

Rahmen für die Folgenabschätzung in Bezug auf den Datenschutz und die Wahrung der Privatsphäre bei RFID-Anwendungen

11. Februar 2011

INHALT

1. Einleitung	3
1.1 Schlüsselbegriffe	4
1.2 Interne Verfahren	5
2. Der Prozess der Datenschutzfolgenabschätzung	6
2.1 Anfangsanalyse	7
2.2 Risikoabschätzung	9
3. Schlussbestimmung	12
ANHANG I: Merkmale der RFID-Anwendungsbeschreibung.....	14
ANHANG II: Datenschutzziele	15
ANHANG III: Datenschutzrisiken	17
ANHANG IV: Beispiele für RFID-Anwendungskontrollen und Folgenminderungsmaßnahmen 20	
Anlage A: Referenzdokumente	23
Anlage B: Glossar	25

1. Einleitung

Die Europäische Kommission („Kommission“) gab am 12. Mai 2009 eine Empfehlung zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen ab („RFID-Empfehlung“). Darin legte sie die Anforderung fest, dass ein von der Branche aufgestellter Folgenabschätzungsrahmen in Bezug auf den Datenschutz und die Wahrung der Privatsphäre bei RFID-Anwendungen von der Artikel-29-Datenschutzgruppe gebilligt werden sollte. Solche Bewertungen werden üblicherweise als Datenschutzfolgenabschätzungen (engl. *PIA*) bezeichnet. Der vorliegende Rahmen für die Datenschutzfolgenabschätzung bei RFID-Anwendungen („Rahmen“) entspricht dieser Anforderung.

Datenschutzfolgenabschätzungen für RFID-Anwendungen bieten zahlreiche Vorteile. Den RFID-Anwendungsbetreibern helfen sie u. a.

- die Einhaltung geltender Vorschriften und Vorgaben für den Datenschutz und die Wahrung der Privatsphäre zu erreichen und dauerhaft zu gewährleisten;
- mit Risiken für ihre Organisationen und ihre Nutzer umzugehen, die sich aus RFID-Anwendungen ergeben (sowohl bezüglich der Einhaltung der Datenschutzvorschriften als auch im Hinblick auf die öffentliche Wahrnehmung und das Vertrauen der Verbraucher);
- der Öffentlichkeit den Nutzen der RFID-Anwendungen zu erschließen und gleichzeitig die Wirksamkeit des „eingebauten Datenschutzes“ (*privacy by design*) schon in den frühen Phasen der Spezifizierung oder des Entwicklungsprozesses abzuschätzen.

Der Prozess der Datenschutzfolgenabschätzung beruht bezüglich der Wahrung der Privatsphäre und des Datenschutzes auf einem Risikomanagementansatz, in dessen Mittelpunkt die Umsetzung der RFID-Empfehlung der EU im Einklang mit dem EU-Rechtsrahmen und den bewährten Verfahren steht.

Der Prozess der Datenschutzfolgenabschätzung soll RFID-Anwendungsbetreibern helfen, die aus RFID-Anwendungen erwachsenden Risiken zu erkennen, ihre Wahrscheinlichkeit abzuschätzen und die unternommenen Schritte zur Bewältigung dieser Risiken zu dokumentieren. In Abhängigkeit davon, ob in den RFID-Anwendungen personenbezogene Informationen verarbeitet werden, können diese Folgen (soweit überhaupt vorhanden) recht unterschiedlich ausfallen. Der Rahmen für die Datenschutzfolgenabschätzung gibt RFID-Anwendungsbetreibern Orientierung im Hinblick auf Risikoabschätzungsmethoden und angemessene Maßnahmen, mit denen etwaige Folgen für den Datenschutz oder die Wahrung der Privatsphäre in effizienter, wirksamer und verhältnismäßiger Weise gemindert werden können.

Schließlich ist der Rahmen für die Datenschutzfolgenabschätzung hinreichend allgemein gehalten, damit er für alle RFID-Anwendungen anwendbar bleibt und es gleichzeitig erlaubt, Besonderheiten und spezifische Merkmale auf Sektoren- oder Anwendungsebene zu bewältigen.

Der Datenschutzfolgenabschätzungsrahmen ist Teil eines ganzen Umfelds von Informationssicherungs-, Datenmanagement- und Betriebsstandards, die gute Werkzeuge für den Umgang mit Daten in RFID- und anderen Anwendungen bereitstellen. Der vorliegende Rahmen könnte als Ausgangspunkt für die Ausarbeitung von branchen-, sektor- und/oder anwendungsorientierten Mustern für Datenschutzfolgenabschätzungen dienen. Wie bei der Umsetzung jedes Grundsatzpapiers könnte es sich als notwendig erweisen, verwendete Begriffe klarzustellen und – gestützt auf praktische Erfahrungen – Orientierungen zum weiteren Vorgehen zu geben, um so die Umsetzung zu erleichtern.

1.1 Schlüsselbegriffe

Zahlreiche Schlüsselbegriffe, die in diesem Rahmen benutzt werden, erfordern eine nähere Erläuterung. **RFID** ist eine Technik, bei der elektromagnetische Wellen zur Kommunikation mit RFID-Tags eingesetzt werden und die die Möglichkeit bietet, die eindeutige Kennung des RFID-Tags oder eventuell andere darin gespeicherte Informationen auszulesen. **RFID-Tags** sind normalerweise klein und können vielfältige Formen haben, bestehen aber oft aus einem auslesbaren und eventuell beschreibbaren elektronischen Speicher und einer Antenne. **RFID-Lesegeräte** werden benutzt, um die in RFID-Tags gespeicherten Informationen auszulesen.

RFID-Anwendungen verarbeiten Informationen, die durch das Zusammenwirken von RFID-Tags und RFID-Lesegeräten entstehen. Solche Anwendungen werden von einem oder mehreren **RFID-Anwendungsbetreibern** betrieben und von Back-End-Systemen und vernetzten Kommunikationsinfrastrukturen unterstützt. Trifft ein RFID-Anwendungsbetreiber Entscheidungen in Bezug auf die Sammlung oder Verwendung personenbezogener Daten, so kann seine Rolle der des für die Datenverarbeitung Verantwortlichen im Sinne der Richtlinie 95/45/EG ähneln; er wäre dann eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel des Betriebs einer RFID-Anwendung, die sich auf personenbezogene Daten auswirkt, entscheidet.

Im Zusammenhang mit der RFID-Technik gilt folgende Taxonomie:

- Eine **Datenschutzfolgenabschätzung** ist ein Prozess, bei dem eine bewusste und systematische Bewertung der Auswirkungen einer konkreten RFID-Anwendung auf die Privatsphäre und den Datenschutz vorgenommen wird, um geeignete Maßnahmen zur Vermeidung oder zumindest zu Minimierung dieser Auswirkungen zu treffen.
- Der **Rahmen** enthält Vorgaben in Bezug auf die mit Datenschutzfolgenabschätzungen für RFID-Anwendungen zu erreichenden Ziele, die in den Folgenabschätzungen zu betrachtenden RFID-Anwendungen sowie den gemeinsamen Aufbau und Inhalt der Berichte über Datenschutzfolgenabschätzungen für RFID-Anwendungen.
- Ein **Bericht über die Datenschutzfolgenabschätzung** ist die Unterlage, die als Ergebnis des Prozesses der Datenschutzfolgenabschätzung den zuständigen Behörden zur Verfügung gestellt wird. Bevor der Datenschutzfolgenabschätzungsbericht extern (z. B. den zuständigen Behörden) zugänglich gemacht wird, können unternehmensinterne oder sicherheitsrelevante Informationen daraus entfernt werden, sofern die Informationen keinen besonderen Bezug zu den Folgen für die Privatsphäre und den Datenschutz aufweisen. Die Mitgliedstaaten bestimmen die Art und Weise, wie der Datenschutzfolgenabschätzungsbericht zur Verfügung zu stellen ist (z. B. auf Anfrage oder nicht). Dabei können sie insbesondere die Verwendung besonderer Datenkategorien sowie andere Faktoren wie die Existenz eines Datenschutzbeauftragten berücksichtigen.
- **Muster für Datenschutzfolgenabschätzungen** können ausgehend vom Rahmen erarbeitet werden, um branchen- oder anwendungsorientierte oder sonstige besondere Vorlagen für Datenschutzfolgenabschätzungen und die daraus resultierenden Berichte bereitzustellen.

Diese und weitere Begriffe wie **Nutzer** oder **Person** werden für die Zwecke dieses Rahmens für die Datenschutzfolgenabschätzung in *Anlage B: Glossar* näher erläutert. Ebenfalls aufgenommen wurden Begriffe aus der Richtlinie 95/46/EG, die sich auf den Datenschutz beziehen.

