

DIN EN 16571

ICS 35.240.60

**Informationstechnik –
Verfahren zur Datenschutzfolgenabschätzung (PIA) von RFID;
Deutsche Fassung EN 16571:2014**

Information technology –
RFID privacy impact assessment process;
German version EN 16571:2014

Technologies de l'information –
Processus d'évaluation d'impact sur la vie privée des applications RFID;
Version allemande EN 16571:2014

Gesamtumfang 109 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (EN 16571:2014) wurde vom Technischen Komitee CEN/TC 225 „AIDC Technologien“ erarbeitet, dessen Sekretariat vom NEN (Niederlande) gehalten wird. Im DIN ist der Arbeitsausschuss NA 043-01-31 AA „Automatische Identifikation und Datenerfassungsverfahren“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA) zuständig.

Diese Europäische Norm stellt einen genormten Satz von Verfahrensweisen zur Entwicklung von PIA — Vorlagen zur Verfügung und beinhaltet dabei auch mit der RFID PIA Methodik kompatible Instrumente.

Darüber hinaus identifiziert sie die Umstände, die es erforderlich machen können, eine existierende PIA zu revidieren, zu korrigieren oder durch einen neuen Bewertungsprozess zu ersetzen.

DIN EN 16571 definiert einzelne Aspekte des Rahmenwerks für die RFID-Datenschutzfolgenabschätzung (englisch: Privacy Impact Assessment (PIA) Framework for RFID) als normative oder informative Verfahrensweisen, um so die Anwendung eines einheitlichen europäischen Verfahrens bei der Durchführung einer RFID-Datenschutzfolgenabschätzung zu ermöglichen.

Dieses Rahmenwerk wurde von den europäischen Datenschutzbehörden in der „Article 29 Data Protection Working Party“ gebilligt und 2011 von der Europäischen Kommission sowie Vertretern aller interessierten Akteure unterzeichnet.

Die Europäische Kommission hat im März 2009 im Rahmen des Mandates M/436 die europäischen Normungsorganisationen CEN, CENELEC und ETSI beauftragt, ein Standardisierungsprogramm für Sektor - spezifische Implementierungen von RFID - Anwendungen zu entwickeln. Die Schwerpunkte des Mandats sind der Datenschutz, der Schutz der Privatsphäre und die Datensicherung.

Die Durchführung des Mandates erfolgt in zwei Phasen. In Phase 1 wurde eine „Roadmap“ entwickelt, die die gegenwärtige Situation in Europa analysiert, bestehende Lücken in der Normung aufzeigt und ein entsprechendes Standardisierungsprogramm beinhaltet. Diese Phase wurde 2011 abgeschlossen. In Phase 2 werden die in Phase 1 identifizierten Lücken geschlossen.

Diese Europäische Norm ist eine der elf als durchzuführen im Rahmen der Phase 2 identifizierten Normungsaktivitäten.

Deutsche Fassung

Informationstechnik —
Verfahren zur Datenschutzfolgenabschätzung (PIA) von RFID

Information technology —
RFID privacy impact assessment process

Technologies de l'information —
Processus d'évaluation d'impact sur la vie privée des
applications RFID

Diese Europäische Norm wurde vom CEN am 14. Mai 2014 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Management-Zentrum des CEN-CENELEC oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

CEN-CENELEC Management-Zentrum: Avenue Marnix 17, B-1000 Brüssel

Inhalt

Seite

Vorwort	6
Einleitung.....	7
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe	8
4 Symbole und Abkürzungen	13
5 Struktur dieser Europäischen Norm	13
6 Anwendungsgebiet dieser Europäischen Norm.....	14
6.1 ‚RFID‘ nach den Festlegungen der EU-RFID-Empfehlung.....	14
6.2 ‚RFID-Anwendung‘ nach den Festlegungen der EU-RFID-Empfehlung.....	15
6.3 ‚RFID-Betreiber‘ nach den Festlegungen der EU-RFID-Empfehlung.....	16
6.4 Zusammenhang von RFID-PIA und Datenschutz und Sicherheit.....	16
6.5 Relevante Eingangsdaten für das PIA-Verfahren.....	19
6.5.1 Allgemeines.....	19
6.5.2 Angabe der Leistungsmerkmale zum Schutz der Privatsphäre	19
6.5.3 Registrierungsstelle	19
6.5.4 RFID-PIA-Vorlagen.....	19
7 Organisatorische Ziele des RFID-Betreibers bei einer RFID-PIA.....	20
7.1 Überblick.....	20
7.2 Einhalten und Übertreffen der gesetzlichen Bestimmungen	21
7.3 Wann ist eine RFID-PIA durchzuführen.....	21
7.3.1 Allgemeines.....	21
7.3.2 Durchführung einer PIA im Entwurfsstadium des RFID-Systems vor dessen Inbetriebnahme	21
7.3.3 Durchführung einer PIA bei Überprüfung und Überarbeitung einer auf dem Entwurfsstadium basierenden PIA	22
7.3.4 Durchführung einer PIA zur Erstellung einer Vorlage	22
7.3.5 Durchführung einer PIA mit einer vorhandenen Vorlage	22
7.3.6 Durchführung einer PIA nach Einführung einer neuen Funktion in die RFID-Anwendung	22
7.3.7 Durchführung einer PIA auf Grund von Änderungen der RFID-Technologie.....	23
7.3.8 Durchführung einer PIA, nachdem eine Verletzung der Privatsphäre angezeigt wurde.....	23
8 Werkzeuge zur Vereinfachung des Verfahrens	23
8.1 Verantwortung des RFID-Betreibers.....	23
8.2 RFID-Technologiewerkzeuge zum Schutz der Privatsphäre – Überblick	23
8.3 Registrierung von Angaben durch RFID-Produkthersteller über die Leistungsmerkmale zum Schutz der Privatsphäre in RFID-Anwendungen.....	24
8.3.1 Allgemeines.....	24
8.3.2 Pflichten der Registrierungsstelle	24
8.3.3 Berufung	25
8.3.4 Kündigung	25
8.3.5 Zuständigkeiten der RFID-Produkthersteller	25
8.4 Werkzeuge der RFID-Technologie zum Schutz der Privatsphäre – ausführliche Angaben.....	26
8.4.1 Leistungsmerkmale von integrierten RFID-Schaltungen zum Schutz der Privatsphäre.....	26
8.4.2 Leistungsmerkmale von RFID-Transpondern zum Schutz der Privatsphäre	26
8.4.3 Leistungsmerkmale von RFID-Lesegeräten zum Schutz der Privatsphäre	26

8.4.4	Standardmäßige Angaben über Leistungsmerkmale zum Schutz der Privatsphäre	26
8.4.5	Anwendung von CEN/TR 16672, um Leistungsmerkmale zum Schutz der Privatsphäre für Produkte zu entwickeln, die unternehmenseigene Protokolle verwenden	27
8.5	Vorlagen	27
8.5.1	Allgemeines	27
8.5.2	Erarbeiten einer Vorlage	28
8.5.3	Wer sollte die Vorlagen erstellen?	28
8.5.4	Rolle der Interessenvertreter bei der Vorlagenentwicklung	29
9	RFID-PIA – ein prozessorientierter Ansatz	29
9.1	Einleitung	29
9.2	Verfahrensschritte	29
9.3	Durchsetzen der richtigen Ausführlichkeit	30
9.3.1	Allgemeines	30
9.3.2	Stufe 0 – keine PIA	31
9.3.3	Stufe 1 – PIA von geringem Umfang	31
9.3.4	Stufe 2 – PIA mit Fokus auf den kontrollierten Bereich der Anwendung	31
9.3.5	Stufe 3 – Vollständige PIA der Anwendung	31
9.3.6	Verringerung des Aufwands für kleine und mittlere Unternehmen (KMU)	31
9.4	Methodik des Verfahrens	32
10	Bereitstellen der Angaben über die RFID-Funktion (RFID-Funktionsbeschreibung)	34
11	Ausarbeiten der RFID-Anwendungsbeschreibung	35
11.1	Einführung	35
11.2	Mehrfachanwendungen	35
11.3	Übersicht über die RFID-Anwendung	36
11.3.1	Allgemeines	36
11.3.2	Festlegen der vorgesehenen oder anzuwendenden RFID-Technologie	36
11.3.3	Festlegen der in der Anwendung zu verwendenden RFID-Komponenten	36
11.3.4	RFID-Anwendungen auf tragbaren Geräten	38
11.4	Daten auf dem RFID-Transponder	40
11.4.1	Allgemeines	40
11.4.2	Festlegen, über welche eigenen identifizierbaren Merkmale der RFID-Transponder verfügt	40
11.4.3	Auflistung der auf dem RFID-Transponder verschlüsselten Datenelemente	41
11.4.4	Ermitteln, ob verschlüsselte Daten als identifizierbar betrachtet werden können	42
11.4.5	Ermitteln, ob personenbezogene Daten auf dem Transponder verschlüsselt sind	42
11.5	Weitere Daten in der Anwendung	43
11.6	Verarbeitung von RFID-Daten	43
11.7	Interne Übertragung von RFID-Daten	43
11.8	Externe Übertragung von RFID-Daten	44
11.9	Unterzeichnen der RFID-Anwendungsbeschreibung	44
12	Risikobewertung	44
12.1	Aus der RFID-Empfehlung abgeleitete prozesstechnische Anforderungen	44
12.1.1	Allgemeine verfahrensspezifische Anforderungen für alle RFID-Betreiber	44
12.1.2	Anforderungen an Einzelhändler, die RFID-Betreiber sind	46
12.1.3	Verfahrensanforderungen an Hersteller von Produkten, die letztendlich an Verbraucher verkauft werden	47
12.2	Ermittlung und Beurteilung des Werts der Privatsphäre	47
12.2.1	Allgemeines	47
12.2.2	Ermittlung des Werts der Privatsphäre	48
12.2.3	Beurteilung der Werte	49
12.3	Ermitteln und Einschätzen von Bedrohungen	52
12.3.1	Allgemeines	52
12.3.2	Ermitteln und Klassifizieren von Bedrohungen	53
12.3.3	Beurteilung von Bedrohungen	55
12.3.4	KMU-Verfahren	55
12.4	Ermitteln der Schwachstellen und Benennen der damit verbundenen Risikostufen	56
12.4.1	Grundlegendes Verfahren	56
12.4.2	Verfahren zur Erfassung der Dauer der Bedrohung	57

12.5	Anfangsrisikostufe	57
12.6	Gegenmaßnahmen.....	58
12.6.1	Allgemeines	58
12.6.2	Ermitteln von Gegenmaßnahmen	59
12.6.3	Neubewertung der Risikostufen.....	61
12.7	Restrisiken.....	62
12.8	Unterzeichnen der RFID-PIA.....	62
13	Ausgearbeitetes Beispiel eines Risikobewertungsprozesses	62
14	Zusammenfassender RFID-PIA-Bericht	62
14.1	Datum des PIA-Berichts	62
14.2	RFID-Anwendungsbetreiber	62
14.3	Überblick über die RFID-Anwendung	62
14.4	Daten auf dem RFID-Transponder	63
14.5	Punktezahl der Datenschutzfolgenabschätzung für RFID	63
14.6	RFID-Gegenmaßnahmen	63
15	Versionskontrolle.....	64
16	Überwachung und Reaktion auf Vorfälle	64
Anhang A (normativ) Einzelheiten zur Registrierungsstelle		65
Anhang B (informativ) Angaben durch den RFID-Hersteller über Leistungsmerkmale des Produkts zum Schutz der Privatsphäre.....		66
B.1	Leistungsmerkmale der integrierten RFID-Schaltung (RFID-Chip) zum Schutz der Privatsphäre	66
B.2	Leistungsmerkmale des RFID-Lesegeräts zum Schutz der Privatsphäre	68
Anhang C (informativ) Ablaufdiagramm für die RFID-Datenschutzfolgenabschätzung		70
Anhang D (informativ) Vorlagenentwicklung.....		72
Anhang E (informativ) Ablaufdiagramm für die Bestimmung der RFID-PIA-Stufe		73
Anhang F (informativ) RFID-Funktionsbeschreibung.....		74
Anhang G (normativ) RFID-Anwendungsbeschreibung		75
Anhang H (informativ) Ermittlung und Bewertung von persönlichen Werten der Privatsphäre		76
H.1	Einzel gespeicherte, persönliche Werte der Privatsphäre	76
H.2	Werte für das Unternehmen.....	81
Anhang I (informativ) RFID-Bedrohungen		82
I.1	Bedrohungen im Zusammenhang mit auf dem RFID-Transponder codierten Daten und mit dem RFID-Transponder (oder der RF-Karte) selbst	82
I.1.1	Allgemeines	82
I.1.2	Seitenkanalattacke.....	83
I.1.3	Physische Datenmodifikation.....	83
I.1.4	Klonen	83
I.1.5	Spoofing	83
I.1.6	Physischer Austausch des Transponders	83
I.1.7	Umlenkung des RF-Transponders	84
I.1.8	Umprogrammierung des Transponders	84
I.1.9	Entfernung des Transponders	84
I.1.10	Zerstörung des Transponders.....	84
I.1.11	Deaktivierung des Transponders durch Befehlsmissbrauch	84
I.1.12	Erschöpfung von Protokollressourcen	85
I.1.13	Desynchronisationsangriff	85
I.2	Bedrohungen im Zusammenhang mit der Luftschnittstelle oder mit der Kommunikation über die Geräteschnittstelle	85
I.2.1	Allgemeines	85
I.2.2	Unberechtigtes Auslesen des Transponders	86
I.2.3	Verfolgung	86
I.2.4	Datenverknüpfung	87

