

RECHT WIRTSCHAFT STEUERN

HANDBUCH

Wybitul / Schultze-Melling

Datenschutz im Unternehmen

2. Auflage

dfv Mediengruppe

R&W
Fachmedien Recht und Wirtschaft

Recht Wirtschaft Steuern

Datenschutz im Unternehmen

von

Tim Wybitul

Rechtsanwalt, Frankfurt a. M.

und

Dr. Jyn Schultze-Melling

Rechtsanwalt, München

2., neu bearbeitete Auflage 2014

Bibliografische Information Der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN 978-3-8005-1572-1

dfv' Mediengruppe

© 2014 Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft, Frankfurt am Main

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Satzkonvertierung: fidus Publikations-Service GmbH, Nördlingen

Druck und Verarbeitung: betz-druck GmbH, 64291 Darmstadt

Printed in Germany

Vorwort zur zweiten Auflage

Datenschutz gewinnt seit Jahren zunehmend an Bedeutung und Dynamik. Technologische Fortentwicklungen sowie gesellschaftliche und politische Veränderungen führen zu intensiven Diskussionen über die konkrete Anwendung des deutschen Datenschutzrechts.

Auch deutsche und europäische Gerichte befassen sich immer öfter mit Fragen des Datenschutzes. Beispielsweise hat der Bundesgerichtshof 2013 zwei Privatermittler wegen des unzulässigen Umgangs mit personenbezogenen Daten zu Haftstrafen verurteilt. Erst kürzlich hat der Europäische Gerichtshof mit seinem Urteil zum viel diskutierten Recht auf Vergessen die Abgrenzung zwischen Presse- und Meinungsfreiheit und dem Recht auf informelle Selbstbestimmung geschärft. Zudem geben deutsche Arbeitsgerichte immer mehr Antworten auf Fragen des Datenschutzes im Beschäftigungsverhältnis. Das Bundesarbeitsgericht etwa geht mittlerweile zunehmend dazu über, Informationen nicht zu werten, die der Arbeitgeber unter Verstoß gegen datenschutzrechtliche Vorgaben gesammelt hat. Dies kann Unternehmen vor erhebliche Herausforderungen stellen und etwa Kündigungen wegen Straftaten, Compliance-Verstößen oder anderen Pflichtverletzungen entscheidend erschweren.

Diese Entwicklungen wirken sich ganz erheblich auf die Rahmenbedingungen für den Umgang mit Informationen in der Wirtschaft aus. Dieses Handbuch ermöglicht es dem Leser, sich schnell und unkompliziert über Fragen des Datenschutzes im Unternehmen zu informieren. Das Buch bietet hierfür Beispiele, Handlungsempfehlungen und Praxistipps, die die Umsetzung der Vorgaben des Datenschutzes erleichtern. Es schildert die Vorgaben der Rechtsprechung in verständlichen und einfachen Worten. Das Handbuch ermöglicht es so, die Bedeutung und die Auswirkungen einzelner Urteile zu verstehen und umzusetzen.

Auch die 2. Auflage behält das von Lesern positiv aufgenommene Konzept der Voraufgabe bei. Sie ist daher nach wie vor in einen Handbuchteil und eine praxisorientierte Kommentierung der für Unternehmen relevanten Vorschriften des Bundesdatenschutzgesetzes aufgegliedert. Ergänzt wird dieser Aufbau nun auch durch ein Praktiker-Glossar. Dieser Teil des Handbuchs erläutert die für Unternehmen wichtigsten Begriffe der täglichen Datenschutzarbeit knapp und prägnant. Er zeigt Querverweise zu thematisch verbundenen Fragen auf und bietet für eine Reihe von konkreten Fragestellungen schnelle und praktikable Antworten.

Wir hoffen, dass das Handbuch vielen Praktikern als verlässliche Informationsquelle für den beruflichen Alltag des betrieblichen Datenschutzes dienen wird.

