

Handbuch Datenschutz im Unternehmen

von

Tim Wybitul

Rechtsanwalt, Frankfurt a. M.



Verlag Recht und Wirtschaft GmbH
Frankfurt am Main

Inhaltsverzeichnis

Vorwort	V
---------------	---

Teil 1: Grundzüge des BDSG

Kapitel 1: Einführung	1
I. Einleitung	1
II. Entwicklung des BDSG von 1977–2010	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. Umgang mit dem BDSG in der Praxis	6
1. Sprachliche Schwächen des BDSG	6
2. Verwendung unbestimmter Rechtsbegriffe	7
3. Fehlende Vorgaben von Gerichten und Aufsichtsbehörden ..	7
IV. Warum müssen Unternehmen das BDSG beachten?	9
V. Wie ist das BDSG aufgebaut?	10
Kapitel 2: Welche Grundregeln des BDSG sollte man kennen? ..	13
I. Verhältnismäßigkeitsgrundsatz, Datenvermeidung, Datensparsamkeit	13
1. Recht auf informationelle Selbstbestimmung	14
2. Interessenabwägung	14
3. Datenvermeidung und Datensparsamkeit, § 3a BDSG	15
4. Prüfung der Verhältnismäßigkeit einer konkreten Maßnahme	16
a) Geeignetheit	17
b) Erforderlichkeit	18
c) Angemessenheit	19
II. Verbot des Umgangs mit personenbezogenen Daten	20
III. Zweckbindung personenbezogener Daten	20

IV. Transparenz gegenüber dem Betroffenen	21
Kapitel 3: Grundbegriffe des BDSG	24
I. Wer ist für die Einhaltung der Regeln des BDSG verantwortlich?	24
II. Für welche Formen des Umgangs mit Daten gilt das BDSG?	25
1. Einsatz von Datenverarbeitungsanlagen oder dateimäßige Verarbeitung	26
2. Keine Anwendung des BDSG für ausschließlich persönliche oder familiäre Tätigkeiten	27
3. Keine Anwendung des BDSG, wenn es durch Spezialgesetze verdrängt wird	28
III. Was sind personenbezogene Daten?	30
1. Einzelangaben	30
2. Persönliche oder sachliche Angaben	31
3. Bestimmbarkeit einer natürlichen Person durch die fraglichen Daten	32
IV. Was sind besondere Arten personenbezogener Daten?	32
Kapitel 4: Was ist das Erheben, Verarbeiten oder Nutzen personenbezogener Daten?	34
I. Was ist das Erheben personenbezogener Daten?	35
1. Grundsatz der Direkterhebung	36
2. Ausnahmen vom Grundsatz der Direkterhebung	36
3. Information des Betroffenen bei der Direkterhebung	39
II. Was ist das Verarbeiten personenbezogener Daten?	40
1. Speichern	40
2. Verändern	41
a) Anonymisieren von Daten	42
b) Pseudonymisieren von Daten	44
3. Übermitteln	46
4. Löschen	48
5. Sperren	49
III. Nutzen	50
IV. Sonderfall Auftragsdatenverarbeitung nach § 11 BDSG	50
1. Anwendungsbereich von § 11 BDSG	51