I.2.5	Erstellen eines Verhaltensprofils.....	87
I.2.6	Erstellen einer Favoritenliste	87
I.2.7	Abhören oder Verkehrsanalyse	87
I.2.8	Energieanalyse	87
I.2.9	Angriffe auf die Verschlüsselung	88
I.2.10	Reverse Engineering.....	88
I.2.11	Datenweitergabe oder Mittelsmannangriff (Man-in-the-middle-Angriff).....	88
I.2.12	Angriff durch Wiedereinspielung.....	88
I.2.13	(Wieder-)Aufbau der Nachricht	88
I.2.14	Datenmodifikation bei der Übertragung an der Luftschnittstelle.....	89
I.2.15	Einfügen von Daten bei der Übertragung an der Luftschnittstelle	89
I.2.16	Rauschen	89
I.2.17	Störsender (Jamming)	89
I.2.18	Böswillige Blocker-Transponder	89
I.2.19	Auswirkungen einer Schwächung der Funkübertragung	90
I.2.20	Abschirmung von Transpondern.....	90
I.3	Bedrohungen im Zusammenhang mit dem Abfragegerät (oder Lesegerät)	90
I.3.1	Allgemeines	90
I.3.2	Seitenkanalattacke	90
I.3.3	Erschöpfung von Protokollressourcen.....	90
I.3.4	Desynchronisationsangriff.....	91
I.4	Bedrohungen im Zusammenhang mit der Host-Anwendung	91
I.4.1	Allgemeines	91
I.4.2	Verletzung der Privatsphäre und des Datenschutzes	91
I.4.3	Gefährdung von Sicherheitsschlüsseln.....	92
I.4.4	Angriff durch Pufferüberlauf	92
I.4.5	Eingeben eines böswilligen Codes	92
I.4.6	Teilweise Dienstverweigerung	92
I.4.7	Vollständige Dienstverweigerung.....	92
Anhang J (informativ)	Gegenmaßnahmen.....	93
J.1	Liste der Gegenmaßnahmen	93
J.2	Zuordnung zwischen Bedrohungen und Gegenmaßnahmen	95
Anhang K (informativ)	Beispiel einer PIA-Risikobewertung.....	98
K.1	Einleitung	98
K.2	Ordnung der Werte nach der Wertigkeit	98
K.3	Berücksichtigung der Bedrohungen in der Transponderschicht und der Luftschnittstellenschicht.....	99
K.4	Berücksichtigung der Bedrohungen in der Lesegeräteschicht	101
K.5	Berücksichtigung der Bedrohungen in der Geräteschnittstellenschicht.....	101
K.6	Berücksichtigung der Bedrohungen in der Anwendungsschicht.....	102
K.7	Berücksichtigung der Schwachstellen	102
K.8	Risikowerte nach Berücksichtigung aller Bedrohungen und Schwachstellen.....	103
K.9	Anwenden von Gegenmaßnahmen	103
K.10	Gesamtrisiko.....	104
Anhang L (informativ)	Zusammenfassung der Datenschutzfolgenabschätzung von RFID	105
Literaturhinweise		106

Vorwort

Dieses Dokument (EN 16571:2014) wurde vom Technischen Komitee CEN/TC 225 „AIDC Technologien“ erarbeitet, dessen Sekretariat vom NEN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Dezember 2014, und etwaige entgegenstehende nationale Normen müssen bis Dezember 2014 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN [und/oder CENELEC] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument wurde unter einem Mandat erarbeitet, das die Europäische Kommission und die Europäische Freihandelszone dem CEN-CENELEC erteilt haben.

Die Europäische Norm ist eine Norm aus einer Reihe verwandter Ergebnisse, die gemeinsam zu Phase 2 des Mandats M/436 gehören.

Die anderen Ergebnisse sind:

- EN 16570, *Informationstechnik — Verfahren zur Datenschutzfolgenabschätzung (PIA) von RFID*;
- EN 16656, *Informationstechnik — Identifizierung von Waren mittels Hochfrequenz (RFID) für das Management des Warenflusses — RFID-Emblem (ISO/IEC 29160:2012, modifiziert)*
- CEN/TR 16669, *Informationstechnik — Geräteschnittstelle zur Unterstützung von ISO/IEC 18000-3*;
- CEN/TR 16670, *Informationstechnik — Analyse zur Bedrohung und Verletzlichkeit durch beziehungsweise von RFID*;
- CEN/TR 16671, *Informationstechnik — Autorisierung von Mobilfunkgeräten als RFID-Lesegeräte*;
- CEN/TR 16672, *Informationstechnik — Leistungsmerkmale für den Schutz der Privatsphäre in gegenwärtigen RFID-Technologien*;
- CEN/TR 16673¹⁾, *Informationstechnik — Verfahren zur Datenschutzfolgenabschätzung (PIA) von RFID für spezifische Sektoren*;
- CEN/TR 16674, *Informationstechnik — Analyse der RFID-Datenschutzfolgenabschätzung für spezifische Sektoren*;
- CEN/TR 16684²⁾, *Informationstechnik — Notifizierung von RFID — Zusätzliche vom Betreiber zur Verfügung zu stellende Information*;
- CEN/TR 16685, *Informationstechnik — Notifizierung von RFID — Informationszeichen, das überall dort angebracht werden muss, wo RFID-Lesegeräte im Einsatz sind*.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die ehemalige jugoslawische Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

1) CEN/TR 16673 enthält praktische Beispiele von PIA-Systemen.

2) CEN/TR 16684 enthält praktische Beispiele von Beschilderungssystemen zur Notifizierung.

Einleitung

Als Reaktion auf den europaweit zunehmenden Einsatz von RFID-Systemen hat die Europäische Kommission im Jahr 2007 die Mitteilung KOM(2007) 96 „Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen“ veröffentlicht. Diese Mitteilung schlägt notwendige Schritte für die Verringerung von Barrieren bei der Einführung von RFID unter Berücksichtigung der grundlegenden rechtlichen Rahmenbedingungen für den Schutz der Grundrechte wie Gesundheits-, Umwelt-, Datenschutz, Schutz der Privatsphäre und Datensicherheit vor.

Im Dezember 2008 hat die Europäische Kommission CEN, CENELEC und ETSI im Bereich der Informations- und Kommunikationstechnik das Mandat M/436 für RFID-Systeme erteilt. Das Mandat M/436 wurde von den Europäischen Normungsorganisationen Anfang 2009 angenommen. Es ist ausgerichtet auf den Datenschutz, den Schutz der Privatsphäre und Informationsaspekte von RFID und wird in zwei Phasen ausgeführt. In Phase 1, die im Mai 2011 abgeschlossen wurde, wurden die erforderlichen Aufgaben für die Aufstellung eines vollständigen Strukturrahmens für zukünftige RFID-Normen ermittelt. Die Ergebnisse der Phase 1 sind im ETSI-Fachbericht TR 187 020 enthalten, der im Mai 2011 veröffentlicht wurde.

Phase 2 betrifft die Ausführung des in der ersten Phase aufgestellten Programms der Normungsaufgaben.

Die vorliegende Europäische Norm ist eines von 11 konkreten Ergebnissen der Phase 2 des Mandats M/436. Sie beruht auf den Untersuchungen in den beiden zugehörigen Technischen Berichten:

- CEN/TR 16673 gibt einen Einblick in die Behandlung der Aspekte des Schutzes der Privatsphäre in RFID-Anwendungen in den vier Branchen: Bibliothekswesen; Einzelhandel; elektronisches Ticket, Mautstraßen, Gebühreneinzug, Veranstaltungsmanagement; sowie Bankwesen und Finanzdienstleistungen;
- CEN/TR 16674 behandelt bereits formal vorliegende PIAs, die aber nicht zwangsläufig in nationale Normen überführt wurden.

Die in der vorliegenden Europäischen Norm definierten Verfahren sind vorgesehen zur Anwendung durch einzelne RFID-Betreiber oder gesamte Branchen für die Durchführung einer PIA für RFID. Insofern zitiert sie als Referenzen andere Ausarbeitungen der Phase 2 von M/436. Eine auf eine Branche bezogene PIA kann als Vorlage für die Erarbeitung einer spezifischen PIA dienen.

1 Anwendungsbereich

Diese Europäische Norm wurde im Rahmen des EU-RFID-Mandats M/436 erarbeitet. Grundlage ist ein von der Industrie in Zusammenarbeit mit Organisationen der Zivilgesellschaft aufgestellter Folgenabschätzungsrahmen in Bezug auf den Datenschutz und die Wahrung der Privatsphäre in RFID-Anwendungen, der von der Artikel-29-Datenschutzgruppe gebilligt und von allen wichtigen Interessenverbänden einschließlich der Europäischen Kommission im Jahr 2011 unterzeichnet wurde.

Es werden normative sowie informative Verfahren des Rahmenwerks einer gesamteuropäischen PIA für RFID-Anwendungen festgelegt.

Es stellt eine Reihe normierter Verfahren zur Erarbeitung von PIA-Vorlagen bereit, dazu gehören Werkzeuge, die mit RFID betreffenden PIA-Methoden kompatibel sind.

Zusätzlich werden die Bedingungen aufgeführt, die es erforderlich machen, dass eine vorhandene PIA durch ein neues Abschätzungsverfahren überarbeitet, geändert oder ersetzt wird.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

CEN/TR 16670, *Informationstechnik — Analyse zur Bedrohung und Verletzlichkeit durch beziehungsweise von RFID*

CEN/TR 16672, *Informationstechnik — Leistungsmerkmale für den Schutz der Privatsphäre in gegenwärtigen RFID-Technologien*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1 zuständige Behörde
Organisation, bei der die PIA entsprechend der RFID-Empfehlung spätestens 6 Wochen vor Einführung der RFID-Anwendung eingehen muss

Anmerkung 1 zum Begriff: Die Empfehlung liefert unter Punkt (5 d)) keine Einzelheiten zur Legitimation der zuständigen Behörde.

3.2 kontrollierter Bereich
Teil einer Anwendung, der unter direkter Kontrolle des RFID-Betreibers (oder Datenverantwortlichen) liegt, einschließlich der Daten auf dem Transponder, die von der Anwendung verarbeitet werden, und der RFID-Luftschnittstellen-Kommunikationen

Anmerkung 1 zum Begriff: Dies zeigt enge Analogien zur Datenverarbeitung unter der Richtlinie 95/46/EG.

3.3 Gegenmaßnahme
Handlung, Gerät, Verfahren oder Methode, die/das einer Bedrohung, einer Schwachstelle oder einem Angriff eliminierend oder schützend begegnet oder gegenübersteht (d. h. entgegenwirkt), indem der mögliche Schaden minimiert wird

3.4

für die Datenverarbeitung Verantwortlicher

Datenverantwortlicher

natürliche oder juristische Person, Behörde oder Dienststelle oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel der Verarbeitung in einzelstaatlichen oder gemeinschaftlichen Rechts- und Verwaltungsvorschriften festgelegt, so kann der Datenverantwortliche bzw. können die spezifischen Kriterien für seine Benennung durch einzelstaatliche oder gemeinschaftliche Rechtsvorschriften bestimmt werden

[QUELLE: Richtlinie 95/46/EG]

3.5

Datenschutzbehörde

DPA

(en: data protection authority)

Organisation oder Organisationen, die für die Umsetzung der Richtlinie 95/46/EG in einem Mitgliedstaat verantwortlich ist

3.6

bestimmte oder bestimmbare Person

Person, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, das/die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität spezifisch ist/sind

[QUELLE: Richtlinie 95/46/EG]

3.7

Einzelperson

natürliche Person, die mit einem oder mehreren Bestandteilen einer RFID-Anwendung (z. B. Back-End-System, Kommunikationsinfrastruktur, RFID-Transponder) interagiert oder anderweitig in diese eingebunden ist, die aber keine RFID-Anwendung betreibt oder eine ihrer Funktionen ausübt

Anmerkung 1 zum Begriff: In dieser Hinsicht unterscheidet sich eine Einzelperson von einem Nutzer. Eine Einzelperson muss nicht direkt in die Funktionsweise der RFID-Anwendung eingebunden sein, sondern besitzt z. B. lediglich einen Gegenstand, der einen RFID-Transponder hat.

3.8

Informationssicherheit

Wahrung der Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Informationen

[QUELLE: Empfehlung K(2009) 3200 endgültig]

3.9

Überwachung

Tätigkeit zur Ermittlung, Beobachtung, Kopie oder Aufzeichnung des Aufenthaltsorts, der Bewegung, der Tätigkeiten oder des Zustands einer identifizierten oder identifizierbaren Person

[QUELLE: RFID-Empfehlung K(2009) 3200 endgültig]

3.10

persönliche verhaltensbezogene Informationen

Daten, die das Verhalten oder Verhaltensweisen einer Einzelperson kennzeichnen

3.11

personenbezogene Daten

Informationen über eine identifizierte oder identifizierbare natürliche Person („betroffene Person“); insofern eine identifizierbare Person eine Person ist, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, das/die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität ist/sind

[QUELLE: Richtlinie 95/46/EG, modifiziert — Definition wurde grammatikalisch verändert]

3.12

Personenkennzeichen

Personenbezeichner

Daten, die zur direkten oder indirekten Identifizierung einer Einzelperson, auf die sich die Daten beziehen, herangezogen werden können

3.13

persönlicher Wert der Privatsphäre

alles, was für eine Person von Wert ist, dem ein bestimmter RFID-Transponder zugeordnet werden kann

Anmerkung 1 zum Begriff: Es ist daher erforderlich, diesen Wert vor Verlust zu schützen.

3.14

Privatsphäre

Recht der identifizierten oder identifizierbaren Person darauf, dass ihre Identität und ihr Handeln vor unrechtmäßiger Kontrolle und ungewollten Eingriffen geschützt werden

Anmerkung 1 zum Begriff Die Privatsphäre wird von dem Persönlichkeitsrecht auf freie Entscheidungen und Selbstbestimmung gestützt, das in Europa zu den Grundrechten aller Menschen gehört.