Die Autoren, im Juni 2014

Vorwort zur ersten Auflage

Die Entwicklung der Informationstechnologie und insbesondere des Internet hat die Wirtschaft in den letzten Jahrzehnten umfassend verändert. Diese Veränderungen ermöglichen das Sammeln von Informationen und die Auswertung von Daten in völlig neuem Umfang. Enorme Rechen- und Speicherkapazitäten sind für überschaubare Kosten erhältlich. Bei vielen Datenverarbeitungen gibt inzwischen nicht mehr die Technik die Grenzen vor, sondern der Datenschutz. Die rechtlichen Rahmenbedingungen für den Umgang mit personenbezogenen Daten verändern sich ähnlich schnell wie die technischen Möglichkeiten. Noch vor wenigen Jahren hatte das Datenschutzrecht für viele Unternehmen eine eher begrenzte Bedeutung. Das hat sich spätestens durch die sogenannten Datenschutzaffären seit 2008 gründlich geändert. Der Kreis der Personen, die Entscheidungen zum Datenschutz im Unternehmen treffen müssen, hat sich erheblich erweitert. Die veränderten Anforderungen beim Umgang mit personenbezogenen Daten führen dabei zu einiger Verunsicherung. Dieses Handbuch trägt diesen Veränderungen Rechnung. Es stellt die wesentlichen Strukturen des Bundesdatenschutzgesetzes (BDSG) knapp und einfach verständlich dar. Auch der Aufbau des Handbuchs zielt darauf ab, ein komplexes Rechtsgebiet praxisingerecht und dennoch leicht nachvollziehbar zu erklären. Beispielsweise werden wesentliche gesetzliche Bestimmungen im Text wiedergegeben, um dem Leser allzu häufiges Nachschlagen in Gesetzen zu ersparen. Zudem gibt das Buch Praxistipps und schildert Vorgehensweisen, die sich beim täglichen Umgang mit personenbezogenen Daten bewährt haben.

Das Handbuch ist in zwei Hauptteile untergliedert. Der erste Teil stellt die Strukturen und Regelungen des BDSG anhand von Beispielen und praktischen Arbeitshilfen dar, der zweite Teil enthält den Gesetzestext und eine kurze Kommentierung der wichtigsten Vorschriften des BDSG. Auch die Regelungen des vom Bundeskabinett am 25.8.2010 beschlossenen „Entwurfs eines Gesetzes zur Regelung des Beschäftigtendatenschutzes“ (BR-Drs. 535/10) werden in Anhang 3 des Handbuchs dargestellt und besprochen.

Der erste Teil des Handbuchs zeigt die wesentlichen Regeln, die Unternehmen beim Datenschutz kennen und beachten müssen und ermöglicht einen unkomplizierten Einstieg in eine komplizierte Materie. Dieser Überblick konzentriert sich auf die für Unternehmen wesentlichen Themen. Der Leser wird mit den Risiken bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Geschäftsleben vertraut gemacht und erfährt, wie man Probleme vermeidet. Stolpersteine und Fallgruben beim Umgang mit personenbezogenen Daten werden dargestellt. Dieser Teil des Buches enthält auch Handlungsempfehlungen und Praxistipps. Das Handbuch zeigt hier anhand von Beispielen und

Checklisten, welche Vorgehensweisen erlaubt und welche problematisch sind. Entsprechend seiner hohen praktischen Bedeutung liegen zwei der Schwerpunkte auf dem Beschäftigtendatenschutz und auf Compliance-Fragen. Zudem werden beispielsweise die Haftung der Geschäftsführung für Verstöße beim Datenschutz, die Aufgaben des Datenschutzbeauftragten, strafrechtliche Risiken von Gesetzesverstößen sowie Datenverarbeitung auf der Grundlage von Einwilligungen und von Betriebsvereinbarungen beschrieben.

Auch der zweite Teil des Handbuchs soll dem Leser den Einstieg in den praktischen Umgang mit dem BDSG erleichtern. Hierfür muss man sehr häufig einzelne Normen des BDSG gründlich durchlesen. Daher enthält die Kurzkomentierung einen vollständigen Abdruck des BDSG und bietet dem Leser damit alle für das Verständnis der Grundlagen des Datenschutzes in Deutschland erforderlichen Informationen in einem einzigen Buch. Zudem findet der Leser eine knappe Erläuterung zu den in der betrieblichen Praxis wichtigsten Paragraphen des BDSG. Die Kurzkomentierung enthält auch Verweise, an welcher Stelle im ersten Teil die fragliche Regelung ausführlicher erläutert ist. Dadurch kann der Leser sich schnell einen Überblick verschaffen, an welcher Stelle des Handbuchs er weiterführende Informationen zu einem bestimmten Thema findet.

Dieses Handbuch richtet sich vor allem an Leser, die einen wissenschaftlich fundierten, aber dennoch gut verständlichen Überblick über den Datenschutz im Wirtschaftsleben suchen. Es eignet sich damit zum einen für Datenschutzbeauftragte, Compliance-Officer, Mitarbeiter in Rechtsabteilungen und andere für die Einhaltung gesetzlicher Vorschriften im Unternehmen verantwortliche Personen. Zum anderen gibt das Buch Vorständen oder Geschäftsführern mit Verantwortung für die Ressorts Datenschutz oder Compliance die Möglichkeit, sich in kompakter Form zu informieren. Auch Richtern, Verwaltungsbeamten, Rechtsanwälten, Referendaren und Studenten, die sich in kompakter Form über Grundzüge und Strukturen des BDSG informieren wollen, soll das Buch einen einfachen Einstieg in das Thema Datenschutz ermöglichen.

