

Inhaltsverzeichnis

Vorwort zur zweiten Auflage	V
Vorwort zur ersten Auflage	VI

Teil 1: Grundzüge des BDSG

Kapitel 1: Einführung	1
I. Einleitung	1
II. Was sollte man zur Entwicklung des BDSG von 1977–2014 wissen?	2
1. Verkündung 1977	3
2. Volkszählungsurteil von 1983	3
3. Erste Neufassung 1990	4
4. BDSG-Reform von 2001	4
5. BDSG-Novelle von 2009	5
6. Entwurf eines „Gesetzes zur Regelung des Beschäftigtendatenschutzes“	5
III. Welche europäischen Entwicklungen haben Auswirkungen auf die Anwendung des BDSG?	6
1. Relevante EuGH-Rechtsprechung zum BDSG	6
a) Entscheidung vom 6.3.2003 (Rs. C-101/01)	6
b) Urteil vom 20.5.2003 (Rs. T-179/02)	7
c) Urteil vom 8.11.2007 (Rs. T-194/04)	7
d) Urteil vom 16.12.2008 (C-524/06)	7
e) Entscheidung vom 9.3.2010 (Rs. C-518/07)	8
f) Entscheidung vom 24.11.2011 (verb. Rs. C-468/10, C-469/10)	8
2. Die EU-Datenschutz-Grundverordnung	9
IV. Mit welchen Problemen muss man beim Umgang mit dem BDSG in der Praxis rechnen?	10
1. Sprachliche Schwächen des BDSG	10
2. Verwendung unbestimmter Rechtsbegriffe	11
3. Fehlende Vorgaben von Gerichten und Aufsichtsbehörden	11
4. Verschachtelter Aufbau des BDSG	13
V. Warum sollten Unternehmen das BDSG beachten?	15
Kapitel 2: Welche Grundprinzipien des BDSG sollte man kennen?	17

I. Was bedeuten Begriffe wie Verhältnismäßigkeitsgrundsatz, Datenvermeidung oder Datensparsamkeit?	17
1. Recht auf informationelle Selbstbestimmung	17
2. Interessenabwägung	18
3. Datenvermeidung und Datensparsamkeit, § 3a BDSG	19
4. Prüfung der Verhältnismäßigkeit einer konkreten Maßnahme	20
a) Geeignetheit	20
b) Erforderlichkeit	21
c) Angemessenheit	22
II. Was hat es mit dem Verbot mit Erlaubnisvorbehalt auf sich?	22
III. Was besagt der Grundsatz der Zweckbindung bei der Verarbeitung personenbezogener Daten?	23
IV. Was bedeutet Transparenz gegenüber dem Betroffenen im deutschen Datenschutzrecht?	24
Kapitel 3: Was gehört zum Basiswissen bei der praktischen Anwendung des BDSG?	26
I. Wer ist für die Einhaltung der Regeln des BDSG verantwortlich?	26
II. Für welche Formen der Datenverarbeitung gilt das BDSG? ...	28
1. Einsatz von Datenverarbeitungsanlagen oder dateimäßige Verarbeitung	28
2. Keine Anwendung des BDSG für ausschließlich persönliche oder familiäre Tätigkeiten	30
3. Keine Anwendung des BDSG, wenn es durch Spezialgesetze verdrängt wird	31
III. Was sind personenbezogene Daten?	32
1. Einzelangaben	32
2. Persönliche oder sachliche Angaben	33
3. Bestimmbarkeit einer natürlichen Person durch die fraglichen Daten	34
IV. Was sind besondere Arten personenbezogener Daten?	34
V. Was bedeutet das Erheben personenbezogener Daten?	34
1. Bedeutung des Begriffs „Erheben“	35
2. Grundsatz der Direkterhebung	36
3. Ausnahmen vom Grundsatz der Direkterhebung	37
4. Information des Betroffenen bei der Direkterhebung	39