[QUELLE: ETSI TR 187 020 V1.1.1 (2011-05), modifiziert — Definition wurde angepasst]

3.15

Verletzung der Privatsphäre

Datenschutzverletzung

Situation, in der personenbezogene Daten in einer RFID-Anwendung unter Nichteinhaltung einer oder mehrerer relevanter Anforderungen an den Schutz der Privatsphäre verarbeitet werden

[QUELLE: ISO/IEC 29100:2011, modifiziert — Definition wurde angepasst]

3.16

Angabe der Leistungsmerkmale zum Schutz der Privatsphäre

Erklärung durch einen RFID-Technologieanbieter von RFID-Transpondern oder -Lesegeräten über die Leistungsmerkmale zum Schutz der Privatsphäre im jeweiligen Produkt

Anmerkung 1 zum Begriff: Beruhend auf CEN/TR 16672 kennzeichnet die Angabe der Leistungsmerkmale zum Schutz der Privatsphäre in einer konsistenten Form den Umfang, in dem die Leistungsmerkmale in einem Produkt einen besseren Schutz der Privatsphäre unterstützen. Die Angabe der Leistungsmerkmale zum Schutz der Privatsphäre liefert einen genaueren Beitrag zum PIA-Verfahren als generische Protokollstandards, da sie produktspezifisch ist.

3.17

Risiken für die Privatsphäre

Datenschutzrisiken

Potential, dass durch eine gegebene Bedrohung die Schwachstelle eines persönlichen Werts der Privatsphäre ausgenutzt und dadurch ein Schaden am angegriffenen System oder an der angegriffenen Organisation verursacht wird

[QUELLE: ETSI TR 187 020 V1.1.1 (2011-05), modifiziert — Definition wurde angepasst und die definierte Benennung war ursprünglich „Risiko“]

3.18

Registrierungsstelle

RA

(en: registration authority)

vom CEN benannte Organisation zur Pflege des öffentlich zugänglichen Verzeichnisses der mit einer Norm verbundenen Faktoren

Anmerkung 1 zum Begriff: Für EN 16571 ist die RA für die Pflege des Verzeichnisses der Angaben der Leistungsmerkmale zum Schutz der Privatsphäre verantwortlich.

3.19

Restrisiko

verbleibendes Risiko nach dem Ergreifen von Gegenmaßnahmen zur Senkung des mit einer bestimmten Bedrohung verbundenen Risikos

[QUELLE: ETSI TR 187 020 V1.1.1 (2011-05)]

3.20

RFID

radiofrequente Identifikation

Nutzung elektromagnetischer Wellen oder der elektromagnetischen Nahfeldkopplung im Funkbereich des Frequenzspektrums für die Kommunikation von oder zu einem Transponder mit Hilfe verschiedener Modulations- und Kodierungstechniken für das Auslesen und Beschreiben eines RFID-Transponders

[QUELLE: RFID-Empfehlung K(2009) 3200 endgültig]

3.21

RFID-Anwendung

Anwendung, die Daten unter Einsatz von Transpondern und Lesegeräten verarbeitet und dabei von einem Back-End-System und einer vernetzten Kommunikationsinfrastruktur unterstützt wird

[QUELLE: RFID-Empfehlung K(2009) 3200 endgültig]

3.22

RFID-Anwendungsbetreiber

RFID-Betreiber

natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel des Betriebs einer Anwendung entscheidet, einschließlich der für die Verarbeitung personenbezogener Daten unter Einsatz einer RFID-Anwendung Verantwortlichen

[QUELLE: RFID-Empfehlung K(2009) 3200 endgültig]

3.23

RFID-Lesegerät

RFID-Abfragegerät

Lesegerät

Abfragegerät

fest installiertes oder mobiles Datenerfassungs- und Identifizierungsgerät, das durch eine elektromagnetische Welle oder durch elektromagnetische Nahfeldkopplung im Funkfrequenzbereich von einem oder mehreren Transpondern eine Antwort in Form modulierter Daten anregt und bewirkt

Anmerkung 1 zum Begriff: Die Benennung „Abfragegerät“ wird oft im Zusammenhang mit Normen zum RFID-Warenflussmanagement verwendet und der Begriff „RFID-Lesegerät“ in allgemeinen Anwendungen. Im Zusammenhang mit Kartenanwendungen wird die Benennung 'Proximity coupling device' und 'Vicinity coupling device' verwendet. Die Funktionsweise ist für jedes einzelne Luftschnittstellenprotokoll die gleiche.

3.24

RFID-PIA-Bericht

detaillierter interner Bericht der Ergebnisse des PIA-Verfahrens

Anmerkung 1 zum Begriff: Mit Ausnahme des Hinweises unter Punkt 5d) der Empfehlung, die Abschätzung der zuständigen Behörde zur Verfügung zu stellen, wird der RFID-PIA-Bericht als vertrauliches Dokument betrachtet.

3.25

zusammenfassender RFID-PIA-Bericht

Teil des RFID-PIA-Verfahrens, der aus Transparenzgründen öffentlich verfügbar ist

3.26

RFID-Transponder

RF-Transponder

Tag

Transponder

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, rückstreut oder reflektiert (je nach Art des Geräts) und moduliert

[QUELLE: RFID-Empfehlung K(2009) 3200 endgültig]

Anmerkung 1 zum Begriff: Die technisch genaueste Benennung ist „Transponder“. Die häufigste und bevorzugte Benennung (im Englischen) im Zusammenhang mit RFID-Warenflussmanagement-Anwendungen ist „tag“ oder „RFID tag“ und im Zusammenhang mit Kartenanwendungen 'Proximity integrated circuit card' oder 'Vicinity integrated circuit card' (letztere Begriffe werden auch im deutschen Sprachraum verwendet).

3.27

RFID-Bedrohung

physikalischer, Hardware- oder Software-Mechanismus, der die Ursache für nachteilige Auswirkungen auf einen persönlichen Wert der Privatsphäre und zugehöriger Datentypen oder auf eine betroffene Person durch unautorisierten Zugriff, Zerstörung, Bekanntgabe, Manipulation von Daten und/oder Dienstverweigerung (en: denial of service) sein könnte

3.28

RFID-Schwachstelle

Angreifbarkeit eines Werts oder einer Gruppe von Werten, die durch eine oder mehrere Bedrohungen ausgenutzt werden kann

[QUELLE: ISO/IEC 27005:2011, modifiziert — Definition wurde angepasst und die definierte Benennung war ursprünglich „Informationssicherheitsrisiko“]

3.29

Vorlage

Eingabeinformationen und -daten, die bei der Verminderung des erforderlichen Aufwands zum Fertigstellen einer PIA helfen sollen, wenn eine Anzahl von RFID-Anwendungen einige gemeinsame Merkmale hat

Anmerkung 1 zum Begriff: Die Detailgenauigkeit einer Vorlage liegt in der Entscheidung des Urhebers eines derartigen Dokuments. Sie kann von einer Beschreibung der Anwendung bis zu einer komplexeren Analyse reichen und als generisches Werkzeug zum Erstellen eines PIA-Berichts verwendet werden, stellt aber niemals einen Ersatz für einen PIA-Bericht dar, für den jeder RFID-Betreiber verantwortlich ist.

3.30

unkontrollierter Bereich

Teil einer Anwendung, den ein RFID-Betreiber (oder Datenverantwortlicher) nicht kontrollieren kann, einschließlich der Befähigung von Dritten, berechtigterweise oder rechtswidrig Daten auf dem RFID-Transponder in irgendeiner Form zu lesen, unabhängig davon, ob die Lesegeräte dem Luftschnittstellenprotokoll entsprechen oder dieses umgehen

4 Symbole und Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Symbole und Abkürzungen.

- AIDC automatische Identifikation und Datenerfassung (Automatic Identification and Data Capture)
- AFI Kennzeichen für Anwendungsfamilie (Application Family Identifier)
- CEN Europäisches Komitee für Normung (Comité Européen de Normalisation)
- DSFID Kennzeichen für das Datenformat (Data Storage Format Identifier)
- EN Europäische Norm
- EPC Elektronischer Produktcode (Electronic Product Code)
- ETSI Europäisches Institut für Telekommunikationsnormen (European Telecommunications Standards Institute)
- GS1 Global Standards One
- HF Hochfrequenz
- IEC Internationale Elektrotechnische Kommission (International Electrotechnical Commission)
- ISO Internationale Organisation für Normung (International Organization for Standardization)
- NFC Nahfeldkommunikation (Near Field Communication)
- PIA Datenschutzfolgenabschätzung (Privacy Impact Assessment)
- RF Funkfrequenz (Hochfrequenz)
- RFID Radiofrequente Identifikation (Radio Frequency Identification)
- SME KMU, kleine und mittlere Unternehmen (Small and medium sized enterprises)
- TR Technischer Bericht (Technical Report)
- TS Technische Spezifikation
- UHF Ultrahochfrequenz

5 Struktur dieser Europäischen Norm

Diese Europäische Norm behandelt die Spezifikation und Beschreibung des Verfahrens zur Datenschutzfolgenabschätzung für RFID. Nachfolgend wird der Inhalt der folgenden Abschnitte und zugehörigen Anhänge angegeben.

- a) Abschnitt 6 gibt an, was aus Sicht der RFID-Empfehlung eine RFID-Technologie ist (dies ist nicht unbedingt deckungsgleich mit der Struktur des Arbeitsgebiets und Aufgabenbereichs unterschiedlicher Standardisierungsgremien für Technologie), was eine RFID-Anwendung ist und was ein RFID-Betreiber ist.
- b) Abschnitt 7 beschreibt einige der strategischen Überlegungen, die ein RFID-Betreiber vor der Durchführung einer RFID-PIA zu berücksichtigen hat. Dies schließt die Übernahme über die Forderungen der Empfehlung hinausgehender Verantwortung ein.
- c) Abschnitt 8 und die damit verbundenen Anhänge beschreiben einige der Werkzeuge und andere Mechanismen, die eingesetzt werden können, um die Durchführung der PIA zu vereinfachen. Diese Werkzeuge bieten den zusätzlichen Vorteil der Konsistenz zwischen vergleichbaren PIA-Berichten.
- d) Abschnitt 9 ist der erste Abschnitt, der das eigentliche Verfahren zur Datenschutzfolgenabschätzung für RFID behandelt. Dieser Abschnitt befasst sich insbesondere mit der Bestimmung der für die RFID-PIA erforderlichen Ausführlichkeit.

- e) Abschnitt 10 befasst sich mit der untersten Ebene der Ergebnisse des PIA-Verfahrens, dabei handelt es sich um eine Aussage zu den RFID-Funktionen. Wenn nach Abschnitt 9 entschieden wird, dass keine PIA erforderlich ist, entspricht dies schon dem Endergebnis.
- f) Abschnitt 11 behandelt im Einzelnen, was zur Erarbeitung der RFID-Anwendungsbeschreibung(en) erforderlich ist. Diese Beschreibung befasst sich mit allen Aspekten vom RFID-Transpondern bis dazu, wie die RFID-Daten innerhalb der Anwendung vorgehalten werden.
- g) Abschnitt 12 behandelt ausführlich die Durchführung der Risikobewertung, beginnend mit den Verweisen auf die Empfehlung, die als Richtlinie für das Verfahren dient. Der Prozess selbst besteht aus:
 - 1) Ermitteln und Zuordnen der Wertigkeiten zu den mit einer Einzelperson verbundenen persönlichen Werten der Privatsphäre;
 - 2) Identifizieren von Bedrohungen für ein RFID-System und Bereitstellen von Mitteln zur Bewertung der Stufe der Bedrohung;
 - 3) Identifizieren der Schwachstellen und Benennen der damit verbundenen Risikostufen;
 - 4) Erreichen einer anfänglichen Risikostufe, ohne Gegenmaßnahmen in Betracht zu ziehen;
 - 5) Berücksichtigen der Gegenmaßnahmen zur Herabsetzung der Bedrohungsstufe, wodurch sich Restrisiken für jeden Bestandwert in der RFID-Anwendung ergeben.
- h) Abschnitt 13 befasst sich ausführlich mit der Zusammenfassung der RFID-PIA, die für die Bürger und Kunden frei zugänglich sein muss.
- i) Abschnitte 14 und 15 befassen sich mit der Notwendigkeit einer Versionskontrolle des Dokuments sowie der Überwachung und der Meldung von Vorfällen, welche die RFID-Anwendung beeinträchtigen.

6 Anwendungsgebiet dieser Europäischen Norm

6.1 'RFID' nach den Festlegungen der EU-RFID-Empfehlung

Auf Grundlage der in der Empfehlung angeführten Definitionen von RFID, RFID-Transponder und RFID-Lesegerät (siehe Abschnitt 3), muss die vorliegende Europäische Norm für alle Technologien gelten, die mit den Frequenzen nach Tabelle 1 übereinstimmen oder arbeiten.

Von daher muss sie für Technologien gelten, die allgemein als RFID, kontaktlose Karten, Nahfeld-Kommunikationsanwendungen (NFC, en: near field communications), persönliche Identifikationskarten und kontaktlose Zahlungskarten bekannt sind und zu Kommunikationszwecken den Funkfrequenzbereich nutzen.

Tabelle 1 — RFID und die entsprechenden Technologienormen innerhalb des Anwendungsbereichs dieser Europäischen Norm

Grundlegende Referenznorm ^a	Verwandte Normen	Frequenz	Siehe Fußnote
ISO/IEC 14443		13,56 MHz	b
ISO/IEC 15693 (alle Teile)	ISO/IEC 18000-3 Mode 1	13,56 MHz	
ISO/IEC 18000-2	ISO 11784 ISO 11785 ISO 14223 (alle Teile)	125 kHz (Typ A) 134,2 kHz (Typ B)	
ISO/IEC 18000-3 Mode 2		13,56 MHz	
ISO/IEC 18000-3 Mode 3		13,56 MHz	c
ISO/IEC 18000-4		2,45 GHz	
ISO/IEC 18000-61	ISO/IEC 18000-6 Type A	860 MHz bis 960 MHz	
ISO/IEC 18000-62	ISO/IEC 18000-6 Type B	860 MHz bis 960 MHz	
ISO/IEC 18000-63	ISO/IEC 18000-6 Type C	860 MHz bis 960 MHz	d
ISO/IEC 18000-64	ISO/IEC 18000-6 Type D	860 MHz bis 960 MHz	
ISO/IEC 18000-7		433 MHz	
ISO/IEC 18092		13,56 MHz	e
ISO/IEC 21481		13,56 MHz	f
JIS X6319-4		13,56 MHz	g
^a Von einigen Normen sind unterschiedliche Ausgaben vorhanden. Mit bestimmten Ausgaben übereinstimmende Artefakte haben gegenüber mit anderen Ausgaben übereinstimmenden Artefakten unterschiedliche Merkmale. ^b ISO/IEC 14443 unterstützt zwei Kommunikationssysteme, die als Typ A und Typ B bekannt sind. Viele im öffentlichen Verkehr verwendete Produkte können ein pre-ISO/IEC 14443, Calypso rev. 1 ein Funkprotokoll nutzen. ^c Auch bekannt als GS1 EPCglobal HF C1. ^d Auch bekannt als GS1 EPCglobal UHF C1 Gen 2. ^e Auch bekannt als NFC IP1. ^f Auch bekannt als NFC IP2. ^g Die Japanische Norm JIS X6319-4 wurde nicht auf ISO-Ebene angenommen, sie wird mitunter aber als FeliCa bezeichnet.			