Die Durchführung von Datenschutzfolgenabschätzungen und die Berichterstattung hierüber sind Verpflichtungen, die zusätzlich zu den sonstigen Pflichten gelten, die dem RFID-Anwendungsbetreiber durch besondere Rechtsvorschriften, Regelungen oder andere verbindliche Vereinbarungen auferlegt werden.

1.2 Interne Verfahren

RFID-Anwendungsbetreiber sollten über eigene interne Verfahren für die Durchführung von Datenschutzfolgenabschätzungen verfügen, insbesondere für die

- *zeitliche Planung des Prozesses der Datenschutzfolgenabschätzung*, damit ausreichend Zeit für ggf. notwendige Anpassungen der RFID-Anwendung und die Übermittlung des Berichts an die zuständige Behörde spätestens sechs Wochen vor dem Einsatz zur Verfügung steht;
- *interne Überprüfung des Prozesses der Datenschutzfolgenabschätzung (einschließlich Anfangsanalyse) und der entsprechenden Berichte* auf ihre Übereinstimmung mit der sonstigen Dokumentation über die RFID-Anwendung wie Dokumentationssystem, Produktunterlagen, Beispiele für Produktverpackungen und die Implementierung der RFID-Tags. Die interne Überprüfung sollte einen Rückmeldungszyklus ermöglichen, damit auf Folgen eingegangen werden kann, die erst nach Einführung der Anwendung bekannt werden, und damit die Ergebnisse früherer Datenschutzfolgenabschätzungen berücksichtigt werden können.
- Sammlung von Nachweisen (darunter beispielsweise Ergebnisse von Sicherheitsüberprüfungen, Kontrollaufbauten und Hinweiskopien) als Belege dafür, dass der RFID-Anwendungsbetreiber seinen Verpflichtungen nachgekommen ist.
- *Festlegung der Personen oder Funktionen innerhalb der Organisation mit Befugnissen für einschlägige Tätigkeiten der Datenschutzfolgenabschätzung* (z. B. Abschluss der Anfangsanalyse und des Berichts, Unterzeichnung des Berichts über die Datenschutzfolgenabschätzung, Führung der einschlägigen Unterlagen sowie die etwaige Aufgabenteilung für diese Funktionen).
- *Festlegung von Kriterien für die Bewertung und Dokumentation, ob die Anwendung einführungsbereit ist oder nicht*, entsprechend dem Rahmen und etwaigen Mustern für die Datenschutzfolgenabschätzung.
- *Betrachtung/Festlegung von Faktoren, die eine neue oder überarbeitete Datenschutzfolgenabschätzung erforderlich machen*. Solche Kriterien wären: beträchtliche Änderungen in der RFID-Anwendung, beispielsweise materielle Änderungen, die den ursprünglichen Zweck erweitern (d. h. auf sekundäre Zwecke); verarbeitete Informationstypen; Verwendungen der Informationen, welche die eingesetzten Kontrollen schwächen; eine unerwartete Verletzung des Schutzes personenbezogener Daten¹ mit gravierenden Auswirkungen, die in der ersten Datenschutzfolgenabschätzung nicht als verbleibende Risiken der Anwendung erfasst waren; Festlegung einer Zeitspanne für die regelmäßige Überprüfung; Reaktion auf wesentliche oder bedeutsame Rückmeldungen oder Aufträge interner oder externer Beteiligter; Beträchtliche technische Änderungen, die sich auf die von der betreffenden RFID-Anwendung ausgehenden Folgen für die Privatsphäre und den Datenschutz auswirken. Materielle Änderungen, die den Umfang der Datensammlung oder -verwendung einschränken, würden dagegen von sich aus keine Überarbeitung der Datenschutzfolgenabschätzung erforderlich machen. Im gesamten Lebenszyklus

¹ In diesem Fall gilt die Begriffsbestimmung in der Richtlinie 2009/136/EG zur Änderung der Richtlinie 2002/58/EG, siehe S. 29:
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:DE:PDF>

der RFID-Anwendung wäre eine neue oder überarbeitete Datenschutzfolgenabschätzung stets dann notwendig, wenn sich die im Abschnitt zur Anfangsanalyse beschriebene Ebene der RFID-Anwendung ändert.

- *Konsultation der Interessengruppen.* Stellungnahmen und Rückmeldungen aus den einschlägigen Interessengruppen in Bezug auf die betreffende RFID-Anwendung sollten als Teil der Überprüfung der Datenschutzfolgenabschätzung auf mögliche Fragen und Probleme berücksichtigt werden. Die Konsultationen sollten der Größenordnung, dem Umfang, der Art und der Ebene der RFID-Anwendung angemessen sein. Innerhalb von Unternehmen werden Einzelpersonen als Beauftragte für die Überwachung und Sicherung des Datenschutzes in der Organisation bzw. Abteilung eingesetzt. Diese Personen sind wesentliche Teilnehmer des Prozesses der Datenschutzfolgenabschätzung, da sie an der konkreten RFID-Anwendung oder deren Beaufsichtigung beteiligt sind. Mitarbeiter mit Kenntnissen in Technik, Marketing oder anderen Gebieten können je nach Art der RFID-Anwendung und ihrer Beziehung dazu ebenfalls benötigte Teilnehmer des Prozesses sein. RFID-Betreiber können über einen Konsultationsmechanismus verfügen, mit dessen Hilfe externe Akteure (Einzelpersonen, Organisationen oder Behörden) mit ihnen zusammenwirken und Rückmeldungen geben können. Die RFID-Betreiber sollten – soweit dies zweckmäßig ist – Konsultationsmechanismen nutzen, um Äußerungen von Interessengruppen einzuholen, die Personen vertreten, deren Privatsphäre direkt von den Vorschlägen betroffen ist, z. B. Mitarbeiter und Kunden des RFID-Betreibers.

2. Der Prozess der Datenschutzfolgenabschätzung

Der Rahmen soll RFID-Anwendungsbetreibern – wie in der Empfehlung verlangt – Orientierung für die Durchführung von Datenschutzfolgenabschätzungen für konkrete RFID-Anwendungen geben sowie den gemeinsamen organisatorischen Aufbau und die Inhaltskategorien der Berichte über die Datenschutzfolgenabschätzung festlegen, in denen die Ergebnisse solcher Datenschutzfolgenabschätzungen dokumentiert werden müssen. Da viele RFID-Anwendungsbetreiber in bestimmten Sektoren den Einsatz gleicher oder ähnlicher RFID-Anwendungen erwägen können, bildet der Rahmen überdies die Grundlage für die Ausarbeitung von Mustern für Datenschutzfolgenabschätzungen für bestimmte Anwendungen oder Wirtschaftssektoren. Solche Folgenabschätzungsmuster können diesen Sektoren helfen, Datenschutzfolgenabschätzungen durchzuführen und die daraus resultierenden Berichte für solche ähnlichen RFID-Anwendungen effizienter zu erstellen². Da gemeinsame RFID-Anwendungen in mehreren Mitgliedstaaten angeboten werden können, dient der Rahmen auch der Harmonisierung der Anforderungen an RFID-Anwendungsbetreiber entsprechend den örtlich geltenden Rechtsvorschriften, Regelungen oder anderen verbindlichen Vereinbarungen.

Der Rahmen behandelt den Prozess der Durchführung von Datenschutzfolgenabschätzungen für RFID-Anwendungen vor deren Einführung und legt den Umfang der daraus resultierenden Berichte fest³.

RFID-Anwendungsbetreiber müssen für jede von ihnen betriebene RFID-Anwendung eine Datenschutzfolgenabschätzung durchführen. Führen sie mehrere miteinander zusammenhängende RFID-Anwendungen (möglicherweise im gleichen Umfeld oder in den

² Das Konzept einer gegenseitigen oder mehrfachen stellen- und sektorenübergreifenden Anerkennung zwecks Einführung zuvor geprüfter RFID-Anwendungen sollte untersucht werden.