Wie fast alle Dinge, die mit einem erheblichen Aufwand verbunden sind, ist auch dieses Handbuch nicht allein das Ergebnis der Bemühungen eines Einzelnen. Daher möchte ich meinen Freunden und Kollegen danken, ohne deren Hilfe und Kritik dieses Buch nie geschrieben worden wäre. Insbesondere danke ich für seine Unterstützung Dr. Mark Hilgard und für Rat und Anregungen Philipp Zikesch, Dennis Heinson und Armin Fladung. Meiner Lektorin Tanja Brücker und Ulla Leis danke ich für ihre wertvolle Hilfe beim Bemühen um eine klare und verständliche Sprache.

Zuletzt und vor allem möchte ich meiner Frau Juliane und meinem kleinen Sohn Erik für ihre Motivation, Geduld und Nachsicht danken.

Frankfurt am Main, Februar 2011

Tim Wytbitul

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 „Sperrern“	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)	Beispielfall: 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
---------------------------	-----

Teil 1: Grundzüge des BDSG

Kapitel 1: Einführung

I. Einleitung

Das deutsche Datenschutzrecht stellt Praktiker vor einige Herausforderungen. Zum einen wird es international als eine der strengsten Umsetzungen der EU-Datenschutzrichtlinie gesehen. Daher wird das Bundesdatenschutzgesetz (BDSG) in der Unternehmenspraxis häufig als Messlatte für europaweite Lösungen verwendet.¹ Zum anderen wird es zu Recht als wenig anwenderfreundlich kritisiert.² Dies liegt unter anderem an der schwer verständlichen Sprache des BDSG und an seiner Unübersichtlichkeit.³ Wer zum ersten Mal einen Blick in das Gesetz wirft, hat Mühe, das zugrunde liegende System zu erkennen oder gar zu verstehen.⁴ Gleichzeitig hat die Bedeutung des Datenschutzes in Deutschland in den vergangenen Jahren enorm zugenommen. Das zeigt sich unter anderem an den vielen Gesetzesvorhaben in diesem Bereich. Die bislang letzten Änderungen des BDSG sind 2010 in Kraft getreten und auch der Gesetzgeber hat sich in mehreren Anläufen an neuen Regelungen für den Beschäftigtendatenschutz versucht, ohne dass es dabei bisher jedoch zu einer Novellierung gekommen ist.⁵

Die aktuelle Rechtsprechung macht deutlich, wie schwerwiegend die Folgen von Fehlern beim Umgang mit personenbezogenen Daten sein können. Beispielsweise hat der Bundesgerichtshof erst kürzlich zwei Privatermittler wegen datenschutzwidriger Überwachungsmaßnahmen zu Haftstrafen verurteilt.⁶ In einer anderen Entscheidung hat das BAG eine Kündigung als un-

1 Vgl. hierzu z. B. v. d. Bussche/Stamm, Data Protection in Germany, Einleitung (Preface).

2 Thüsing formuliert dies im Vorwort zu seinem Buch Arbeitnehmerdatenschutz und Compliance, für den in der Praxis besonders wesentlichen Bereich des Arbeitnehmerdatenschutzes wie folgt: „Die Abwägung des Persönlichkeitsschutzes des Arbeitnehmers mit den Aufklärungsinteressen der verantwortlichen Stelle kann nur im Einzelfall gelingen und bleibt oft unscharf; klare Hinweise der Rechtsprechung fehlen zumeist.“

3 So auch Bergmann/Möhrle/Herb, Datenschutzrecht, § 28 Rn. 1; Gola/Jaspers, Das novellierte BDSG im Überblick, S. 9. Zudem enthält das deutsche Datenschutzrecht viele bereichsspezifische Sonderregeln (z. B. § 25c Abs. 2 Satz 2 KWG oder § 80d Abs. 1 Satz 3 VAG).

4 Vgl. zur mäßigen Lesbarkeit und Verständlichkeit des BDSG bereits in der Fassung vor der BDSG-Novelle 2009 Simitis, in: Simitis, BDSG, Einleitung Rn. 125.

5 Siehe etwa den in BT-Drs. 535/10 abgedruckten „Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes“.

6 BGH, ZD 2013, 509 ff. m. Anm. Wybitul.

wirksam beurteilt, weil der Arbeitgeber maßgebliche Informationen unter Verstoß gegen § 32 BDSG erhoben hatte. Das BAG nahm bezüglich der so gesammelten Kündigungsgründe ein Beweisverwertungsverbot an.⁷