6.2 ‚RFID-Anwendung‘ nach den Festlegungen der EU-RFID-Empfehlung

Die in der Empfehlung angeführte Definition für RFID-Anwendung (siehe Abschnitt 3) bestimmt genau das Anwendungsgebiet der in dieser Europäischen Norm behandelten RFID-Anwendungen.

6.3 ‚RFID-Betreiber‘ nach den Festlegungen der EU-RFID-Empfehlung

Auf Grundlage der in der Empfehlung angeführten Definition für RFID-Betreiber muss diese Europäische Norm für alle Betreiber gelten, die an einem RFID-Transponder einen Lesevorgang (Entschlüsselung) vornehmen. Sie muss auch für alle Betreiber gelten, die an einem RFID-Transponder einen Schreibvorgang (Verschlüsselung) vornehmen.

Die Anforderung eine PIA durchzuführen, die an eine Organisation, die lediglich Verschlüsselungen vornimmt, gestellt wird, beruht auf zwei Grundvoraussetzungen:

- Allgemein betrachtet, fordert die Europäische Menschenrechtskonvention den Schutz der Privatsphäre von Einzelpersonen und dies gilt für die personenbezogenen Daten und die Möglichkeit der Verfolgung von Standorten und Bewegungen im öffentlichen Raum oder das Erstellen von persönlichen Bewegungsmustern.
- Speziell verweist die Empfehlung, insbesondere in den einleitenden Absätzen 5 und 6 sowie im Empfehlungspunkt 5 (a) ausdrücklich darauf, dass „Betreiber ... eine Abschätzung der Folgen der Anwendungseinführung auf den Schutz personenbezogener Daten und die Wahrung der Privatsphäre durchführen und dabei auch klären, ob die Anwendung zur Überwachung einer Person verwendet werden könnte. Die Ausführlichkeit der Folgenabschätzung sollte den möglichen Datenschutzrisiken, die mit der Anwendung verbunden sind, angemessen sein“.

Dies bedeutet nicht, dass die Organisation, die den Transponder beschreibt, Kenntnisse über andere Anwendungen haben muss, die möglicherweise von anderen RFID-Betreibern genutzt werden, sondern vielmehr, dass der als Beschreiber fungierende RFID-Betreiber die Risiken bezüglich der Wahrung der Privatsphäre beurteilen muss, die von den verschlüsselten Daten und jedem Chip-Identifizierer auf dem Transponder ausgehen, der zur Ortsbestimmung oder zum Erstellen eines persönlichen Verhaltensmusters verwendet wird.

6.4 Zusammenhang von RFID-PIA und Datenschutz und Sicherheit

In Bild 1 ist der Zusammenhang zwischen der RFID-PIA und der Anwendung und zwei weiteren Schlüsselfunktionen dargestellt. Obwohl das PIA-Verfahren unabhängig angewendet wird, gibt es einige Verbindungen zu Prozessen, die die Systemsicherheit und den Datenschutz gewährleisten.

In einigen der in dieser Europäischen Norm beschriebenen Methoden gibt es Parallelen zu den in ISO/IEC 27005 festgelegten Sicherheitsverfahren. Mit der Durchführung der Datenschutzfolgenabschätzung für RFID könnten zudem Risiken erkannt werden, die darauf hinweisen, dass die Sicherheitsaspekte der Anwendung zu überprüfen sind.

Auf Grundlage der Richtlinie 95/46/EG ist der Datenschutz in Europa durch das nationale Recht gesichert. Die RFID-PIA bezieht sich ausschließlich auf den Schutz der in einem RFID-Transponder gespeicherten bzw. die einer RFID-Anwendung zugeordneten Daten. Das heißt, dass die Kombination der RFID-Transponder mit den im Anwendungssystem gespeicherten Daten im öffentlichen Umfeld bezüglich des Datenschutzes zusätzliche Berücksichtigung finden muss. Diese Aspekte werden in dieser Europäischen Norm behandelt.

Alle drei Funktionen haben eines gemeinsam: der Ausfall auch nur einer Funktion hat negative Auswirkungen auf das Ansehen der Organisation. Zum Zeitpunkt der Erarbeitung dieser Europäischen Norm hat eine Organisation jedoch lediglich die rechtlichen Anforderungen an den Datenschutz zu befolgen; derzeit gelten für den Schutz der Privatsphäre und der Datensicherheit die Regeln der guten Praxis („good practice“).

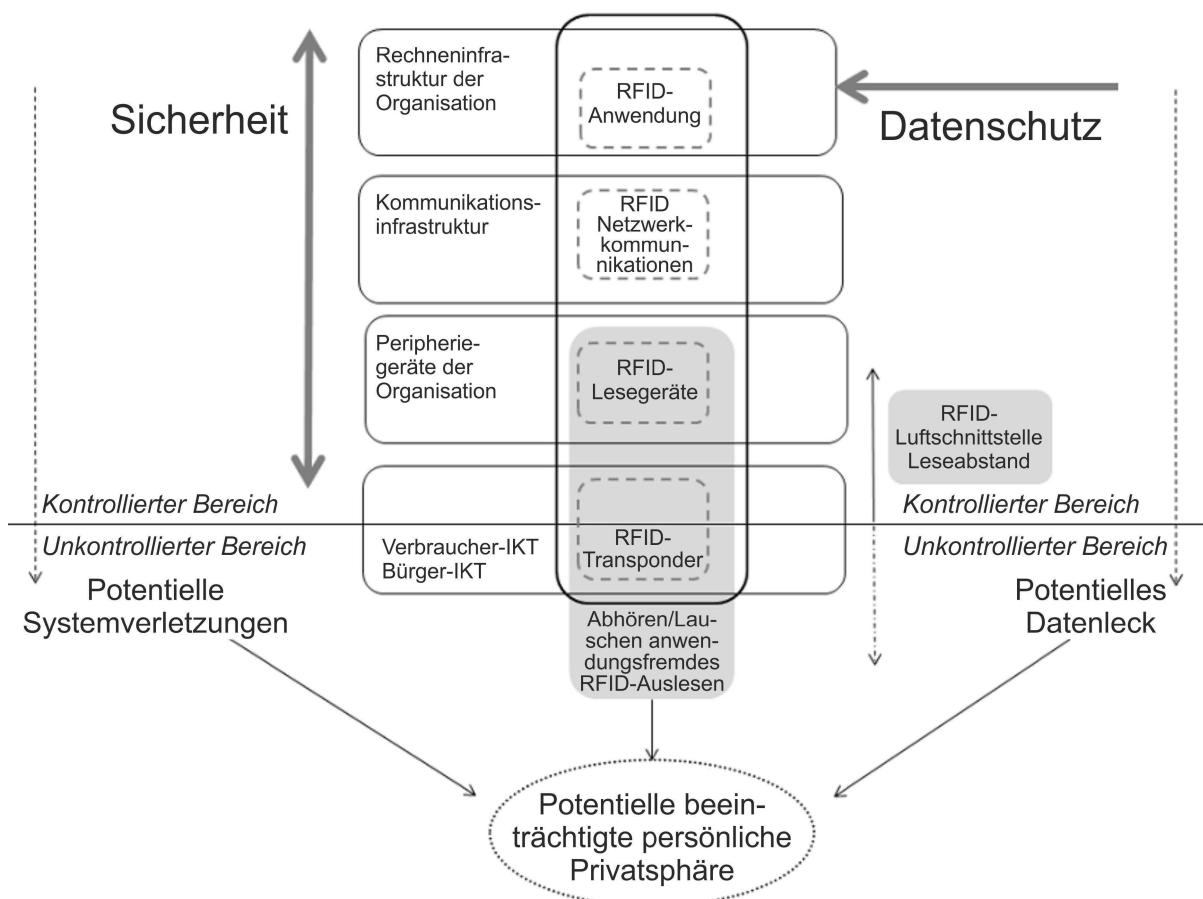


Bild 1 — Wechselseitige Beziehung zwischen den Funktionen des Schutzes der Privatsphäre, der Sicherheit und des Datenschutzes in RFID-Anwendungen

Der Datenschutz betrifft alle Datenverarbeitungsvorgänge wie Datensammlung, Datengenauigkeit und Datenverwendung. Am wichtigsten ist die an ihn gestellte gesetzliche Anforderung an die Einhaltung, wie in der Richtlinie 95/46/EG beschrieben. CEN CWA 16113 definiert eine Reihe freigestellter guter Praktiken, um Unternehmen und Datenverwalter bei der Einhaltung der Richtlinie 95/46/EG zu unterstützen. Das Dokument ist auf die Anwendung durch KMU in der Europäischen Union ausgerichtet.

Die Datensicherheit wird zusätzlich durch Umsetzung von Sicherheitsmaßnahmen zum Schutz von Rechnersystemen erhöht, z. B. durch Anwendung der in der Normenreihe ISO/IEC 270xx festgelegten Verfahren. Es besteht keine rechtliche Vorgabe für die Einführung derartiger Systeme, jedoch können einige Verletzungen der Rechtersicherheit der direkte Grund für eine Datenschutz-Rechtsverletzung sein. Während die Privatsphäre das Recht des Einzelnen ist, über die Verwendung jeder Information über ihn zu bestimmen, stellt dies aus Sicht der RFID-Technik eine Herausforderung zwischen Datenschutz, Datensicherheit und Privatsphäre dar.

Es ist wichtig, die Auswirkungen von kontrollierten und unkontrollierten Bereichen zu verstehen. Innerhalb des kontrollierten Bereichs trägt der RFID-Betreiber (oder Datenverantwortliche) nicht nur die volle Verantwortung, sondern hat auch die Kontrolle über die Anwendung. Wenn ein RFID-Transponder den kontrollierten Bereich verlässt, kann er immer noch in einem der drei folgenden Zustände lesbar sein:

- Er hat das Ende seiner Zweckbestimmung erreicht, kann aber noch gelesen werden, z. B. ein RFID-Transponder auf einem Einzelhandelsprodukt nach Abschluss des Verkaufsgeschäfts in einem Einzelhandelsgeschäft mit RFID-Datenerfassung;
- Er ist dafür vorgesehen zu einem späteren Zeitpunkt oder einem anderen Ort lesbar zu sein, z. B. Beförderungskarte, kontaktlose Zahlungskarte oder Angestelltenzugangsausweis;

- c) Er wurde mit einer RFID-Funktion versehen, jedoch befindet sich am Endpunkt im Prozess keine RFID-Datenerfassung, wobei der RFID-Transponder diesen Punkt im lesbaren Zustand verlässt. Beispiele sind:
- 1) RFID-Gepäckanhänger, wenn der Flughafen beim Abflug eine RFID-Datenerfassung anwendet, aber der Zielflughafen nicht;
 - 2) Einzelhandelsprodukte, die vom Hersteller oder Lieferanten quellenkodiert wurden, aber in Einzelhandelsgeschäften ohne RFID-Möglichkeiten verkauft werden;
 - 3) Bibliotheksbücher, die als Teil eines Bibliothekenverbunds quellenkodiert wurden, aber in einer Bibliothek ohne RFID-Möglichkeiten gehandhabt werden.

Diese drei Zustände stellen drei verschiedene Szenarien für Bürger oder Verbraucher und den Umfang der Kontrolle, die er/sie bei Kenntnis der Verwendung von RFID-Transpondern ausüben kann, dar. Im Fall des Zustands a) sollten Vorortinformationen die Anwendung der RFID-Datenerfassung anzeigen. Beim Zustand b) muss der Person bewusst sein, dass der RFID-Transponder oder die RFID-Karte lesbar bleiben muss, damit sie zukünftig nutzbar ist, was Gegenstand jeglicher Leistungsmerkmale zum Schutz der Privatsphäre ist, die möglicherweise vom Kartenaussteller angewendet werden. Beim Zustand c) gibt es keinen logisch zu erwartenden RFID-Betreiber, und der jeweilige Betreiber wird in der Empfehlung nicht als RFID-Betreiber erachtet, jedoch wird diese Verantwortlichkeit näher zur oder auf die Quelle der Verschlüsselungsdaten auf dem RFID-Transponder übertragen. Die Empfehlung definiert den RFID-Betreiber (siehe Abschnitt 3) eindeutig als die Instanz mit alleiniger oder gemeinsamer Verantwortung für eine RFID-Anwendung.

