

Inhaltsübersicht

Geleitwort.....	V
1. Einführung in die Untersuchung.....	1
1.1 Wandel der Informationsgesellschaft - Informatisierung des Alltages	1
1.2 Gegenstand der Untersuchung	22
1.3 Gang der Untersuchung.....	23
2. Der Einsatz von RFID-Systemen als ein Auto-ID-Verfahren	27
2.1 Bedeutung des Einsatzes von RFID-Systemen als Auto-ID- Verfahren in der Wirtschaft	27
2.2 Technische Grundlagen der RFID-Systeme	46
2.3 Szenarische Darstellung des Einsatzes von RFID-Systemen im Kontext allgegenwärtiger Datenverarbeitung	78
2.4 Potentiale und Risiken des Einsatzes von RFID-Systemen durch ihre technischen Charakteristika	99
2.5 Gesellschaftliche Diskussion des Einsatzes von RFID-Systemen	105
3. Datenschutzrechtliche Regulation des Einsatzes von RFID- Systemen	119
3.1 Verfassungsrechtliche Grundlagen für den Einsatz von RFID- Systemen	119
3.2 Rechtsrahmen.....	160
3.3 Anwendbarkeit des bereichsspezifischen Datenschutzrechts	167
3.4 Allgemeine Anwendungsvoraussetzungen des Datenschutzrechts ...	205
3.5 Umgang mit personenbezogenen Daten durch RFID-Systeme	217
3.6 Verantwortlichkeit für den Umgang mit personenbezogenen Daten ..	279
4. Datenschutzrechtliche Anforderungen	315
4.1 Datenschutzrechtlicher Zulassungstatbestand.....	315
4.2 Datenschutzrechtliche Anforderungen an automatisierte Einzelentscheidungen	347

4.3 Datenschutzrechtliche Anforderungen an mobile personenbezogene Speicher- und Verarbeitungsmedien	371
4.4 Datenschutzrechtliche Rechte für den Betroffenen	438
4.5 Datenschutzrechtliche Anforderungen an die Datensicherheit und technisch organisatorische Schutzmaßnahmen	484
5. Schutzbedarf und Schutzansätze	539
5.1 Herausforderungen des Einsatzes von RFID-Systemen – ausgewählte Problemkreise	539
5.2 Konzeptionelle Schutzansätze	560
6. Reformperspektiven des Datenschutzrechts durch eine europäische Datenschutz-Grundverordnung	583
6.1 Rechtsgrundlage und Regelungskonzept der Datenschutz- Grundverordnung	585
6.2 Regelungsinhalt der europäischen Datenschutz-Grundverordnung...	587
6.3 Bedeutung für den Einsatz von RFID-Systemen	595
7. Ausblick	621
Literaturverzeichnis	623

Inhaltsverzeichnis

Geleitwort.....	V
Inhaltsübersicht.....	VII
Inhaltsverzeichnis	IX
Abbildungen und Tabellen.....	XXI
Abkürzungsverzeichnis.....	XXIII
Zusammenfassung - Abstract	XXXI
 1. Einführung in die Untersuchung.....	 1
1.1 Wandel der Informationsgesellschaft - Informatisierung des Alltages	1
1.1.1 Idee einer Welt allgegenwärtiger Datenverarbeitung - Ubiquitous Computing	3
1.1.1.1 Grundlage allgegenwärtiger Datenverarbeitung.....	4
1.1.1.2 Paradigmenwechsel in der Informationsgesellschaft.....	9
1.1.1.3 Versprechen allgegenwärtiger Datenverarbeitung	9
1.1.2 Auto-ID-Verfahren als Baustein der Welt allgegenwärtiger Datenverarbeitung.....	11
1.1.3 Im Kontext allgegenwärtiger Datenverarbeitung - Perspektiven und Herausforderungen	12
1.1.3.1 Einbettung der Datenverarbeitung in die Umweltbedingungen	13
1.1.3.1.1 Datenverarbeitung integriert in Handlungen und Alltagsabläufe.....	13
1.1.3.1.2 Einbringen von Informationen aus der realen Welt in die virtuelle Welt.....	14
1.1.3.2 Allgegenwärtigkeit im Alltag	15
1.1.3.2.1 Vervielfachung der Datenverarbeitung	16
1.1.3.2.2 Erschließung von anonymen Daten aufgrund zunehmender Personalisierung und Individualisierung	16
1.1.3.2.3 Zersplitterung der Administration	17
1.1.3.2.4 Intransparenz datenverarbeitender Vorgänge	17
1.1.3.3 Sensibilität und Reaktionsfähigkeit.....	18
1.1.3.3.1 Profilbildung – umfassend und implizit (Totalbilder)	19
1.1.3.3.2 Vielfalt der Zwecke	19
1.1.3.3.3 Unvorhersehbare und wechselnde Zwecke.....	20