2. Wesentliche Voraussetzung einer Auftragsdatenverarbeitung: Weisungsgebundenheit des Auftragnehmers	53
3. Auftragsdatenverarbeitung nur innerhalb der EU oder EWR	54
4. Auswahl und Überwachung des Auftragnehmers	55
Kapitel 5: Erlaubnis zum Umgang mit Daten	57
I. Einwilligung des Betroffenen, § 4a BDSG	58
1. Nebeneinander von gesetzlicher Erlaubnis zur Datenverarbeitung und einer Einwilligung des Betroffenen ..	59
a) Praktische Probleme bei der Verwendung von Einwilligungen	59
b) Zulässigkeit von Einwilligungen auch beim Vorliegen gesetzlicher Erlaubnistatbestände	61
2. Zeitpunkt der Einwilligung	63
3. Widerruf der Einwilligung	63
4. Inhaltliche und formelle Anforderungen an eine Einwilligung des Betroffenen	64
a) Freiwilligkeit der Einwilligung	65
b) Informierte Einwilligung	67
c) Formelle Anforderungen an Einwilligungserklärungen ...	68
d) Checkliste Einwilligungserklärung nach § 4a BDSG	70
II. Erlaubnis durch gesetzliche Aufgabenzuweisung oder Erlaubnis	72
1. Umgang mit personenbezogenen Daten zur Erfüllung gesetzlicher Pflichten	72
a) Welche Vorschriften können den Umgang mit personenbezogenen Daten zur Erfüllung gesetzlicher Vorschriften erlauben?	72
b) Reichweite von Spezialvorschriften zur Verarbeitung, Erhebung oder Nutzung personenbezogener Daten	75
2. Umgang mit personenbezogenen Daten aufgrund einer Erlaubnisnorm des BDSG	75
III. Umgang mit personenbezogenen Daten zur Begründung, Durchführung oder Beendigung von Schuldverhältnissen, § 28 Abs. 1 Satz 1 Nr. 1 BDSG	76
1. Voraussetzungen von § 28 Abs. 1 Satz 1 Nr. 1 BDSG	77
a) Anbahnung, Vorliegen oder Beendigung eines Schuldverhältnisses	77
b) Für das Schuldverhältnis erforderlich	78

c) Angemessene Berücksichtigung der schutzwürdigen Interessen des Betroffenen	79
IV. Umgang mit personenbezogenen Daten zur Wahrung berechtigter Interessen der verantwortlichen Stelle, § 28 Abs. 1 Satz 1 Nr. 2 BDSG	79
1. Voraussetzungen von § 28 Abs. 1 Satz 1 Nr. 2 BDSG	80
a) Zweck der Erfüllung eigener Geschäftszwecke (Geeignetheit)	80
b) Zur Wahrung berechtigter Interessen (Erforderlichkeit) ..	82
c) Überwiegende schutzwürdige Interessen des Betroffenen (Angemessenheit)	83
e) Anwendung von § 28 Abs. 3 BDSG, Verarbeiten oder Nutzen für Zwecke des Adresshandels oder der Werbung	87
V. Umgang mit sensiblen Daten, § 28 Abs. 6–9 BDSG	89
VI. Umgang mit Daten im Rahmen des Beschäftigungsverhältnisses, § 32 BDSG	91
1. Umgang mit Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses, § 32 Abs. 1 Satz 1 BDSG	95
a) Geeignet für Zwecke des Beschäftigungsverhältnisses ..	96
b) Erforderlich für Zwecke des Beschäftigungsverhältnisses	98
c) Berücksichtigung schutzwürdiger Interessen des Betroffenen (Angemessenheit)	99
d) Sonderfall: „Whistleblowing“ (Hinweisgebersysteme) und § 32 Abs. 1 Satz 1 BDSG	103
e) Sonderfall: Kontrolle der E-Mails von Beschäftigten	105
aa) Bei verbotener Privatnutzung der E-Mail-Systeme ...	105
bb) Bei erlaubter Privatnutzung der E-Mail-Systeme ...	107
cc) Reichweite des Fernmeldegeheimnisses	108
2. Umgang mit Beschäftigtendaten zur Aufdeckung von Straftaten im Beschäftigungsverhältnis, § 32 Abs. 1 Satz 2 BDSG	109
a) Anwendungsbereich von § 32 Abs. 1 Satz 2 BDSG	110
b) Anforderungen an den Umgang mit Beschäftigtendaten zur Aufdeckung von Straftaten	112
aa) Geeignet für Zwecke der Aufdeckung von Straftaten	112
bb) Erforderlich zum Zweck der Aufdeckung von Straftaten	113
cc) Angemessene Berücksichtigung schutzwürdiger Interessen des Betroffenen	114
c) Empfehlungen zum Umgang mit Beschäftigtendaten	117