Der unkontrollierte Bereich hat folgende potenzielle Angriffsstellen:

- Sicherheitsnormen werden entwickelt, um alle Datenverarbeitungsvorgänge des Betreibers vor Zugriff und Verlust zu schützen, und die Normenreihe ISO/IEC 270xx befasst sich tiefgründig mit der Sicherheit vom Kern bis zur Peripherie von Systemen und Netzwerken. Sicherheitsverletzungen können dazu führen, dass Daten der Organisation über ihre Kontrolle hinaus verfügbar werden.
- Datenschutz von Daten, die über Einzelpersonen zusammengetragen wurden, wurde hauptsächlich im kontrollierten Bereich angewendet, wobei einige wenige Anforderungen im Zusammenhang mit dem Schutz von personenbezogenen Daten gelten, wenn ein Transponder den kontrollierten Bereich verlässt. Schlüsseldatenschutz-Herausforderungen für RFID sind Handlungen, zu denen beispielsweise Datensammlung ohne Befugnis, Zweckentfremdung und unkontrollierter Datenaustausch gehören.
- Einige Angriffe auf die Privatsphäre können hinter der Grenze einer rechtmäßigen RFID-Anwendung auftreten, was dem RFID-Betreiber eine gewisse Verantwortung auferlegt, insbesondere hinsichtlich des Menschenrechts auf Schutz der Privatsphäre. Die Privatsphäre konzentriert sich auf die Einzelperson und den Schutz gegen unrechtmäßigen, unbefugten oder unangemessenen und absichtlichen Zugang zur internen Verarbeitung ihrer personenbezogenen Daten und zu ihren personenbezogenen Daten.

Sobald ein RFID-Betreiber eine Kommunikationstransaktion zwischen dem Betreiber-Abfragegerät und dem RFID-Transponder abgeschlossen hat, wird davon ausgegangen, dass der noch von einem anderen Abfragegerät lesbare Transponder in den unkontrollierten Bereich eintritt. Bei RFID-Transpondern, die für den Mehrfachgebrauch vorgesehen sind, ist dies ein normaler Vorgang. Bei Einmalgebrauch-Transpondern kann der RFID-Betreiber davon ausgehen, dass der funktionelle Gebrauch beendet ist. Solange der Transponder jedoch Daten enthält, mit denen eine Person identifizierbar ist, wird die den Transponder mitführende Person begründet erwarten, dass ihre Privatsphäre geschützt ist. Diese Erwartung erstreckt sich bis in den unkontrollierten Bereich und muss vom RFID-Betreiber berücksichtigt werden.

In dem in Bild 1 gezeigten unkontrollierten Bereich gibt es einige Gefährdungen der Privatsphäre, die mit den Daten auf dem Transponder und dessen Leistungsfähigkeit hinsichtlich der Bereitstellung des Schutzes der Privatsphäre zusammenhängen. Diese können durch potenzielle Sicherheitsverletzungen und mögliche Datenlecks bei unkontrolliertem Datenaustausch innerhalb einer Organisation mit anderen Anwendungen oder zwischen Organisationen mit Vereinbarungen zum Datenaustausch „verschärft“ werden. Das mit diesen Datenverlustwegen verbundene Schlüsselproblem für die RFID-Datenschutzfolgenabschätzung ist die Verknüpfbarkeit jeglichen Datenverlusts mit dem RFID-Transponder und dessen Daten.

Mit der laufenden Entwicklung und Ausbreitung der RFID-Technik in einen breiteren Anwendungsbereich ist verbunden, dass durch den RFID-Betreiber jegliche aktuellen oder beabsichtigten Gesetzesänderungen im Hinblick auf die gesetzeswidrige Nutzung der RFID-Technologie durch Einzelpersonen stetig überprüft werden müssen.

Der Einsatz von RFID bringt viele Vorteile mit sich, aber die über die eigentliche Anwendung hinaus auftretenden externen Risiken müssen beachtet werden. Wenn diese äußeren Risiken nicht ausreichend berücksichtigt werden, können RFID-Anwendungen eine Einzelperson Bedrohungen der Privatsphäre und folglich auch eine Organisation einem erhöhten Sicherheits- und Datenschutzrisiko und Reputationsverlust gegenüber der Einzelperson aussetzen.

6.5 Relevante Eingangsdaten für das PIA-Verfahren

6.5.1 Allgemeines

Für die Aufgabenstellung, Barrieren für das RFID-PIA-Verfahren durch Kosten- und Aufwandverringerung zu verringern, beschreibt die vorliegende Europäische Norm in Abschnitt 8 eine Reihe von Effizienzwerkzeugen und Prozessen.

Der Zusammenhang zwischen diesen Maßnahmen und dem Kernprozess ist in den folgenden Unterabschnitten beschrieben.

6.5.2 Angabe der Leistungsmerkmale zum Schutz der Privatsphäre

Die RFID-Technologieanbieter erstellen dieses Dokument, um für bestimmte Transponderprodukte und Lesegeräte die Merkmale für den Schutz der Privatsphäre aufzuzeichnen. Das Dokument fließt früh in das PIA-Verfahren des RFID-Betreibers ein.

6.5.3 Registrierungsstelle

Um die Kosten und den Aufwand für RFID-Technologieanbieter und RFID-Anwendungsbetreiber zu verringern, pflegt die Registrierungsstelle das Verzeichnis der freiwillig eingereichten Angaben der Leistungsmerkmale zum Schutz der Privatsphäre, um als eine gemeinsame Quelle für diese Angaben zu wirken.

Zu den Nutzeffekten gehört eine einmalige Bereitstellung derartiger Angaben durch Technologieanbieter unabhängig von der Kenntnis, welche Anwendungen dem RFID-PIA-Verfahren unterzogen werden. Die RA bietet Anwendungsbetreibern eine leicht zugängliche Quelle für Eingangsdaten, die für ihre PIA notwendig sind. Die RA kann auch Angaben der Leistungsmerkmale zum Schutz der Privatsphäre für bestimmte Transponder und Lesegeräte bereitstellen, die nicht mehr gehandelt werden, aber trotzdem in eine Anwendung integriert werden.

6.5.4 RFID-PIA-Vorlagen

Wenn zwischen RFID-Anwendungen, die von einer Vielzahl von RFID-Betreibern genutzt werden, ein hoher Grad an Gemeinsamkeit besteht, darf von der verantwortlichen gemeinsamen Instanz im Auftrag derartiger Betreiber eine Vorlage erstellt werden, die die für diese Gruppe von Betreibern gemeinsame PIA-Analyse und -Dokumentation enthält. Ein bevorzugter Ansatz für die Vorlage, sofern anwendbar (z. B. die gleiche Anwendung wird über den Binnenmarkt vertrieben), ist eine einzige gesamteuropäische PIA-Vorlage. Derartige gesamteuropäische Vorlagen müssen relevant sein und im Binnenmarkt und europäischen Ländern verwendet werden, ohne dass Änderungen notwendig sind und Beeinträchtigungen für bestimmte Länder oder nationale Vorlieben entstehen.

Die Vorlage ist für einen Betreiber ein Beitrag zum PIA-Verfahren. Sie ermöglicht RFID-Betreibern, die die Vorlage nutzen können, die RFID-PIA mit beträchtlich weniger Aufwand abzuschließen. Die RFID-Betreiber müssen lediglich die Informationen, die in der Vorlage nicht enthalten sind, sowie diejenigen Teile der Datenschutzfolgenabschätzung, die für ihre Anwendung einzigartig sind, bereitstellen, um ihre RFID-PIA fertigzustellen.

7 Organisatorische Ziele des RFID-Betreibers bei einer RFID-PIA

7.1 Überblick

Diese Europäische Norm räumt ein, dass die Wahl der Geschäftssysteme und der Risikomanagementverfahren Unternehmensentscheidungen sind. Insofern müssen die Entscheidungsträger des Unternehmens ausreichend informiert sein, um die geeigneten Entscheidungen bezüglich ihrer RFID-Anwendungen treffen zu können.

In den die technischen Aspekte der RFID-PIA behandelnden Abschnitten werden die Aspekte des Schutzes der Privatsphäre und der Sicherheit in RFID-Anwendungen, die sich überschneiden, gemeinsam als Adressaten einer Risikoanalyse betrachtet. Daher sollten die RFID-Betreiber zur Durchführung der RFID-PIA die Normenreihe ISO/IEC 270xx (siehe Literaturhinweise) heranziehen, die die allgemeinen Sicherheitsfragen genauer beschreibt.

Die organisatorischen Ziele einer RFID-PIA bestehen darin:

- sicherzustellen, dass bei der Anfangsbetrachtung des Entwurfs einer RFID-Anwendung und während des gesamten Systementwicklungsprozesses das Hauptaugenmerk auf dem Schutz der Privatsphäre von Personen liegt;
- sicherzustellen, dass den jeweils verantwortlichen Systementwicklern, Administratoren sowie allen Mitwirkenden einschließlich der anderer Organisationen, zuständiger Stellen und Bereiche die Verantwortung für den Schutz der Privatsphäre eindeutig zugewiesen wird;
- die Entscheidungsträger mit den notwendigen Informationen in die Lage zu versetzen, sachkundig Entscheidungen zu treffen bezüglich der Strategie, des Systementwurfs und der Beschaffungsentscheidung für die RFID-Systeme, Hardware und Transponder für die beabsichtigte RFID-Anwendung;
- die Entscheidungsträger in die Lage zu versetzen, die Auswirkungen und Risiken der RFID-Anwendung für die Privatsphäre zu verstehen, deren Wahrscheinlichkeit des Auftretens abzuschätzen und die zur Verfügung stehenden Möglichkeiten zur Vermeidung und/oder Minderung dieser Risiken sowohl für diese bestimmte RFID-Anwendung als auch für eine den RFID-Transponder mitführende Person über die Grenzen der Anwendung hinaus zu erkennen;
- die Entscheidungsträger durch Informationen in die Lage zu versetzen, dafür zu sorgen, dass das für eine Einzelperson bestehende Restrisiko auf einem vertretbaren Niveau verbleibt;
- ausreichend Informationen zur Verfügung zu stellen, um die Anforderungen in der EU-Empfehlung zur Informationsversorgung und Transparenz in Bezug auf den RFID-Einsatz und die Erarbeitung und Herausgabe kurzgefasster, genauer und leicht verständlicher Angaben zu jeder Anwendung zu erfüllen;
- eine Dokumentation über die Geschäftsprozesse und den Fluss persönlicher Daten im Zusammenhang mit der RFID-Anwendung zur Nutzung und Überprüfung auf Abteilungs- und Geschäftsstellenebene zur Verfügung zu stellen und um unter Berücksichtigung (sofern für die Organisation von Bedeutung) der Interessen bestimmter Verbraucher und Belange von öffentlichem Interesse als Grundlage für Konsultationen mit Kunden, Datenschutzbeauftragten und Vertretern anderer Interessengruppen zu dienen.

Das RFID-PIA-Verfahren muss Folgendes herausarbeiten:

- den internen Kontext in Bezug auf die gesamte vorgesehene Kommunikation zwischen dem RFID-Transponder und der RFID-Anwendung;
- den externen Kontext in Bezug auf den die Anwendungsumgebung der Organisation verlassenden, aber noch funktionstüchtigen RFID-Transponder.

Schließlich sollte das PIA-Verfahren während der Entwicklung, Einführung und Nutzungsdauer einer RFID-Anwendung durchgeführt werden.

7.2 Einhalten und Übertreffen der gesetzlichen Bestimmungen

Diese Europäische Norm wurde im Rahmen der auf der Grundlage der RFID-Empfehlung laufenden Vorhaben erarbeitet. Die gesetzlichen Bestimmungen für Back-End-Systeme sind in der Datenschutzrichtlinie (95/46/EG) festgelegt. Zum Zeitpunkt der Veröffentlichung dieser Europäischen Norm ist keine europäische Gesetzgebung vorhanden, die sich ausdrücklich auf den Schutz der Privatsphäre in RFID-Anwendungen bezieht, welche aber weitestgehend durch die Menschenrechtsbestimmungen und deren Recht auf Privatsphäre abgedeckt ist. In Anbetracht der von jeder Organisation für die RFID-Anwendung vorgenommenen erheblichen Investitionen und der Risiken der Rufschädigung, wenn die mit dieser Technologie verbundenen Leistungsmerkmale nicht untersucht werden, ist es betriebswirtschaftlich sinnvoll, die Datenschutzfolgenabschätzung für RFID durchzuführen.

Die Durchführung einer RFID-PIA sollte für RFID-Betreiber in nationalen, regionalen oder lokalen Verwaltungen oberste Priorität haben.

7.3 Wann ist eine RFID-PIA durchzuführen

7.3.1 Allgemeines

Es gibt viele Situationen, die in den folgenden Unterabschnitten genau bestimmt sind, in denen eine RFID-PIA in Betracht gezogen werden muss. Sofern nach der in den folgenden Unterabschnitten genau beschriebenen Art und Weise vorgegangen wird, kann ein günstiger und kosteneffizienter Ansatz darin bestehen, die RFID-PIA folgendermaßen zu betrachten:

- bei Beginn einer RFID-Anwendung;
- an die Lebensdauer der RFID-Anwendung gekoppelt;
- erneut hinterfragt bei jeder neuen Projektphase, neuen Situation, wesentlichen Änderungen in der Anwendung und/oder Technologie, Änderung in der Verwendung oder Verarbeitung von Informationen/Daten;
- regelmäßig überprüft zu festgelegten Zeitabständen (vergleichbar zu Qualitätsaudits).

7.3.2 Durchführung einer PIA im Entwurfsstadium des RFID-Systems vor dessen Inbetriebnahme

Entsprechend der RFID-Empfehlung ist die RFID-PIA spätestens sechs Wochen vor Inbetriebnahme der Anwendung der zuständigen Stelle zur Verfügung zu stellen (Punkt 5d)). Das bedeutet, dass das PIA-Verfahren zu einem früheren Zeitpunkt beginnen sollte, damit die Risiken ermittelt und behandelt werden können, ehe sie in die Entwicklung einer RFID-Anwendung eingearbeitet werden.

Wenn während der Entwurfsphase keine PIA durchgeführt wird, müssen die Gründe dafür dokumentiert und bei den Datenschutzbehörden bei Bedarf vorgelegt werden.

RFID-Betreiber, die Transponder verschlüsseln, die von anderen gelesen werden, müssen auf Anforderung des RFID-Betreibers, der RFID-Transponder zur Datenerfassung verwendet, ihre PIA zur Verfügung stellen. In vielen Fällen kennt ein RFID-Betreiber, der Transponder verschlüsselt (z. B. in einer Lieferkette, auf einem Flughafen für die Gepäckabfertigung, für kontaktlose Zahlungskarten), nicht die Organisationen, welche die RFID-Datenerfassung implementiert haben. Dies hat in der Praxis zwei Konsequenzen:

- Die von der den RFID-Transponder verschlüsselnden Organisation erstellte PIA muss die Präsenz derartiger Transponder in unkontrollierten Bereichen in Betracht ziehen.
- Zur Verbreitung oder Veröffentlichung des zusammenfassenden PIA-Berichts, die Einzelheiten zu den Daten auf dem Transponder enthält, bedarf es einiger Hilfsmittel.