³ Nummer 5 Buchstabe a der Empfehlung der Europäischen Kommission vom 12. Mai 2009 zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen, K(2009) 3200 endg.

gleichen Räumen) ein, brauchen sie nur einen Folgenabschätzungsbericht anzufertigen, falls in dem Bericht die Grenzen und Unterschiede zwischen den Anwendungen ausdrücklich dargelegt werden. Wenn RFID-Anwendungsbetreiber eine RFID-Anwendung auf gleiche Weise für mehrere Produkte, Dienste oder Prozesse wiederverwenden, brauchen sie nur einen Folgenabschätzungsbericht für alle ähnlichen Produkte, Dienste oder Prozesse anzufertigen (z. B. ein Fahrzeughersteller, der die gleiche Diebstahlsicherung in allen Fahrzeugen unter gleichen Betriebsbedingungen einsetzt). Die Durchführung von Datenschutzfolgenabschätzungen und die Berichterstattung hierüber sind Verpflichtungen, die zusätzlich zu den sonstigen Pflichten gelten, die dem RFID-Anwendungsbetreiber durch besondere Rechtsvorschriften, Regelungen oder andere verbindliche Vereinbarungen auferlegt werden.

Der Prozess der Datenschutzfolgenabschätzung besteht aus zwei Phasen:

1. **Anfangsanalyse:** der RFID-Anwendungsbetreiber stellt anhand der hier genannten Schritte fest,
 - a) ob für seine RFID-Anwendung eine Datenschutzfolgenabschätzung erforderlich ist oder nicht,
 - b) ob eine vollständige oder eine vereinfachte Datenschutzfolgenabschätzung erforderlich ist.
2. **Risikoabschätzung:** Darlegung der Kriterien und Elemente für vollständige und vereinfachte Datenschutzfolgenabschätzungen.

2.1 Anfangsanalyse

Als Voraussetzung für die Durchführung einer Datenschutzfolgenabschätzung für eine konkrete Anwendung muss jede Organisation zunächst einmal verstehen, wie ein solcher Prozess in Abhängigkeit von der Art und Sensibilität der verarbeiteten Daten, der Art der Verarbeitung oder des Umgangs mit Informationen unter ihrer Verantwortung und dem Typ der fraglichen RFID-Anwendung umzusetzen ist. Denjenigen Organisationen, die bereits Prozesse für Datenschutz-Risikoabschätzungen für andere Anwendungen haben, dürften die vorhandenen Klassifizierungskriterien und Prozessschritte helfen, ihre bestehenden Prozesse in den vorliegenden Rahmen einzuordnen.

Zur Durchführung der Anfangsanalyse muss ein RFID-Anwendungsbetreiber den Entscheidungsablauf in Abbildung 1 absolvieren. Dies hilft dem RFID-Anwendungsbetreiber bei der Feststellung, ob und in welchem Umfang für die betreffende RFID-Anwendung eine Datenschutzfolgenabschätzung erforderlich ist.

Die sich daraus ergebende Ebene der Anfangsanalyse ist auch bei der Bestimmung der notwendigen Ausführlichkeit für die Risikoabschätzung (d. h. entweder vollständige oder vereinfachte Datenschutzfolgenabschätzung) hilfreich.

Diese Anfangsanalyse muss dokumentiert und den Datenschutzbehörden auf Anfrage vorgelegt werden. Hinweise zur Dokumentation sind Anhang I zu entnehmen.

Vollständige Datenschutzfolgenabschätzung

Eine vollständige Datenschutzfolgenabschätzung ist erforderlich für Anwendungen, die entsprechend der Anfangsanalyse (Abschnitt 2.1) in Ebene 2 oder Ebene 3 eingestuft werden. Zu solchen Anwendungen, die eine vollständige Folgenabschätzung erfordern, gehören beispielsweise Anwendungen, die personenbezogene Daten verarbeiten (Ebene 2) oder bei denen RFID-Tags personenbezogene Daten enthalten (Ebene 3). Die Ebenen 2 und 3 führen zwar zu einer vollständigen Datenschutzfolgenabschätzung, sie beziehen sich

aber auf unterschiedliche Risikoumfelder und erfordern unterschiedliche Folgenminderungsstrategien. Beispielsweise können Anwendungen der Ebene 2 Schutzvorrichtungen für Back-End-Daten haben, während Anwendungen der Ebene 3 Schutzvorrichtungen sowohl für Back-End-Daten als auch Tag-Daten haben können. Anhand weiterer Erfahrungen kann die Branche diese Ebenen und ihre Auswirkungen auf den Prozess der Folgenabschätzung noch präzisieren. Da die Anwendung personenbezogene Daten verarbeitet, ist eine sehr ausführliche (vollständige) Folgenabschätzung erforderlich, um sicherzustellen, dass geeignete Folgenminderungsmaßnahmen ausgearbeitet werden. Dies hilft dem RFID-Anwendungsbetreiber bei der Ermittlung der bestehenden Risiken und der Entwicklung angemessener Kontrollmaßnahmen. In diesem Zusammenhang sollten die Betreiber auch darüber nachdenken, inwiefern sich die im RFID-Tag enthaltenen Informationen über den ursprünglichen, vom Einzelnen noch überschauten Zweck oder Anwendungszusammenhang für andere Verwendungen eignen, insbesondere wenn sie benutzt werden könnten, um personenbezogene Daten zu verarbeiten oder zu verknüpfen, und ob eine neue Datenschutzfolgenabschätzung erforderlich ist oder andere folgenmindernde Kontrollmaßnahmen getroffen werden sollten.

Vereinfachte Datenschutzfolgenabschätzung

Vereinfachte Datenschutzfolgenabschätzungen durchlaufen den gleichen Prozess wie vollständige Folgenabschätzungen, ihr Umfang und ihre Ausführlichkeit sind angesichts des niedrigeren Risikoprofils aber sowohl bei der Untersuchung als auch der Berichterstattung geringer als bei vollständigen Datenschutzfolgenabschätzungen. Vereinfachte Datenschutzfolgenabschätzungen kommen für Anwendungen der Ebene 1 in Betracht. Eine vereinfachte Datenschutzfolgenabschätzung durchläuft zwar einen ähnlichen Prozess wie die vollständige Folgenabschätzung, da die einschlägigen Risiken einer Anwendung der Ebene 1 geringer sind als in den Ebenen 2 und 3, sind aber die erforderlichen Kontrollmaßnahmen und die entsprechende Dokumentation im Bericht über die Datenschutzfolgenabschätzung vereinfacht.

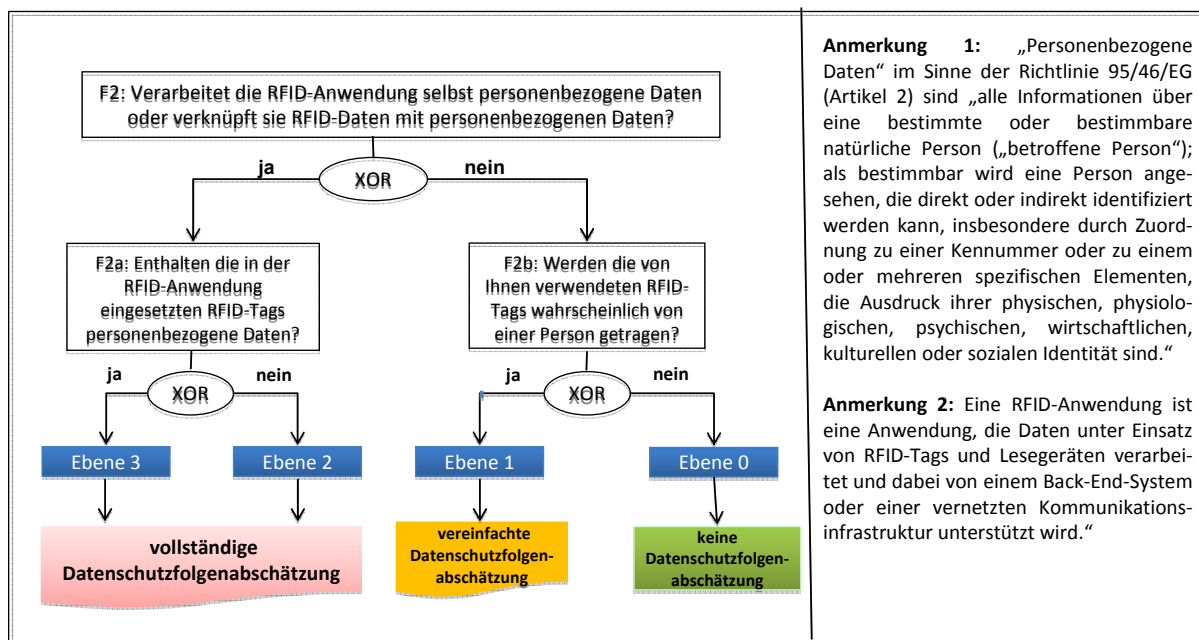


Abbildung 1: Entscheidungsablauf, ob und auf welcher Detailebene eine Datenschutzfolgenabschätzung durchzuführen ist