d) Mitbestimmungsrechte des Betriebsrats	119
aa) Gesetzliche Aufgaben des Betriebsrats	120
bb) Information des Betriebsrats	120
cc) Mitbestimmungsrechte des Betriebsrats	121
e) Betriebsvereinbarungen als Rechtsgrundlage für Datenumgang	122
aa) Regelungsrahmen von Betriebsvereinbarungen	122
bb) Beispielsfall: Betriebsvereinbarung zur Videoüberwachung nach BAG	124
Kapitel 6: Der Datenschutzbeauftragte im Unternehmen	133
I. Welche Unternehmen müssen einen Datenschutzbeauftragten bestellen?	133
1. Unternehmen, die 10 oder mehr Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen	135
2. Unternehmen, die 20 oder mehr Personen mit der nicht-automatisierten Verarbeitung personenbezogener Daten beschäftigen	137
3. Unternehmen, die besondere Voraussetzungen erfüllen	138
a) Geschäftsmäßige Datenverarbeitung zum Zweck der Übermittlung oder der Markt- oder Meinungsforschung	139
b) Verarbeitungen, die einer Vorabkontrolle unterliegen	139
II. Welche Stellung und Rechte muss der Datenschutzbeauftragte im Unternehmen haben?	139
1. Erforderliche Fachkunde	140
2. Erforderliche Zuverlässigkeit	140
III. Welche Aufgaben hat der Datenschutzbeauftragte?	141
1. Hinwirken auf die Befolgung der Vorschriften über den Datenschutz	141
2. Überwachung der ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen	142
3. Schulung der bei der Verarbeitung personenbezogener Daten tätigen Personen	143
4. Bekanntmachung des Verfahrensverzeichnis	143
5. Durchführung einer Vorabkontrolle	145
a) Besonders riskante automatisierte Verfahren	145
b) Durchführung der Vorabkontrolle durch den Datenschutzbeauftragten	147

c) Umfang der Vorabkontrolle	148
IV. Welche Stellung und Befugnisse hat der betriebliche Datenschutzbeauftragte?	148
1. Direkte Berichtslinie zur Unternehmensleitung	149
2. Kündigungsschutz, Widerruf der Bestellung und Benachteiligungsverbot	149
3. Unterstützung, Kontrollbefugnisse und Fortbildung	150
a) Unterstützung bei Kontrollaufgaben des Datenschutzbeauftragten	150
b) Kontrollbefugnisse des betrieblichen Datenschutzbeauftragten	151
c) Fort- und Weiterbildung des Datenschutzbeauftragten ...	151
4. Verschwiegenheitspflichten des betrieblichen Datenschutzbeauftragten	152
Kapitel 7: Anforderungen an den grenzüberschreitenden Datenverkehr	153
I. 1. Stufe: Zulässigkeit der Übermittlung an sich	154
II. 2. Stufe: Zulässigkeit der grenzüberschreitenden Datenübermittlung	155
1. Liegt der Sitz des Datenempfängers in einem EU- bzw. EWR-Staat oder in einem Drittstaat?	155
2. Liegt ein entgegenstehendes schutzwürdiges Interesse vor, insbesondere Fehlen eines angemessenen Datenschutz-niveaus?	155
a) Drittstaaten mit angemessenem Schutzniveau	156
b) Sonderregelung für Datenempfänger in den USA: Safe Harbor-Abkommen	157
c) Ausnahmen vom Verbot der Übermittlung an Stellen ohne angemessenes Schutzniveau	159
aa) Einwilligungen	160
bb) Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen	160
d) Sonderfälle: Standardvertragsklauseln oder verbindliche Unternehmensregelungen („Binding Corporate Rules“) ..	162
aa) Verwendung von Standard-Vertragsklauseln	162
bb) Verbindliche Unternehmensregelungen („Binding Corporate Rules“)	163

