

# Inhaltsübersicht

<b>Vorwort</b> .....	VII
<b>Inhalt</b> .....	XI
<b>Einleitung</b> .....	1
I. Problemstellung .....	1
II. Gang der Untersuchung .....	2
<b>1. Teil Grundlagen der RFID-Technologie</b> .....	5
I. Begriff, Aufbau und Charakteristika eines RFID-Systems .....	5
II. Technische Grundlagen und praktische Konsequenzen .....	12
III. Ausgewählte Anwendungsbereiche der RFID-Technologie .....	24
<b>2. Teil Datenschutz bei RFID-Systemen</b> .....	31
I. Anwendbares Recht .....	31
II. Anwendungsbereich des Datenschutzrechts .....	38
III. Grundsätze des Datenschutzrechts .....	74
IV. Zulässigkeit der Datenverarbeitung .....	87
V. Datenschutzrechtliche Beurteilung der einzelnen Szenarien .....	142
VI. Pflichten und Konsequenzen der Pflichtverletzung .....	193
VII. Rechte des Betroffenen .....	233
VIII. Grenzen des geltenden Datenschutzrechts und Schutzdefizite .....	254
<b>3. Teil Recht der Datensicherheit bei RFID-Systemen</b> .....	257
I. Zum Verhältnis von Datenschutz und Datensicherung .....	257
II. Risiken für die Sicherheit von RFID-Systemen .....	258
III. Rechtlicher Schutz .....	264
IV. Technische Schutzmöglichkeiten .....	290
V. Grenzen des Rechts der Datensicherheit .....	301
<b>4. Teil Handlungsbedarf des Gesetzgebers</b> .....	303
I. Regulierungsbedarf hinsichtlich des Datenschutzes bei RFID .....	303
II. Regulierungsinstrumente .....	305
III. Regulierungsbestrebungen und Vorschlag für eine Regulierung .....	402
<b>5. Teil Zusammenfassung, Schlussbemerkung und Thesen</b> .....	423
I. Zusammenfassung .....	423
II. Schlussbemerkung .....	425
III. Thesen .....	426
<b>Abkürzungen</b> .....	431

*Inhaltsübersicht*

---

<b>Literatur</b> .....	435
<b>Internetquellen</b> .....	457
<b>Sachregister</b> .....	467

# Inhalt

<b>Vorwort</b> .....	VII
<b>Inhaltsübersicht</b> .....	IX
<b>Einleitung</b> .....	1
I. <i>Problemstellung</i> .....	1
II. <i>Gang der Untersuchung</i> .....	2
<b>1. Teil Grundlagen der RFID-Technologie</b> .....	5
I. <i>Begriff, Aufbau und Charakteristika eines RFID-Systems</i> .....	5
1.    Aufbau und Funktion eines RFID-Systems .....	5
2.    Vergleich der RFID-Technologie mit dem Barcode .....	6
II. <i>Technische Grundlagen und praktische Konsequenzen</i> .....	12
1.    Technische Grundlagen .....	12
a)    Art der Energieversorgung .....	12
b)    Frequenzen .....	13
c)    Leistungsfähigkeit von RFID-Systemen .....	14
d)    Kopplungsverfahren (Übertragungsverfahren) .....	16
e)    Datenübertragung .....	18
f)    Sendereichweiten .....	18
g)    Bauweisen .....	20
2.    Praktische Konsequenzen .....	20
a)    Fehlende Transparenz und Kontrollmöglichkeit .....	20
b)    Einmalige und eindeutige Kennzeichnung und Objektverantwortlichkeit ..	21
c)    Umfassende Profilbildung .....	22
d)    Neue Qualität der Datenerhebung .....	23
III. <i>Ausgewählte Anwendungsbereiche der RFID-Technologie</i> .....	24
1.    RFID-Systeme im Einzelhandel .....	24
2.    RFID-Systeme im Gesundheitswesen .....	27
3.    RFID-Ticketing im öffentlichen Personennahverkehr .....	28
<b>2. Teil Datenschutz bei RFID-Systemen</b> .....	31
I. <i>Anwendbares Recht</i> .....	31
1.    Nationales Datenschutzrecht .....	31
2.    Europäisches Datenschutzrecht .....	32
3.    Verhältnis von DS-GVO und nationalem Recht .....	36
II. <i>Anwendungsbereich des Datenschutzrechts</i> .....	38
1.    Vorliegen von personenbezogenen Daten als Grundvoraussetzung .....	38
	XI