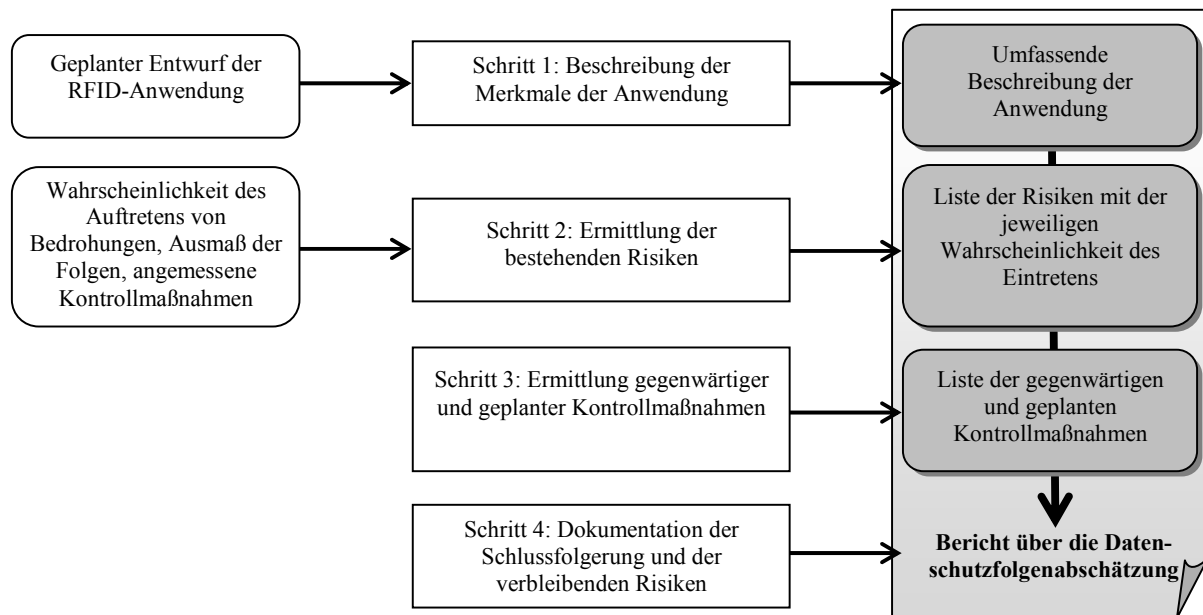
2.2 Risikoabschätzung

Das Ziel einer Risikoabschätzung besteht darin, (in einer möglichst frühen Phase der Systementwicklung) die von einer RFID-Anwendung ausgehenden Datenschutzrisiken zu ermitteln und zu dokumentieren, wie diese Risiken *auf proaktive Weise* durch technische und organisatorische Kontrollmaßnahmen gemindert werden können. Auf diese Weise spielt die Datenschutzfolgenabschätzung einerseits eine wichtige Rolle bei der Einhaltung der Datenschutzvorschriften (Richtlinie 95/46/EG) und erlaubt andererseits die Beurteilung der Wirksamkeit der Verfahren zur Risikominderung. Zur Einsparung von Zeit und Kosten wird empfohlen, die Risikoabschätzung rechtzeitig vor dem Treffen der endgültigen Entscheidungen über die Architektur einer RFID-Anwendung durchzuführen, damit Strategien zur technischen Minderung der Datenschutzrisiken in den Systementwurf eingebettet werden können und nicht erst später „aufgesetzt“ werden müssen.

Im Prozess der Risikoabschätzung werden normalerweise in erster Linie die Risiken einer RFID-Anwendung betrachtet, die sich aus der Wahrscheinlichkeit und dem Ausmaß der von ihr möglicherweise verursachten Folgen ergeben. Die RFID-Anwendungsbetreiber sind gut beraten, die Datenschutzziele der EU-Richtlinie als Ausgangspunkt für ihre Risikoabschätzung zu nehmen (siehe Anhang II). Es können hohe Risiken bestehen, weil die RFID-Anwendung für bösartige Angriffe anfällig sein könnte oder weil in der Organisation bzw. im Umfeld keine Datenschutzkontrollen existieren. Die Datenschutzrisiken können aber auch gering sein, und zwar einfach deshalb, weil in der Organisation oder im betreffenden Umfeld Datenschutzfolgen unwahrscheinlich sind oder weil die RFID-Anwendung bereits in einer hochgradig datenschutzfreundlichen Weise konfiguriert ist. Im Prozess der Datenschutzfolgenabschätzung soll auf alle potenziellen Risiken eingegangen und deren Ausmaß, Wahrscheinlichkeit und Minderungspotenzial betrachtet werden. Das Ergebnis dieser Überlegungen ist die Feststellung jener Datenschutzrisiken, die für die konkrete Einführung der RFID-Anwendung der Organisation von Bedeutung sind und denen mit wirksamen Kontrollmaßnahmen begegnet werden muss.

Im Zuge der (in Abbildung 2 dargestellten) Datenschutzfolgenabschätzung muss der RFID-Anwendungsbetreiber

1. die RFID-Anwendung beschreiben;
2. ermitteln und auflisten, inwiefern von der geprüften RFID-Anwendung eine Gefahr für den Datenschutz ausgehen könnte, sowie das Ausmaß und die Wahrscheinlichkeit dieser Risiken abschätzen;
3. gegenwärtige und geplante technische und organisatorische Kontrollmaßnahmen zur Minderung der festgestellten Risiken dokumentieren;
4. die Lösung (Ergebnis der Analyse) für die Anwendung dokumentieren.



Schritt 1: Merkmale der Anwendung

Die Beschreibung der Merkmale der Anwendung sollte ein umfassendes und vollständiges Bild der Anwendung, ihres Umfelds und der Systemgrenzen ergeben. Zu beschreiben sind darin der Anwendungsentwurf, die entsprechenden Schnittstellen zu anderen Systemen und die Informationsflüsse. Zur Visualisierung der Informationsflüsse werden Datenflussdiagramme empfohlen, aus denen die Verarbeitung der primären und sekundären Daten ersichtlich ist. Auch die Datenstrukturen müssen dokumentiert werden, damit potenzielle Verbindungen analysiert werden können. In Anhang I sind die Elemente zusammengefasst, die die Merkmale einer RFID-Anwendung für die Zwecke der Datenschutzfolgenabschätzung beschreiben.

Darüber hinaus wird empfohlen, Angaben zum betrieblichen und strategischen Umfeld der Anwendung zu machen. Dazu gehören beispielsweise die unmittelbare und längerfristige Aufgabe des Systems, die an der Informationssammlung Beteiligten, Funktionsanforderungen, alle potenziellen Nutzer und eine Beschreibung der Architektur und Datenflüsse der RFID-Anwendung (insbesondere Schnittstellen zu externen Systemen, die personenbezogene Daten verarbeiten können).

Schritt 2: Ermittlung der Risiken

In diesem Schritt geht es um die Ermittlung von Umständen, die zu einer Gefährdung oder Beeinträchtigung personenbezogener Daten führen können, wobei die EU-Richtlinie als Richtschnur für wichtige, zu erreichende Datenschutzziele dient. Risiken können sich ergeben aus den Komponenten der RFID-Anwendungen, dem Betrieb (Infrastruktur für die Erfassung, Speicherung und Verarbeitung) sowie dem Umfeld für die gemeinsame Nutzung und weitere Verarbeitung, in die die Anwendung eingebettet ist.

Anhang III enthält eine Liste möglicher Datenschutzrisiken. Sie dient als Orientierung für eine systematische Ermittlung potenzieller Risiken, die den Zielen der EU-Richtlinie (Anhang II) entgegenstehen.

Zusätzlich zur Feststellung der Risiken erfordert die Datenschutzfolgenabschätzung auch eine relative Quantifizierung dieser Risiken. Ein RFID-Anwendungsbetreiber sollte unter dem Gesichtspunkt des Grundsatzes der Verhältnismäßigkeit und unter angemessenen Bedingungen erwägen, wie hoch die *Wahrscheinlichkeit* ist, dass Datenschutzrisiken

tatsächlich eintreten. Risiken können innerhalb sowie gegebenenfalls auch außerhalb der betreffenden konkreten RFID-Anwendung auftreten. Diese Risiken können sich sowohl aus wahrscheinlichen Nutzungen als auch aus möglichen Missbräuchen der Informationen ergeben, insbesondere auch dann, wenn die für die RFID-Anwendung benutzten RFID-Tags im Besitz von Personen betriebsfähig bleiben.

Die Risikoabschätzung erfordert die Beurteilung der jeweiligen Risiken aus Sicht des Datenschutzes. Der RFID-Betreiber sollte Folgendes beurteilen:

1. Risikohöhe und Eintrittswahrscheinlichkeit,
2. Ausmaß der Folgen bei Eintritt des Risikos.

Die daraus resultierende Risikoebene kann als niedrig, mittel oder hoch eingestuft werden.