Kapitel 8: Umgang mit Datenpannen nach § 42a BDSG	165
I. Überblick über § 42a BDSG	165
II. Welche Voraussetzungen hat § 42a Satz 1 BDSG?	167
1. Unrechtmäßige Kenntniserlangung durch Dritte	167
2. Feststellung der Datenpanne	169
3. Daten nach § 42a Satz 1 Nr. 1–4 BDSG	169
a) Besondere Arten personenbezogener Daten nach § 3 Abs. 9 BDSG	170
b) Personenbezogene Daten, die einem Berufsgeheimnis unterliegen	170
c) Personenbezogene Daten, die im Zusammenhang mit Straftaten oder Ordnungswidrigkeiten stehen	170
d) Personenbezogene Daten zu Bank- oder Kreditkartenkonten	171
3. Drohende schwerwiegende Beeinträchtigungen	171
a) Schwere der drohenden Beeinträchtigungen	172
b) Beurteilungsspielraum des Unternehmens	172
III. Rechtsfolgen von § 42a Satz 1 BDSG	173
1. Information der Aufsichtsbehörde	174
2. Information der Betroffenen	174
Kapitel 9: Organisatorische und technische Maßnahmen zum Schutz personenbezogener Daten	176
I. Zutrittskontrolle, Zugangskontrolle und Zugriffskontrolle ..	177
II. Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle und Verfügbarkeitskontrolle	179
III. Trennungsgebot zur Zweckbindung	180
Kapitel 10: Unterrichtung des Betroffenen	181
I. Benachrichtigung des Betroffenen bei der Speicherung für eigene Zwecke ohne Kenntnis des Betroffenen, § 33 BDSG ..	181
1. Welche Voraussetzungen hat die Benachrichtigungspflicht nach § 33 BDSG?	182
2. Welchen Umfang hat die Benachrichtigungspflicht?	182
3. Welche Ausnahmen gibt es von der Benachrichtigungs- pflicht?	183

4. Welche Folgen sieht das BDSG bei Nichtbeachtung der Benachrichtigungspflicht vor?	183
II. Auskunft an den Betroffenen auf dessen Verlangen, § 34 BDSG	183
1. Welche Voraussetzungen hat die Auskunftspflicht nach § 34 BDSG?	184
2. Welchen Umfang hat die Auskunftspflicht?	185
3. Welche Ausnahmen gibt es von der Auskunftspflicht?	187
4. Welche Folgen sieht das BDSG bei Nichtbeachtung der Auskunftspflicht vor?	187
Kapitel 11: Welche Folgen haben Verstöße gegen das BDSG? ...	188
I. Wen verpflichtet das BDSG?	188
II. Welche strafrechtlichen Risiken drohen bei Datenschutzverstößen?	188
1. Anforderungen an eine Strafbarkeit nach § 44 BDSG	189
a) Begehung einer vorsätzlichen Ordnungswidrigkeit nach § 43 Abs. 2 BDSG	190
b) Gegen Entgelt	190
c) In Bereicherungsabsicht	192
d) In Schädigungsabsicht	192
e) Strafantrag nach § 44 Abs. 2 BDSG	195
2. Kritik an dem geltenden § 44 BDSG	195
3. Weitere Strafnormen zur Verletzung des persönlichen Lebens- und Geheimbereichs	196
4. Welchen Personen im Unternehmen drohen Strafbarkeitsrisiken?	197
a) Strafbarkeit des Datenschutzbeauftragten	197
b) Strafbarkeit der Unternehmensleitung	199
III. Welche ordnungsrechtlichen Risiken drohen nach § 43 BDSG?	200
IV. Welche zivilrechtlichen Risiken drohen?	201
1. Ansprüche nach § 7 BDSG	201
a) Vermögensschaden	202
b) Kausalität	202
c) Verschulden	203
2. Sonstige zivilrechtliche Ansprüche wegen Verstößen gegen das BDSG	203