1.1.3.4 Kommunikationsfähigkeit und Vernetzung der „smarten Artefakte“	21
1.2 Gegenstand der Untersuchung	22
1.3 Gang der Untersuchung	23
2. Der Einsatz von RFID-Systemen als ein Auto-ID-Verfahren	27
2.1 Bedeutung des Einsatzes von RFID-Systemen als Auto-ID-Verfahren in der Wirtschaft	27
2.1.1 Kennzeichnung und Identifikation	27
2.1.1.1 Aufgabe und Ziel von Auto-ID-Verfahren	27
2.1.1.2 Historische Kennzeichnungs- und Identifikationssysteme	27
2.1.1.3 Moderne Kennzeichnungs- und Identifikationssysteme	29
2.1.2 Einführung von Auto-ID-Verfahren als ökonomisch gebotener Entwicklungsschritt	30
2.1.2.1 Auto-Identifikation als Ansatzpunkt in der Wirtschaft zur Effizienzsteigerung	30
2.1.2.2 Einführung von Auto-ID-Verfahren als Maßnahme zur Effizienzsteigerung	32
2.1.2.3 Voraussetzungen für die Einführung von RFID-Systemen als Auto-ID-Verfahren	33
2.1.3 Anwendungsbeispiele für den Einsatz von RFID-Systemen	38
2.1.3.1 Überwachung von Zeit und Raum	40
2.1.3.2 Überwachung von Zustand und Qualität	42
2.1.3.3 Überwachung von Berechtigungen	44
2.2 Technische Grundlagen der RFID-Systeme	46
2.2.1 Grundlegender Aufbau eines RFID-Systems	47
2.2.2 Unterscheidungsmerkmale	50
2.2.2.1 Energieversorgung der RFID-Marke	50
2.2.2.2 Reichweite und Kommunikationsfrequenzen von RFID-Systemen	51
2.2.2.3 Rechenkapazität und Speichertechnologien	53
2.2.2.4 Kommunikationsverfahren	57
2.2.2.5 Betriebsarten	58
2.2.2.6 Kommunikationsfrequenz	59
2.2.3 Prinzipielle Funktionsweise von RFID-Kommunikation	60
2.2.3.1 Ein-Bit-RFID-Systeme	60
2.2.3.2 Kapazitiv gekoppelte RFID-Systeme	60
2.2.3.3 Induktiv gekoppelte RFID-Systeme	61

2.2.3.4	Lastmodulation mit und ohne Hilfsträger	61
2.2.3.5	RFID-Systeme im Rückstreuverfahren	62
2.2.4	Vielfachzugriffsverfahren	63
2.2.4.1	Aloha, Slotted Aloha und Dynamisches Aloha- Verfahren	64
2.2.4.2	Suchbaum-, auch Tree-Walking- oder Binary-Search- Verfahren	65
2.2.4.3	Kooperative Übertragungsverfahren	65
2.2.5	Bauformen und Produktionsverfahren	66
2.2.5.1	Bauformen der RFID-Komponenten	66
2.2.5.2	Produktionsverfahren der RFID-Komponenten	67
2.2.6	Normungsstandards	69
2.2.6.1	Normungsstandards Spezifikation	69
2.2.6.2	Datenstruktur	72
2.2.6.3	Kenngößen der RFID-Technik	73
2.2.6.4	Entwicklungsperspektiven der RFID-Technologie	75
2.2.7	Alternative Auto-ID-Verfahren	75
2.2.7.1	Auto-ID-Technik RuBee	75
2.2.7.2	Auto-ID-Technik NFC	76
2.2.7.3	Auto-ID-Technik Super-Label	77
2.3	Szenarische Darstellung des Einsatzes von RFID-Systemen im Kontext allgegenwärtiger Datenverarbeitung	78
2.3.1	Folgenabschätzung durch Szenarientechnik	78
2.3.1.1	Ziel und Arten von Szenarienbildung	78
2.3.1.2	Rechtswissenschaftliches Interesse an der Szenarienbildung	81
2.3.1.3	Methodik der Szenarienbildung	82
2.3.1.4	Datenschutzrechtlich relevante Leitlinien für die Szenarienbildung	86
2.3.1.4.1	Datenschutzrechtliche Anforderungen bei der Szenarien-konstruktion	86
2.3.1.4.1.1	Verschiedene Lebensbereiche und unterschiedlicher Daten-umgang	86
2.3.1.4.1.2	Datenschutzrechtliche Konfliktkonstellation	88
2.3.1.4.1.3	Integration von datenschutzgerechten Lösungsansätzen	89
2.3.1.4.2	Anforderungen bei der Ausarbeitung der Szenarien	89
2.3.2	Szenarische Darstellung vom Leben im Kontext allgegenwärtiger Datenverarbeitung	90
2.3.2.1	Funktion der vorgestellten Szenariodarstellung	90