Ein Risiko, das bislang im Mittelpunkt der Debatte steht, erwächst daraus, dass RFID-Tags benutzt werden könnten, um Persönlichkeits- oder Bewegungsprofile von Personen zu erstellen. In diesen Fällen würden die im RFID-Tag gespeicherten Informationen (vor allem ihre Kennungen) benutzt, um eine bestimmte Person wiederzuerkennen. Einzelhändler, die RFID-Tags an ihre Kunden weitergeben, ohne diese an der Kasse automatisch zu deaktivieren oder zu entfernen, *könnten* ein solches Risiko unbeabsichtigt herbeiführen. Eine wichtige Frage ist daher, ob dieses Risiko wahrscheinlich ist und als *unausweichliches* Risiko tatsächlich eintritt oder nicht. Laut Nummer 11 der RFID-Empfehlung sollten Einzelhändler die in ihrer Anwendung genutzten RFID-Tags am Verkaufsort deaktivieren oder entfernen, es sei denn, die Verbraucher stimmen nach Aufklärung entsprechend diesem Rahmen der weiteren Betriebsfähigkeit der RFID-Tags zu. Einzelhändler sind nicht zur Deaktivierung oder Entfernung der Tags verpflichtet, 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 im Sinne von Nummer 12 der RFID-Empfehlung darstellen. 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.

Auf die Risikoermittlung kann ausführlicher in sektorspezifischen Mustern eingegangen werden, die auf der Grundlage dieses Rahmens nach und nach für die Verwendung in den verschiedenen Branchen aufgestellt werden können.

Schritt 3: Ermittlung und Empfehlung von Kontrollmaßnahmen

In diesem Schritt geht es um die Analyse der Kontrollmaßnahmen, die implementiert wurden oder geplant sind, um die festgestellten Datenschutzrisiken zu minimieren, zu vermindern oder zu beseitigen.

Kontrollmaßnahmen können entweder technischer oder nichttechnischer Art sein. Ihre Integration in die Anwendung erfolgt durch architektonische Entscheidungen oder durch technisch durchsetzbare Vorgaben, z. B. durch Standardeinstellungen, Authentifizierungsmechanismen und Verschlüsselungsmethoden. Bei nichttechnischen Kontrollmaßnahmen handelt es sich dagegen um Management- und Betriebskontrollen, beispielsweise in Form betrieblicher Verfahren. Kontrollmaßnahmen können als präventiv oder erkennend eingestuft werden. Präventive Maßnahmen verhindern Verletzungsversuche, während erkennende Maßnahmen vor Verletzungen und Verletzungsversuchen warnen.

Überdies kann es „natürliche“ Kontrollen geben, die aus dem Umfeld heraus entstehen. Wenn z. B. keine Lesegeräte angebracht sind, die Objekte oder Personen verfolgen könnten (weil daran kein geschäftliches Interesse besteht), dann erwächst hieraus auch kein (plausibles) Risiko.

Die Entscheidung darüber, welche der festgestellten Kontrollmaßnahmen zweckmäßig sind und daher implementiert werden müssen, sollte aufgrund der ermittelten Risiken und der damit verbundenen Risikoebene getroffen werden. Aus den Unterlagen über die Datenschutzfolgenabschätzung sollte ersichtlich sein, inwiefern sich die Kontrollmaßnahmen auf konkrete Risiken beziehen und wie mit Hilfe der Gegenmaßnahmen ein annehmbares Risikoniveau erreicht wird.

Beispiele für Kontrollmaßnahmen sind in Anhang IV aufgeführt.

Schritt 4: Dokumentation der Schlussfolgerung und der verbleibenden Risiken

Nach Abschluss der Risikoabschätzung sollten im Bericht über die Datenschutzfolgenabschätzung die endgültige Schlussfolgerung über die Anwendung dokumentiert werden, ergänzt durch weitere Bemerkungen über Risiken, Kontrollen und verbleibende Risiken.

- Eine RFID-Anwendung wird für den Betrieb freigegeben, sobald der Prozess der Datenschutzfolgenabschätzung abgeschlossen ist, in dem die betreffenden Risiken ermittelt und geeignete Folgenminderungsmaßnahmen getroffen wurden, damit keine erheblichen Restrisiken verbleiben und somit den einschlägigen Vorschriften entsprochen wird, wobei angemessene interne Prüfungen und Abnahmen stattfinden.
- Wird eine RFID-Anwendung in ihrem derzeitigen Zustand nicht für den Betrieb freigegeben, muss ein konkreter Plan für Abhilfemaßnahmen aufgestellt werden; anschließend muss eine neue Datenschutzfolgenabschätzung durchgeführt werden, um festzustellen, ob die Anwendung dadurch einen Zustand erreicht hat, der eine Freigabe ermöglicht.

In der Schlussfolgerung sollten folgende Angaben enthalten sein:

- Name der unterzeichnenden Person,
- Funktionsbezeichnung der Person,
- Datum der Schlussfolgerung.

Bericht über die Datenschutzfolgenabschätzung

Datenschutzfolgenabschätzungen sind interne Prozesse, die sensible Informationen beinhalten und sich auf die Sicherheit, aber auch möglicherweise vertrauliche oder unternehmensinterne Informationen über Produkte oder Verfahren auswirken. Unter Beachtung dessen sollten Berichte über Datenschutzfolgenabschätzungen normalerweise Folgendes enthalten:

1. die Beschreibung der RFID-Anwendung entsprechend Anhang I,
2. die Dokumentation der oben erläuterten vier Schritte.

Der unterzeichnete Bericht über die Datenschutzfolgenabschätzung mit der gebilligten Schlussfolgerung sollte entsprechend den internen Verfahren des RFID-Anwendungsbetreibers dem benannten Datenschutzbeauftragten des Unternehmens übergeben werden. Die Vorlage dieses Berichts erfolgt unbeschadet der aus der Richtlinie 95/46/EG erwachsenen Pflichten der für die Datenverarbeitung Verantwortlichen, vor allem der davon unabhängigen Meldepflicht gegenüber der zuständigen Kontrollstelle gemäß Abschnitt IX der Richtlinie 95/46/EG.

3. Schlussbestimmung

Der Rahmen für die Datenschutzfolgenabschätzung tritt spätestens 6 Monate nach seiner Veröffentlichung und Billigung durch die Artikel-29-Datenschutzgruppe in Kraft. Für zum

Zeitpunkt des Inkrafttretens des Rahmens bereits bestehende RFID-Anwendungen ist der Rahmen für die Datenschutzfolgenabschätzung nur dann anwendbar, wenn entsprechend dem Rahmen die Bedingungen für das Dokumentieren einer neuen oder überarbeiteten Datenschutzfolgenabschätzung gegeben sind.

ANHANG I: Merkmale der RFID-Anwendungsbeschreibung

Der RFID-Anwendungsbetreiber sollte im Bericht über die Datenschutzfolgenabschätzung – soweit zutreffend – folgende Angaben machen.

RFID-Anwendungsbetreiber	<ul style="list-style-type: none"> • Name und Sitz der Rechtsperson • Person oder Stelle, die für die rechtzeitige Datenschutzfolgenabschätzung verantwortlich ist • Ansprechpartner und Verfahren für Anfragen an den Betreiber
Überblick über die RFID-Anwendung	<ul style="list-style-type: none"> • Bezeichnung der RFID-Anwendung • Zweck(e) der RFID-Anwendung(en) • Grundlegendes Nutzungsszenario der RFID-Anwendung • Komponenten und Technik der RFID-Anwendung (z. B. Frequenzen u. a.) • geografische Reichweite der RFID-Anwendung • Arten von Nutzern/Personen, auf die sich die RFID-Anwendung auswirkt • Individueller Zugang und Kontrolle
Nummer des Datenschutzfolgenabschätzungsberichts	<ul style="list-style-type: none"> • Versionsnummer des Berichts über die Datenschutzfolgenabschätzung (mit Unterscheidung zwischen einer neuen Datenschutzfolgenabschätzung und kleineren Änderungen) • Datum der letzten Änderung des Berichts über die Datenschutzfolgenabschätzung
RFID-Datenverarbeitung	<ul style="list-style-type: none"> • Aufstellung der Arten der verarbeiteten Datenelemente • Vorhandensein sensibler Informationen in den verarbeiteten Daten (z. B. Gesundheitsdaten)
RFID-Datenspeicherung	<ul style="list-style-type: none"> • Aufstellung der Arten der verarbeiteten Datenelemente • Dauer der Speicherung
Interne RFID-Datenübertragung (falls zutreffend)	<ul style="list-style-type: none"> • Beschreibung oder Diagramme der Datenflüsse im internen Betrieb, die RFID-Daten betreffen • Zweck(e) der Übertragung personenbezogener Daten
Externe RFID-Datenübertragung (falls zutreffend)	<ul style="list-style-type: none"> • Art der/der Datenempfänger • Zweck(e) der Übertragung oder des Zugriffs im Allgemeinen • Festgestellte und/oder feststellbare (Ebene der) personenbezogenen Daten, die übertragen werden • Datenübertragung außerhalb des Europäischen Wirtschaftsraums (EWR)