7.3.3 Durchführung einer PIA bei Überprüfung und Überarbeitung einer auf dem Entwurfsstadium basierenden PIA

Es ist nicht ungewöhnlich, an dem ursprünglichen Systementwurf zwischen Entwurf, Implementierung und der Schulung des zuständigen Personals, Änderungen vorzunehmen. Derartige Änderungen könnten auf die in der Entwurfsphase vorgenommene RFID-PIA Auswirkung haben. Aus diesem Grund sollte die RFID-PIA 6 Monate nach Systemeinführung überprüft werden, um festzustellen, ob die ursprünglichen Risikobewertungen noch Bestand haben oder überarbeitet werden müssen.

Nach Ablauf dieser 6 Monate sollte die RFID-PIA regelmäßig (z. B. einmal im Jahr) überprüft werden.

Außerdem ist bei Änderung der Art von verschlüsselten Daten auf einem RFID-Transponder vom RFID-Betreiber, der diesen Verschlüsselungsprozess fordert oder kontrolliert, außerdem darauf zu achten, dass die PIA überprüft und aktualisiert wird. Diese ist besonders wichtig, wenn personenbezogene Daten, die die Privatsphäre betreffen, hinzugefügt oder dauerhaft vom RFID-Transponder gelöscht werden.

7.3.4 Durchführung einer PIA zur Erstellung einer Vorlage

Angesichts der Tatsache, dass in einigen Branchen eine schon erhebliche Anzahl an RFID-Systemen existiert, sollten die Geschäftsführungen in Betracht ziehen, ein RFID-PIA-Verfahren einer in vollem Umfang funktionsfähigen RFID-Anwendung durchzuführen. Dieser Ansatz könnte Industrieverbände und andere Gruppen in die Lage zu versetzen, auf der Grundlage einer großen Anzahl von praxisbewährten Anwendungen Leitfäden und Vorlagen zu erstellen. Dies steht auch im Einklang mit den Anforderungen in der RFID-Empfehlung zur Informationsversorgung und Transparenz in Bezug auf den RFID-Einsatz. Punkt 7d) fordert „eine Zusammenfassung der Datenschutzfolgenabschätzung“ als Teil der veröffentlichten Angaben zu jeder RFID-Anwendung.

Bei der Gestaltung einer solchen Vorlage sollten externe Interessenvertreter mit einbezogen werden, da dies zu höherem Vertrauen in eine derartige PIA führen kann. Dabei müssen bei der Vorlagenentwicklung bei Teilnahme von gesellschaftlichen Interessenvertretern keine wirtschaftlich sensiblen Daten offengelegt werden.

Ein Vorteil der Erstellung einer branchenbezogenen Vorlage ist die Gewährleistung von branchenweiter Konsistenz, indem die Vorlage ein gewisses Maß von Genauigkeit und Logik innerhalb der branchenbezogenen RFID-PIA-Methodik verfügbar macht.

7.3.5 Durchführung einer PIA mit einer vorhandenen Vorlage

Eine vorhandene Vorlage kann für einen RFID-Betreiber bei der Durchführung einer PIA den Aufwand senken und macht deutlich, dass die betreffende Organisation die Anforderungen der Peer-Group erfüllt oder möglicherweise darüber hinausgeht.

Ein Vorteil einer Vorlage ist, dass sie gemeinsame Merkmale einer Anwendung benennt und somit die Konsistenz bei der Durchführung des PIA-Verfahrens ermöglicht.

Der RFID-Betreiber muss eine gesamteuropäische Vorlage verwenden, wenn es eine derartige Vorlage gibt. Von daher sollte keine andere nationale Vorlage verwendet werden, außer zur Bereitstellung sprachspezifischer Anforderungen.

7.3.6 Durchführung einer PIA nach Einführung einer neuen Funktion in die RFID-Anwendung

Sobald der RFID-Anwendung eine neue Funktion hinzugefügt wird, sollte die vorhandene PIA nach 7.3.3 überprüft werden.

Erfolgt keine neue PIA, sobald der RFID-Anwendung eine neue Funktion hinzugefügt wurde, müssen die Gründe dafür dokumentiert und auf Anforderung bei den Datenschutzbehörden vorgelegt werden.

7.3.7 Durchführung einer PIA auf Grund von Änderungen der RFID-Technologie

Sowie den RFID-Transpondern und Lesegeräten in Zukunft durch Überarbeitung der Ausführung Merkmale des Schutzes der Privatsphäre hinzugefügt werden, sollten diese Erweiterungen entweder fortlaufend (soweit möglich) oder in einer neuen Projektphase berücksichtigt werden. Es wird anerkannt, dass technologische Entwicklungen nicht unmittelbar in eine Anwendung überführt werden können und im Rahmen einer unternehmerischen Gesamtlösung betrachtet werden müssen.

Sobald an der RFID-Anwendung Änderungen der RFID-Technologie vorgenommen werden, ist eine der folgenden Maßnahmen durchzuführen:

- das RFID-PIA-Verfahren muss nach einer Beurteilung durch den RFID-Betreiber überarbeitet werden oder
- sofern kein RFID-PIA-Verfahren durchgeführt wird, müssen die Gründe dafür in der Anwendungsbeschreibung (siehe Abschnitt 11) im Feld für den Bezeichner des PIA-Berichts dokumentiert werden.

BEISPIEL Ein Beispiel dafür könnte sein, dass der RFID-Betreiber das Installieren neuer Lesegeräte dokumentieren möchte, die verbesserte Sicherheitsmerkmale an einigen Transpondern betreffen können. Dies trifft aber bisher für nicht einmal 20 % des Bestands zu. Sobald ein sehr viel größerer Bestand erreicht wurde, erfolgt eine PIA-Neubewertung.

7.3.8 Durchführung einer PIA, nachdem eine Verletzung der Privatsphäre angezeigt wurde

Nach dem Auftreten einer Verletzung der Privatsphäre in der eigenen Anwendung des RFID-Betreibers muss dieser die PIA überprüfen. Es gibt weitere Verletzungen der Privatsphäre von außen, in denen der RFID-Betreiber eine Überprüfung der PIA in Betracht ziehen sollte. Dies schließt Situationen ein, in denen eine Verletzung in dem/der gleichen oder einem/einer ähnlichen:

- Geschäfts- oder Verbandsbereich, in dem der RFID-Betreiber tätig ist;
- Anwendung des RFID-Betreibers;
- vom RFID-Betreiber verwendeten RFID-Produkt

erkannt wurde. Wenn keine PIA durchgeführt wird, nachdem eine Verletzung der Privatsphäre von außen festgestellt wurde, müssen die Gründe dafür dokumentiert und auf Anforderung bei den Datenschutzbehörden vorgelegt werden.

8 Werkzeuge zur Vereinfachung des Verfahrens

8.1 Verantwortung des RFID-Betreibers

Obwohl für die Durchführung der PIA und die Erstellung des PIA-Berichts der RFID-Betreiber verantwortlich ist, können ohne Beeinträchtigung der geforderten Präzision einige Mechanismen verwendet werden, um das Verfahren zu vereinfachen. Nachfolgend werden zusammen mit Hinweisen zur Erarbeitung einige Werkzeuge beschrieben.

8.2 RFID-Technologiewerkzeuge zum Schutz der Privatsphäre – Überblick

Ein Problem bei der Durchführung einer RFID-Datenschutzfolgenabschätzung besteht darin, ausreichend Kenntnis über die von den spezifischen RFID-Produkten unterstützten Merkmale zum Schutz der Privatsphäre und der Sicherheit zu erlangen. Viele Produkte können für sich in Anspruch nehmen, den in Tabelle 1 festgelegten Internationalen Normen zu entsprechen. Da diese Normen aber zahlreiche optionale Leistungsmerkmale besitzen, kann ein RFID-Betreiber oder selbst ein Systemintegrator nicht alle Merkmale kennen, die ein bestimmter Transponder oder ein bestimmtes Lesegerät unterstützt.

Eine allgemeine Faustregel für das RFID-PIA-Verfahren bei einer RFID-Anwendung ist die Annahme, dass die Leistungsfähigkeit der RFID-Lesegeräte das Leistungsmerkmal ist, welches das Luftschnittstellenprotokoll beschränkt. Wenn zum Beispiel ein Lesegerät einen Befehl nicht aufrufen kann, der in dem verwendeten RFID-Transponder für ein bestimmtes Leistungsmerkmal zum Schutz der Privatsphäre und der Sicherheit benutzt wird, trägt dieses Leistungsmerkmal nur wenig oder gar nicht zur unmittelbaren Verbesserung der Gegenmaßnahmen zum Schutz der Privatsphäre und bezüglich Sicherheit über die Luftschnittstelle bei. Derartige Unstimmigkeiten, die durch unterschiedlich vorgenommene Investitionen und verschiedene Produktlebenszyklen von RFID-Lesegeräten und RFID-Transponders bestimmt werden, sind zu erwarten. Während RFID-Lesegeräte grundsätzlich als festinstallierter Teil der Systeminfrastruktur zu betrachten sind, ist es innerhalb der zu erwartenden Lebensdauer der Lesegeräte sehr wahrscheinlich, dass neuere Ausführungen von RFID-Transpondern eingeführt werden.

Einige Produkte können Gegenstand zusätzlicher Interoperabilitäts-, Konformitäts- und Zertifizierungsanforderungen sein. Diese Tatsachen können der Angabe der Leistungsmerkmale zum Schutz der Privatsphäre hinzugefügt werden.

ANMERKUNG Bei einigen Lesegeräten besteht die Möglichkeit, eine Aktualisierung der Firmware oder der Software vorzunehmen, mit der deren Funktionalität verbessert wird. Dieses Leistungsmerkmal ist bei der Erstellung der RFID-PIA zu berücksichtigen.

8.3 Registrierung von Angaben durch RFID-Produkthersteller über die Leistungsmerkmale zum Schutz der Privatsphäre in RFID-Anwendungen

8.3.1 Allgemeines

Dieser Unterabschnitt legt die formalen Anforderungen an ein allgemein zugängliches Verzeichnis der Angaben der Leistungsmerkmale einzelner RFID-Produkte zum Schutz der Privatsphäre in RFID-Anwendungen (z. B. integrierte Schaltungen, Transponder und Lesegeräte) fest, zu denen in 8.4 genauere Angaben gemacht werden.

Um RFID-Betreibern und Systemintegratoren den öffentlichen Zugang zu erleichtern, wurde eine Registrierungsstelle eingerichtet, die mit dem Führen eines solchen Verzeichnisses betraut ist. In den folgenden Unterabschnitten werden die Pflichten der Registrierungsstelle und die Zuständigkeiten der Technologieanbieter festgelegt.

8.3.2 Pflichten der Registrierungsstelle

Die Registrierungsstelle steht gegenüber CEN/TC 225 in der Verantwortung. Ihre Verantwortung besteht darin:

- a) formale Angaben der Leistungsmerkmale zum Schutz der Privatsphäre in RFID-Anwendungen für Produkte zu entwickeln für alle diejenigen in 8.4 beschriebenen Kategorien, die den Anspruch der Übereinstimmung mit einem Luftschnittstellenprotokoll erheben, welches von der vorliegenden Europäischen Norm nicht abgedeckt wird;
- b) Angaben der Leistungsmerkmale zum Schutz der Privatsphäre in RFID-Anwendungen von Organisationen entgegenzunehmen und zu bestätigen, die derartige Angaben zu ihren Produkten bereitstellen, um damit die Durchführung der RFID-PIA in einheitlicher Form zu unterstützen;
- c) nach Erhalt von Angaben der Leistungsmerkmale zum Schutz der Privatsphäre in RFID-Anwendungen diese innerhalb von 30 Tagen auf einer allgemein zugänglichen Datenbank zugänglich zu machen;
- d) die einreichende Organisation darüber zu informieren, dass ihre Angaben der Leistungsmerkmale zum Schutz der Privatsphäre in RFID-Anwendungen in der Datenbank veröffentlicht worden sind;
- e) die Datenbank nach den Festlegungen in 8.3.5 zu pflegen;

- f) Anfragen von RFID-Betreibern zu bearbeiten, die nach Informationen über bestimmte RFID-Produkte suchen, für die in der Datenbank keine Angaben der Leistungsmerkmale zum Schutz der Privatsphäre zur Verfügung stehen; die Registrierungsstelle muss sich mit dem entsprechenden Produkthersteller in Verbindung setzen, die Vorteile hervorheben, in der Datenbank vertreten zu sein und die zur Verfügung zu stellenden Informationen anfordern;
- g) CEN/TC 225 vor jeder Plenarsitzung eine aktuelle Liste aller Angaben der Leistungsmerkmale zum Schutz der Privatsphäre zur Verfügung zu stellen, die der Registrierungsstelle vom RFID-Produkthersteller vorgelegt wurden;
- h) eine öffentliche Quelle einzurichten für aktualisierte Listen der Werte der Privatsphäre, der zugehörigen Datentypen (siehe 12.2), Bedrohungen (siehe 12.3), Schwachstellen und Gegenmaßnahmen (siehe 12.6).

8.3.3 Berufung

Als Registrierungsstelle muss eine vom CEN BT (Technischer Lenkungsausschuss) benannte Körperschaft eingesetzt werden.

Die Informationen über die berufene Registrierungsstelle, ihre Kontaktdetails und die Internetadresse für das Verzeichnis der Angaben der Leistungsmerkmale zum Schutz der Privatsphäre in RFID-Anwendungen können Anhang A entnommen werden.