Kapitel 12: Welche Aufgaben und Rechte haben die Aufsichtsbehörden für den Datenschutz?	205
I. Kontrolle der Einhaltung des Datenschutzes in Unternehmen	206
1. Anlässe für die Durchführung von Datenschutz-Kontrollen ..	207
2. Beginn einer Datenschutz-Kontrolle	207
3. Auskunftspflicht des Unternehmens gegenüber der Aufsichtsbehörde	207
4. Kontrollen der Aufsichtsbehörden in Unternehmen	208
II. Maßnahmen zur Beseitigung festgestellter Verstöße	209
1. Anordnung von Maßnahmen zur Beseitigung festgestellter Verstöße	210
2. Untersagung schwerwiegender Verstöße	210
a) Schwerwiegende Verstöße oder Mängel	211
b) Erfolgreiche Anordnung zur Beseitigung	211
3. Anordnung der Abberufung des betrieblichen Datenschutzbeauftragten	211
III. Tätigkeitsberichte	213
IV. Beratung und Unterstützung	213
V. Abstimmung einzelner Maßnahmen mit den Aufsichtsbehörden	214
VI. Zuständigkeit für die Ahndung von Ordnungswidrigkeiten .	215

Teil 2: Abdruck und Kurzkomentierung der wichtigsten Vorschriften des BDSG

Einleitung	217
Erster Abschnitt: Allgemeine und gemeinsame Bestimmungen	
§ 1 Zweck und Anwendungsbereich des Gesetzes	218
§ 2 Öffentliche und nicht-öffentliche Stellen	221
§ 3 Weitere Begriffsbestimmungen	223
§ 3a Datenvermeidung und Datensparsamkeit	228
§ 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung .	230
§ 4a Einwilligung	234
§ 4b Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen	237

§ 4c	Ausnahmen	241
§ 4d	Meldepflicht	246
§ 4e	Inhalt der Meldepflicht	250
§ 4f	Beauftragter für den Datenschutz	251
§ 4g	Aufgaben des Beauftragten für den Datenschutz	258
§ 5	Datengeheimnis	260
§ 6	Rechte des Betroffenen	262
§ 6a	Automatisierte Einzelentscheidung	264
§ 6b	Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (<i>nicht kommentiert</i>)	266
§ 6c	Mobile personenbezogene Speicher- und Verarbeitungsmedien (<i>nicht kommentiert</i>)	267
§ 7	Schadensersatz	267
§ 8	Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen (<i>nicht kommentiert</i>)	268
§ 9	Technische und organisatorische Maßnahmen	269
§ 9a	Datenschutzaudit (<i>nicht kommentiert</i>)	271
§ 10	Einrichtung automatisierter Abrufverfahren (<i>nicht kommentiert</i>)	272
§ 11	Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag	273

Zweiter Abschnitt: Datenverarbeitung der öffentlichen Stellen

Erster Unterabschnitt: Rechtsgrundlagen der Datenverarbeitung

§ 12	Anwendungsbereich (<i>nicht kommentiert</i>)	276
§ 13	Datenerhebung (<i>nicht kommentiert</i>)	277
§ 14	Datenspeicherung, -veränderung und -nutzung (<i>nicht kommentiert</i>)	278
§ 15	Datenübermittlung an öffentliche Stellen (<i>nicht kommentiert</i>)	280
§ 16	Datenübermittlung an nicht-öffentliche Stellen (<i>nicht kommentiert</i>)	281
§ 17	(weggefallen)	282
§ 18	Durchführung des Datenschutzes in der Bundesverwaltung (<i>nicht kommentiert</i>)	282