ANHANG II: *Datenschutzziele*

Es gibt derzeit 9 Datenschutzziele, die in der Richtlinie 95/46/EG verankert sind. Der Prozess der Datenschutzfolgenabschätzung wurde unter Berücksichtigung dieser Ziele und der zugehörigen Risiken der RFID-Technik ausgearbeitet. Diese Datenschutzziele werden im vorliegenden Anhang zusammengefasst. Alle diese Ziele sind zwar von wesentlicher Bedeutung für die Einhaltung der Vorschriften durch die Organisation, in vielen Fällen wird aber nur ein Teil dieser Anforderungen für die betreffende RFID-Anwendung von Belang sein. Diese Ziele spielen daher eher eine Rolle bei Entwurf und Ausarbeitung des Prozesses der Datenschutzfolgenabschätzung als bei der Durchführung einer konkreten Datenschutzfolgenabschätzung.

Beschreibung der Datenschutzziele	
(entnommen aus den betreffenden EU-Datenschutzrichtlinien, hier Richtlinie 95/46/EG)	
Gewährleistung der Qualität personenbezogener Daten	Die zu erreichenden Hauptziele sind Datenvermeidung und Datenminimierung, Angabe und Eingrenzung des Zwecks, Qualität der Daten und Transparenz.
Rechtmäßigkeit der Verarbeitung personenbezogener Daten	Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten wird dadurch gewährleistet, dass sie nur aufgrund einer Zustimmung, vertraglichen Vereinbarung, rechtlichen Verpflichtung usw. erfolgen darf.
Rechtmäßigkeit der Verarbeitung <i>sensibler</i> personenbezogener Daten	Die Rechtmäßigkeit der Verarbeitung <i>sensibler</i> personenbezogener Daten muss dadurch gewährleistet werden, dass sie nur nach ausdrücklicher Zustimmung oder auf besonderer rechtlicher Grundlage usw. erfolgen darf.
Einhaltung des Informationsrechts der Betroffenen	Es muss gewährleistet werden, dass die betroffene Person rechtzeitig über die Erfassung ihrer Daten informiert wird.
Einhaltung des Auskunfts-, Berichtigungs- und Löschrechts der Betroffenen	Es muss gewährleistet werden, dass dem Verlangen der betroffenen Person, ihre Daten einzusehen, zu berichtigen, zu löschen oder zu blockieren rechtzeitig nachgekommen wird.
Einhaltung des Widerspruchsrechts der Betroffenen	Es muss gewährleistet werden, dass die Daten der betroffenen Person nicht weiter verarbeitet werden, wenn sie dem widersprochen hat. Insbesondere muss bei automatisierten Entscheidungen in Bezug auf Personen die Transparenz garantiert werden.
Wahrung der Vertraulichkeit und Sicherheit der Verarbeitung	Hauptziele sind die Verhinderung des unbefugten Zugriffs, die Protokollierung der Datenverarbeitung, die Sicherheit der Netze und der Datenübertragung sowie die Verhinderung des zufälligen Verlusts von Daten.
Einhaltung der Meldeanforderungen	Hauptziele sind die Meldung der Datenverarbeitung, die Vorabkontrolle der Rechtmäßigkeit und die Dokumentation.
Einhaltung der Datenspeicherungsanforderungen	Die Dauer der Datenspeicherung sollte entsprechend ihrem Zweck oder anderen rechtlichen Erfordernissen so kurz wie möglich sein.

ANHANG III: Datenschutzrisiken

Dieser Abschnitt enthält eine Aufstellung möglicher Datenschutzrisiken im Zusammenhang mit der Nutzung der zu prüfenden RFID-Anwendung. Insbesondere bei einer vollständigen Datenschutzfolgenabschätzung wird empfohlen, systematisch alle Risiken, einschließlich der Bedrohungen und Anfälligkeiten einer RFID-Anwendung, mit Hilfe standardisierter Risikoabschätzungsverfahren zu ermitteln.

Die nachstehende Tabelle enthält Beispiele für Risiken, die dazu führen können, dass die in Anhang II genannten Datenschutzziele nicht erreicht werden können. RFID-Anwendungsbetreiber können diese Liste als Ausgangspunkt nehmen, wenngleich nicht alle diese Risiken für alle RFID-Anwendungen von Belang sein mögen. Die RFID-Betreiber sollten dafür Sorge tragen, dass für jedes festgestellte Risiko geeignete Minderungsmaßnahmen getroffen werden, indem je nach Eintrittswahrscheinlichkeit und Ausmaß der Folgen eine oder mehrere Kontrollen vorgesehen werden. RFID-Anwendungsbetreiber müssen dazu möglicherweise mehrere Kontrollmaßnahmen miteinander kombinieren oder bestehende Kontrollen verstärken, und zwar in Abhängigkeit von Faktoren wie genutzte Technik, Reife der Implementierung, Art der Informationen, geltende Vorgaben usw.

Datenschutzrisiko	Beschreibung und Beispiel
Unbestimmter oder unzureichend eingegrenzter Zweck	<p>Der Zweck der Datenerfassung wurde nicht angegeben oder dokumentiert oder es werden mehr Daten verwendet als für den angegebenen Zweck notwendig sind.</p> <p>Beispiel: Keine Dokumentation der Zwecke, zu denen RFID-Daten benutzt werden bzw. Nutzung von RFID-Daten für alle möglichen Analysen.</p>
Datenerfassung geht über den Zweck hinaus	<p>Daten werden in einer bestimmaren Form erfasst, die über das zweckmäßige Maß hinausgeht.</p> <p>Beispiel: Informationen über RFID-Zahlungskarten werden nicht nur für die Transaktionsabwicklung verwendet, sondern auch für den Aufbau individueller Kundenprofile.</p>
Unvollständige Informationen oder mangelnde Transparenz	<p>Die der betroffenen Person gegebenen Informationen über den Zweck und die Verwendung der Daten ist unvollständig, die Datenverarbeitung wird nicht transparent gemacht oder die Informationen werden nicht rechtzeitig bereitgestellt.</p> <p>Beispiel: Die RFID-Informationen, die dem Verbraucher gegeben werden, enthalten keine klaren Angaben über Verarbeitung und Verwendung der RFID-Daten, die Identität des Betreibers oder die Nutzerrechte.</p>
Verknüpfung von Daten geht über den Zweck hinaus	<p>Personenbezogene Daten werden in einem Umfang verknüpft, der für den angegebenen Zweck unnötig ist.</p> <p>Beispiel: Informationen von der RFID-Zahlungskarte werden mit personenbezogenen Daten eines Dritten verknüpft.</p>