- 3 Dieses Handbuch soll Praktikern einen verständlichen Überblick darüber geben, wie man die Regelungen des BDSG schnell versteht und sie in der Praxis sicher anwendet. Damit richtet es sich an Leser, die einen leichten Einstieg in ein komplexes Thema suchen. Das Buch bietet eine knappe Zusammenfassung der in der Praxis wichtigen Bestimmungen und Mechanismen.⁸ Es ist keine abschließende Darstellung aller denkbaren Probleme und sämtlicher in der Fachliteratur diskutierten Streitigkeiten, sondern soll dem Praktiker einen alltagstauglichen Überblick über Probleme des Datenschutzes geben – und vor allem über deren mögliche Lösungen. Themen, die nur wenige Unternehmen betreffen, werden bewusst umfangreicheren Darstellungen des gesamten Datenschutzrechts überlassen.⁹
- 4 Das Handbuch zielt in erster Linie darauf ab, Entscheidungsträgern in Unternehmen bei der Anwendung der Regeln des Datenschutzes zu helfen. Allerdings lassen sich viele Grundsätze und Überlegungen auch auf den Umgang mit Daten bei öffentlichen Stellen (vgl. § 2 Abs. 1–3 BDSG) übertragen. Zudem gelten die meisten der in den nachstehenden Kapiteln dargestellten Prinzipien und Begriffsbestimmungen sowohl für private Unternehmen¹⁰ als auch für öffentliche Stellen.

II. Was sollte man zur Entwicklung des BDSG von 1977–2014 wissen?

- 5 Dieser Abschnitt gibt einen kurzen Überblick über die Entstehung des BDSG in seiner heutigen Form. Für das Verständnis der wesentlichen Regelungen des Datenschutzes ist diese Entwicklung des Gesetzes zwar nicht zwingend

7 BAG, 20.6.2013 – 2 AZR 546/12, BB 2014, 179 (Ls.) = NZA 2014, 143; vgl. hierzu *Wybitul/Pötters*, BB 2014, 437 ff.

8 Diese Auswahl beruht auf der subjektiven Einschätzung und praktischen Erfahrung der Autoren.

9 Für Leser, die sich intensiver mit einzelnen Problemen befassen möchten, sind etwa die Gesamtdarstellungen von *Taege/Gabel*, BDSG, 2. Aufl. 2013, *Wolff/Brink*, Datenschutz in Bund und Ländern (BeckOK BDSG), 1. Aufl. 2013, *Simitis*, Kommentar zum BDSG, 7. Aufl. 2011, *Bergmann/Möhrle/Herb*, Datenschutzrecht, *Gola/Schomerus*, BDSG, 11. Aufl. 2012, *Däubler/Klebe/Wedde/Weichert*, BDSG, 4. Aufl. 2013, oder auch *Forgó/Helfrich/Schneider*, Betrieblicher Datenschutz, 1. Aufl. 2014, sowie andere in diesem Handbuch zitierte Werke empfehlenswert. Als Einstieg in die Materie ist das Buch von *Taege*, Einführung in das Datenschutzrecht, 1. Aufl. 2014, zu empfehlen.

10 Mit privaten Unternehmen sind vorliegend nicht-öffentliche Stellen gemäß § 2 Abs. 4 BDSG und öffentlich-rechtliche Wettbewerbsunternehmen gemäß § 27 Abs. 1 Satz 1 Nr. 2 BDSG gemeint.

erforderlich. Allerdings hilft die Lektüre dieses Abschnitts durchaus dabei, zu verstehen, wieso das BDSG in seiner heutigen Form existiert.

Beispielsweise sind die vielen sogenannten „Buchstabenparagrafen“ (z. B. §§ 4a–4g BDSG) Folge vieler Überarbeitungen des BDSG. Das Gesetz wurde stets nur in einzelnen Teilen, aber niemals gründlich und vollständig reformiert. Um nicht auch die Nummerierung der nachfolgenden Paragraphen des Gesetzes ändern zu müssen, fügte der Gesetzgeber eine Vielzahl solcher Buchstabenparagrafen ein. Leser, die neben der reinen Beschreibung des aktuellen Gesetzes daran interessiert sind, die Hintergründe einzelner Regelungen und Strukturen zu verstehen, können beim Lesen dieses Abschnitts zudem interessante Hintergrundinformationen erfahren.¹¹ **6**

1. Verkündung 1977

Das BDSG wurde bislang vielfach geändert – aber niemals im Hinblick auf Einfachheit und klare Struktur. Das Gesetz wurde bereits bei seiner Verkündung im Jahr 1977¹² als praxisfern, formalistisch und schwer verständlich kritisiert.¹³ Seitdem wurden viele Regelungen des BDSG unstrukturiert geändert,¹⁴ man kann durchaus von einem „Patchwork-Gesetz“ sprechen.¹⁵ **7**

2. Volkszählungsurteil von 1983

In seinem Urteil zum Volkszählungsgesetz stellte das Bundesverfassungsgericht am 15.12.1983 fest, dass staatliche Eingriffe in das Recht der Bürger auf informationelle Selbstbestimmung einer verfassungsgemäßen gesetzlichen Grundlage bedürfen, „die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.“¹⁶ Damit erteilte das höchste Gericht Deutschlands dem umfassenden Informationsverlangen des **8**