a)	Definition nach dem BDSG a.F. ....	38
aa)	Einzelangaben über persönliche oder sachliche Verhältnisse ....	38
bb)	Personenbezug ....	39
cc)	Natürliche Person ....	40
dd)	Abgrenzung zu anonymen und pseudonymen Daten ....	40
b)	Definition nach der DS-GVO ....	42
aa)	Alle Informationen ....	43
bb)	Bezug zu einer identifizierten oder identifizierbaren Person ....	43
cc)	Natürliche Person ....	44
dd)	Abgrenzung zu pseudonymen und anonymen Daten ....	45
2.	Vorliegen von personenbezogenen Daten beim Einsatz von RFID ....	45
a)	Speicherung personenbezogener Daten direkt auf dem Tag ....	45
b)	Speicherung neutraler Daten auf dem Tag ....	46
aa)	Personenbeziehbare Daten ....	46
bb)	Schutzlücke des BDSG a.F. und der DS-GVO ....	53
cc)	Lösungsmöglichkeiten ....	56
(1)	Ausdehnung des Begriffes der personenbezogenen Daten ....	56
(2)	Widerlegbare Vermutung der Personenbeziehbarkeit ....	57
(3)	Vorsorgeregungen ....	57
dd)	Bewertung der Lösungsmöglichkeiten ....	61
3.	Öffentliche und nicht-öffentliche Stellen ....	68
a)	Rechtslage nach dem BDSG a.F. ....	68
b)	Rechtslage nach der DS-GVO ....	70
4.	Die einzelnen Phasen des Datenumgangs ....	71
a)	Rechtslage nach dem BDSG a.F. ....	71
aa)	Erheben ....	71
bb)	Verarbeiten ....	72
cc)	Nutzen ....	73
b)	Rechtslage nach der DS-GVO ....	73
<i>III.</i>	<i>Grundsätze des Datenschutzrechts</i> ....	74
1.	Datenschutzrechtliche Grundsätze im BDSG a.F. und ihre Entsprechung in der DS-GVO ....	74
a)	Verbot mit Erlaubnisvorbehalt ....	74
b)	Grundsatz der Direkterhebung ....	75
aa)	Rechtslage nach dem BDSG a.F. ....	75
(1)	Erhebung beim Betroffenen gemäß § 4 Abs. 2 S. 1 BDSG a.F. ...	75
(2)	Erhebung ohne Mitwirkung des Betroffenen gemäß § 4 Abs. 2 S. 2 BDSG a.F. ....	77
bb)	Regelungen in der DS-GVO ....	79
c)	Transparenzgebot ....	80
d)	Grundsatz der Zweckbindung ....	80
e)	Grundsatz der Erforderlichkeit ....	83
f)	Grundsatz der Datenvermeidung und Datensparsamkeit ....	84
2.	Weitere Grundsätze der DS-GVO ....	87
<i>IV.</i>	<i>Zulässigkeit der Datenverarbeitung</i> ....	87
1.	Zulässigkeit durch Einwilligung des Betroffenen ....	87
a)	Rechtslage nach dem BDSG a.F. ....	87