VI. Was ist das Verarbeiten personenbezogener Daten?	40
1. Bedeutung des Begriffs „Speichern“	40
2. Bedeutung des Begriffs „Verändern“	40
a) Anonymisieren von Daten	42
b) Pseudonymisieren von Daten	44
3. Bedeutung des Begriffs „Übermitteln“	45
4. Bedeutung des Begriffs „Löschen“	47
5. Bedeutung des Begriffs „Sperrn“	48
VII. Was versteht man unter dem Nutzen von personenbezogenen Daten?	49
VIII. Was ist eine Auftragsdatenverarbeitung?	50
1. Anwendungsbereich von § 11 BDSG	50
2. Wesentliche Voraussetzung einer Auftragsdatenverarbeitung: Weisungsgebundenheit des Auftragnehmers	52
3. Auftragsdatenverarbeitung nur innerhalb der EU oder EWR ...	53
4. Auswahl und Überwachung des Auftragnehmers	54
5. Sonderfall: Cloud Computing	54
Kapitel 4: Was muss man zur Verwendung von Einwilligungen wissen?	57
I. Kann man Einwilligungen der Betroffenen auch neben gesetzlichen Erlaubnistatbeständen einsetzen?	58
II. Welche praktischen Probleme müssen bei der Verwendung von Einwilligungen berücksichtigt werden?	60
1. Zeitpunkt	62
2. Widerrufbarkeit	62
3. Inhaltliche und formelle Anforderungen an eine Einwilligung des Betroffenen	63
a) Transparenz der Einwilligung	63
b) Freiwilligkeit der Einwilligung	64
c) Informierte Einwilligung	66
d) Formelle Anforderungen an Einwilligungserklärungen	67
Kapitel 5: Gesetzliche Erlaubnisnormen des BDSG.	71
I. Datenverarbeitung aufgrund gesetzlicher Anordnung	72
1. Beispiele für anordnende Gesetzesnormen	72
2. Inhaltliche Anforderungen an derartige Spezialnormen	73
3. Reichweite derartiger Spezialvorschriften	75

II. Datenverarbeitung aufgrund gesetzlicher Erlaubnis (§ 28 BDSG)	75
1. Datenverarbeitung zur Begründung, Durchführung oder Beendigung von Schuldverhältnissen, § 28 Abs. 1 Satz 1 Nr. 1 BDSG	76
a) Das Schuldverhältnis im Sinne von § 28 Abs. 1 Satz 1 Nr. 1 BDSG	77
b) Erforderlichkeit im Sinne von § 28 Abs. 1 Satz 1 Nr. 1 BDSG	78
c) Angemessene Berücksichtigung der schutzwürdigen Interessen des Betroffenen	79
2. Datenverarbeitung zur Wahrung berechtigter Interessen der verantwortlichen Stelle, § 28 Abs. 1 Satz 1 Nr. 2 BDSG	79
a) Erfüllung eigener Geschäftszwecke	80
b) Wahrung berechtigter Interessen	82
c) Überwiegende schutzwürdige Interessen des Betroffenen ..	83
3. Datenverarbeiten für Zwecke des Adresshandels oder der Werbung, § 28 Abs. 3 BDSG	87
4. Verarbeitung sensibler Daten, § 28 Abs. 6–9 BDSG	89
III. Datenverarbeitung im Rahmen des Beschäftigungsverhältnisses (§ 32 BDSG)	90
1. Umgang mit Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses, § 32 Abs. 1 Satz 1 BDSG	96
a) Geeignet für Zwecke des Beschäftigungsverhältnisses	96
b) Erforderlich für Zwecke des Beschäftigungsverhältnisses ...	99
c) Berücksichtigung schutzwürdiger Interessen des Betroffenen (Angemessenheit)	100
d) Sonderfall: „Whistleblowing“ (Hinweisgebersysteme) und § 32 Abs. 1 Satz 1 BDSG	103
e) Sonderfall: Kontrolle der E-Mails von Beschäftigten	107
aa) Bei verbotener Privatnutzung der E-Mail-Systeme	107
bb) Bei erlaubter Privatnutzung der E-Mail-Systeme	108
cc) Regelungen zur Nutzung betrieblicher IT-Systeme	111
dd) Durchführung von E-Mail-Kontrollen	113
2. Aufdeckung von Straftaten im Beschäftigungsverhältnis, § 32 Abs. 1 Satz 2 BDSG	115
a) Anwendungsbereich von § 32 Abs. 1 Satz 2 BDSG	115
b) Anforderungen an den Umgang mit Beschäftigtendaten zur Aufdeckung von Straftaten	118
aa) Geeignet für Zwecke der Aufdeckung von Straftaten ...	118
bb) Erforderlich zum Zweck der Aufdeckung von Straftaten	119
cc) Angemessene Berücksichtigung schutzwürdiger Interessen des Betroffenen	119