<p>Fehlende Vorgaben oder Mechanismen für das Löschen von Daten</p>	<p>Daten werden länger gespeichert als für den angegebenen Zweck notwendig.</p> <p>Beispiel: Personenbezogene Daten werden als Teil der Anwendung erfasst und länger als rechtlich zulässig gespeichert.</p>
<p>Unzulässige Erlangung der ausdrücklichen Einwilligung</p>	<p>Die Einwilligung wird unter Androhung von Nachteilen erlangt.</p> <p>Beispiel: Rückgabe/Umtausch des Produkts oder gesetzliche Garantieleistungen werden verweigert, wenn der RFID-Tag deaktiviert oder entfernt wird.</p>
<p>Geheime Datenerfassung durch den RFID-Betreiber</p>	<p>Einige Daten werden geheim aufgezeichnet und sind der betroffenen Person daher unbekannt, z. B. Bewegungsprofile.</p> <p>Beispiel: Vor einem Ladengeschäft oder beim Durchqueren eines Einkaufszentrums werden Verbraucherdaten ausgelesen, aber kein Logo oder Symbol weist den Verbraucher auf die RFID-Lesevorgänge hin.</p>
<p>Unmöglichkeit der Auskunftserteilung</p>	<p>Die betroffene Person hat keine Möglichkeit, eine Berichtigung oder Löschung ihrer Daten einzuleiten.</p> <p>Beispiel: Der Arbeitgeber kann seinen Mitarbeitern keinen vollständigen Überblick über die Daten geben, die aufgrund von RFID-Zugriffs- und Herstellungsdaten über sie gespeichert werden.</p>
<p>Verhinderung des Einlegens von Widersprüchen</p>	<p>Es gibt keine technischen oder betrieblichen Mittel, um dem Widerspruch einer betroffenen Person Folge zu leisten.</p> <p>Beispiel: Ein Krankenhausbesucher kann das Auslesen sensibler personenbezogener Daten von RFID-Tags (z. B. über verordnete Arzneimittel) nicht verhindern.</p>
<p>Mangelnde Transparenz bei automatisierten Entscheidungen</p>	<p>Es werden automatisierte Einzelentscheidungen getroffen, die auf persönlichen Merkmalen beruhen, aber die betroffene Person wird nicht über die Logik des Entscheidungsvorgangs informiert.</p> <p>Beispiel: Ein RFID-Betreiber liest ohne Information der Verbraucher alle von einer Person getragenen Tags aus, darunter auch Tags von Dritten, und entscheidet dann, welche Marketingbotschaft die betreffende Person aufgrund der Tags erhalten sollte.</p>
<p>Unzureichende Verwaltung der Zugriffsrechte</p>	<p>Zugriffsrechte werden nicht aufgehoben, wenn sie nicht mehr erforderlich sind.</p> <p>Beispiel: Mittels einer RFID-Karte erhält ein ehemaliger Praktikant Zugang zu Teilen eines Unternehmens, zu denen er keinen Zugang haben sollte.</p>

<p>Unzureichende Authentifizierungsverfahren</p>	<p>Eine auffällige Zahl von Identifizierungs- und Authentifizierungsversuchen wird nicht verhindert.</p> <p>Beispiel: Personenbezogene Daten auf RFID-Tags sind nicht standardmäßig mit einem Passwort oder einem anderen Authentifizierungsmechanismus geschützt.</p>
<p>Unrechtmäßige Datenverarbeitung</p>	<p>Die Verarbeitung personenbezogener Daten beruht nicht auf Einwilligung, Vertrag, Rechtspflicht usw.</p> <p>Beispiel: Ein RFID-Betreiber gibt erfasste Informationen ohne Unterrichtung der Einwilligung oder andere rechtliche Ermächtigung an Dritte weiter.</p>
<p>Unzureichende Protokollierung</p>	<p>Die eingerichteten Protokollierungsmechanismen sind unzureichend. Verwaltungsvorgänge werden nicht protokolliert.</p> <p>Beispiel: Es wird nicht protokolliert, wer auf die Daten der RFID-Karte eines Mitarbeiters zugegriffen hat.</p>
<p>Unkontrollierte Datenerfassung von RFID-Tags</p>	<p>Es besteht das Risiko, dass RFID-Tags für einen regelmäßigen Aufbau von Persönlichkeits- und/oder Bewegungsprofilen von Personen verwendet werden könnten.</p> <p>Beispiel: Einzelhändler lesen alle RFID-Tags aus, die in ihre Reichweite kommen.</p>

ANHANG IV: Liste der Beispiele für RFID-Anwendungskontrollen und Folgenminderungsmaßnahmen

Dieser Abschnitt enthält eine Liste von Beispielen für mögliche Kontrollmaßnahmen, die RFID-Anwendungsbetreibern helfen können, geeignete Minderungsstrategien zu finden. Den Risiken, die in Schritt 2 der Risikoabschätzung als für den RFID-Anwendungsbetreiber relevant eingestuft wurden, kann durch eine oder mehrere Minderungsstrategien entgegengewirkt werden, die in diesem Anhang IV angerissen werden. Das Ziel besteht darin, dass der RFID-Anwendungsbetreiber im Prozess der Datenschutzfolgenabschätzung die Kontrollmaßnahmen feststellt und implementiert, die notwendig sind, um die betreffenden Datenschutzrisiken zu mindern.

Mögliche Kontrollmaßnahmen sind:

- Regelungs- und Verwaltungspraktiken für RFID-Anwendungen
- Individueller Zugang und Kontrolle,
- Systemschutzmaßnahmen (einschließlich Sicherheitskontrollen),
- Schutz der Tags,
- Maßnahmen zur Verantwortlichkeit.

Alle diese Maßnahmen gelten neben dem bestehenden Datenschutz-Rahmenbestimmungen der EU und sollen diese weder ersetzen noch ihren Anwendungsbereich verändern.

Regelungs- und Verwaltungspraktiken für RFID-Anwendungen

Mögliche Regelungs- und Verwaltungspraktiken sind u. a.:

- Managementpraktiken des RFID-Anwendungsbetreibers,
- Vorgaben für die Vernichtung und Löschung von RFID-Daten,
- Vorgaben für die rechtmäßige Verarbeitung personenbezogener Daten,
- Bestimmungen für eine Datenminimierung beim Umgang mit RFID-Daten, falls möglich,
- Verarbeitung oder Speicherung der Informationen von Tags, die dem RFID-Betreiber nicht gehören,
- Regelungs- und Verwaltungspraktiken in Bezug auf die Sicherheit.

Individuelle Zugangsgewährung und Kontrolle

- Bereitstellung von Informationen über die Zwecke der Verarbeitung und die Kategorien der betroffenen personenbezogenen Daten,
- Beschreibung, wie der Verarbeitung personenbezogener Daten widersprochen oder die Einwilligung widerrufen werden kann,
- Festlegung des Verfahrens zur Beantragung der Berichtigung oder Löschung unvollständiger und unrichtiger personenbezogener Daten.

Systemschutz

Der **Systemschutz** im Hinblick auf einen angemessenen Schutz der Privatsphäre und der personenbezogenen Daten ist ebenfalls in diesem Abschnitt des Berichts über die Datenschutzfolgenabschätzung zu dokumentieren. Systemschutzkonzepte betreffen Back-

End-Systeme und Kommunikationsinfrastrukturen, soweit sie für die RFID-Anwendung von Bedeutung sind. Soweit dies zutrifft, sollte beachtet werden, dass Back-End-Systeme häufig sehr komplex sind und möglicherweise einer eigenen Datenschutzfolgenabschätzung unterworfen werden. Eine solche Abschätzung ist ggf. erneut zu prüfen, um sicherzustellen, dass Informationen der Art, wie sie in der RFID-Anwendung benutzt werden, darin berücksichtigt wurden. Liegt keine solche Datenschutzfolgenabschätzung vor, sollten folgende Komponenten des Back-End-Systems geprüft werden:

- Vorhandensein von Zugriffskontrollen für bestimmte personenbezogene Daten und Systemfunktionen,
- Vorhandensein von Kontrollen und Vorgaben, die sicherstellen, dass der Betreiber personenbezogene Daten in der RFID-Anwendung nicht in einer Weise verknüpft, die nicht im Einklang mit dem Bericht über die Datenschutzfolgenabschätzung steht,
- bestehende Maßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten in den Systemen und Kommunikationsinfrastrukturen,
- Vorgaben für die Speicherung und Vernichtung der personenbezogenen Daten,
- Vorhandensein und Implementierung von Informationssicherheitskontrollen, z. B.
 - Maßnahmen zur Sicherung der Netze und der Übertragung von RFID-Daten,
 - Maßnahmen für eine höhere Verfügbarkeit von RFID-Daten durch geeignete Sicherungskopien und Wiederherstellungsmöglichkeiten.

Schutz der RFID-Tags

Kontrollmaßnahmen zum **Schutz der RFID-Tags** im Hinblick auf die Privatsphäre und den Datenschutz sollten angegeben werden. Sie sind insbesondere für RFID-Anwendungen von Bedeutung, bei denen die RFID-Tags personenbezogene Daten enthalten.

Zu diesen Schutzmaßnahmen gehören:

- Kontrolle des Zugriffs auf Funktionen und Informationen, einschließlich Authentifizierung von Lese- und Schreibgeräten, zugrundeliegende Prozesse und Befugnisse zum Umgang mit RFID-Tags,
- Methoden zur Wahrung der Vertraulichkeit der Informationen (z. B. durch Verschlüsselung des gesamten RFID-Tags oder ausgewählter Datenfelder),
- Methoden zur Gewährleistung der Unversehrtheit der Informationen,
- Speicherung von Informationen nach der ursprünglichen Erfassung (z. B. Dauer der Speicherung, Verfahren für die Beseitigung der Daten zum Ende der Speicherdauer oder für die Löschung der Daten im RFID-Tag, Verfahren für eine selektive Speicherung oder Löschung bestimmter Datenfelder).
- Fälschungssicherheit des RFID-Tags selbst,
- Deaktivierung oder Entfernung, falls erforderlich oder anderweitig vorgesehen.