aa)	Verfassungsrechtliche Einordnung und Bedeutung der Einwilligung . . .	88
bb)	Verhältnis der Einwilligung zu den gesetzlichen Ermächtigungsgrundlagen . . . . .	89
cc)	Anwendungsbereich . . . . .	91
dd)	Wirksamkeitsvoraussetzungen . . . . .	91
	(1) Formale Anforderungen . . . . .	91
	(a) Einsichtsfähigkeit oder Geschäftsfähigkeit des Betroffenen (Rechtsnatur der Einwilligung) . . . . .	91
	(b) Zeitpunkt . . . . .	92
	(c) Form . . . . .	94
	(d) Formulareinwilligungen . . . . .	97
	(2) Inhaltliche Anforderungen . . . . .	97
	(a) Bestimmtheit . . . . .	98
	(b) Informiertheit . . . . .	99
	(c) Freiwilligkeit . . . . .	103
ee)	Einwilligung bei sensiblen Daten . . . . .	109
ff)	Widerruf der Einwilligung . . . . .	109
b)	Rechtslage nach der DS-GVO . . . . .	110
aa)	Verhältnis der Einwilligung zu den übrigen gesetzlichen Erlaubnistatbeständen . . . . .	110
bb)	Formale Anforderungen . . . . .	111
cc)	Inhaltliche Anforderungen . . . . .	112
	(1) Informiertheit . . . . .	112
	(2) Bestimmtheit . . . . .	113
	(3) Freiwilligkeit . . . . .	113
dd)	Einwilligung bei sensiblen Daten . . . . .	115
ee)	Widerruf der Einwilligung . . . . .	116
ff)	Einwilligung eines Kindes . . . . .	116
c)	Stellungnahme und Grenzen der Einwilligung beim Einsatz von RFID . . . . .	117
2.	Gesetzliche Erlaubnistatbestände für den Datenumgang mittels RFID . . . . .	122
a)	Rechtslage nach dem BDSG a.F. . . . .	122
aa)	Allgemeines . . . . .	122
bb)	Datenerhebung, -verarbeitung und -nutzung für die Erfüllung eigener Geschäftszwecke gemäß § 28 BDSG a.F. . . . .	122
	(1) Erfüllung eigener Geschäftszwecke . . . . .	122
	(2) Verhältnis der Zulässigkeitsalternativen . . . . .	123
	(3) Zulässigkeit nach § 28 Abs. 1 BDSG a.F. . . . .	124
	(a) Rechtsgeschäftliches oder rechtsgeschäftsähnliches Schuldverhältnis, § 28 Abs. 1 S. 1 Nr. 1 BDSG a.F. . . . .	124
	(b) Wahrung berechtigter Interessen, § 28 Abs. 1 S. 1 Nr. 2 BDSG a.F. . . . .	126
	(c) Allgemein zugängliche Daten, § 28 Abs. 1 S. 1 Nr. 3 BDSG a.F. . . . .	127
	(4) Übermittlung oder Nutzung für einen anderen Zweck, § 28 Abs. 2 BDSG a.F. . . . .	129
	(5) Datenverarbeitung zu Zwecken der Werbung, § 28 Abs. 3 BDSG a.F. . . . .	130
	(a) Einwilligung . . . . .	130