2.3.2.2 Grenzen der vorgestellten Szenariodarstellung	91
2.3.2.3 Ausrichtung der vorgestellten Szenariodarstellung	92
2.3.2.4 Beteiligte und Ressourcen	92
2.3.2.5 Szenarische Darstellung eines Tages von Claudia und Alfonso	93
2.4 Potentiale und Risiken des Einsatzes von RFID-Systemen durch ihre technischen Charakteristika	99
2.4.1 Technisch bedingte Verwendungsmöglichkeiten der RFID- Systeme	100
2.4.2 Folgen durch die Verwendungsmöglichkeiten von RFID- Systemen	101
2.4.3 Angriffe auf RFID-Systeme	103
2.5 Gesellschaftliche Diskussion des Einsatzes von RFID-Systemen	105
2.5.1 Organisation Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN)	105
2.5.2 Digitalcourage e.V.	106
2.5.3 Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre	107
2.5.4 Unabhängiges Landeszentrum für Datenschutz Schleswig- Holstein	108
2.5.5 Stellungnahme der Bundesregierung der 15. Legislaturperiode	108
2.5.6 Unternehmen Microsoft	109
2.5.7 Artikel-29-Datenschutzgruppe	109
2.5.8 Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BitKom)	110
2.5.9 Deutscher Fußball-Bund (DFB) zur Fußballweltmeisterschaft 2006	111
2.5.10 Organisation EPCglobal	112
2.5.11 Konferenzen der Datenschutzbeauftragten des Bundes und der Länder	112
2.5.12 Organisation European Expert Group for IT-Security (EICAR)	113
2.5.13 Center for Democracy and Technology (CDT)	113
2.5.14 US – National Institute of Standards and Technology (NIST) ..	114
2.5.15 Metro-Gruppe	115
2.5.16 Kommission der Europäischen Union	115
2.5.17 Verbraucherzentrale Bundesverband (vzbv)	116
2.5.18 Bundesbeauftragter für Datenschutz und Informationsfreiheit	117

2.5.19 Fazit zur gesellschaftlichen Diskussion	118
3. Datenschutzrechtliche Regulation des Einsatzes von RFID-Systemen	119
3.1 Verfassungsrechtliche Grundlagen für den Einsatz von RFID-Systemen	119
3.1.1 Funktion und Geltung der Grundrechte	119
3.1.1.1 Grundrechte als Abwehr- und Partizipationsrechte	119
3.1.1.2 Grundrechte als Pflicht des Staates zur Schutzgewährung und zur Vorsorge	120
3.1.2 Recht auf informationelle Selbstbestimmung	123
3.1.2.1 Entstehung und Hintergrund	124
3.1.2.2 Europäische Entsprechung	126
3.1.2.3 Schutzbereich und Grundrechtsbeschränkungen	129
3.1.2.3.1 Schutzbereich	129
3.1.2.3.2 Beschränkungen der informationellen Selbstbestimmung	131
3.1.2.4 Anforderungen an eine rechtmäßige Datenverarbeitung	133
3.1.2.4.1 Zulässigkeit der Datenverarbeitung	134
3.1.2.4.2 Gebot der Normenklarheit	135
3.1.2.4.3 Grundsatz der Zweckbindung	136
3.1.2.4.4 Erforderlichkeit der Datenverarbeitung	137
3.1.2.4.5 Transparenz der Datenverarbeitung	139
3.1.2.4.6 Schutz durch technisch-organisatorische Maßnahmen und Verfahrensrechte	140
3.1.2.4.7 Grundsatz der Datenvermeidung und Datensparsamkeit	141
3.1.3 Fernmeldegeheimnis	142
3.1.3.1 Entstehung und Hintergrund	142
3.1.3.2 Europäische Entsprechung	143
3.1.3.3 Schutzbereich	143
3.1.3.4 Grundrechtsbeschränkungen	145
3.1.4 Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	147
3.1.4.1 Hintergrund	147
3.1.4.2 Schutzbereich und Beschränkung	148
3.1.4.2.1 Schutzbedarf vor qualitativ neuen Risiken	149
3.1.4.2.2 Schutzbereich	151
3.1.4.2.3 Beschränkung	154
3.1.4.3 Verhältnis zu anderen Grundrechten	156
3.1.4.4 Bedeutung für die Untersuchung	158

