

DIN EN 16571

ICS 35.240.60

Einsprüche bis 2013-07-06

Entwurf**Verfahren zur Datenschutzfolgenabschätzung (PIA) von RFID;
Deutsche Fassung prEN 16571:2013**

RFID Privacy Impact Assessment (PIA) process;
German version prEN 16571:2013

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2013-05-06 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN, 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 89 Seiten

Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN

Nationales Vorwort

E DIN EN 16571:2013 wurde vom Europäischen 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 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.

E 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.

Verfahren zur Datenschutzfolgenabschätzung (PIA) von RFID

RFID Privacy Impact Assessment (PIA) process

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: CEN-Umfrage
Dokument-Sprache: D

STD Version 2.5a

Inhalt

Seite

Vorwort	6
Einleitung.....	7
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe	8
4 Symbole und Abkürzungen	10
5 Struktur dieser Europäischen Norm	11
6 Anwendungsgebiet dieser Europäischen Norm.....	12
6.1 ‚RFID‘ nach den Festlegungen der EU-RFID-Empfehlung.....	12
6.2 ‚RFID-Anwendung‘ nach den Festlegungen der EU-RFID-Empfehlung.....	13
6.3 ‚RFID-Betreiber‘ nach den Festlegungen der EU-RFID-Empfehlung.....	13
6.4 Zusammenhang von RFID-PIA und Datenschutz und Sicherheit.....	13
7 Organisatorische Ziele des RFID-Betreibers bei einer RFID-PIA.....	15
7.1 Überblick.....	15
7.2 Einhalten und Übertreffen der gesetzlichen Bestimmungen	16
7.3 Wann ist eine RFID-PIA durchzuführen.....	16
7.3.1 Allgemeines	16
7.3.2 Durchführung einer PIA im Entwurfsstadium des RFID-Systems vor dessen Inbetriebnahme	16
7.3.3 Durchführung einer PIA bei Überprüfung und Überarbeitung einer auf dem Entwurfsstadium basierenden PIA	17
7.3.4 Durchführung einer PIA zur Erstellung einer branchenbezogenen Vorlage	17
7.3.5 Durchführung einer PIA für eine Anwendung auf der Grundlage einer vorhandenen Vorlage.....	17
7.3.6 Durchführung einer PIA nach Einführung einer neuen Funktion in die RFID-Anwendung	17
7.3.7 Durchführung einer PIA auf Grund von Änderungen der RFID-Technologie.....	17
7.3.8 Durchführung einer PIA, nachdem eine Verletzung der Privatsphäre angezeigt wurde.....	18
8 Werkzeuge zur Vereinfachung des Prozesses	18
8.1 Verantwortung des RFID-Betreibers.....	18
8.2 RFID-Technologiewerkzeuge zum Schutz der Privatsphäre – Überblick	18
8.3 Registrierung von Angaben durch RFID-Produkthersteller über die Leistungsmerkmale zum Schutz der Privatsphäre in RFID-Anwendungen.....	19
8.3.1 Allgemeines	19
8.3.2 Pflichten der Registrierungsstelle	19
8.3.3 Berufung	19
8.3.4 Kündigung	20
8.3.5 Zuständigkeiten der RFID-Produkthersteller	20
8.4 Werkzeuge der RFID-Technologie zum Schutz der Privatsphäre – ausführliche Angaben.....	20
8.4.1 Leistungsmerkmale von integrierten RFID-Schaltungen zum Schutz der Privatsphäre.....	20
8.4.2 Leistungsmerkmale von RFID-Transpondern zum Schutz der Privatsphäre	21
8.4.3 Leistungsmerkmale von RFID-Lesegeräten zum Schutz der Privatsphäre	21
8.4.4 Standardmäßige Angaben über Leistungsmerkmale zum Schutz der Privatsphäre.....	21
8.4.5 Anwendung von CEN/TR [00225074], um Leistungsmerkmale zum Schutz der Privatsphäre für Produkte zu entwickeln, die unternehmenseigene Protokolle verwenden	21
8.5 Branchenbezogene Vorlagen	21
8.5.1 Branchensektoren	21
8.5.2 Erarbeiten einer branchenbezogenen Vorlage	22
8.6 Anwendungsbezogene Vorlagen	23
8.6.1 Anwendungen	23

8.6.2	Erarbeiten einer anwendungsbezogenen Vorlage	23
8.7	Erarbeitung einer gemischten Vorlage	23
9	RFID-PIA – ein prozessorientierter Ansatz	24
9.1	Einleitung	24
9.2	Prozessschritte	24
9.3	Durchsetzen der richtigen Ausführlichkeit	25
9.3.1	Allgemeines	25
9.3.2	Stufe 0 – keine PIA	25
9.3.3	Stufe 1 – PIA von geringem Umfang	25
9.3.4	Stufe 2 – PIA für den kontrollierten Bereich der Anwendung	26
9.3.5	Stufe 3 – PIA für den kontrollierten und unkontrollierten Bereich der Anwendung	26
9.4	Methodik des Prozesses	26
10	Bereitstellen der Angaben über die RFID-Funktion	28
11	Ausarbeiten der RFID-Anwendungsbeschreibung	29
11.1	Einführung	29
11.2	Mehrfachanwendungen	29
11.3	Übersicht über die RFID-Anwendung	29
11.3.1	Allgemeines	29
11.3.2	Festlegen der anzuwendenden RFID-Technologie	29
11.3.3	Festlegen der in der Anwendung anzuwendenden RFID-Komponenten	30
11.3.4	RFID-Anwendungen auf tragbaren Geräten	32
11.4	Daten auf dem RFID-Transponder	33
11.4.1	Allgemeines	33
11.4.2	Festlegen, über welche eigenen identifizierbaren Merkmale der RFID-Transponder verfügt	33
11.4.3	Auflistung der auf dem RFID-Transponder verschlüsselten Datenelemente	34
11.4.4	Ermitteln, ob verschlüsselte Daten als identifizierbar betrachtet werden können	34
11.4.5	Ermitteln, ob personenbezogene Daten auf dem Transponder verschlüsselt sind	35
11.5	Weitere Daten in der Anwendung	35
11.6	Verarbeitung von RFID-Daten	35
11.7	Interne Übertragung von RFID-Daten	36
11.8	Externe Übertragung von RFID-Daten	36
11.9	Unterzeichnen der RFID-Anwendungsbeschreibung	36
12	Risikobewertung	37
12.1	Aus der RFID-Empfehlung abgeleitete prozesstechnische Anforderungen	37
12.1.1	Allgemeine prozessspezifische Anforderungen für alle RFID-Betreiber	37
12.1.2	Verfahrensanforderungen an Einzelhändler, die RFID-Betreiber sind	38
12.1.3	Verfahrensanforderungen an Hersteller von Produkten, die möglicherweise an Verbraucher verkauft werden	39
12.2	Ermittlung und Beurteilung des Werts der Privatsphäre	40
12.2.1	Allgemeines	40
12.2.2	Ermittlung des Werts der Privatsphäre	40
12.2.3	Beurteilung der Werte	42
12.3	Ermitteln und Einschätzen von Bedrohungen	45
12.3.1	Allgemeines	45
12.3.2	Ermitteln und Klassifizieren von Bedrohungen	46
12.3.3	Beurteilung von Bedrohungen	47
12.3.4	Vereinfachung des Prozesses für KMUs	48
12.4	Ermitteln der Schwachstellen und Benennen der damit verbundenen Risikostufen	49
12.4.1	Grundlegendes Verfahren	49
12.4.2	Verfahren zur Erfassung der Dauer der Bedrohung	49
12.5	Anfangsrisikostufe	50
12.6	Gegenmaßnahmen	51
12.6.1	Allgemeines	51
12.6.2	Ermitteln von Gegenmaßnahmen	52
12.6.3	Neubewertung der Risikostufen	54
12.7	Restrisiken	54
12.8	Unterzeichnen der RFID-PIA	54