8.3.4 Kündigung

Sofern die Registrierungsstelle die Notwendigkeit sieht, die Berufung aufzugeben, muss dem Sekretariat von CEN/TC 225 die Kündigung 12 Monate vorher mitgeteilt werden. Das Sekretariat von CEN/TC 225 muss die Ausschreibung einer neuen Registrierungsstelle einleiten. Sollte es innerhalb von 12 Monaten nicht gelingen, eine neue Registrierungsstelle einzusetzen, muss das Sekretariat von CEN/TC 225 zeitweilig die Zuständigkeit übernehmen, bis ein Ersatz gefunden wurde.

Die kündigende Registrierungsstelle muss die aktuelle Datenbankstruktur und die Inhalte dem Sekretariat von CEN/TC 225 so zur Verfügung stellen, dass alles mit minimalem Aufwand der neuen Registrierungsstelle übermittelt werden kann.

8.3.5 Zuständigkeiten der RFID-Produkthersteller

Die Hersteller von RFID-Produkten, wie in 8.4 festgelegt, sind aufgefordert, für alle ihre Produkte die Leistungsmerkmale zum Schutz der Privatsphäre in RFID-Anwendungen vollständig anzugeben. Musterformulare sind in Anhang B enthalten und werden von der Registrierungsstelle in elektronischer Ausführung zur Verfügung gestellt, welche ausführlich in Anhang A dargestellt ist.

ANMERKUNG Die genaue Ausführung der Formulare wird sich von den in Anhang B dargestellten Mustern unterscheiden, sie werden aber von ähnlicher Beschaffenheit sein.

Die RFID-Produkthersteller müssen sich bewusst sein, dass, obwohl die Angaben der Leistungsmerkmale zum Schutz der Privatsphäre in RFID-Anwendungen ein wesentlicher Bestandteil für die Durchführung der RFID-PIA sind, letztendlich die RFID-Betreiber unter Berücksichtigung von Faktoren, die auch die Verwendung der RFID-Produkte einschließt, die Verantwortung für die Durchführung der PIA tragen.

Die RFID-Produkthersteller sollten ihre Rolle bei der Bereitstellung der Angaben der Leistungsmerkmale zum Schutz der Privatsphäre in RFID-Anwendungen als ihren Beitrag zu genauen und einheitlichen RFID-PIAs für RFID-Anwendungen mit ihren Produkten betrachten. Diese Europäische Norm verpflichtet den RFID-Produkthersteller juristisch nicht zu Prüfungen durch eine unabhängige Prüforganisation oder etwa dazu, die vorgelegten Angaben der Leistungsmerkmale zum Schutz der Privatsphäre in RFID-Anwendungen offiziell zertifizieren zu lassen. Es wird davon ausgegangen, dass die Angaben nach bestem Wissen gemacht wurden.

Die Angaben der Leistungsmerkmale zum Schutz der Privatsphäre in RFID-Anwendungen müssen als Selbsterklärung nach bestem Wissen einer bevollmächtigten und fachlich kompetenten Person, die diese Aufgabe übernommen hat, erfolgen.

8.4 Werkzeuge der RFID-Technologie zum Schutz der Privatsphäre – ausführliche Angaben

8.4.1 Leistungsmerkmale von integrierten RFID-Schaltungen zum Schutz der Privatsphäre

Die formalen Angaben der Leistungsmerkmale von integrierten Schaltungen zum Schutz der Privatsphäre sind in B.1 festgelegt. Sie bestehen aus zwei Teilen, und zwar grundlegenden Produkteinheiten und einer eigenständigen Tabelle für die Angaben der Leistungsmerkmale zum Schutz der Privatsphäre. Ausführliche Angaben zum Transponder wie Antennengröße und Lesereichweite sind in den Angaben der Leistungsmerkmale des Transponders enthalten.

Obwohl dieser Anhang die generischen Angaben der Leistungsmerkmale beschreibt, sollte die Registrierungsstelle (siehe 8.3.2) formale Angaben für alle Luftschnittstellenprotokolle erarbeiten. Dies bedeutet, dass derartige Angaben der Leistungsmerkmale zum Schutz der Privatsphäre nur den Bereich der möglichen Funktionen abdecken, die obligatorisch oder optional für das jeweilige Luftschnittstellenprotokoll sind.

8.4.2 Leistungsmerkmale von RFID-Transpondern zum Schutz der Privatsphäre

Die formalen Angaben der Leistungsmerkmale zum Schutz der Privatsphäre sind nicht nur auf die Funktion des Transponders ausgerichtet, verweisen aber auch auf die verwendete integrierte Schaltung. Die formalen Angaben der Leistungsmerkmale zum Schutz der Privatsphäre sind in Anhang B festgelegt. Sie bestehen aus zwei Teilen, und zwar grundlegenden Produkteinheiten und einer eigenständigen Tabelle für die Angaben der Leistungsmerkmale zum Schutz der Privatsphäre.

Obwohl dieser Anhang die Angaben der Leistungsmerkmale für ein spezielles Luftschnittstellenprotokoll beschreibt, sollte die Registrierungsstelle (siehe 8.3.2) formale Angaben für jedes Luftschnittstellenprotokoll erarbeiten. Dies bedeutet, dass solche Angaben der Leistungsmerkmale zum Schutz der Privatsphäre nur den Bereich der möglichen Funktionen abdecken, die obligatorisch oder optional für das jeweilige Luftschnittstellenprotokoll sind.

8.4.3 Leistungsmerkmale von RFID-Lesegeräten zum Schutz der Privatsphäre

Die formalen Angaben der Leistungsmerkmale zum Schutz der Privatsphäre sind in B.2 festgelegt. Sie bestehen aus zwei Teilen, und zwar grundlegenden Produkteinheiten und einer eigenständigen Tabelle für die Angaben der Leistungsmerkmale zum Schutz der Privatsphäre.

Obwohl dieser Anhang die generischen Angaben der Leistungsmerkmale beschreibt, sollte die Registrierungsstelle (siehe 8.3.2) formale Angaben für jedes Luftschnittstellenprotokoll erarbeiten. Dies bedeutet, dass solche Angaben der Leistungsmerkmale zum Schutz der Privatsphäre nur den Bereich der möglichen Funktionen abdecken, die obligatorisch oder optional für das jeweilige Luftschnittstellenprotokoll sind.

8.4.4 Standardmäßige Angaben über Leistungsmerkmale zum Schutz der Privatsphäre

Sofern ein oder mehrere gerätespezifische Angaben über Leistungsmerkmale zum Schutz der Privatsphäre für eine bestimmte Anwendung fehlen, sollten standardmäßige Angaben verwendet werden. Die standardmäßige Angabe über Leistungsmerkmale zum Schutz der Privatsphäre beruht auf der Protokollfestlegung unter Verwendung des Formblatts in Anhang B. Dieser Anhang legt die standardmäßigen Leistungsmerkmale zum Schutz der Privatsphäre für ISO/IEC 18000-63 fest; das Formblatt für andere Luftschnittstellenprotokolle kann abweichen.

Die Reihe der standardmäßigen Angaben über Leistungsmerkmale zum Schutz der Privatsphäre sind dem Verzeichnis zu entnehmen und identifizieren nur die durch einen bestimmten Standard unterstützten obligatorischen Funktionen für den Schutz der Privatsphäre. Da diese standardmäßigen Angaben nicht die optionalen oder unternehmenseigenen Funktionen vom Gerätehersteller enthalten, sollten die RFID-Betreiber darin bestärkt werden, mehr produktbezogene Informationen von ihren Lieferanten anzufordern.

8.4.5 Anwendung von CEN/TR 16672, um Leistungsmerkmale zum Schutz der Privatsphäre für Produkte zu entwickeln, die unternehmenseigene Protokolle verwenden

CEN/TR 16672 kennzeichnet für einen Teil der bekannten RFID-Technologien die Kennwerte von Leistungsmerkmalen zum Schutz der Privatsphäre. Auf dieser Grundlage sollten diese gekennzeichneten Funktionen für die Entwicklung der Angaben der Leistungsmerkmale zum Schutz der Privatsphäre für unternehmenseigene Produkte und Luftschnittstellenprotokolle verwendet werden.

Von den Herstellern von RFID-Produkten, die auf unternehmenseigenen Technologien beruhen, wird dennoch erwartet, das RFID-PIA-Verfahren zu unterstützen, wobei die Angaben der Leistungsmerkmale zum Schutz der Privatsphäre in RFID-Anwendungen ihrer Produkte nur Kunden mitgeteilt werden müssen, die ihre Produkte in RFID-Anwendungen verwenden. Jeder Hersteller, der in einem RFID-Produkt unternehmenseigene Leistungsmerkmale zum Schutz der Privatsphäre einbindet und dies in einer öffentlich verfügbaren Produktspezifikation angibt, sollte eine Angabe der Leistungsmerkmale zum Schutz der Privatsphäre für die Vorlage bei der Registrierungsstelle erarbeiten.

8.5 Vorlagen

8.5.1 Allgemeines

Der Zweck einer Vorlage ist die Verminderung des Aufwands für RFID-Betreiber, die in ihren RFID-Anwendungen gemeinsame Leistungsmerkmale haben, bei der Erstellung eines PIA-Berichts.

Die Verwendung einer Vorlage sollte erwogen werden, wenn eine von Organisationen mit einer gemeinsamen Funktion und/oder um einen bestimmten RFID-Anwendungsstandard herum entwickelte logische Gruppe von ähnlichen RFID-Anwendungen vorliegt. Eine Vorlage ist auch für eine logisch ähnliche Funktion, die RFID-Datenerfassung nutzt, relevant.

Beispiele umfassen, sind aber nicht beschränkt auf:

- Fluggepäckabfertigung;
- Tagungs- und Messeausweise;
- kontaktlose Zahlungssysteme;
- Mitarbeiter-Zutrittskontrollsysteme;
- Lagerverwaltung und Inventur;
- Bibliotheken mit RFID zur Umlaufkontrolle sowie zu anderen Kontrollzwecken;
- Einzelhandelsanwendungen für ein bestimmtes Marksegment;
- RF-basierte Mitgliedskarten, z. B. für Freizeitzentren;
- kontaktlose RF-Karten in öffentlichen Verkehrsmitteln;
- RFID-Apps auf Mobiltelefonen.

Bei der Gestaltung einer Vorlage sollten RFID-Betreiber mit einbezogen werden, da dies zu höherem Vertrauen in eine derartige PIA führen kann. Dabei müssen bei der Vorlagenentwicklung unter Teilnahme der gesellschaftlichen Interessenvertreter keine wirtschaftlich sensiblen Daten offengelegt werden.

Der RFID-Betreiber muss eine gesamteuropäische Vorlage verwenden, wenn es eine derartige Vorlage gibt. Von daher sollte keine andere nationale Vorlage verwendet werden, außer zur Bereitstellung sprachspezifischer Anforderungen.

8.5.2 Erarbeiten einer Vorlage

Es sollte bestimmt werden, ob eine gesamteuropäische Vorlage angemessen ist.

Vorlagen dürfen in einer beliebigen Anzahl von Ausführungen und mit unterschiedlichen Graden der Ausführlichkeit erstellt werden (wie es die Kapazitäten und Erfahrung der Stelle, die die Vorlage erarbeitet, zulassen):

- als formaler PIA-Bericht, der von einzelnen RFID-Betreibern, die Anwendungen mit gemeinsamen Merkmalen haben, eingesetzt wird;
- als eine Analyse der Risiken für den Schutz der Privatsphäre einzelner Datenelemente;
- als Teil des PIA-Verfahrens, wie in den Abschnitten 9 bis 12 festgelegt, möglichst in der Reihenfolge der Abschnitte;
- auf eine oder mehrere der Schichten im RFID-System-Stack ausgerichtet;
- diverse Werkzeuge, Richtlinien oder Prüfverfahren vorbereitend, die auf bestimmte Aspekte des PIA-Verfahrens zielen.

8.5.3 Wer sollte die Vorlagen erstellen?

Vorlagen können von einer Hauptmitgliedsorganisation oder einer begrenzten Anzahl von Mitgliedsorganisationen, zu denen viele der RFID-Betreiber in der Branche gehören, erstellt werden. Diese Tatsache bedeutet, dass die verschiedenen RFID-Betreiber in diesem Branchensektor eine gemeinsame Zielsetzung und grundlegende Regeln haben, nach denen sie kooperieren, aber dennoch (sofern erforderlich) wettbewerbsfähig bleiben. Obwohl es wünschenswert wäre, gibt es keine Anforderungen an derartige Organisationen, und damit auch nicht an die Vorlagen, die sie erstellen, letztere auf die gesamteuropäische Ebene auszuweiten.

Eine die RFID-Betreiber vertretende Organisation darf die Vorlage wie folgt entwickeln:

- Sie kann auf bereits eingeführten zusammengehörigen RFID-Anwendungen beruhen, die es ermöglichen, bei der Erarbeitung der Vorlage auf Erfahrungswerte zurückzugreifen.
- Sie kann parallel zur Entwicklung einer gemeinsamen RFID-Anwendung oder eines Dateninhaltsstandards erarbeitet werden. Dadurch wird sichergestellt, dass die Merkmale zum Schutz der Privatsphäre frühzeitig, während der Standard entwickelt wird, Berücksichtigung finden.
- Lösungsanbieter können ebenfalls Vorlagen erarbeiten.

Wo Lösungsanbietern eine Mitgliedsorganisation zur Seite steht (z. B. ein Handels- oder Berufsverband), sollte diese die Führung bei der Entwicklung einer Vorlage übernehmen. Aufgrund der Wettbewerbssituation bei der Vermarktung einiger Anwendungen ist es für einzelne Unternehmen ein alternativer Ansatz, eine Vorlage für ihre Kundenbasis zu erarbeiten.

Ein Lösungsanbieter oder eine repräsentative Organisation können die Vorlage entwickeln:

- auf der Grundlage eines bereits eingeführten Produkts oder einer Funktion, die es ermöglicht, bei der Erarbeitung der Vorlage auf Erfahrungswerte zurückzugreifen;
- parallel zur Entwicklung neuer Produkteinführungen, wodurch sichergestellt wird, dass die Merkmale zum Schutz der Privatsphäre frühzeitig während der Produkteinführung auf dem Markt Berücksichtigung finden.