c) Vorgaben der Rechtsprechung	122
d) Allgemeine Empfehlungen zum Umgang mit Beschäftigtendaten	123
e) Mitbestimmungsrechte des Betriebsrats	125
aa) Gesetzliche Aufgaben des Betriebsrats	126
bb) Information des Betriebsrats	126
cc) Mitbestimmungsrechte des Betriebsrats	127
f) Betriebsvereinbarungen als Rechtsgrundlage für Datenumgang	128
aa) Regelungsrahmen von Betriebsvereinbarungen	128
bb) Beispielsfall: Betriebsvereinbarung zur Videoüberwachung	130
Kapitel 6: Der Datenschutzbeauftragte im Unternehmen	141
I. Wann müssen Unternehmen einen betrieblichen Datenschutzbeauftragten bestellen?	143
1. Unternehmen, die 10 oder mehr Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen	145
2. Unternehmen, die 20 oder mehr Personen mit der nicht-automatisierten Verarbeitung personenbezogener Daten beschäftigen	147
3. Unternehmen, die besondere Voraussetzungen erfüllen	148
a) Geschäftsmäßige Datenverarbeitung zum Zweck der Übermittlung oder der Markt- oder Meinungsforschung	149
b) Verarbeitungen, die einer Vorabkontrolle unterliegen	149
II. Welche Stellung und Rechte muss der Datenschutzbeauftragte im Unternehmen haben?	149
1. Erforderliche Fachkunde	150
2. Erforderliche Zuverlässigkeit	150
III. Welche Aufgaben hat der Datenschutzbeauftragte?	151
1. Hinwirken auf die Befolgung der Vorschriften über den Datenschutz	151
2. Überwachung der ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen	152
3. Schulung der bei der Verarbeitung personenbezogener Daten tätigen Personen	153
4. Bekanntmachung des Verfahrenszeichnisses	153
5. Durchführung einer Vorabkontrolle	155
a) Besonders riskante automatisierte Verfahren	155

b) Durchführung der Vorabkontrolle durch den Datenschutzbeauftragten.	157
c) Umfang der Vorabkontrolle.	157
IV. Welche Stellung und Befugnisse hat der betriebliche Datenschutzbeauftragte?	158
1. Direkte Berichtslinie zur Unternehmensleitung.	158
2. Kündigungsschutz, Widerruf der Bestellung und Benachteiligungsverbot	159
3. Unterstützung, Kontrollbefugnisse und Fortbildung	159
a) Unterstützung bei Kontrollaufgaben des Datenschutzbeauftragten.	159
b) Kontrollbefugnisse des betrieblichen Datenschutzbeauftragten.	160
c) Fort- und Weiterbildung des Datenschutzbeauftragten.	161
4. Verschwiegenheitspflichten des betrieblichen Datenschutzbeauftragten	161
Kapitel 7: Anforderungen an den grenzüberschreitenden Datenverkehr	162
I. Wie prüft man in der ersten Stufe die Zulässigkeit der Übermittlung an sich?	164
II. Wie wird in der zweiten Stufe die Zulässigkeit der grenzüberschreitenden Datenübermittlung geprüft?	164
1. Der Sitz des Datenempfängers als Ausgangspunkt	164
2. Entgegenstehende schutzwürdige Interessen.	165
a) Drittstaaten mit anerkanntem angemessenen Schutzniveau	166
b) Sonderregelung für Datenempfänger in den USA: Safe Harbor-Abkommen.	166
c) Ausnahmen vom Verbot der Übermittlung an Stellen ohne angemessenes Schutzniveau	168
aa) Einwilligungen.	169
bb) Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen	170
d) Sonderfälle: Standardvertragsklauseln oder verbindliche Unternehmensregelungen („Binding Corporate Rules“)	171
aa) Verwendung der EU-Standard-Vertragsklauseln	171
bb) Verbindliche Unternehmensregelungen („Binding Corporate Rules“)	172
cc) Verbindliche Unternehmensregelungen für Auftragsverarbeiter („Binding Corporate Rules for Processors“)	173