13	Zusammenfassender RFID-PIA-Bericht	54
13.1	Datum des PIA-Berichts	54
13.2	RFID-Anwendungsbetreiber	54
13.3	Überblick über die RFID-Anwendung	55
13.4	Daten auf dem RFID-Transponder	55
13.5	Punktezahl der Datenschutzfolgenabschätzung für RFID	55
13.6	RFID-Kontroll- und Schutzmaßnahmen	55
14	Versionskontrolle.....	56
15	Überwachung und Reaktion auf Vorfälle	56
Anhang A (normativ) Einzelheiten zur Registrierungsstelle		57
Anhang B (informativ) Angaben durch den RFID-Hersteller über Leistungsmerkmale des Produkts zum Schutz der Privatsphäre		58
B.1	Leistungsmerkmale der integrierten RFID-Schaltung (RFID-Chip) zum Schutz der Privatsphäre	58
B.2	Leistungsmerkmale des RFID-Transponders zum Schutz der Privatsphäre	60
B.3	Leistungsmerkmale des RFID-Lesegeräts zum Schutz der Privatsphäre	61
Anhang C (informativ) RFID-Funktionsbeschreibung		63
Anhang D (informativ) RFID-Anwendungsbeschreibung.....		64
Anhang E (informativ) Ermittlung und Bewertung von persönlichen Werten der Privatsphäre		65
E.1	Einzel gespeicherte, persönliche Werte der Privatsphäre	65
E.2	Werte für das Unternehmen.....	69
Anhang F (informativ) RFID-Bedrohungen		70
F.1	Bedrohungen im Zusammenhang mit auf dem RFID-Transponder codierten Daten und mit dem RFID-Transponder (oder der RF-Karte) selbst	70
F.1.1	Allgemeines	70
F.1.2	Seitenkanalattacke.....	71
F.1.3	Physische Datenmodifikation.....	71
F.1.4	Klonen	71
F.1.5	Spoofing	71
F.1.6	Physischer Austausch des Transponders	71
F.1.7	Umlenkung des RF-Transponders	72
F.1.8	Umprogrammierung des Transponders	72
F.1.9	Entfernung des Transponders	72
F.1.10	Zerstörung des Transponders.....	72
F.1.11	Deaktivierung des Transponders durch Befehlsmissbrauch	72
F.1.12	Erschöpfung von Protokollressourcen	73
F.1.13	Desynchronisationsangriff	73
F.2	Bedrohungen im Zusammenhang mit der Luftschnittstelle oder mit der Kommunikation über die Geräteschnittstelle	73
F.2.1	Allgemeines	73
F.2.2	Unberechtigtes Auslesen des Transponders	74
F.2.3	Verfolgung	74
F.2.4	Datenverknüpfung	75
F.2.5	Erstellen eines Verhaltensprofils	75
F.2.6	Erstellen einer Favoritenliste.....	75
F.2.7	Abhören oder Verkehrsanalyse.....	75
F.2.8	Energieanalyse.....	75
F.2.9	Angriffe auf die Verschlüsselung.....	76
F.2.10	Reverse Engineering	76
F.2.11	Datenweitergabe oder Mittelsmannangriff (man-in-the-middle-Angriff).....	76
F.2.12	Angriff durch Wiedereinspielung	76
F.2.13	(Wieder-)Aufbau der Nachricht.....	76
F.2.14	Datenmodifikation bei der Übertragung an der Luftschnittstelle	77
F.2.15	Einfügen von Daten bei der Übertragung an der Luftschnittstelle.....	77
F.2.16	Rauschen	77

F.2.17	Störsender (Jamming)	77
F.2.18	Böswillige Blocker-Transponder	77
F.2.19	Auswirkungen einer Schwächung der Funkübertragung	78
F.2.20	Abschirmung von Transpondern	78
F.3	Bedrohungen im Zusammenhang mit dem Lesegerät	78
F.3.1	Allgemeines	78
F.3.2	Seitenkanalattacke	78
F.3.3	Erschöpfung von Protokollressourcen	78
F.3.4	Desynchronisationsangriff	78
F.4	Bedrohungen im Zusammenhang mit der Host-Anwendung	79
F.4.1	Allgemeines	79
F.4.2	Verletzung der Privatsphäre und des Datenschutzes	79
F.4.3	Gefährdung von Sicherheitsschlüsseln	80
F.4.4	Angriff durch Pufferüberlauf	80
F.4.5	Eingeben eines böswilligen Codes	80
F.4.6	Teilweise Dienstverweigerung	80
F.4.7	Vollständige Dienstverweigerung	80
Anhang G (informativ)	Gegenmaßnahmen	81
G.1	Liste der Gegenmaßnahmen	81
G.2	Zuordnung zwischen Bedrohungen und Gegenmaßnahmen	83
Anhang H (informativ)	Zusammenfassung der Datenschutzfolgenabschätzung von RFID	86
Literaturhinweise		87