3.1.5 Kollidierendes Verfassungsrecht	159
3.2 Rechtsrahmen.....	160
3.2.1 Nationaler Rechtsrahmen	160
3.2.2 Internationale Regelungen	163
3.3 Anwendbarkeit des bereichsspezifischen Datenschutzrechts	167
3.3.1 Verhältnis des allgemeinen zum bereichsspezifischen Datenschutzrechts.....	168
3.3.2 Regelungsebenen des Telekommunikations-, Multimedia- und allgemeinen Datenschutzrechts.....	170
3.3.3 Regelungskomplex des Telekommunikationsrechts	172
3.3.3.1 Diensteanbieter als Anknüpfungspunkt für die Anwendbarkeit	173
3.3.3.2 RFID-Kommunikation als Telekommunikation	175
3.3.3.2.1 Telekommunikation mittels Telekommunikationsanlagen	175
3.3.3.2.2 Angebot gegenüber Dritten	177
3.3.3.2.3 Telekommunikation im RFID-Vordergrundsystem.....	178
3.3.3.2.4 Telekommunikation im RFID-Hintergrundsystem	178
3.3.3.2.5 Telekommunikation im RFID-System mit Kommunikationsschnittstelle für Dritte.....	179
3.3.4 Regelungskomplex des Telemedienrechts	181
3.3.4.1 Qualifizierung eines RFID-Systems als Telemediendienst.....	181
3.3.4.1.1 Abgrenzung zu Angeboten im Bereich des Telekommunikations- und Rundfunkrechts	182
3.3.4.1.1.1 Geltungsvorrang des Telekommunikationsgesetzes ...	182
3.3.4.1.1.2 Geltungsvorrang des Rundfunk-Staatsvertrages	185
3.3.4.1.2 Elektronischer Informations- oder Kommunikationsdienst	186
3.3.4.1.2.1 Anbieten zur Nutzung	186
3.3.4.1.2.2 Funktion der Information und Kommunikation	190
3.3.4.1.3 Multimedialer Charakter des Angebots.....	193
3.3.4.1.3.1 Funktionale Betrachtung.....	194
3.3.4.1.3.2 Zweistufige Prüfung	196
3.3.4.1.4 Vorläufiges Zwischenergebnis	200
3.3.4.2 Inadäquates Regelungsprogramm des Telemediengesetzes	201
3.4 Allgemeine Anwendungsvoraussetzungen des Datenschutzrechts ...	205
3.4.1 Personenbezogene Daten.....	205