11 Eine detaillierte Darstellung der Entwicklung des BDSG geben beispielsweise *Taeger/Schmidt*, in: *Taeger/Gabel, BDSG, Einf. Rn. 10 ff.*, oder *Simitis*, in: *Simitis, BDSG, Einl. Rn. 1 ff.*

12 BGBl. I, S. 201.

13 *Gola/Schomerus, BDSG, Einl. Rn. 5.*

14 Vgl. zur ungeordneten Struktur des BDSG schon vor der Novelle von 2009 *Kühling/Seidel/Sivridis, Datenschutzrecht, S. 97*. Einen anschaulichen Überblick über die Entstehung und Entwicklung des BDSG geben *Gola/Schomerus, BDSG, Einl. Rn. 1–29 ff.*

15 Vgl. zur Unübersichtlichkeit des reformierten BDSG, *Gola/Klug, NJW 2009, 2577, 2583.*

16 Sog. Volkszählungs-Urteil, BVerfGE 65, 1 f.

deutschen Staats gegenüber seinen Bürgern eine klare Absage.¹⁷ Wenn der Gesetzgeber das Recht seiner Bürger auf informationelle Selbstbestimmung durch umfassende Datenerhebung und Verarbeitung im Rahmen einer Volkszählung einschränke, so müsse er hierfür hinreichend klare und transparente Normen schaffen,¹⁸ den Verhältnismäßigkeitsgrundsatz angemessen berücksichtigen¹⁹ und die Daten nur für den Zweck verwenden, zu dem sie auch erhoben wurden.²⁰

- 9 Das Urteil des Bundesverfassungsgerichts richtete sich nicht direkt an Unternehmen, sondern an den Gesetzgeber, also an den Staat. Dennoch sind Unternehmen gut beraten, sich im Rahmen ihrer täglichen Arbeit mit dem Datenschutz an den Grundsätzen zu orientieren, die das Gericht 1983 aufgestellt hat.²¹ Denn auch private Wirtschaftsunternehmen sind bei der Anwendung (und Auslegung) des BDSG und anderer Gesetze an die von der Verfassung vorgegebenen Grundsätze nach der sogenannten mittelbaren Drittwirkung der Grundrechte gebunden.²²

3. Erste Neufassung 1990

- 10 1990 verabschiedete der Gesetzgeber eine erste Neufassung des BDSG.²³ Diese Gesetzesänderung wurde teilweise scharf kritisiert.²⁴ Nach Inkrafttreten der EG-Datenschutzrichtlinie 95/46/EG²⁵ im Jahre 1995 war der deutsche Gesetzgeber verpflichtet, das BDSG innerhalb von drei Jahren den Vorgaben des Europarechts anzupassen.

4. BDSG-Reform von 2001

- 11 Im Jahre 2001 trat eine neue Fassung des BDSG in Kraft, die um die europarechtlichen Vorgaben aus der EG-Datenschutzrichtlinie 95/46/EG ergänzt war.²⁶ Ein bekannter Kommentar beschrieb die Neuregelung zutreffend so: „Insgesamt hat das Gesetz an Umfang und Regelungsdichte erheblich zugenommen, so dass die ebenfalls als Kernpunkt modernen Datenschutzrechts

17 Einen Überblick über verfassungsrechtliche Rahmenbedingungen des Datenschutzes gibt *Gurlit*, NJW 2010, 1035.

18 BVerfGE 65, 1, 43 f.

19 BVerfGE 65, 1, 45.

20 BVerfGE 65, 1, 61 ff.

21 Vgl. zur mittelbaren Drittwirkung der Grundrechte im Datenschutz durch nicht-öffentliche Stellen, *Wybitul*, BB 2010, 889 f.; *Rath/Karner*, K&R 2010, 469, 472.

22 *Taege/Schmidt*, in: *Taege/Gabel*, BDSG, Einf. Rn. 44; vgl. auch *Rath/Karner*, K&R 2010, 469, 472.

23 BGBl. I, S. 2954.

24 *Gola/Schomerus*, BDSG, 11. Aufl. 2012, Einl. Rn. 7 mit weiteren Nachweisen.

25 Veröffentlicht in ABI. EG 1995, L 281, 31; nachstehend ohne Fundstellennachweis zitiert.

26 BGBl. I, S. 904.

angestrebte Rückkehr zu lesbaren und für Betroffene und Praxis noch überschaubaren Regelungen weitgehend konterkariert wird.²⁷

5. BDSG-Novelle von 2009

In erster Linie als Reaktion auf Datenschutzskandale bei einer Reihe von Großunternehmen²⁸ beschloss der Gesetzgeber 2009 eine weitere Novelle zum BDSG. Das neue Datenschutzrecht führte unter anderem zu einer Ausweitung der Rechte der Aufsichtsbehörden, zu höheren Bußgeldern und Regelungen zur Abschöpfung von Gewinnen und zu einem neuen Beschäftigtendatenschutz.²⁹ **12**