8.5.4 Rolle der Interessenvertreter bei der Vorlagenentwicklung

Es gilt als gute Praxis, Interessenvertreter in die Datenschutzfolgenabschätzung einzubinden. Es kann jedoch Schwierigkeiten geben, sollte eine direkte Einbeziehung von Interessenvertretern in ein PIA-Verfahren eines Anwendungsbetreibers die Offenlegung von wirtschaftlich sensiblen Daten beinhalten.

Um diesem Problem zu begegnen, sollten die Interessenvertreter dazu eingeladen werden, an der Entwicklung der PIA-Vorlage teilzunehmen, bei der für einen Betreiber wirtschaftlich sensible Daten nicht einbezogen werden müssen. Die Teilnahme von Interessenvertretern bei der Vorlagenentwicklung kann höheres Vertrauen und Vollständigkeit bei PIAs schaffen, die derartige Vorlagen nutzen.

Aus Sicht vieler Interessenvertreter ist es wünschenswert, dass die Vorlagen innerhalb Europas möglichst breit anwendbar sind, um die Konsistenz des Ansatzes sicherzustellen.

9 RFID-PIA – ein prozessorientierter Ansatz

9.1 Einleitung

Ziel der Datenschutzfolgenabschätzung für RFID ist es, festzustellen, wie angreifbar die Privatsphäre des Einzelnen durch Ausnutzung der Folgeerscheinungen der RFID-Technologie ist, sobald der RFID-Transponder von einer Person getragen wird oder mit einer Person in Verbindung gebracht werden kann.

Zusätzlich werden die RFID-bezogenen Daten im Anwendungssystem gespeichert. Im Allgemeinen ist die Datenschutzrichtlinie 95/46/EG für diese Daten zuständig. Die Einführung von RFID hat jedoch eine komplexere Situation zur Folge, bei der interne und externe Risiken wechselseitig auszuloten sind. Zum Beispiel könnte eine Schwachstelle der RFID-Technologie das Auslesen von Daten aus einem Transponder sein und die Gefahr eines Angriffs auf das Anwendungssystem erhöhen. Sofern aber der RFID-Betreiber die Gegenmaßnahmen für die internen Bedrohungen verstärkt, kann die böswillige „Ausnutzung“ dieser RFID-Schwachstelle reduziert werden. Dies erstreckt sich weit über das hinaus, womit bisher der reine Datenschutz verbunden wurde.

Das RFID-PIA-Verfahren erfordert ein Verständnis des Systems und für die mit dem System verbundenen Bedrohungen der Privatsphäre und die Bedrohungen der Privatsphäre jeder Einzelperson, die durch den Besitz eines RFID-Transponders identifizierbar ist. Das Verfahren erfordert auch eine methodische Kosten-Wirksamkeit-Analyse der Risiken und Gegenmaßnahmen. Ohne diese kann keine geeignete Wahl der Gegenmaßnahmen erfolgen. Die Hervorhebung der „methodischen Kosten-Wirksamkeit-Analyse“ soll den Zusammenhang zur PIA betonen.

BEISPIEL Von einem medizinischen Zentrum, das in der Woche Tausende von RFID-Transaktionen von pharmazeutischen Produkten verarbeitet, wird eine strengere RFID-PIA erwartet, als für einen Einzelhandelsablauf mit der gleichen Anzahl von Transaktionen je Woche mit Lebensmitteln. Der Grund dafür ist, dass die pharmazeutischen Produkte mit dem zu tun haben, was die Richtlinie 95/46/EG als eine indirekte Verbindung mit der „physischen, physiologischen, psychischen“ Identität einer Person definiert.

Es ist wichtig, dass der RFID-Betreiber das PIA-Verfahren in die Anwendungsentwicklung einbindet. Der RFID-Betreiber sollte eine Person oder eine Gruppe von Personen benennen, die für die Durchführung der RFID-PIA verantwortlich ist und die Verantwortung für die Überprüfung der PIA und die fortgesetzte Zweckmäßigkeit der technischen und organisatorischen Maßnahmen trägt, um den Schutz personenbezogener Daten und der Privatsphäre sicherzustellen.

9.2 Verfahrensschritte

Bei der Durchführung der RFID-PIA ist eine Anzahl von Verfahrensschritten einzuhalten. Diese sind:

- a) **SCHRITT 0:** Bereitstellen der Angaben über die RFID-Funktion. Für zahlreiche Anwendungen ist dies die einzige Anforderung und kann gewissermaßen damit gleichgesetzt werden, keine RFID-PIA durchführen zu müssen.
- b) **SCHRITT 1:** Bereitstellen einer ausführlichen Anwendungsbeschreibung.

- c) SCHRITT 2: Erkennen und Zuordnen des Risikos zu den Werten der Privatsphäre wie folgt:
 - 1) persönliche Werte der Privatsphäre einer Einzelperson, die im Besitz eines RFID-Transponders innerhalb einer RFID-Anwendung sowie über die Grenzen der Anwendung hinaus ist;
 - 2) Unternehmenswerte, die mit einer Verletzung der Privatsphäre oder dem Verlust von personenbezogenen Daten durch die RFID-Datenverarbeitung verknüpft sein können.
- d) SCHRITT 3: Ermittlung und Bewertung der Bedrohungen für die Werte der Privatsphäre. Dies gilt für individuelle Werte außerhalb des Bereichs der Anwendung, d. h. Sicherstellung des Schutzes der Privatsphäre. Weiterhin gilt dies auch für und ist verbunden mit Bedrohungen der personenbezogenen Daten, die vom RFID-Betreiber/Datenverantwortlichen gespeichert werden.
- e) SCHRITT 4: Ermittlung der Schwachstellen in Zusammenhang mit den Bedrohungen und den Werten der Privatsphäre.
- f) SCHRITT 5: Durchführen einer Risikobewertung für die Werte der Privatsphäre, wobei das Risiko eine Funktion des Werts, der Bedrohung bzw. der Schwachstelle sein kann, unter Berücksichtigung dessen, dass es eine Reihe von Risiken geben kann.
- g) SCHRITT 6: Ermittlung bestehender und neuer Gegenmaßnahmen, die die Risiken mindern können.
- h) SCHRITT 7: Bestimmung der Restrisiken. Sofern die Abschätzung zu hoch ausfällt, ist ab Schritt 2 neu zu beginnen.
- i) SCHRITT 8: RFID-PIA-Bericht fertigstellen und unterzeichnen.
- j) SCHRITT 9: Fertigstellen und Unterzeichnen des zusammenfassenden RFID-PIA-Berichts, der zu veröffentlichen ist.

Anhang C zeigt ein Ablaufdiagramm für das gesamte PIA-Verfahren.

Anhang D zeigt, wie verschiedene Organisationen zur Entwicklung von Vorlagen beitragen können.

Zur Unterstützung der einzelnen RFID-Betreiber, die den gesamten Prozess durchführen müssen, dienen die in Abschnitt 8 festgelegten Werkzeuge dazu, den Arbeitsaufwand für jeden einzelnen RFID-Betreiber bei der Durchführung der RFID-PIA zu verringern. Dies bedeutet allerdings für die Entwicklung von Vorlagen, dass diese sehr viel genauer, mit mehr Kompetenz und mit mehr ermittelten Risiken erarbeitet werden müssen. Dies heißt nicht, dass eine RFID-PIA-Vorlage zwangsläufig mehr Restrisiken aufzeigt. Stattdessen besteht das grundlegende Ziel darin, sowohl RFID-Betreibern als auch den einzelnen Bürgern in hohem Maß zuzusichern, dass die RFID-PIA einen Großteil der Aspekte berücksichtigt.

9.3 Durchsetzen der richtigen Ausführlichkeit

9.3.1 Allgemeines

Es wird anerkannt, dass die Bestimmung der notwendigen Ausführlichkeit bei der Durchführung eines solchen Prozesses eine Herausforderung bei der Erarbeitung einer RFID-PIA darstellt. Obwohl diese auf der Größenordnung der RFID-Anwendung beruhen könnte, ist es nicht der geeignete Weg, um das Risiko abzuschätzen. Je nach Anwendung kann ein Kleinunternehmen Risiken für eine Einzelperson aufdecken, die so maßgeblich sind wie diejenigen eines großen Unternehmens.

Im PIA-Rahmenwerk wurden vier Stufen der PIA (0 bis 3) vorgeschlagen und ausdrücklich erklärt, dass „die Industrie im Verlauf des Sammelns weiterer Erfahrungen bezüglich ihres Einflusses auf das PIA-Verfahren diese Stufen weiter verfeinern kann“. Diese Europäische Norm ändert nicht die Anzahl der Stufen, aber wie in den nachfolgenden Unterabschnitten dargelegt, wird mit Bezug auf die Prozessschritte in 9.2 präzisiert, wofür jede Stufe steht. Der persönliche Wert der Privatsphäre und die der RFID-Anwendung zugeordneten Datentypen bestimmen weitgehend die Anforderung an eine PIA-Stufe 1, 2, oder 3. Werte der Privatsphäre und die Datentypen sind in 12.2 definiert.

Die folgenden Unterabschnitte und das Ablaufdiagramm in Anhang E definieren den Prozess für jede PIA-Stufe.

9.3.2 Stufe 0 – keine PIA

Sofern ein RFID-Transponder nicht von einer Einzelperson mitgeführt wird oder dieser zugeordnet ist, kann das PIA-Verfahren bei Schritt 0 abgeschlossen werden. Die ausführlichen Anforderungen an die Erarbeitung von Funktionsbeschreibungen sind in Abschnitt 10 festgelegt.

9.3.3 Stufe 1 – PIA von geringem Umfang

Sofern kein Wert und keine Datentypen auf dem RFID-Transponder und zur Anwendung in der Kategorie der persönlichen Privatsphäre nach 12.2 und dem damit verbundenen Anhang festgelegt sind, wird die Analyse des Restrisikos rationalisiert. Wenn Datentypen zur persönlichen Privatsphäre (oder genauer ausgedrückt, die in 12.2 und im zugehörigen Anhang als „PI“ und „PB“ kodierten Datentypen) ausgeschlossen werden können, wird das Abschätzungsverfahren beträchtlich vereinfacht. Trotzdem muss das PIA-Verfahren die Bedrohungen berücksichtigen, die für die Luftschnittstelle bezüglich der verbleibenden Werte und zugehörigen Datentypen sowohl für den kontrollierten als auch den unkontrollierten Bereich gelten (d. h. kodiert als „IT“, „RV“, „TH“ und „TL“).

9.3.4 Stufe 2 – PIA mit Fokus auf den kontrollierten Bereich der Anwendung

Diese Stufe der PIA ist erforderlich, wenn die Anwendung personenbezogene Daten verarbeitet, aber derartige Daten über die persönliche Privatsphäre auf dem RFID-Transponder nicht gespeichert werden. Die Definitionen von Werten und Datentypen für die Kategorie der persönlichen Privatsphäre sind in 12.2 enthalten. Der Prozess der Risikobewertung für eine PIA der Stufe 2 gilt hauptsächlich für den kontrollierten Bereich der Anwendung, wie folgt:

- Das PIA-Verfahren wird auf persönliche Werte der Privatsphäre und ihre zugehörigen Datentypen (oder genauer ausgedrückt, die in 12.2 und im zugehörigen Anhang als „PI“ und „PB“ kodierten Datentypen) nur für die mit RFID verbundenen Daten der Anwendung und des Host-Rechners angewendet. Es kann andere Datenelemente zur Anwendung geben, die außerhalb des Anwendungsbereiches dieser Europäischen Norm liegen, für die aber auch Datenschutzanforderungen gelten.
- Das PIA-Verfahren wird auf alle anderen Datentypen (d. h. kodiert als „IT“, „RV“, „TH“ und „TL“) in allen Schichten im Konzept des gestaffelten Schutzes der Privatsphäre in RFID-Anwendungen angewendet (Bild 2).

9.3.5 Stufe 3 – Vollständige PIA der Anwendung

Diese Stufe der PIA ist die höchste und erforderlich, wenn der RFID-Transponder Datentypen zur persönlichen Privatsphäre, die in 12.2 und im zugehörigen Anhang als „PI“ und „PB“ kodiert sind, enthält. Das PIA-Verfahren wird auf alle Werte angewendet, die mit der RFID-Anwendung verbunden sind. Alle relevanten Bedrohungen müssen in allen Schichten im Konzept des gestaffelten Schutzes der Privatsphäre (Bild 2) risikobeurteilt werden.

9.3.6 Verringerung des Aufwands für kleine und mittlere Unternehmen (KMU)

Die Unternehmen verfügen nicht alle über die gleichen Ressourcen, um eine PIA mit der gleichen Ausführlichkeit vornehmen zu können. Diese Europäische Norm stellt ein Mittel für KMUs zur Verfügung, innerhalb der anerkannten Beschränkungen auf begrenzte Ressourcen eine gründliche PIA durchzuführen.

Diese Verringerung des Aufwands erfolgt, da das Niveau der Expertise und Spezialisierung im kleinsten Unternehmen im Vergleich zu größeren Unternehmen wahrscheinlich geringer ist. Die Verminderung des erforderlichen Aufwands wird auf Werte und ihre Datentypen angewendet, wie in 12.2.3.3 definiert, und auf die in 12.3.4 definierten Bedrohungen. Die Verminderung des Aufwands verringert ungeachtet der Größe des Unternehmens nicht das mit einer RFID-Anwendung verbundene Gesamtrisiko. Das KMU wird nur von der zusätzlichen Verarbeitung geringerer Werte und Bedrohungen entbunden. Ein größeres Unternehmen kann die Ressourcen für eine ganzheitliche Betrachtung aller Werte und Bedrohungen und Ressourcen zum Einführen eines Projekts bezüglich Systemänderungen haben. Das KMU hat voraussichtlich weniger oder keine Ressourcen dafür und kann vollständig auf marktübliche Hardware, Software und externe Expertenberatung angewiesen sein.