(b) Listen	131
(c) Widerspruchsrecht	132
(6) Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten	133
(a) Erhebung, Verarbeitung und Nutzung von besonderen Arten personenbezogener Daten für eigene Geschäftszwecke, § 28 Abs. 6 BDSG a.F.	134
(b) Erhebung, Verarbeitung und Nutzung von besonderen Arten personenbezogener Daten im Gesundheitsbereich, § 28 Abs. 7 BDSG a.F.	136
(c) Übermittlung und Nutzung für andere Zwecke, § 28 Abs. 8 BDSG a.F.	136
b) Rechtslage nach der DS-GVO	136
aa) Erfüllung eines Vertrages	137
bb) Erfüllung einer rechtlichen Verpflichtung	138
cc) Lebenswichtige Interessen	138
dd) Öffentliches Interesse	138
ee) Berechtigtes Interesse	139
ff) Öffnungsklauseln	140
gg) Besondere Kategorien personenbezogener Daten, Art. 9 DS-GVO	141
c) Stellungnahme	142
V. <i>Datenschutzrechtliche Beurteilung der einzelnen Szenarien</i>	142
1. RFID-Systeme im Einzelhandel	143
a) Erfassung der Kundendaten beim Bezahlvorgang	143
aa) Zum Zweck der Abwicklung eines Bonusprogrammes	143
(1) Rechtslage nach dem BDSG a.F.	143
(2) Rechtslage nach der DS-GVO	146
(3) Stellungnahme	146
bb) Zu Werbe- oder Marktforschungszwecken	146
(1) Rechtslage nach dem BDSG a.F.	146
(2) Rechtslage nach der DS-GVO	148
(3) Stellungnahme	150
b) Erfassung der Warenentnahme	151
aa) Rechtslage nach dem BDSG a.F.	151
bb) Rechtslage nach der DS-GVO	153
cc) Stellungnahme	154
c) Erfassung von Bewegungsdaten des Kunden	154
aa) Rechtslage nach dem BDSG a.F.	154
bb) Rechtslage nach der DS-GVO	157
cc) Stellungnahme	158
d) Bildung von Kundenprofilen	158
aa) Rechtslage nach dem BDSG a.F.	158
bb) Rechtslage nach der DS-GVO	164
cc) Stellungnahme	165
e) Zwischenergebnis	166
2. RFID-Systeme im Gesundheitswesen	166
a) Lokalisierung	167
aa) Erhebung von Bewegungsdaten	170

(1) Schutzsystem für ältere oder verwirrte Personen . . . . .	171
(a) Rechtslage nach dem BDSG a.F. . . . .	171
(b) Rechtslage nach der DS-GVO . . . . .	174
(c) Stellungnahme . . . . .	175
(2) Baby-Sicherheitssystem . . . . .	175
(a) Rechtslage nach dem BDSG a.F. . . . .	176
(b) Rechtslage nach der DS-GVO . . . . .	177
(c) Stellungnahme . . . . .	177
bb) Erhebung von Gesundheitsdaten . . . . .	177
(1) Rechtslage nach dem BDSG a.F. . . . .	177
(2) Rechtslage nach der DS-GVO . . . . .	179
(3) Stellungnahme . . . . .	180
b) Patientenidentifikation und personalisierte Patientenmedikation . . . . .	180
aa) Rechtslage nach dem BDSG a.F. . . . .	180
bb) Rechtslage nach der DS-GVO . . . . .	181
cc) Stellungnahme . . . . .	182
c) Prozesssteuerung und Dokumentation . . . . .	182
aa) Rechtslage nach dem BDSG a.F. . . . .	182
bb) Rechtslage nach der DS-GVO . . . . .	185
cc) Stellungnahme . . . . .	186
d) Messdatenüberwachung . . . . .	186
aa) Rechtslage nach dem BDSG a.F. . . . .	186
bb) Rechtslage nach der DS-GVO . . . . .	188
cc) Stellungnahme . . . . .	188
3. RFID-Ticketing im öffentlichen Personennahverkehr . . . . .	188
a) Erfassung der Nutzungs- und Abrechnungsdaten . . . . .	189
aa) Rechtslage nach dem BDSG a.F. und der DS-GVO . . . . .	189
bb) Stellungnahme . . . . .	190
b) Erfassung von Statistikdaten . . . . .	190
c) Erfassung von Bewegungsdaten und Profilerstellung . . . . .	190
aa) Rechtslage nach dem BDSG a.F. . . . .	191
bb) Rechtslage nach der DS-GVO . . . . .	192
cc) Stellungnahme . . . . .	193
VI. <i>Pflichten und Konsequenzen der Pflichtverletzung</i> . . . . .	193
1. Rechtslage nach dem BDSG a.F. . . . .	193
a) Informationspflichten nach § 4 Abs. 3 BDSG a.F. bei der Direkterhebung . . . . .	193
aa) Die einzelnen Unterrichtungspflichten nach § 4 Abs. 3 S. 1 Nr. 1 bis 3 BDSG a.F. . . . .	193
(1) Identität . . . . .	193
(2) Zweckbestimmung . . . . .	196
(3) Empfängerkategorien . . . . .	197
bb) Weitergehende Informationspflicht über die angebrachten RFID-Tags bzw. die Infrastruktur der Lesegeräte . . . . .	198
cc) Rechtsfolgen unterlassener Aufklärung . . . . .	200
b) Benachrichtigungspflicht gemäß § 33 BDSG a.F. . . . .	201
c) Unterrichtungspflicht nach § 6c BDSG a.F. . . . .	205
aa) Anwendbarkeit des § 6c BDSG a.F. auf RFID-Transponder . . . . .	206
(1) Ausgabe an den Betroffenen, § 3 Abs. 10 Nr. 1 BDSG a.F. . . . .	206