6. Entwurf eines „Gesetzes zur Regelung des Beschäftigtendatenschutzes“

Am 31.3.2010 legte das Bundesinnenministerium ein Eckpunktepapier vor, in dem es zeitnahe weitere Änderungen des Gesetzes im Bereich des Beschäftigtendatenschutzes ankündigte. Kurz darauf kursierte bereits ein Referentenentwurf zu einem neuen Beschäftigtendatenschutzgesetz, dessen einzelne Regelungen teilweise kontrovers diskutiert wurden und werden.³⁰ **13**

Knapp ein Jahr nach Inkrafttreten des derzeit nach wie vor geltenden § 32 BDSG hat sich das Bundeskabinett am 25.8.2010 auf einen „Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes“ verständigt. Ein neuer Unterabschnitt des Bundesdatenschutzgesetzes sollte künftig den erlaubten Umgang mit den Daten von Beschäftigten umfassend regeln. Die politischen Gespräche hierzu führten jedoch zu keinem Ergebnis. Ein neuer Anlauf im Frühjahr 2013, bei dem kurzfristig die BDSG-Novelle erneut politischer Diskussionsgegenstand wurde, wurde aufgrund energischer Kritik an dem Vorhaben von allen Seiten kurzerhand wieder eingestellt. Seitdem gibt es keine neuen Vorstöße zu einer Modernisierung des deutschen Beschäftigtendatenschutzes. Auch der Koalitionsvertrag der aktuellen Bundesregierung lässt nicht vermuten, dass der Gesetzgeber in absehbarer Zeit eine Neurege- **14**

27 Gola/Schomerus, BDSG, 11. Aufl. 2012, Einl. Rn. 13.

28 BT-Drs. 16/13657, S. 20.

29 Einen kritischen Überblick über den in § 32 BDSG geregelten Beschäftigtendatenschutz gibt Thüsing, NZA 2009, 865 ff.; vgl. zu ersten Erfahrungen im praktischen Umgang mit dem neuen Beschäftigtendatenschutz des § 32 BDSG: Wybitul, BB 2010, 1085 ff.

30 Vgl. zu der geplanten Neuregelung Niclas/von Blumenthal, ITRB 2010, 149. Eine kritische Stellungnahme zum Referentenentwurf des Bundesministeriums des Inneren vom 28.6.2010 gibt Thüsing, RDV 2010, 147 ff. Einen knappen Überblick über den Kabinettsentwurf vom 28.5.2010 gibt Wybitul, BB 2010, 2235; vgl. zur europarechtlichen Unzulässigkeit der Einschränkung der Möglichkeit zur Einwilligung nach § 4a BDSG im Beschäftigungsverhältnis: Forst, RDV 2010, 150 ff.; Thüsing, NZA 2011, 16.

lung des BDSG plant. Die Entwicklung des Datenschutzrechts auf europäischer Ebene kommt ebenfalls schleppend voran.³¹ Derzeit ist offen, ob und wann die geplante EU-Datenschutz-Grundverordnung in Kraft treten soll.

III. Welche europäischen Entwicklungen haben Auswirkungen auf die Anwendung des BDSG?

- 15 Nach 2010 entwickelte sich das deutsche Datenschutzrecht im Wesentlichen aufgrund europäischer Impulse und durch die nationale Rechtsprechung weiter. Insbesondere das Bundesarbeitsgericht hat in einer Reihe von aktuellen Entscheidungen grundlegende Vorgaben zum Umgang mit personenbezogenen Daten im Beschäftigungsverhältnis gemacht.³² Diese Vorgaben lassen sich weitgehend auch auf die sonstigen Regelungen zum Datenschutz übertragen. Zudem gibt es mehrere richtungsweisende Entscheidungen des Europäischen Gerichtshofes (EuGH), die eine richtlinienkonforme Auslegung der Regelungen des BDSG bestimmen.³³ Zum anderen laufen derzeit intensive Bemühungen auf EU-Ebene, die mittlerweile als veraltet angesehene EU-Datenschutzrichtlinie zu modernisieren.

1. Relevante EuGH-Rechtsprechung zum BDSG

- 16 Der Europäische Gerichtshof (EuGH) mit Sitz in Luxemburg ist das oberste rechtsprechende Organ der Europäischen Union und sichert gemäß Art. 19 Abs. 1 Satz 2 EUV die Wahrung des Rechts bei der Auslegung und Anwendung der EU-Verträge. Als Bestandteil dessen achtet der EuGH auch darauf, dass die Umsetzung von Richtlinien durch die Gesetzgeber der Mitgliedsstaaten mit primärem wie sekundärem EU-Recht vereinbar ist. In diesem Zusammenhang wurden im Zuge der Anrufung des EuGH durch die Gerichte der Mitgliedsstaaten auch einige Entscheidungen zu datenschutzrechtlichen Fragestellungen veröffentlicht, die im Rahmen der Anwendung des BDSG Relevanz aufweisen.