3.4.1.1 Einzelangaben über persönliche oder sachliche Verhältnisse	205
3.4.1.2 Bezug zu einer Person	207
3.4.2 Anonymisierte und pseudonymisierte Daten	214
3.5 Umgang mit personenbezogenen Daten durch RFID-Systeme	217
3.5.1 Erheben von personenbezogenen Daten	218
3.5.1.1 Erheben durch RFID-Lesegeräte	219
3.5.1.2 Erheben durch RFID-Marken	227
3.5.1.3 Erheben durch Hintergrundinformationssysteme	229
3.5.2 Verarbeiten von personenbezogenen Daten	230
3.5.2.1 Speichern im RFID-System	230
3.5.2.1.1 Speichern durch RFID-Lesegeräte	232
3.5.2.1.2 Speichern durch RFID-Marken	235
3.5.2.1.3 Speichern durch Hintergrundinformationssysteme	239
3.5.2.2 Verändern von Daten im RFID-System	240
3.5.2.2.1 Verändern durch RFID-Lesegeräte	241
3.5.2.2.2 Verändern durch RFID-Marken	242
3.5.2.2.3 Verändern durch Hintergrundinformationssysteme	243
3.5.2.3 Übermitteln von Daten im RFID-System	244
3.5.2.3.1 Übermitteln durch RFID-Lesegeräte	246
3.5.2.3.2 Übermitteln durch RFID-Marken	250
3.5.2.3.3 Übermitteln durch Hintergrundinformationssysteme	259
3.5.2.4 Löschen und Sperren von Daten im RFID-System	260
3.5.2.4.1 Löschen und Sperren durch RFID-Lesegeräte	262
3.5.2.4.2 Löschen und Sperren durch RFID-Marken	262
3.5.2.4.3 Löschen und Sperren durch Hintergrundinformationssysteme	266
3.5.3 Nutzen von personenbezogenen Daten	266
3.5.3.1 Nutzen durch RFID-Lesegeräte	267
3.5.3.2 Nutzen durch RFID-Marken	268
3.5.3.3 Nutzen durch Hintergrundinformationssysteme	270
3.5.4 Automatisierte Verarbeitung gemäß § 3 Abs. 2 BDSG	271
3.5.4.1 Automatisierte Verarbeitung durch RFID-Lesegeräte	274
3.5.4.2 Automatisierte Verarbeitung durch RFID-Marken	275
3.5.4.3 Automatisierte Verarbeitung durch RFID- Hintergrundinformationssysteme	279
3.6 Verantwortlichkeit für den Umgang mit personenbezogenen Daten ..	279
3.6.1 Verantwortlichkeit beim Einsatz von RFID-Lesegeräten	284

3.6.1.1	RFID-Anwendung mit einfachen Datenverarbeitungsverhältnissen	284
3.6.1.2	RFID-Anwendung unter Einbeziehung externer Stellen	284
3.6.1.3	RFID-Anwendungen unter Zusammenarbeit mehrerer Beteiligter	289
3.6.2	Verantwortlichkeit beim Einsatz von RFID-Marken	303
3.6.2.1	RFID-Anwendung mit einfachen Datenverarbeitungsverhältnissen	303
3.6.2.2	RFID-Anwendung unter Einbeziehung externer Stellen und Einrichtungen	303
3.6.2.3	RFID-Anwendungen unter Zusammenarbeit mehrerer Beteiligter	309
3.6.3	Verantwortlichkeit beim Einsatz von Hintergrundinformationssystemen	313
4.	Datenschutzrechtliche Anforderungen	315
4.1	Datenschutzrechtlicher Zulassungstatbestand	315
4.1.1	Erlaubnistatbestände des § 28 BDSG	316
4.1.1.1	Umgang mit Vertragsdaten	319
4.1.1.2	Interessenbezogener Datenumgang	324
4.1.1.3	Umgang mit allgemein zugänglichen Daten	327
4.1.1.4	Zweckbestimmung	333
4.1.2	Datenschutzrechtliche Einwilligung	334
4.1.2.1	Funktion der Einwilligung	334
4.1.2.2	Inhaltliche Wirksamkeitsanforderungen der datenschutzrechtlichen Einwilligung	336
4.1.2.3	Zeitliche Wirksamkeitsanforderungen der Einwilligung	339
4.1.2.4	Formale Wirksamkeitsanforderungen der Einwilligung	339
4.1.2.5	Grenzen der datenschutzrechtlichen Einwilligung	340
4.2	Datenschutzrechtliche Anforderungen an automatisierte Einzelentscheidungen	347
4.2.1	Verbot automatisierter Einzelentscheidung	349
4.2.2	Ausnahmen vom Verbot automatisierter Einzelentscheidung	356
4.2.3	Erweiterung des allgemeinen Auskunftsrechts	369
4.3	Datenschutzrechtliche Anforderungen an mobile personenbezogene Speicher- und Verarbeitungsmedien	371
4.3.1	Rechtsnatur von § 6c BDSG	372
4.3.2	Anwendungsbereich des § 6c BDSG	375
4.3.2.1	Mobile personenbezogene Speicher- und Verarbeitungsmedium	375