(2) Automatisierte Datenverarbeitung, § 3 Abs. 10 Nr. 2 BDSG a.F.	208
(a) RFID-Systeme im High-End-Bereich	209
(b) RFID-Systeme im Low-End-Bereich	209
(c) RFID-Systeme mittlerer Leistungsfähigkeit	210
(3) Gebrauch des Mediums, § 3 Abs. 10 Nr. 3 BDSG a.F.	214
bb) Inhalt und Umfang der Unterrichtungspflicht nach § 6c Abs. 1 BDSG a.F.	216
(1) Adressat der Unterrichtungspflicht	216
(2) Berechtigter	218
(3) Umfang der Unterrichtung	219
(4) Zeitpunkt und Form der Unterrichtung	220
(5) Ausnahme von der Unterrichtung	222
cc) Sonstige Anforderungen nach § 6c Abs. 2 und 3 BDSG a.F.	222
dd) Information über den Ort der Anbringung von RFID-Tags	224
ee) Rechtsnatur des § 6c BDSG a.F.	224
d) Folgen eines Verstoßes gegen datenschutzrechtliche Vorschriften	225
2. Rechtslage nach der DS-GVO	225
a) Informationspflichten bei Erhebung von personenbezogenen Daten bei der betroffenen Person, Art. 13 DS-GVO	225
b) Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden, Art. 14 DS-GVO	226
c) Keine entsprechende Regelung zu mobilen personenbezogenen Speicher- und Verarbeitungsmedien	227
d) Folgen eines Verstoßes gegen datenschutzrechtliche Vorschriften	228
3. Stellungnahme	228
<i>VII. Rechte des Betroffenen</i>	233
1. Rechtslage nach dem BDSG a.F.	233
a) Auskunftsanspruch des Betroffenen gemäß § 34 BDSG a.F.	233
b) Anspruch auf Berichtigung, Löschung und Sperrung von Daten gemäß § 35 BDSG a.F.	235
aa) Berichtigung	235
bb) Löschung	236
(1) Recht auf Löschung und Löschungspflicht	236
(2) Anspruch auf Löschung der Daten in der Hintergrunddatenbank der verantwortlichen Stelle	238
(3) Anspruch auf Löschung der auf den RFID-Tags gespeicherten Daten	238
cc) Sperrung	242
2. Rechtslage nach der DS-GVO	244
a) Auskunftsanspruch nach Art. 15 DS-GVO	244
b) Recht auf Berichtigung, Art. 16 DS-GVO	245
c) Recht auf Löschung (»Recht auf Vergessenwerden«), Art. 17 DS-GVO	246
aa) Allgemeines	246
bb) Recht auf Löschung beim Einsatz von RFID	247
d) Recht auf Einschränkung der Verarbeitung, Art. 18 DS-GVO	249
e) Recht auf Datenübertragbarkeit, Art. 20 DS-GVO	249
3. Stellungnahme	250