a) Entscheidung vom 6.3.2003 (Rs. C-101/01)

- 17 Die sogenannte Lindqvist-Entscheidung beruht auf einem Vorabentscheidungsersuchen, bei dem es allgemein um den Anwendungsbereich der EU-Datenschutzrichtlinie und konkret die Frage ging, ob die Verwendung personenbezogener Daten auf einer Webseite eine automatisierte Verarbeitung im

31 Vgl. KOM(2010) 609 endgültig.

32 Vgl. nachstehend Abschnitt III. 1.

33 Vgl. hierzu insbesondere BAG v. 20.6.2013, 2 AZR 546/12 sowie die ausführliche Darstellung der aktuellen Vorgaben der Rechtsprechung von *Wybitul/Pötters*, BB 2014, 437.

Sinne der Richtlinie ist. Während der EuGH diese Frage positiv beschied, klärte er zugleich, dass das Anbieten von Informationen im Internet nicht automatisch einer Übermittlung in Drittländer außerhalb der EU gleichzusetzen ist.³⁴

b) Urteil vom 20.5.2003 (Rs. T-179/02)

Grundlage dieser Entscheidung war ein Fall, in dem ein Angestellter der Europäischen Zentralbank (EZB) seinem Arbeitgeber vorwarf, für eine jährliche Beurteilung ohne sein Wissen seine E-Mail-Korrespondenz gesammelt zu haben, um sie dann in der Beurteilung zu verwenden. Im Rahmen der Begründung prägte der EuGH einen weitreichenden Begriff der “personenbezogenen Daten”. **18**

c) Urteil vom 8.11.2007 (Rs. T-194/04)

In der sog. „Bavarian Lager“-Entscheidung des EuGH vom Herbst 2007 definiert der EuGH auf Grundlage der Formulierung des Art. 2 lit. a der Verordnung Nr. 45/2001 die Anforderungen an die Bestimmbarkeit einer Person zur Begründung des Personenbezuges von bestimmten Daten. Als bestimmbar sah der EuGH danach eine Person an, die durch die konkreten Daten direkt oder indirekt identifiziert werden kann, und stellte dabei fest, dass dies insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck der physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, geschehen kann.³⁵ Die Absolutheit dieser Bezugspunkte ist insbesondere im Hinblick auf die in Deutschland immer noch existierende Lehre vom “relativen Personenbezug” relevant. **19**

d) Urteil vom 16.12.2008 (C-524/06)

Bei diesem Vorabentscheidungsersuchen vom Dezember 2008 ging es um die Frage, welche Daten im Ausländerzentralregister (AZR) als erforderlich für die Durchführung staatlicher Aufgaben im Sinne von Art. 7 lit. e) der EU-Datenschutzrichtlinie anerkannt werden können. Hierzu setzte sich der EuGH intensiv mit der Frage auseinander, wozu eine Datenbank wie das AZR gebraucht würde und differenzierte in seiner Bewertung: obgleich ein derartiges Register als zur Anwendung aufenthaltsrechtlicher Vorschriften im Sinne von Art. 7 Buchst. e) der EU-Datenschutzrichtlinie als erforderlich anzusehen sei, könne dies nur dann gelten, wenn die Zugriffsberechtigungen auf Behörden mit Befugnissen in diesen Bereichen beschränkt würden. Zu dem Argument, **20**

³⁴ Rs. C-101/01, Rn. 69.

³⁵ Vgl. Rs. T-194/04, Rn. 104.

dass ein weiterer wesentlicher Zweck des AZR in der Bekämpfung der Kriminalität zu sehen sei, führte der EuGH aus, dass hierfür die Staatsangehörigkeit der Täter keine Rolle spielte, und aberkannte dem AZR diesbezüglich die Erforderlichkeit der Datenverarbeitung. Zusätzlich zur tatsächlichen Erforderlichkeit verlangte das Gericht als weitere Voraussetzung, dass gerade der zentralisierte Charakter einer Datenbank wie dem AZR eine effizientere Anwendung der legitimierenden Vorschriften erlaubt, und erweiterte damit die objektive Erforderlichkeit um einen Effizienz Gesichtspunkt. Diese Entscheidung des EuGH entfaltet seine Auswirkungen bei der Anwendung aller Regelungen des BDSG, die auf die Erforderlichkeit einer Datenverarbeitung abzielen, also insbesondere auch im Rahmen der §§ 28, 29 und 32 BDSG.

e) Entscheidung vom 9.3.2010 (Rs. C-518/07)