4.3.2.2 Ausgabe des Mediums.....	375
4.3.2.3 Automatisierte Verarbeitung.....	382
4.3.2.4 Alleiniger Einfluss durch Gebrauch des Mediums	391
4.3.3 Unterrichtungspflichten.....	397
4.3.3.1 Adressat der Norm – Verpflichtete Stelle	397
4.3.3.2 Adressat der Unterrichtung – Betroffener.....	403
4.3.3.3 Umfang der Unterrichtung.....	407
4.3.3.4 Form und Zeitpunkt der Unterrichtung	419
4.3.3.5 Ausnahme von der Unterrichtungspflicht	423
4.3.4 Technische Unterstützungspflicht nach § 6c Abs. 2 BDSG	424
4.3.5 Unterrichtungspflicht nach § 6c Abs. 3 BDSG	431
4.4 Datenschutzrechtliche Rechte für den Betroffenen.....	438
4.4.1 Recht auf Auskunft.....	439
4.4.1.1 Auskunft bei RFID-Lesegeräten.....	440
4.4.1.2 Auskunft bei RFID-Marken.....	456
4.4.1.3 Auskunft bei Hintergrundinformationssystemen	464
4.4.2 Berichtigung, Löschung und Sperrung	465
4.4.2.1 Berichtigung, Löschung und Sperrung bei RFID- Lesegeräten	466
4.4.2.2 Berichtigung, Löschung und Sperrung bei RFID-Marken ..	470
4.4.2.3 Berichtigung, Löschung und Sperrung bei Hintergrundinformationssystemen.....	473
4.4.3 Recht auf Widerspruch.....	473
4.4.3.1 Das Widerspruchsrecht gemäß § 35 Abs. 5 BDSG.....	473
4.4.3.2 Das Widerspruchsrecht gemäß § 28 Abs. 4 BDSG.....	477
4.4.4 Schadenersatzhaftung beim Einsatz von RFID-Systemen	479
4.5 Datenschutzrechtliche Anforderungen an die Datensicherheit und technisch organisatorische Schutzmaßnahmen.....	484
4.5.1 Angriffsmöglichkeiten gegen RFID-Systeme	485
4.5.2 Schutz durch technische und organisatorische Maßnahmen ..	485
4.5.2.1 Normadressat	485
4.5.2.2 Anforderungen der Datensicherheit	486
4.5.2.3 Anforderungen der Anlage zu § 9 Satz 1 BDSG	487
4.5.2.3.1 Reichweite der Anlage zu § 9 Satz 1 BDSG.....	489
4.5.2.3.2 Zutrittskontrolle.....	490
4.5.2.3.3 Zugangskontrolle.....	492
4.5.2.3.4 Zugriffs- und Zweckbestimmungskontrolle	494
4.5.2.3.5 Weitergabekontrolle	499
4.5.2.3.6 Eingabekontrolle	504

4.5.2.3.7	Auftragskontrolle	507
4.5.2.3.8	Verfügbarkeitskontrolle	508
4.5.2.4	Vorbehalt der Verhältnismäßigkeit	511
4.5.3	Schutz durch Maßnahmen des Selbst- und Systemdatenschutzes	518
4.5.3.1	Präventive Gestaltungspflicht des § 3a BDSG	519
4.5.3.2	Schutz vor unbefugtem Zugang	520
4.5.3.3	Schutz vor unbefugtem Zugriff und Missachtung der Zweckbestimmung	527
4.5.3.4	Schutz vor der unbefugten Weitergabe	533
4.5.3.5	Umsetzungschancen	536
5.	Schutzbedarf und Schutzansätze	539
5.1	Herausforderungen des Einsatzes von RFID-Systemen – ausgewählte Problemkreise	539
5.1.1	Anwendbarkeit und Reichweite des Datenschutzrechts	539
5.1.1.1	Personalisierung von zunächst nicht personenbezogenen Daten	539
5.1.1.2	Erstmalige Personalisierung von Daten	542
5.1.1.3	Rückbezug von Daten	543
5.1.2	Vorkehrungen zum Schutz der Selbstbestimmung	545
5.1.2.1	Schutzdefizit durch irreversible Eingriffe	545
5.1.2.2	Schutzdefizit wegen funktional gelockerter Zweckbindung	546
5.1.2.3	Schutzdefizit hinsichtlich ungenügender Transparenz	549
5.1.2.4	Schutzdefizit durch Umgehung von datenschutzrechtlichen Vorgaben	549
5.1.2.5	Schutzdefizit durch risikoinadäquates Schutzprogramm	550
5.1.3	Verantwortlichkeit und Erlaubnis zur Datenverarbeitung	551
5.1.3.1	Schutz vor Registrierung im Ansprechbereich eines RFID-Lesegeräts	551
5.1.3.1.1	Schutz vor Abfrage der weiteren Nutzdaten einer RFID-Marke	552
5.1.3.1.2	Schutz vor Abfrage einer RFID-Markenennung	557
5.1.3.1.3	Defizit der geltenden Schutzregeln	558
5.2	Konzeptionelle Schutzansätze	560
5.2.1	Stärkung des Datenschutzes durch Verarbeitungsregeln	560
5.2.1.1	Privilegierung technisch bedingter Verarbeitung	560
5.2.1.2	Maßnahmen zum Schutz technisch bedingter Verarbeitung	561