Vorwort

Dieses Dokument (prEN 16571:2013) wurde vom Technischen Komitee CEN/TC 225 „AIDC Technologies“ erarbeitet, dessen Sekretariat vom NEN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Die Europäische Norm „Verfahren zur Datenschutzfolgenabschätzung (PIA) von RFID“ ist eine Norm aus einer Reihe durchzuführender Arbeiten, die gemeinsam zu Phase 2 des Mandats M/436 gehören.

Die anderen Ergebnisse sind:

- EN ISO/IEC 29160: Informationstechnik — Identifizierung von Waren mittels Hochfrequenz (RFID) für das Management des Warenflusses — RFID-Emblem
- CEN-Spezifikation: Notifizierung von RFID — Das Informationszeichen, das in Bereichen bereitgestellt werden muss, in denen RFID-Lesegeräte eingesetzt werden
- CEN-Fachbericht: Notifizierung von RFID — Zusätzliche Informationen, die von den Betreibern bereitgestellt werden müssen
- Europäische CEN-Norm: Notifizierung von RFID — Das Informationszeichen und zusätzliche Informationen, die bei der Datenerfassung mittels RFID von den Betreibern entsprechender Anwendungen bereitgestellt werden müssen
- CEN/TR [00225074]: AIDC-Verfahren — Aspekte des Schutzes von Informationen, der Privatsphäre und der Daten im Zusammenhang mit RFID-Anwendungen — Leistungsmerkmale für den Schutz der Privatsphäre in gegenwärtigen RFID-Technologien
- CEN/TR [00225076]: AIDC-Verfahren — Aspekte des Schutzes von Informationen, der Privatsphäre und der Daten im Zusammenhang mit RFID-Anwendungen — Analyse von PIA-Methoden für RFID
- CEN/TR [00225075]: AIDC-Verfahren — Aspekte des Schutzes von Informationen, der Privatsphäre und der Daten im Zusammenhang mit RFID-Anwendungen — RFID-PIA-Analyse für spezielle Branchen
- CEN-Fachbericht: Bedrohungs- und Gefährdungsanalyse für RFID
- CEN-Fachbericht: Autorisierung von Mobiltelefonen bei Verwendung als RFID-Lesegeräte
- CEN-Spezifikation: Geräteschnittstelle für Mode-1- und Mode-3-Tags nach ISO/IEC 18000-3

ANMERKUNG Referenznummern werden bei Verfügbarkeit ergänzt und die Titel werden gegenwärtig in Übereinstimmung mit den CEN-Bestimmungen überarbeitet.

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 elf durchzuführenden Arbeiten der Phase 2 des Mandats M/436. Sie beruht auf den Untersuchungen in den beiden zugehörigen Fachberichten:

- *RFID-PIA-Analyse für spezielle Branchen*, der 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 gibt;
- *Analyse von PIA-Methoden für RFID*, welcher bereits formal vorliegende PIAs, die aber nicht zwangsläufig in nationale Normen überführt wurden, untersucht.

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 und damit im Zusammenhang stehende Technologien. Insofern dient sie als Referenz für die anderen 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 sind eine Reihe normierter Verfahren zur Erarbeitung von PIA-Vorlagen enthalten, dazu gehören Werkzeuge, die mit RFID betreffenden PIA-Methoden kompatibel sind.

Zusätzlich werden die Bedingungen aufgeführt, die erforderlich sind, um eine vorhandene PIA durch einen neuen Bewertungsprozess zu überarbeiten, zu ändern oder zu ersetzen.

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).

prCEN/TR [00225074]¹, *AIDC - Verfahren - Aspekte des Schutzes von Informationen, der Privatsphäre und der Daten im Zusammenhang mit RFID-Anwendungen - Leistungsmerkmale für den Schutz der Privatsphäre in gegenwärtigen RFID-Technologien*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1 Gegenmaßnahme
Maßnahme, Gerät, Verfahren oder Methode, die einer Bedrohung, einer Schwachstelle oder einem Angriff eliminierend oder schützend begegnet oder gegenübersteht (d. h. entgegenwirkt), indem sie den möglichen Schaden begrenzt, bzw. ihn aufdeckt und anzeigt, damit Korrekturmaßnahmen ergriffen werden können

[Quelle: IETF 4949]

3.2 Überwachung
jede Tätigkeit zur Ermittlung, Beobachtung, Kopie oder Aufzeichnung des Aufenthaltsorts, der Bewegung, der Tätigkeiten oder des Zustands einer Person

[Quelle: RFID-Empfehlung C(2009) 3200 endgültig]

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

[Quelle: Richtlinie 95/46/EG]

1) prCEN/TR [00225074] ist gegenwärtig in Bearbeitung und wird Ende 2013 zur Verfügung stehen.

3.4

persönlicher Wert der Privatsphäre

alles, was für eine natürliche Person von Wert ist, der ein bestimmter RFID-Transponder oder eine RF-Karte zugeordnet werden kann; es ist erforderlich, diesen Wert vor Verlust zu schützen

3.5

Privatsphäre

Recht des Einzelnen darauf, dass seine Identität, seine Tätigkeit und sein 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]

3.6

RFID (Radio Frequency Identification)

Identifizierung mittels Hochfrequenz

Verwendung elektromagnetischer Funkwellen oder induktiver Kopplung im Funkfrequenzbereich des Spektrums, um eine Kommunikation von oder zu einem Transponder durch unterschiedliche Modulations- und Codierungsschemata aufzubauen, sodass die Identität eines RF-Transponders eindeutig bestimmt werden kann

[Quelle: ISO/IEC 19762-3]

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 der Kennung eines RFID-Transponders oder anderer darin gespeicherter Daten

[Quelle: RFID-Empfehlung C(2009) 3200 endgültig]

3.7

Restrisiko

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

[Quelle: ETSI TR 187 020]

3.8

RFID-Anwendungsbetreiber

RFID-Betreiber

natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten einer RFID-Anwendung entscheidet, dazu gehören die für die Verarbeitung personenbezogener Daten Verantwortlichen, die eine RFID-Anwendung benutzen

[Quelle: RFID-Empfehlung C(2009) 3200 endgültig]

3.9

RFID-Transponder

RF-Transponder

Tag

Transponder

auf einem Objekt befestigter Transponder, einschließlich des Mechanismus zur Speicherung von Informationen

Anmerkung 1 zum Begriff: Obwohl Transponder der technisch genaueste Ausdruck ist, ist (im englischen Sprachraum) die Bezeichnung Tag oder RFID-Tag geläufiger und wird bevorzugt.

[Quelle: ISO/IEC 19762-3]

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

[Quelle: RFID-Empfehlung C(2009) 3200 endgültig]

3.10

RFID-Bedrohung

Physikalischer, Hardware oder Software -Mechanismus, der die Ursache für nachteilige Auswirkungen auf einen Bestandswert durch unautorisierten Zugriff, Zerstörung, Bekanntgabe, Manipulation von Daten und/oder Dienstverweigerung (en denial of service) sein könnte

[Quelle: ENISA, modifiziert]

3.11

RFID-Schwachstelle

Angreifbarkeit eines Bestandswerts oder mehrerer Bestandswerte, die durch eine oder mehrere Bedrohungen ausgenutzt werden kann

[Quelle: ISO/IEC 27005, modifiziert]

3.12

Risiko

Möglichkeit, dass eine bestimmte Bedrohung Schwachstellen eines Bestandswerts oder mehrerer Bestandswerte ausnutzt und damit dem angegriffenen System oder der angegriffenen Organisation Schaden zufügt

[Quelle: ETSI TR 187 020]

4 Symbole und Abkürzungen

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

EPC Elektronischer Produktcode (Electronic Product Code)

GS1 Global Standards One

HF Hochfrequenz (High Frequency)

NFC Nahfeldkommunikation (Near Field Communication)

PIA Datenschutzfolgenabschätzung (Privacy Impact Assessment)

RF Funkfrequenz (Radio Frequency)

RFID Identifizierung mittels Hochfrequenz (Radio Frequency Identification)

SME KMU, kleine und mittlere Unternehmen (Small and medium sized enterprises)

UHF Ultrahochfrequenz (Ultra High Frequency)

5 Struktur dieser Europäischen Norm

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

- Abschnitt 6 gibt an, was aus Sicht der RFID-Empfehlung eine RFID-Technologie ist und was ein RFID-Betreiber ist (dies ist nicht unbedingt deckungsgleich mit der Struktur des Arbeitsgebiets und Aufgabenbereichs unterschiedlicher Technologie –Standards-setzender Komitees verschiedener Standardisierungsgremien für Technologie – Standards.
- 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.
- 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.
- Abschnitt 9 ist der erste Abschnitt, der den eigentlichen Prozess der Datenschutzfolgenabschätzung für RFID behandelt. Dieser Abschnitt befasst sich insbesondere mit der obersten Ebene, in der die erforderliche Ausführlichkeit der PIA bestimmt wird.
- Abschnitt 10 befasst sich mit der untersten Ebene der Ergebnisse des PIA-Prozesses, 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.
- 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.
- 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:
 - Ermitteln und Zuordnen der Wertigkeiten zu den mit einer Einzelperson verbundenen persönlichen Werten der Privatsphäre;
 - Identifizieren von Bedrohungen für ein RFID-System und Bereitstellen von Mitteln zur Bewertung der Stufe der Bedrohung;
 - Identifizieren der Schwachstellen und Benennen der damit verbundenen Risikostufen;
 - Erreichen einer anfänglichen Risikostufe, ohne Gegenmaßnahmen in Betracht zu ziehen;
 - Berücksichtigen der Gegenmaßnahmen zur Herabsetzung der Bedrohungsstufe, wodurch sich Restrisiken für jeden Bestandwert in der RFID-Anwendung ergeben.
- Abschnitt 13 befasst sich ausführlich mit der Zusammenfassung der RFID-PIA, die für die Bürger und Kunden frei zugänglich sein muss.
- 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

In der Empfehlung sind drei Begriffe festgelegt, mit denen das Anwendungsgebiet der in dieser Europäischen Norm behandelten Technologien genauer bestimmt werden kann:

- a) „Identifizierung mittels Hochfrequenz“ (RFID) ist die Nutzung elektromagnetischer Wellen oder der elektromagnetischen Nahfeldkopplung im Funkbereich des Frequenzspektrums für die Kommunikation von oder zu einem RFID-Transponder mit Hilfe verschiedener Modulations- oder Kodierungstechniken für das eindeutige Auslesen der Kennung eines RFID-Transponders oder anderer darin gespeicherter Daten;
- b) „RFID-Transponder“ oder „Tag“ ist entweder ein RFID-Gerät, das in der Lage ist, ein Funksignal zu erzeugen, oder ein RFID-Gerät, das ein von einem Lese- oder Schreibgerät empfangenes Trägersignal rückkoppelt, rückwärtsstret oder reflektiert (je nach Art des Geräts) und moduliert;
- c) „RFID-Lese- oder Schreibgerät“ oder „Lesegerät“ ist ein festes oder mobiles Datenerfassungs- und Identifizierungsgerät, das durch eine elektromagnetische Welle oder durch elektromagnetische Nahfeldkopplung im Funkfrequenzbereich von einem oder mehreren RFID-Transpondern eine Antwort in Form modulierter Daten anregt und bewirkt.

Dies bedeutet, dass diese Europäische Norm für jene Technologien gelten muss, die im Allgemeinen unter den Begriffen RFID, Chipkarten, persönliche Identifikationskarten und kontaktlose Zahlungskarten bekannt sind, welche zu Kommunikationszwecken den Funkfrequenzbereich nutzen. Insbesondere gilt sie für die in Tabelle 1 aufgeführten bzw. die mit den hier angegebenen Frequenzen operierenden Technologien.

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

Grundlegende Referenznorm	Verwandte Normen	Frequenz
ISO/IEC 14443		13,56 MHz
ISO/IEC 15693	ISO/IEC 18000-3 Mode 1	13,56 MHz
ISO/IEC 18000-2	ISO 11784 ISO 11785 ISO 14223	
ISO/IEC 18000-3 Mode 3	GS1 EPCglobal HF C1	13,56 MHz
ISO/IEC 18000-4		
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 GS1 EPCglobal UHF C1 Gen 2	860 MHz bis 960 MHz
ISO/IEC 18000-64	ISO/IEC 18000-6 Type D	860 MHz bis 960 MHz
ISO/IEC 18000-7		433 MHz
ISO/IEC 18092	NFC IP1	
ISO/IEC 21481	NFC IP2	
JIS X6319-4	FeliCa	13,56 MHz
ANMERKUNG 1 Von einigen Normen sind unterschiedliche Ausgaben vorhanden. Mit bestimmten Ausgaben übereinstimmende Artefakte haben von mit anderen Ausgaben übereinstimmenden Artefakten sich unterscheidende Merkmale.		
ANMERKUNG 2 ISO/IEC 14443 unterstützt zwei Kommunikationssysteme, die als Typ A und Typ B bekannt sind. Viele im öffentlichen Verkehr verwendete Produkte können mit Calypso rev. 1 ein Funkprotokoll vor ISO/IEC 14443, das als Typ B bekannt ist, nutzen. Die Japanische Norm JIS X6319-4 wurde nicht auf ISO-Ebene angenommen, sie wird mitunter aber als ISO/IEC 14443, Typ C, bezeichnet.		

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

In der Empfehlung ist eine Definition festgelegt, mit der das Anwendungsgebiet der in dieser Europäischen Norm behandelten Technologien genauer bestimmt werden kann:

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

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

Der in der Empfehlung festgelegte Begriff, mit dem das Anwendungsgebiet der in dieser Europäischen Norm behandelten Technologien genauer bestimmt werden kann, ist:

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

Dies bedeutet, dass diese Europäische Norm für alle Betreiber gelten muss, 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.

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 der PIA - Prozess unabhängig von der RFID-Anwendung angewendet wird, gibt es einige Verbindungen zu Prozessen, welche 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 Datenschutzfolgenabschätzung für RFID 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-Transponders 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; deren Verletzung kann zusätzlich zu einem Imageschaden auch zu Geldstrafen führen.

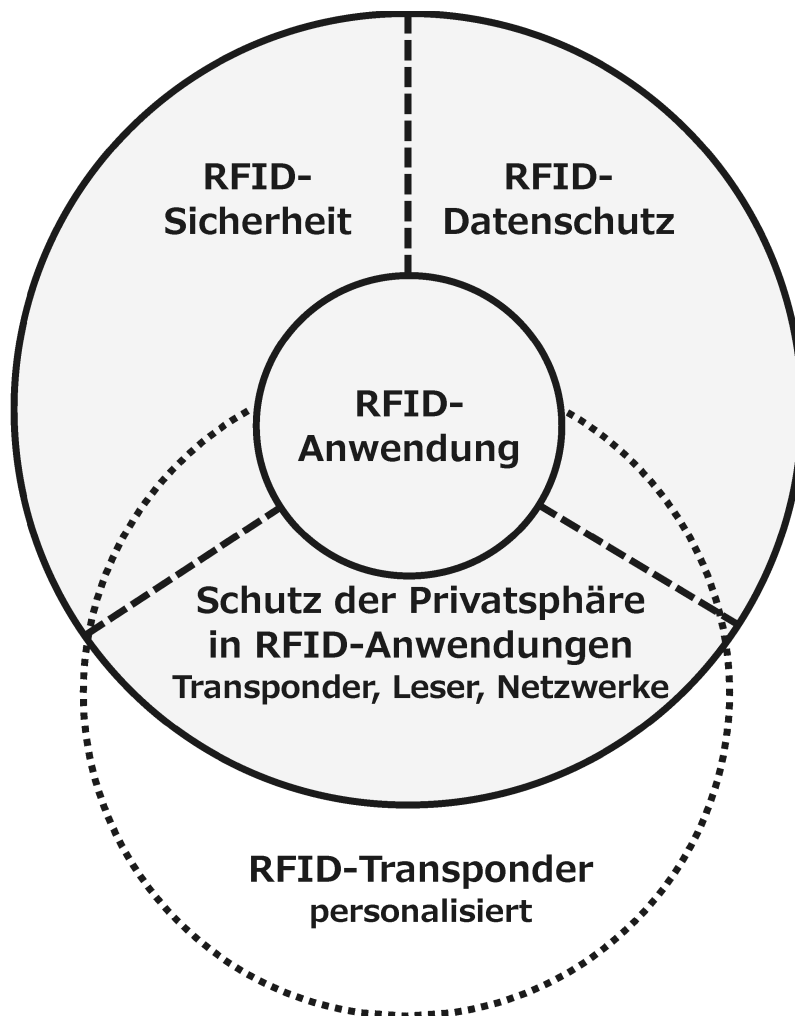


Bild 1 — Wechselseitige Beziehung zwischen den Funktionen des Schutzes der Privatsphäre, der Sicherheit und des Datenschutzes in RFID-Anwendungen

Der schraffierte Kreis mit durchgehender äußerer Begrenzungslinie stellt die RFID-Anwendung dar. Der RFID-PIA-Prozess verlangt vom RFID-Betreiber die Konsequenzen aus dem Speichern der Daten auf dem RFID-Transponder, die im Kreis mit gepunkteter Linie dargestellt sind, zu bedenken. Dies verdeutlicht die Einfluss des RFID-Transponders auf die Privatsphäre und ebenso auf die Sicherheit und den Datenschutz. Die Verantwortung des RFID-Betreibers über die Anwendung erweitert sich darüber hinaus auf den Bereich der Privatsphäre. Der schraffierte Kreis stellt den „kontrollierten“ Bereich dar, während der Kreisabschnitt mit gepunkteter Linie, aber außerhalb des kontrollierten Bereichs, als „unkontrollierter“ Bereich angesehen werden kann. Der Anwendungsrahmen dieser Europäischen Norm erstreckt sich über diesen Bereich, in dem die RFID-Schwachstellen ausgenutzt werden können.

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

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. Obwohl diese Europäische Norm auf den Schutz der Privatsphäre in RFID-Anwendungen ausgerichtet ist, darf der Prozess der RFID-PIA auch um die Sicherheitsaspekte, welche die Geschäftsrisiken abdecken und die völlig unabhängig von den Risiken des Schutzes der Privatsphäre sind, erweitert werden.

BEISPIEL Während die mit der drahtlosen Geräteschnittstelle (zwischen RFID-Lesegerät und Anwendung) zusammenhängenden Risiken der Privatsphäre für eine Einzelperson, die im Besitz eines Transponders oder einer RF-Karte ist, gelten können, kann die gleiche Schnittstelle anfällig für die Bedrohung einer Dienstverweigerung für das Unternehmen sein.

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, welche die allgemeinen Sicherheitsfragen genauer beschreibt.

Die organisatorischen Ziele einer RFID-PIA bestehen darin:

- zu gewährleisten, dass bei der Anfangsbetrachtung des Entwurfs einer RFID-Anwendung und während des gesamten Systementwicklungsprozesses das Hauptaugenmerk auf dem Schutz der Privatsphäre von Personen liegt;
- zu gewährleisten, 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 Einschränkung 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 nicht auf einem unannehmbaren Niveau verbleibt;
- ausreichend Informationen zur Verfügung zu stellen, um die Anforderungen in der 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.

Der RFID-PIA-Prozess muss Folgendes herausarbeiten:

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

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 festgelegt (95/46/EG). 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 Abschnitten genau bestimmt sind, in denen eine RFID-PIA in Betracht gezogen werden muss. Sofern nach der in den folgenden Abschnitten genau beschriebenen Art und Weise vorgegangen wird, kann ein günstiger und kosteneffizienter Ansatz darin bestehen, die RFID-PIA zu betrachten als:

- einen fortwährenden Prozess;
- an die Lebensdauer der RFID-Anwendung gekoppelt und
- erneut zu hinterfragen in jeder neuen Projektphase oder neuen Situation.

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

Der RFID-Empfehlung gemäß soll die RFID-PIA spätestens sechs Wochen vor Inbetriebnahme der Anwendung der zuständigen Stelle zur Verfügung gestellt werden (Punkt 5d). Das hat zur Folge, dass der PIA-Prozess zu einem früheren Zeitpunkt beginnen sollte, damit die Risiken ermittelt und behandelt werden können ehe sie in das Design einer RFID-Anwendung eingearbeitet werden.

Sofern keine PIA während der Entwurfsphase 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 ist es einem RFID-Betreiber, der Transponder verschlüsselt (z. B. in einer Lieferkette, auf einem Flughafen für die Gepäckabfertigung, für kontaktlose Zahlungskarten), unmöglich, die Organisationen, welche die RFID-Datenerfassung implementiert haben, zu kennen. Dies hat in der Praxis zwei Konsequenzen:

- Die von der den RFID-Transponder verschlüsselnden Organisation erstellte PIA muss die Präsenz solcher Transponder in unkontrollierten Bereichen in Betracht ziehen.
- Zur Verbreitung oder Veröffentlichung solch einer PIA bedarf es einiger Hilfsmittel. In den zuvor aufgeführten Beispielen könnte dies über einen Branchenverband geschehen, insbesondere wenn dieser bereits eine branchenbezogene PIA erarbeitet hat.

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

Es ist nicht ungewöhnlich, an dem ursprünglichen Systementwurf nach dessen Einführung und der Schulung des zuständigen Personals Änderungen vorzunehmen. Solche Änderungen könnten auf die in der Entwurfsphase vorgenommene RFID-PIA Auswirkung haben. Die RFID-PIA sollte 6 Monate nach Systemeinführung überprüft werden, um festzustellen, ob die ursprüngliche Risikobewertung noch Bestand hat oder überprüft werden muss.

Bei Änderung von verschlüsselten Daten auf einem RFID-Transponder ist vom RFID-Betreiber darauf zu achten, dass der Verschlüsselungsprozess überprüft und die PIA überarbeitet wird.

7.3.4 Durchführung einer PIA zur Erstellung einer branchenbezogenen Vorlage

Angesichts der Tatsache, dass in einigen Branchen eine schon erhebliche Anzahl an RFID-Systemen existiert, könnten die Geschäftsführungen in Betracht ziehen, einen RFID-PIA-Prozess 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 den Empfehlungen 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 branchenbezogenen Vorlage sollten als vertrauensbildende Maßnahme in eine solche PIA gesellschaftliche Interessenvertreter mit einbezogen werden. Dabei müssen bei der Vorlagen – Entwicklung unter Teilnahme der gesellschaftlichen Interessenvertreter keine wirtschaftlich sensiblen Informationen enthüllt 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 für eine Anwendung auf der Grundlage einer vorhandenen Vorlage

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

Ein Vorteil der Erstellung einer anwendungsbezogenen Vorlage ist die Gewährleistung der Konsistenz dieser Anwendung durch Verfügbarmachung einer vertretbaren und überzeugenden Aussage bezüglich besagter Anwendung.

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:

- der RFID-PIA-Prozess muss nach einer Beurteilung durch den RFID-Betreiber überarbeitet werden oder
- sofern kein RFID-PIA-Prozess durchgeführt wird, müssen die Gründe dafür in der Anwendungsbeschreibung (Anhang D) 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 erkannt oder bekannt gegeben wurde, und zwar:

- im gleichen oder einem ähnlichen Geschäfts- oder Verbandsbereich, in dem der RFID-Betreiber tätig ist;
- in der gleichen oder einer ähnlichen Anwendung des RFID-Betreibers;
- in gleichen oder ähnlichen vom RFID-Betreiber verwendeten RFID-Produkten.

Sofern 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 Prozesses

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 den Prozess 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 Bewertung des Einflusses von RFID auf die Privatsphäre 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 den RFID-PIA-Prozess 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 Kontrolle der Privatsphäre und der Sicherheit über die Luftschnittstelle bei. Solche 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.

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 Abschnitt 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 Abschnitten 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 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 diese Angaben zu ihren Produkten öffentlich zugänglich machen wollen, 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 vierteljährlich eine Liste mit RFID-Produktherstellern zur Verfügung zu stellen, die auf Anfrage keinerlei Informationen über die Leistungsmerkmale zum Schutz der Privatsphäre in RFID-Anwendungen übermittelt haben.

8.3.3 Berufung

Als Registrierungsstelle muss eine durch CEN BT zugelassene Körperschaft eingesetzt werden.

Die berufene Registrierungsstelle ist XXXXXX [Redaktionelle Anmerkung: genaue Angaben können bis zur Berufung der Registrierungsstelle nicht gemacht werden] und ihre Kontaktangaben 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 ohne großen 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. Alle in den Angaben gefundenen Folgefehler können jedoch dem Ruf des Unternehmens schaden, wenn sie nicht korrigiert werden.

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 der 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 solche Angaben der Leistungsmerkmale zum Schutz der Privatsphäre nur den Bereich der möglichen Funktionen abdecken, die obligatorisch oder optional für das jeweilige Luftschnittstellenprotokoll sind.

8.4.2 Leistungsmerkmale von RFID-Transpondern zum Schutz der Privatsphäre

Die formalen Angaben der Leistungsmerkmale zum Schutz der Privatsphäre sind 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 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 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.3 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. Diese 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 [00225074], um Leistungsmerkmale zum Schutz der Privatsphäre für Produkte zu entwickeln, die unternehmenseigene Protokolle verwenden

Redaktionelle Anmerkung: Die im Titel erwähnte Arbeitsauftragsnummer wird durch die korrekte Bezeichnung des Fachberichts ersetzt, sobald dieser zur Veröffentlichung freigegeben wurde.

CEN/TR [00225074] 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.

ANMERKUNG Auf diese Weise werden von Herstellern von RFID-Produkten, die auf unternehmenseigenen Technologien beruhen, weiterhin erwartet, den RFID-PIA-Prozess 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.

8.5 Branchenbezogene Vorlagen

8.5.1 Branchensektoren

Ein Branchensektor kann als logische Gruppe von ähnlichen RFID-Anwendungen angesehen werden, die von Organisationen mit einer gemeinsamen Funktion und/oder um einen bestimmten RFID-Anwendungsstandard herum entwickelt worden sind, .

Beispiele umfassen, sind aber nicht beschränkt auf:

- Einzelhandelsanwendungen, welche die GS1/EPCglobal-Standards verwenden, wohingegen ein allgemeiner Branchensektor für den Einzelhandel wahrscheinlich zu vielfältig wäre, um sinnvoll sein;
- RFID-Technologie für die Gepäckabfertigung, festgelegt durch den IATA-Standard RP1740C;
- RFID-Technologie für Bibliotheken zur Umlaufkontrolle sowie zu anderen Kontrollzwecken, wohingegen ein mehr allgemeiner Leih- und Mietsektor wahrscheinlich zu unübersichtlich wäre;
- die Verwendung von kontaktlosen RF-Karten in öffentlichen Verkehrsmitteln.

Ein weiteres Merkmal des Branchensektors ist, dass es in der Regel eine Hauptmitgliedsorganisation oder eine begrenzte Anzahl von Mitgliedsorganisationen gibt, zu denen viele der RFID-Betreiber in der Branche gehören. 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, soweit möglich, wünschenswert wäre, gibt es keine Anforderungen an solche auf einen Branche bezogenen Organisationen, und damit auch nicht an die Vorlagen, die sie produzieren, letztere auf die gesamteuropäische Ebene auszuweiten.

8.5.2 Erarbeiten einer branchenbezogenen Vorlage

Auf einen Branchensektor bezogene Organisationen (z. B. ein Handelsverband oder eine andere Mitgliedsorganisation) sollten bei der Entwicklung einer branchenbezogenen Vorlage die Führung übernehmen.

Für die Entwicklung der ersten branchenbezogenen Vorlage gibt es zwei logische Vorgehensweisen:

- auf der Grundlage von in der Branche bereits eingeführten RFID-Anwendungen, die es ermöglichen, bei der Erarbeitung der Vorlage auf Erfahrungswerte zurückzugreifen;
- parallel zur Entwicklung einer branchenbezogenen RFID-Anwendung oder eines Dateninhaltsstandards. Dadurch wird sichergestellt, dass die Merkmale zum Schutz der Privatsphäre frühzeitig, während der Standard entwickelt wird, Berücksichtigung finden.

Danach sollte die führende Organisation in der Branche die Vorlage regelmäßig überprüfen.

Die Vorlagen können in einer beliebigen Anzahl von Ausführungen erarbeitet werden:

- als formaler PIA-Bericht, der von einzelnen RFID-Betreibern in diesem Branchensektor eingesetzt wird;
- als eine Analyse der Risiken für den Schutz der Privatsphäre einzelner Datenelemente;
- als Teil des PIA-Prozesses, 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-Prozesses zielen.

8.6 Anwendungsbezogene Vorlagen

8.6.1 Anwendungen

Eine Anwendung kann als eine durch eine oder mehrere Organisationen entwickelte Lösung für eine logisch ähnliche Operation, die zur RFID-Datenerfassung verwendet wird, betrachtet werden. Beispiele umfassen, sind aber nicht beschränkt auf:

- Mitarbeiter-Zutrittskontrollsysteme;
- RF-basierte Mitgliedskarten, z. B. für Freizeitzentren, wohingegen eine Kundenkarte wahrscheinlich solche speziellen Verknüpfungen mit der Anwendung hat, die eine einzelne Behandlung erfordern;
- RFID-Apps auf Mobiltelefonen;
- kontaktlose Zahlungssysteme, die auf einem der in Tabelle 1 festgelegten RFID-Luftschnittstellenprotokollen basieren;
- Konferenz- und Ausstellungsausweise;
- Lagerverwaltung und Inventur;
- Gepäckabfertigung.

Ein bestimmendes Merkmal für solche Anwendungen ist, dass sie als „Fertigprodukt“ angeboten werden können, möglicherweise einschließlich der zugehörigen Software. Im Allgemeinen verteilt sich die Umsetzung von RFID-Systemen dieser Art über mehrere Branchensektoren, deren Ursprung aber vernünftigerweise auf wenige Lösungsanbieter begrenzt ist.

8.6.2 Erarbeiten einer anwendungsbezogenen Vorlage

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

Für die Entwicklung der ersten anwendungsbezogenen Vorlage gibt es zwei logische Vorgehensweisen:

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

Die Vorlagen können in einer beliebigen Anzahl von Formaten hergestellt werden, wie in 8.5.2 beschrieben.

8.7 Erarbeitung einer gemischten Vorlage

Zusätzlich zur Bewältigung der Kernaufgaben eines bestimmten Branchensektors kann es für anwendungsbezogene Vorlagen (z. B. Mitgliedskarten und kontaktlose Zahlungskarten) vorkommen, dass sie in einer bestimmten Weise innerhalb des Sektors behandelt werden müssen. Zum Beispiel könnten einer Mitgliedskarte besondere Privilegien (z. B. Vielflieger) oder Einschränkungen (z. B. Benutzerausweise für Erwachsene gegenüber solchen für Kinder) zugeordnet werden. In solchen Fällen kann die anwendungsbezogene Vorlage als Grundlage verwendet werden, auf der bestimmte branchenbezogene Belange zum Schutz der Privatsphäre bewertet werden.

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 verstärkte Maßnahmen gegen die internen Bedrohungen unternimmt, kann die böswillige „Ausnutzung“ dieser RFID-Schwachstelle reduziert werden. Dies erstreckt sich weit über das hinaus, womit bisher der reine Datenschutz verbunden wurde.

Der RFID-PIA-Prozess 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. Der Prozess erfordert auch eine methodische Kosten-Nutzen-Analyse der Risiken und Gegenmaßnahmen. Ohne diese kann keine geeignete Wahl der Kontrollen und Gegenmaßnahmen erfolgen. Die Hervorhebung der „methodischen Kosten-Nutzen-Analyse“ soll den Zusammenhang zur PIA betonen.

BEISPIEL 1 Von einem Händler, der Tausende von RFID-Transaktionen pro Woche verarbeitet, kann nicht erwartet werden, das gleiche Maß an Ressourcen für den PIA-Prozess bereitzustellen, wie der Händler mit Millionen von Transaktionen pro Woche. Wenn jedoch ein Risiko vorhanden ist und ausgenutzt wird, könnte der Schaden für jeden Einzelhändler relativ gleich sein.

BEISPIEL 2 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 pro Woche mit Lebensmitteln. Der Grund dafür ist, dass die pharmazeutischen Produkte mit dem zu tun haben, was die Richtlinie 95/46/EG mit der indirekten „physischen, physiologischen, psychischen“ Identität einer Person definiert.

Es ist wichtig, als RFID-Betreiber eine Person oder eine Gruppe von Personen zu 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 zu gewährleisten.

9.2 Prozessschritte

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

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.

SCHRITT 1 Bereitstellen einer ausführlichen Anwendungsbeschreibung.

SCHRITT 2 Erkennen und Zuordnen des Risikos zu den Werten der Privatsphäre wie folgt:

- persönliche Werte der Privatsphäre einer Einzelperson, die im Besitz eines RFID-Transponders innerhalb einer RFID-Anwendung sowie über die Grenzen der Anwendung hinaus ist;
- Unternehmenswerte, die mit einer Verletzung der Privatsphäre oder dem Verlust von personenbezogenen Daten durch die RFID-Datenverarbeitung verknüpft sein können.

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 bzw. dem für die Datenverarbeitung Verantwortlichen gespeichert werden.

- SCHRITT 4 Ermittlung der Schwachstellen in Zusammenhang mit den Bedrohungen und den Werten der Privatsphäre.
- 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.
- SCHRITT 6 Ermittlung bestehender und neuer Kontrollmaßnahmen, die die Risiken mindern können.
- SCHRITT 7 Ermitteln der Restrisiken. Sofern die Abschätzung zu hoch ausfällt, ist ab Schritt 2 neu zu beginnen.
- SCHRITT 8 RFID-PIA-Bericht fertigstellen und unterzeichnen.
- SCHRITT 9 Fertigstellen und Unterzeichnen des zusammenfassenden RFID-PIA-Berichts, der zu veröffentlichten ist.

Damit nicht jeder einzelne RFID-Betreiber den gesamten Prozess durchführen muss, 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 branchenbezogenen und anwendungsbezogenen 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 zu 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 4) vorgeschlagen und ausdrücklich erklärt, dass „die Industrie im Verlauf des Sammelns weiterer Erfahrungen bezüglich ihres Einflusses auf den PIA – Prozess diese Stufen weiter verfeinern kann“. Diese Europäische Norm ändert nicht die Anzahl der Stufen, aber wie in den nachfolgenden Abschnitten dargelegt, wird mit Bezug auf die Prozessschritte in 9.2 präzisiert, wofür jeder Stufe steht. Der persönliche Wert der Privatsphäre und die der RFID-Anwendung zugeordneten Datentypen bestimmen weitgehend die Anforderung an eine PIA-Stufe 2, 3, oder 4. Werte der Privatsphäre und die Datentypen sind in 12.2 definiert.

9.3.2 Stufe 0 – keine PIA

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

9.3.3 Stufe 1 – PIA von geringem Umfang

Sofern ein RFID-Transponder dauerhaft oder zeitweise von einer Einzelperson mitgeführt wird oder dieser zugeordnet ist, müssen alle Prozessschritte behandelt werden. Sofern kein Wert und keine Datentypen in der Kategorie der persönlichen Privatsphäre nach 12.2 und dem damit verbundenen Anhang festgelegt sind, wird die Analyse des Restrisikos vereinfacht. Ausführliche Anforderungen sind im angegebenen Abschnitt festgelegt.