Kapitel 8: Umgang mit Datenpannen nach § 42a BDSG	175
I. Wozu dient § 42a BDSG?	175
II. Welche Voraussetzungen hat § 42a Satz 1 BDSG?	177
1. Unrechtmäßige Kenntniserlangung durch Dritte	177
2. Feststellung der Datenpanne	179
3. Relevante Datenarten nach § 42a Satz 1 Nr. 1– 4 BDSG	179
a) Besondere Arten personenbezogener Daten nach § 3 Abs. 9 BDSG	180
b) Personenbezogene Daten, die einem Berufsgeheimnis unterliegen.	180
c) Personenbezogene Daten, die im Zusammenhang mit Straftaten oder Ordnungswidrigkeiten stehen.	180
d) Personenbezogene Daten zu Bank- oder Kreditkartenkonten	181
4. Drohende schwerwiegende Beeinträchtigungen	181
a) Schwere der drohenden Beeinträchtigungen	181
b) Beurteilungsspielraum des Unternehmens	182
III. Was sind die Rechtsfolgen von § 42a Satz 1 BDSG?	183
1. Information der Aufsichtsbehörde	183
2. Information der Betroffenen	184
 Kapitel 9: Organisatorische und technische Maßnahmen zum Schutz personenbezogener Daten.	187
I. Was umfassen Zutritts-, Zugangs- und Zugriffskontrollen?	188
II. Worum geht es bei Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrollen?	190
III. Was verlangt das Trennungsgebot?	191
 Kapitel 10: Die Unterrichtung des Betroffenen	192
I. Wann muss man den Betroffenen nach § 33 BDSG informieren? 192	
1. Voraussetzungen der Benachrichtigungspflicht	193
2. Umfang der Benachrichtigungspflicht	193
3. Ausnahmen von der Benachrichtigungspflicht	194
4. Folgen einer Nichtbeachtung der Benachrichtigungspflicht	194
II. Wann muss dem Betroffenen Auskunft erteilt werden?	195
1. Voraussetzungen der Auskunftspflicht nach § 34 BDSG	195
2. Umfang der Auskunftspflicht.	196
3. Ausnahmen von der Auskunftspflicht	198
4. Folgen bei Nichtbeachtung der Auskunftspflicht.	198

Kapitel 11: Folgen von Verstößen gegen das BDSG	199
I. Wen trifft die Verantwortung für Datenschutzverstöße im Unternehmen?	199
II. Welche strafrechtlichen Risiken drohen bei Datenschutzverstößen?	200
1. Anforderungen an eine Strafbarkeit nach § 44 BDSG	200
a) Begehung einer vorsätzlichen Ordnungswidrigkeit nach § 43 Abs. 2 BDSG	201
b) Handeln gegen Entgelt	201
c) Handeln in (Selbst- oder Fremd-)Bereicherungsabsicht	203
d) Handeln mit Schädigungsabsicht	203
e) Strafantrag nach § 44 Abs. 2 BDSG	206
2. Kritik an dem geltenden § 44 BDSG	206
3. Weitere Strafnormen zur Verletzung des persönlichen Lebens- und Geheimbereichs	207
4. Von Strafbarkeitsrisiken bedrohte Betroffene im Unternehmen	207
a) Strafbarkeit des Datenschutzbeauftragten	208
b) Strafbarkeit der Unternehmensleitung	210
III. Welche ordnungsrechtlichen Sanktionen drohen bei Datenschutzverstößen?	211
IV. Welche zivilrechtlichen Risiken drohen bei Datenschutzverstößen?	212
1. Ansprüche nach § 7 BDSG	212
a) Vermögensschaden	212
b) Kausalität	213
c) Verschulden	213
2. Sonstige zivilrechtliche Ansprüche wegen Verstößen gegen das BDSG	214
Kapitel 12: Welche Aufgaben und Rechte haben die Aufsichtsbehörden für den Datenschutz?	215
I. Wie ist die Datenschutzaufsicht in Deutschland organisiert?	215
II. Wie kontrollieren die Aufsichtsbehörden die Einhaltung des Datenschutzes in Unternehmen?	216
1. Anlässe für die Durchführung von Datenschutz-Kontrollen	216
2. Ablauf einer Datenschutz-Kontrolle	217
III. Was passiert, wenn die Aufsichtsbehörde anlässlich der Kontrolle tatsächlich Mängel feststellt?	219

1. Anordnung von Maßnahmen zur Beseitigung festgestellter Verstöße	219
2. Untersagung schwerwiegender Verstöße	220
a) Schwerwiegende Verstöße oder Mängel	220
b) Erfolgreiche Anordnung zur Beseitigung	220
3. Zuständigkeit für die Ahndung von Ordnungswidrigkeiten	221
IV. Wann kann die Aufsicht den betrieblichen Datenschutzbeauftragten abberufen?	221
V. Welche weiteren Aufgaben haben Aufsichtsbehörden?	223
1. Veröffentlichen von Tätigkeitsberichten	223
2. Beratung und Unterstützung der Unternehmen	223