5.2.2	Stärkung des Datenschutzes durch Technikgestaltung	561
5.2.2.1	Säule des technischen Datenschutzes	562
5.2.2.2	Effektivierung der präventiven Gestaltungspflicht	563
5.2.2.3	Maßnahmen zur Datenvermeidung und Datensparsamkeit	564
5.2.3	Stärkung des Datenschutzrechts durch Risikovorsorge	564
5.2.3.1	Schutzinteresse der noch nicht betroffenen Person	565
5.2.3.2	Idee der Risikovorsorge	568
5.2.3.3	Verfassungsrechtliche Begründung der Risikovorsorge	569
5.2.3.3.1	Wandel des staatlichen Handelns	569
5.2.3.3.2	Gewährleistungspflicht des Staates	570
5.2.3.3.3	Folgen der Risikovorsorge	570
5.2.3.3.3.1	Ziel und Gegenstand der Risikovorsorge bei RFID- Systemen	570
5.2.3.3.3.2	Verantwortlicher der Risikovorsorge	571
5.2.3.3.4	Rechtfertigung und Grenzen der Risikovorsorge	571
5.2.3.3.4.1	Unzumutbares Risiko als Eingriffsschwelle	571
5.2.3.3.4.2	Rechte Dritter als Übermaßverbot	573
5.2.3.3.5	Ansätze der Risikovorsorge bei RFID-Systemen	574
5.2.3.3.5.1	Form der Maßnahmen	574
5.2.3.3.5.2	Art der Maßnahmen	575
5.2.3.3.5.2.1	Grundsatz der Kontextwahrung	575
5.2.3.3.5.2.2	Grundsatz der Offenlegung	577
5.2.3.3.5.2.3	Stärkung der Position der potenziell Betroffenen	578
5.2.3.3.5.2.4	Grundsatz der Datensparsamkeit	579
6.	Reformperspektiven des Datenschutzrechts durch eine europäische Datenschutz-Grundverordnung	583
6.1	Rechtsgrundlage und Regelungskonzept der Datenschutz- Grundverordnung	585
6.2	Regelungsinhalt der europäischen Datenschutz-Grundverordnung	587
6.2.1	Vorschlag der EU-Kommission und die In-Kraft-getretene Datenschutz-Grundverordnung	587
6.2.2	Standpunkt des Europäischen Parlaments	593
6.2.3	Allgemeine Ausrichtung des Rates der Europäischen Union	594
6.3	Bedeutung für den Einsatz von RFID-Systemen	595
6.3.1	Anwendbarkeit und Grundprinzipien des europäischen Datenschutzrechts	595

6.3.2	Transparenzanforderungen und Betroffenenrechte im europäischen Datenschutzrecht	603
6.3.3	Datenschutz durch Technik und präventive Evaluationsinstrumente im europäischen Datenschutzrecht ...	611
6.3.4	Vorläufige Würdigung des europäischen Datenschutzrechts ..	618
7.	Ausblick	621
	Literaturverzeichnis	623

Auto-ID-Verfahren im Kontext allgegenwärtiger
Datenverarbeitung
Datenschutzrechtliche Betrachtung des Einsatzes von
RFID-Systemen
Müller, J.
2018, XXXI, 652 S. 6 Abb., 4 Abb. in Farbe., Softcover
ISBN: 978-3-658-19124-5