeitet, wenn die RFID-Tags von Einzelpersonen oder Nutzern mitgeführt werden. Diesen Definitionen zufolge wären die meisten Anwendungen somit in Stufe 2 einzuordnen. **Anwendungen der Stufen 0 oder 1 gäbe es demnach nur in seltenen Fällen, wenn RFID-Tags zwar von Personen mitgeführt werden, aber keine eindeutige Kennung besitzen.**

Die Datenschutzgruppe geht davon aus, dass die Verfasser des Rahmens nicht die Absicht hatten, die Anwendungen der Stufen 0 und 1 so eng zu fassen, und dass sich ihre Definitionen auf Anwendungen bezogen, die nur eine Art personenbezogener Daten verarbeiten, nämlich die eindeutige Kennung des RFID-Tags. Alle Definitionen der Anwendungsstufen lassen sich ohne weiteres so abändern, dass sie nicht mehr missverständlich sind. Zudem könnte die Festlegung einer geeigneten Risikobewertungsmethodik ebenfalls zu einer Neufassung dieser Definitionen führen.

Die Datenschutzgruppe stellt fest, dass im Rahmen von RFID-Tags die Rede ist, die sich *im Besitz* von Nutzern oder Einzelpersonen *befinden*. Dieser Begriff ist zu eng und sollte durch „mitführen“ ersetzt werden, weil damit die vorliegenden Risikoszenarios wesentlich besser erfasst werden.

Die Datenschutzgruppe ist der Auffassung, dass der im Rahmen vorgeschlagene Prozess der Datenschutzfolgenabschätzungen auch eine Konsultation der Beteiligten einschließen sollte, die eine Anhörung aller Seiten (Gruppen, Gewerkschaften, Verbände ...), auf die sich die RFID-Anwendung auswirken kann, sowie den Austausch von Ideen, Vorschlägen und Verbesserungen umfasst, die darauf gerichtet sind, dass die Anwendung offen und ohne datenschutzrechtliche Bedenken zum Nutzen des RFID-Betreibers und der beteiligten Nutzer bzw. Einzelpersonen eingesetzt werden kann. Eine solche Konsultationsphase ist ein sinnvoller Beitrag zu den in der RFID-Empfehlung vorgesehenen „*Informationen und Transparenz in Bezug auf die RFID-Nutzung*“ und „*Sensibilisierungsmaßnahmen*“.

Die Datenschutzgruppe betont ferner, dass für die rechtmäßige und sichere Verarbeitung besonderer Kategorien von Daten¹⁷ besondere Voraussetzungen erforderlich sind. Der Rahmen sollte den RFID-Anwendungsbetreibern genauere Orientierungshilfen zu den spezifischen Fragen im Zusammenhang mit der Verarbeitung besonderer Kategorien von Daten geben. Im Rahmen jedes Risikobewertungsprozesses sollte auch ermittelt werden, wie besondere Kategorien von Daten verwendet werden sollen.

Der Rahmen sollte die RFID-Anwendungsbetreiber auch dahingehend anleiten, zu welchem Zeitpunkt und unter welchen Bedingungen im Entwicklungszyklus eines RFID-Produkts eine Datenschutzfolgenabschätzung am besten durchzuführen ist, damit dem von der Empfehlung unterstützten Grundsatz der „*eingebauten Sicherheit und Privatsphäre*“ voll und ganz Rechnung getragen wird.

¹⁶ Als Kennung eines RFID-Tags bezeichnen wir jede eindeutige Kennnummer (oder Seriennummer), auf die im RFID-Tag zugegriffen werden kann und mit der ein RFID-Tag in einem bestimmten Kontext eindeutig bezeichnet werden kann.

¹⁷ Artikel 8 der Richtlinie 95/46/EG.

3 Fazit

Aufgrund der in dieser Stellungnahme aufgeführten Bedenken, insbesondere was das Fehlen eines klaren und umfassenden Konzeptes für Risikobewertungen im Hinblick auf den Datenschutz betrifft, **befürwortet die Datenschutzgruppe den vorgeschlagenen Rahmen in seiner vorliegenden Form nicht.**

Hervorzuheben ist, dass die Einbeziehung eines geeigneten Risikobewertungsprozesses wesentlich dazu beitragen kann, die meisten anderen in dieser Stellungnahme erkannten Probleme abzustellen. Wenn nämlich ein RFID-Anwendungsbetreiber zur Durchführung einer Risikobewertung verpflichtet wäre, würde er vor allem Risiken im Zusammenhang mit der unbefugten Überwachung von RFID-Tags, die von Personen mitgeführt werden, erkennen. Außerdem könnte sie im Einzelhandel eine gute Begründung dafür liefern, dass bestimmte (in speziellen Anwendungen verwendete) RFID-Tags, die *„nach Verlassen des Verkaufsorts betriebsfähig bleiben, wahrscheinlich keine Bedrohung für die Privatsphäre oder den Schutz personenbezogener Daten darstellen.“*

Die Datenschutzgruppe ist davon überzeugt, dass die Branche unter Berücksichtigung der in dieser Stellungnahme dargelegten Bedenken einen verbesserten Rahmen vorlegen kann, und wird jede Möglichkeit nutzen, einen Beitrag zur weiteren Verbesserung und raschen Verabschiedung des vorgeschlagenen Rahmens zu leisten.

Brüssel, den 13. Juli 2010

*Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM*