

# DIN EN 16571:2014-10 (D)

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

---

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	Punktzahl 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