Teil 2: Abdruck und Kurzkomentierung der wichtigsten Vorschriften des BDSG

Einleitung	227
Erster Abschnitt: Allgemeine und gemeinsame Bestimmungen	
§ 1 Zweck und Anwendungsbereich des Gesetzes	228
§ 2 Öffentliche und nicht-öffentliche Stellen	231
§ 3 Weitere Begriffsbestimmungen	233
§ 3a Datenvermeidung und Datensparsamkeit	238
§ 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung	239
§ 4a Einwilligung	242
§ 4b Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen	245
§ 4c Ausnahmen	250
§ 4d Meldepflicht	254
§ 4e Inhalt der Meldepflicht	258
§ 4f Beauftragter für den Datenschutz	259
§ 4g Aufgaben des Beauftragten für den Datenschutz	265
§ 5 Datengeheimnis	267
§ 6 Rechte des Betroffenen	269
§ 6a Automatisierte Einzelentscheidung	271
§ 6b Beobachtung öffentlich zugänglicher Räume mit optisch- elektronischen Einrichtungen	272
§ 6c Mobile personenbezogene Speicher- und Verarbeitungsmedien ..	275
§ 7 Schadensersatz	277
§ 8 Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen	278
§ 9 Technische und organisatorische Maßnahmen	278

§ 9a	Datenschutzaudit	282
§ 10	Einrichtung automatisierter Abrufverfahren	282
§ 11	Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag	284

Zweiter Abschnitt: Datenverarbeitung der öffentlichen Stellen

§ 12	Anwendungsbereich	287
§ 13	Datenerhebung	288
§ 14	Datenspeicherung, -veränderung und -nutzung	289
§ 15	Datenübermittlung an öffentliche Stellen	291
§ 16	Datenübermittlung an nicht-öffentliche Stellen	292
§ 17	(weggefallen)	292
§ 18	Durchführung des Datenschutzes in der Bundesverwaltung	292
§ 19	Auskunft an den Betroffenen	293
§ 19a	Benachrichtigung	294
§ 20	Berichtigung, Löschung und Sperrung von Daten; Widerspruchsrecht	295
§ 21	Anrufung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit	296
§ 22	Wahl des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit	297
§ 23	Rechtsstellung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit	298
§ 24	Kontrolle durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit	300
§ 25	Beanstandungen durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit	301
§ 26	Weitere Aufgaben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit	302

**Dritter Abschnitt: Datenverarbeitung nicht-öffentlicher Stellen und
öffentlich-rechtlicher Wettbewerbsunternehmen**

§ 27	Anwendungsbereich	303
§ 28	Datenerhebung und -speicherung für eigene Geschäftszwecke	304
§ 28a	Datenübermittlung an Auskunfteien	314
§ 28b	Scoring	316
§ 29	Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung	318
§ 30	Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung in anonymisierter Form	321
§ 30a	Geschäftsmäßige Datenerhebung und -speicherung für Zwecke der Markt- oder Meinungsforschung	323
§ 31	Besondere Zweckbindung	324

§ 32	Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses	326
§ 33	Benachrichtigung des Betroffenen	330
§ 34	Auskunft an den Betroffenen	332
§ 35	Berichtigung, Löschung und Sperrung von Daten	337
§§ 36 und 37	(weggefallen)	340
§ 38	Aufsichtsbehörde	340
§ 38a	Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen	344

Vierter Abschnitt: Sondervorschriften

§ 39	Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen	345
§ 40	Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen	347
§ 41	Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Medien	347
§ 42	Datenschutzbeauftragter der Deutschen Welle	348
§ 42a	Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten	349

Fünfter Abschnitt: Schlussvorschriften

§ 43	Bußgeldvorschriften	351
§ 44	Strafvorschriften	354

Sechster Abschnitt: Übergangsvorschriften

§ 45	Laufende Verwendungen	355
§ 46	Weitergeltung von Begriffsbestimmungen	356
§ 47	Übergangsregelung	356
§ 48	Bericht der Bundesregierung	356

Anhang

1.	German Federal Data Protection Act (BDSG)	359
2.	Praktiker-Glossar	417
3.	Ausgewählte Beschlüsse des Düsseldorfer Kreises von 2006 bis 2014	455
4.	Ausgewählte Stellungnahmen und Entscheidungen der Artikel 29 Datenschutzgruppe von 2008 – 2014	457

Sachregister		465
---------------------	--	-----