VIII. Grenzen des geltenden Datenschutzrechts und Schutzdefizite	254
<b>3. Teil Recht der Datensicherheit bei RFID-Systemen</b>	<b>257</b>
I. Zum Verhältnis von Datenschutz und Datensicherung	257
II. Risiken für die Sicherheit von RFID-Systemen	258
1. Grundlegendes	258
2. Bedrohungslage für die aktive Partei	260
a) Abhören der Kommunikation	260
b) Fälschung des Inhalts oder der Identität	261
c) Denial of Service-Angriffe (Störung des Datenaustauschs)	262
3. Bedrohungslage für die passive Partei	263
a) Bedrohung der Data Privacy	263
b) Bedrohung der Location Privacy	264
III. Rechtlicher Schutz	264
1. Schutz durch das BDSG a.F.	264
a) Allgemeines	264
b) Technische und organisatorische Maßnahmen nach § 9 BDSG a.F.	264
aa) Gegenstand der technischen und organisatorischen Maßnahmen	265
bb) Erforderlichkeit und Verhältnismäßigkeit der Maßnahmen (Grundsatz der Verhältnismäßigkeit, § 9 S. 2 BDSG a.F.)	265
cc) Maßnahmen nach der Anlage zu § 9 S. 1 BDSG a.F.	268
(1) Zutrittskontrolle (Nr. 1)	268
(2) Zugangskontrolle (Nr. 2)	272
(3) Zugriffskontrolle (Nr. 3)	274
(4) Weitergabekontrolle (Nr. 4)	276
(5) Eingabekontrolle (Nr. 5)	277
(6) Auftragskontrolle (Nr. 6)	278
(7) Verfügbarkeitskontrolle (Nr. 7)	278
(8) Trennungsgebot (Nr. 8)	279
2. Schutz durch die DS-GVO	280
a) Allgemeines	280
b) Sicherheit der Verarbeitung, Art. 32 DS-GVO	280
aa) Technische und organisatorische Maßnahmen	281
(1) Allgemeines	281
(2) Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO)	282
(3) Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)	282
(4) Wiederherstellung der Verfügbarkeit und des Zugangs (Art. 32 Abs. 1 lit. c DS-GVO)	283
(5) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO)	284
bb) Angemessenes Schutzniveau	284
c) Art. 24 und Art. 25 DS-GVO	285
3. Stellungnahme	287
IV. Technische Schutzmöglichkeiten	290

1.	Die einzelnen technischen Sicherheitsmaßnahmen	290
a)	Authentifizierung	290
b)	Verschlüsselung	292
c)	Pseudonymisierung	293
d)	Deaktivierung	295
e)	Verhindern des Auslesens	298
f)	Weitere technische Sicherheitsmaßnahmen	299
2.	Bewertung der technischen Sicherheitsmaßnahmen	300
V.	<i>Grenzen des Rechts der Datensicherheit</i>	301
<b>4. Teil</b>	<b>Handlungsbedarf des Gesetzgebers</b>	<b>303</b>
I.	<i>Regulierungsbedarf hinsichtlich des Datenschutzes bei RFID</i>	303
II.	<i>Regulierungsinstrumente</i>	305
1.	Überblick über die Regulierungsinstrumente	305
2.	Selbstregulierung	306
a)	Vorbemerkung	306
b)	Selbstregulierung des Marktes auf der Grundlage von Selbstverpflichtungserklärungen der Wirtschaft	307
aa)	Anforderungen an eine effektive Selbstverpflichtung	310
(1)	Allgemeine Anforderungen	310
(2)	Inhaltliche Anforderungen	310
bb)	Selbstverpflichtungserklärung der EPC-Anwender	312
(1)	Grundsätze der Selbstverpflichtung	312
(2)	Bewertung der EPC-Grundsätze	313
c)	Selbstregulierung durch Güte- bzw. Vertrauenssiegel	318
aa)	Das Europäische Datenschutz-Gütesiegel EuroPriSe – European Privacy Seal	318
(1)	Allgemeine Zertifizierungsvoraussetzungen	318
(2)	RFID als Zertifizierungsgegenstand	320
(3)	Bewertung	321
bb)	Trusted-RFID-Vertrauenssiegel	322
d)	Abschließende Bewertung einer Selbstregulierung	324
3.	Gesetzliche (staatliche) Regulierung	324
a)	Kompetenz des nationalen Gesetzgebers	324
b)	Allgemeine Anforderungen an ein gesetzliches Einschreiten	325
c)	Änderung des BDSG a.F.	325
aa)	Möglicher Inhalt	325
(1)	Einbeziehung potentiell personenbezogener Daten	325
(2)	Erweiterung der Informationspflichten	326
(3)	Änderung des § 6c BDSG a.F.	326
(4)	Sanktionen für Verstöße gegen die Selbstverpflichtungserklärung der Wirtschaft	327
bb)	Bewertung	328
d)	Schaffung einer bereichsspezifischen Regelung außerhalb des BDSG a.F. (RFID-Gesetz)	330
aa)	Möglicher Inhalt	330