Mögliche Minderungsmaßnahmen sind vom Nutzer ausgehende Kontrollen in Situationen, in denen unterschiedliche Bedürfnisse oder Empfindlichkeiten bezüglich des Datenschutzes zu beachten sind. Deaktivierung oder Entfernung sind gegenwärtig die beiden häufigsten Formen der Risikominderung für Endnutzer/Verbraucher. Diese können als Teil der Datenschutzfolgenabschätzung erforderlich sein, sind unter gewissen Voraussetzungen gesetzlich vorgeschrieben oder stellen eine Wahlmöglichkeit des Kunden beim Verlassen des Verkaufsbereichs dar, um das Vertrauen zu steigern. Zudem werden in der Empfehlung der Kommission zur Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten

Anwendungen bestimmte Methoden und empfehlenswerte Praktiken in Bezug auf die Deaktivierung oder Entfernung von RFID-Tags im Einzelhandel vorgeschlagen⁴.

Maßnahmen zur Verantwortlichkeit

Diese Maßnahmen dienen der Stärkung des verfahrensmäßigen Datenschutzes in Bezug auf die Verantwortlichkeit. Durch diese Maßnahmen wird die externe Wahrnehmung von RFID-Anwendungen gesteigert.

- Gewährleistung der leichten Zugänglichkeit umfassender **Informationen** einschließlich
 - Identität und Adresse des RFID-Anwendungsbetreibers,
 - Zweck der RFID-Anwendung,
 - Art der durch die RFID-Anwendung verarbeiteten Daten, insbesondere ob personenbezogene Daten verarbeitet werden,
 - etwaige Beobachtung der Standorte von RFID-Tags im Besitz von Einzelpersonen,
 - etwaige wahrscheinliche Folgen für die Privatsphäre und den Datenschutz, die mit dem Einsatz von RFID-Tags in der RFID-Anwendung zusammenhängen, und vorhandene Maßnahmen zur Minderung dieser Folgen.
- Gewährleistung kurzer, präziser und leicht verständlicher Hinweise auf das Vorhandensein von RFID-Lesegeräten, einschließlich:
 - Identität und Adresse des RFID-Anwendungsbetreibers,
 - Ansprechstelle, bei der Einzelpersonen Informationen einholen können.
- Hinweise, ob und wie **Rechtsbehelfe** bereitgestellt werden:
 - verantwortliche Rechtsperson(en) des RFID-Anwendungsbetreibers (möglicherweise eine für jedes Rechts- oder Betriebsgebiet),
 - Ansprechpartner der Person oder Stelle, 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,
 - Verfahren für Anfragen (d. h. Wege der Erreichbarkeit des RFID-Anwendungsbetreibers für Fragen, Anliegen, Beschwerden oder die Wahrnehmung von Rechten),
 - Verfahren für den Widerspruch gegen die Verarbeitung, für die Ausübung des Auskunftsrechts über personenbezogene Daten (einschließlich Lösung und Berichtigung), den Widerruf einer Einwilligung oder die Änderung von Kontrollen oder anderen Wahlmöglichkeiten in Bezug auf die Verarbeitung personenbezogener Daten, falls erforderlich oder anderweitig vorgesehen,
 - sonstige Rechtsmittel, falls erforderlich oder anderweitig vorgesehen.

⁴ Nummer 12/13 der Empfehlung der Kommission vom 12. Mai 2009, {SEK(2009) 585}: *Die Deaktivierung oder Entfernung der RFID-Tags sollte für den Verbraucher kostenlos ein, entweder sofort oder später erfolgen und die Rechtspflichten des Einzelhändlers oder Herstellers gegenüber dem Verbraucher keinesfalls verringern oder aufheben.*

Anlage A: Referenzdokumente

In diesem Abschnitt werden Referenzdokumente aufgeführt, die bei der Ausarbeitung des Rahmens benutzt wurden.

- „Empfehlung der Kommission zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen“, Kommission der Europäischen Gemeinschaften, 12. Mai 2009, K(2009) 3200, abrufbar unter: http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf
- „Arbeitsdokument der Kommissionsdienststellen, Begleitdokument zur Empfehlung der Kommission zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen“, Zusammenfassung der Folgenabschätzung, Kommission der Europäischen Gemeinschaften, 12. Mai 2009, SEK(2009) 586, abrufbar unter: http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid200i9impact.pdf
- „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“, Amtsblatt der Europäischen Gemeinschaften L 281 vom 23.11.1995, S. 31, abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
- „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)“, Amtsblatt der Europäischen Gemeinschaften L 201 vom 31.7.2002, S. 37, abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:DE:PDF>
- „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“, Amtsblatt der Europäischen Union L 337 vom 18.12.2009, S. 11, abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:DE:PDF>
- Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, Artikel-29-Datenschutzgruppe, 20. Juni 2007, 01248/07/DE WP 136, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf
- „*Privacy Impact Assessment Handbook*“ (Handbuch für die Folgenabschätzung auf dem Gebiet der Privatsphäre) abrufbar unter: http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/files/PIAhandbookV2.pdf
- „*Status of Implementation of Directive 95/46 on the protection of Individuals in regards to the Processing of Personal Data*“ (Stand der Umsetzung der Richtlinie

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten),
abrufbar unter: [http://ec.europa.eu/justice/policies/privacy/law/
implementation_en.htm](http://ec.europa.eu/justice/policies/privacy/law/implementation_en.htm)

- „Arbeitspapier zu Datenschutzfragen im Zusammenhang mit der RFID-Technik“,
Artikel-29-Datenschutzgruppe, 19. Januar 2005, 10107/05/DE WP 105, abrufbar
unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_de.pdf

Anlage B: Glossar

In diesem Rahmen werden zahlreiche Termini benutzt, die mit Begriffen aus dem Bereich der Privatsphäre und des Datenschutzes sowie mit der Anwendung der RFID-Technik in vielfältigen Umfeldern zusammenhängen. Für die Zwecke dieses Rahmens gelten in Bezug auf die Privatsphäre und den Datenschutz die Begriffsbestimmungen der Richtlinie 95/46/EG.

Folgende Begriffsbestimmungen in Bezug auf die RFID-Technik und ihre Anwendung sind für den Rahmen von Bedeutung:

Person – eine natürliche Person, die mit einer oder mehreren Komponenten einer RFID-Anwendung (z. B. Back-End-System, Kommunikationsinfrastrukturen, RFID-Tag) in Wechselwirkung tritt oder anderweitig damit zu tun hat, aber selbst keine RFID-Anwendung betreibt oder eine ihrer Funktionen ausübt. In dieser Hinsicht unterscheidet sich eine Person von einem Nutzer. Eine Person hat möglicherweise nicht direkt mit den Funktionen der RFID-Anwendung zu tun, sondern kann beispielsweise lediglich einen Gegenstand besitzen, an dem ein RFID-Tag angebracht ist.

Informationssicherheit – Wahrung der Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Informationen.

Überwachen – Durchführung einer Tätigkeit zum Ermitteln, Beobachten, Kopieren oder Aufzeichnen des Aufenthaltsorts, der Bewegung, der Tätigkeiten oder des Zustands einer Person.

Personenbezogene Daten – alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person“); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Faktoren, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

RFID-Anwendung – 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.

RFID-Anwendungsbetreiber – 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.

Funkwellenidentifikation (RFID) – 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.

RFID-Lesegerät – 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.

RFID-Tag oder RFID-Transponder oder RFID-Etikett – ein RFID-Gerät, das in der Lage ist, ein Funksignal zu erzeugen, oder ein RFID-Gerät, das ein von einem Lese- oder Schreibgerät empfangenes Trägersignal rückkoppelt, rückwärtsstretet oder reflektiert (je nach Art des Geräts) und moduliert.

RFID-Tag-Informationen oder **in RFID-Tags gespeicherte Informationen** – Informationen, die ein RFID-Tag enthält und die übertragen werden, wenn der RFID-Tag von einem RFID-Lesegerät ausgelesen wird.

Nutzer – hier ein RFID-Anwendungsnutzer, d. h. eine Person (oder eine Stelle, z. B. eine Rechtsperson) die mit einer oder mehreren Komponenten einer RFID-Anwendung (z. B. Back-End-System, Kommunikationsinfrastrukturen, RFID-Tag) in direkte Wechselwirkung tritt, um eine RFID-Anwendung zu betreiben oder eine oder mehrere ihrer Funktionen auszuüben.