Zweiter Unterabschnitt: Rechte des Betroffenen

§ 19	Auskunft an den Betroffenen (<i>nicht kommentiert</i>)	282
§ 19a	Benachrichtigung (<i>nicht kommentiert</i>)	284
§ 20	Berichtigung, Löschung und Sperrung von Daten; Widerspruchsrecht (<i>nicht kommentiert</i>)	285

§ 21	Anrufung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (<i>nicht kommentiert</i>)	286
------	---	-----

**Dritter Unterabschnitt: Bundesbeauftragter für den
Datenschutz und die Informationsfreiheit**

§ 22	Wahl des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (<i>nicht kommentiert</i>)	287
§ 23	Rechtsstellung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (<i>nicht kommentiert</i>)	288
§ 24	Kontrolle durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (<i>nicht kommentiert</i>)	290
§ 25	Beanstandungen durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (<i>nicht kommentiert</i>)	291
§ 26	Weitere Aufgaben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (<i>nicht kommentiert</i>)	292

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

**Erster Unterabschnitt: Rechtsgrundlagen der
Datenverarbeitung**

§ 27	Anwendungsbereich	293
§ 28	Datenerhebung und -speicherung für eigene Geschäftszwecke	295
§ 28a	Datenübermittlung an Auskunftseien (<i>nicht kommentiert</i>)	304
§ 28b	Scoring (<i>nicht kommentiert</i>)	305
§ 29	Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung (<i>nicht kommentiert</i>)	306
§ 30	Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung in anonymisierter Form (<i>nicht kommentiert</i>)	307
§ 30a	Geschäftsmäßige Datenerhebung und -speicherung für Zwecke der Markt- oder Meinungsforschung (<i>nicht kommentiert</i>)	308
§ 31	Besondere Zweckbindung (<i>nicht kommentiert</i>)	309
§ 32	Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses	309

Zweiter Unterabschnitt: Rechte des Betroffenen

§ 33	Benachrichtigung des Betroffenen	313
§ 34	Auskunft an den Betroffenen	316
§ 35	Berichtigung, Löschung und Sperrung von Daten	320

Dritter Unterabschnitt: Aufsichtsbehörde

§§ 36 und 37 (weggefallen) 324
§ 38 Aufsichtsbehörde 324
§ 38a Verhaltensregeln zur Förderung der Durchführung
datenschutzrechtlicher Regelungen (*nicht kommentiert*) 328

Vierter Abschnitt: Sondervorschriften

§ 39 Zweckbindung bei personenbezogenen Daten, die einem
Berufs- oder besonderen Amtsgeheimnis unterliegen
(*nicht kommentiert*) 328
§ 40 Verarbeitung und Nutzung personenbezogener Daten durch
Forschungseinrichtungen (*nicht kommentiert*) 329
§ 41 Erhebung, Verarbeitung und Nutzung personenbezogener
Daten durch die Medien (*nicht kommentiert*) 329
§ 42 Datenschutzbeauftragter der Deutschen Welle
(*nicht kommentiert*) 330
§ 42a Informationspflicht bei unrechtmäßiger Kenntniserlangung
von Daten 331

Fünfter Abschnitt: Schlussvorschriften

§ 43 Bußgeldvorschriften 334
§ 44 Strafvorschriften 337

Sechster Abschnitt: Übergangsvorschriften

§ 45 Laufende Verwendungen (*nicht kommentiert*) 338
§ 46 Weitergeltung von Begriffsbestimmungen (*nicht kommentiert*) 338
§ 47 Übergangsregelung (*nicht kommentiert*) 339
§ 48 Bericht der Bundesregierung (*nicht kommentiert*) 339

Anhang

1. German Federal Data Protection Act (BDSG) 341
2. Glossar Datenschutz Deutsch/Englisch 405
3. Regierungsentwurf zur Neuregelung des
Beschäftigtendatenschutzes 411

Literaturverzeichnis 525

Sachregister 533