bb)	Bewertung	331
e)	Handlungspflicht des Gesetzgebers	332
aa)	Bestehen einer staatlichen Schutzpflicht	332
bb)	Inhalt und Reichweite der Schutzpflicht	333
cc)	Schutzpflichten des Staates in Bezug auf die Risiken durch die RFID-Technologie	334
(1)	Bestehen einer Schutzpflicht	334
(2)	Inhalt und Reichweite der Schutzpflicht	339
(3)	Verletzung der Schutzpflicht	340
f)	Abschließende Bewertung einer gesetzlichen Regulierung	343
4.	Regulierte Selbstregulierung	343
a)	Vorbemerkung	345
b)	Rahmenwerk zur sog. Datenschutzfolgenabschätzung	345
aa)	Hintergrund und rechtliche Qualifikation des Rahmenwerks	346
(1)	Hintergrund des Rahmenwerks	346
(a)	Konsultationsprozess der EU-Kommission	346
(b)	Mitteilung der EU-Kommission vom 15. März 2007 zur Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen	347
(c)	Empfehlung der EU-Kommission vom 12. Mai 2009	347
(d)	Umsetzung der Empfehlung	349
(2)	Rahmenwerk als Beispiel einer Co-Regulierung (regulierten Selbstregulierung)	350
bb)	Begriffsklärung und Anwendungsbereich des Rahmenwerks	352
cc)	Inhalt	354
(1)	Anfangsanalyse	354
(2)	Risikoabschätzung	357
dd)	Technische Richtlinie RFID des BSI für den sicheren RFID-Einsatz	360
(1)	Inhalt und Bedeutung der Technischen Richtlinie	360
(2)	PIA Leitfaden des BSI	361
ee)	Bewertung des Rahmenwerks	365
(1)	Vorteile des Rahmenwerks	365
(2)	Nachteile und Lücken des Rahmenwerks	366
(a)	Unklarheiten beim Begriff der personenbezogenen Daten	366
(b)	Fehlende Orientierungshilfe für besondere Arten personenbezogener Daten	369
(c)	Rechtliche Unverbindlichkeit/Keine Sanktionsmechanismen	371
ff)	Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO	373
(1)	Begriff der Datenschutz-Folgenabschätzung	373
(2)	Anforderungen des Art. 35 DS-GVO	373
(a)	Erforderlichkeit der Durchführung einer Datenschutz-Folgenabschätzung	373
(b)	Zeitpunkt der Durchführung	375
(c)	Inhaltliche Anforderungen	375
(d)	Rechtsfolgen	378
(e)	Überprüfung	378
(3)	Vergleich mit dem nationalen Recht	378

(4) Erforderlichkeit der Durchführung einer Datenschutz-Folgenabschätzung beim Einsatz von RFID .....	381
(5) Verhältnis von Art. 35 DS-GVO zur EU-Empfehlung .....	382
c) Weitere Selbstregulierungsansätze im BDSG a.F. und in der DS-GVO ..	383
aa) Verhaltensregeln .....	384
(1) Rechtslage nach dem BDSG a.F. ....	384
(a) Anforderungen des § 38a BDSG a.F. ....	384
(b) Defizite der Verhaltensregeln nach § 38a BDSG a.F. ....	386
(c) Zwischenergebnis .....	388
(2) Rechtslage nach der DS-GVO .....	389
(3) Stellungnahme .....	390
bb) Datenschutzaudit und Zertifizierung .....	391
(1) Rechtslage nach dem BDSG a.F. ....	391
(a) Sinn und Zweck eines Datenschutzaudits .....	391
(b) Voraussetzungen des § 9a BDSG a.F. ....	392
(aa) Verfahrensaudit .....	393
(bb) Produktaudit .....	394
(c) RFID-Technologie als Gegenstand eines Verfahrens- oder Produktaudits .....	394
(d) Zwischenergebnis .....	396
(2) Rechtslage nach der DS-GVO .....	397
(a) Sinn und Zweck der Zertifizierung .....	397
(b) Unterschied zwischen Zertifizierung und Auditierung .....	397
(c) Voraussetzungen und Rechtsfolgen nach Art. 42 DS-GVO ..	398
(d) RFID-Technologie als Gegenstand der Zertifizierung .....	399
(3) Stellungnahme .....	400
d) Abschließende Bewertung einer regulierten Selbstregulierung .....	401
5. Ergebnis .....	402
<i>III. Regulierungsbestrebungen und Vorschlag für eine Regulierung .....</i>	<i>402</i>
1. Überblick über die bisherigen nationalen Regulierungsbestrebungen .....	402
2. Aktuelle Regulierungsbestrebungen .....	405
a) EU-Ebene/Datenschutzaktivitäten in Europa .....	405
aa) Standardisierung im Bereich der RFID-Technologie .....	405
bb) Folgen für die Regulierung .....	408
b) Nationale Ebene/Datenschutzaktivitäten in Deutschland .....	409
3. Zusammenfassung der Schutzlücken und Vorschlag für eine Regulierung ...	409
a) Rechtliche Pflicht zur Durchführung von Datenschutz-Folgenabschätzungen bei RFID-Anwendungen .....	409
aa) Schutzlücke .....	409
bb) Lösungsmöglichkeiten .....	410
(1) Einführung einer gesetzlichen Regelung .....	410
(2) Erstellung einer Positivliste nach Art. 35 Abs. 4 DS-GVO .....	411
cc) Bewertung der Lösungsmöglichkeiten .....	411
dd) Vorschlag für eine Regulierung .....	411
b) Begriff der personenbezogenen Daten .....	413
aa) Schutzlücke .....	413
bb) Lösungsmöglichkeiten .....	413
(1) Vorsorgeregulungen .....	413

---

(2) Aufnahme in die Positivliste nach Art. 35 Abs. 4 DS-GVO . . . . .	413
cc) Bewertung der Lösungsmöglichkeiten . . . . .	415
dd) Vorschlag für eine Regulierung . . . . .	415
c) Datenschutzrechtliche Einwilligung . . . . .	417
aa) Grenzen der Einwilligung . . . . .	417
bb) Lösungsmöglichkeiten . . . . .	417
cc) Bewertung der Lösungsmöglichkeiten . . . . .	419
dd) Stellungnahme . . . . .	420
d) Umgang mit den weiteren Schutzlücken . . . . .	420
4. Ergebnis . . . . .	422
<b>5. Teil Zusammenfassung, Schlussbemerkung und Thesen . . . . .</b>	<b>423</b>
<i>I. Zusammenfassung . . . . .</i>	<i>423</i>
1. RFID-Technologie als Bedrohung für den Datenschutz und die Datensicherheit . . . . .	423
2. Schutzlücken im Bereich des Datenschutzes . . . . .	423
3. Lösung über eine regulierte Selbstregulierung . . . . .	424
4. Regulierungsvorschlag . . . . .	424
<i>II. Schlussbemerkung . . . . .</i>	<i>425</i>
<i>III. Thesen . . . . .</i>	<i>426</i>
<b>Abkürzungen . . . . .</b>	<b>431</b>
<b>Literatur . . . . .</b>	<b>435</b>
<b>Internetquellen . . . . .</b>	<b>457</b>
<b>Sachregister . . . . .</b>	<b>467</b>