- 21 Der EuGH entschied im Frühjahr 2010 eine Vertragsverletzungsklage nach Art. 226 EG vom 22. November 2007, bei der es um die Anforderungen an die Unabhängigkeit der Aufsichtsbehörden ging. In diesem Zusammenhang kam der EuGH zu dem Schluss, dass die deutsche Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich nicht unabhängig genug seien und die Bundesrepublik Deutschland folglich gegen Art. 28 Abs. 1 der Richtlinie 95/46/EG verstoße. Hintergrund des Verfahrens war, dass in Deutschland die für die Überwachung der Verarbeitung personenbezogener Daten durch nichtöffentliche Stellen zuständigen Kontrollstellen in den Bundesländern einer staatlichen Aufsicht unterstellt sind und damit nicht dem Erfordernis entsprechen, dass diese ihre Aufgaben „in völliger Unabhängigkeit“ wahrnehmen. Die Aufsichtsbehörden dürfen folglich nicht mehr der Aufsicht eines Ministeriums unterstellt werden und müssen zudem vor politischem Einfluss besonders geschützt werden, damit gewährleistet sei, dass sie völlig frei von Weisungen und Druck handeln können.³⁶ Diese Rechtsansicht des EuGH, die dieser später auch gegenüber Österreich erneut zum Ausdruck brachte,³⁷ kann weitreichende Auswirkungen auf die Stellung der deutschen Aufsichtsbehörden haben.

f) Entscheidung vom 24.11.2011 (verb. Rs. C-468/10, C-469/10)

- 22 Bei dieser Entscheidung handelt es sich um ein Vorabentscheidungsverfahren aus Spanien zu der Frage, ob die Datenschutzrichtlinie 95/46/EG eine Voll- oder Mindestharmonisierung verlangt. Der Aussage des Gerichts hierzu fehlt es nicht an Deutlichkeit: Art. 7 Buchst. f der Richtlinie 95/46 hat nicht nur unmittelbare Wirkung, sondern bestimmt auch abschließend die Voraussetzungen einer Verarbeitung personenbezogener Daten. Die Regelung im

³⁶ Entscheidung vom 9.3.2010, Rs. C-518/07, Rn. 19.

³⁷ Urteil vom 16.10.2012, Rs. C-614/10.

spanischen Recht, die zusätzlich zur Interessenabwägung verlangte, dass die Daten aus öffentlich zugänglichen Quellen stammten, erklärte das Gericht für nichtig, da sie nicht nur Leitlinien für diese Abwägung aufstellte, sondern sie nach Ansicht des Gerichts unzulässigerweise einschränkte.

Diese Entscheidung kann auch Auswirkungen für die Regelungen des BDSG **23** haben, in denen gesetzliche Erlaubnistatbestände definiert werden. Obgleich dies bislang in Deutschland noch nicht gerichtlich überprüft worden ist, wird eine richtlinienkonforme Auslegung der §§ 28, 28a und § 32 BDSG wohl zu dem Ergebnis führen, dass auch dort einzig die Abwägung zwischen den berechtigten Interessen der verantwortlichen Stelle und den schützenswerten Interessen der Betroffenen legitimes Tatbestandsmerkmal sein kann. Darüber hinausgehende Anforderungen dieser Regelungen sind, soweit sie nicht nur diese Abwägung konkretisieren, dem Risiko ausgesetzt, gegen die insoweit vollharmonisierende Regelung des Art. 7 Buchst. f der Datenschutzrichtlinie zu verstoßen.

2. Die EU-Datenschutz-Grundverordnung

Die EU-Datenschutz-Richtlinie 95/46/EG vom 24.10.1995 galt seinerzeit als wegweisender Rechtsakt und wurde die Grundlage für die Datenschutzgesetze der Mitgliedsstaaten. Angesichts der technologischen Weiterentwicklung und der wachsenden Bedeutung von Suchmaschinen, sozialer Netzwerke und des mobilen Internets entschied die Europäische Kommission jedoch, dass es an der Zeit sei, diese Richtlinie zu überarbeiten und legte dazu nach einer mehrmonatigen öffentlichen Konsultation am 4. November 2010 ein Gesamtkonzept vor.³⁸ Vorrangiges Ziel der Reformbestrebungen sollte es sein, ein einheitliches und hohes Datenschutzniveau für alle Bürgerinnen und Bürger der EU im Zeitalter moderner Informations- und Kommunikationstechnologien sicherzustellen.

Dazu gehörte nach der Überzeugung der Kommission insbesondere die zu **25** steigende Transparenz der Datenverarbeitung, die Stärkung der Betroffenenrechte, sowie eine Verpflichtung der Unternehmen, datenschutzfreundliche Technologien und Anwendungen von vornherein in ihre Produkte zu integrieren. Ausgehend von diesen Prämissen legte die Kommission am 25.1.2012 einen Vorschlag für die Änderung der EU-Datenschutzrichtlinie vor.³⁹ Dieser umfasste zum einen den Entwurf einer Datenschutz-Grundverordnung und zum anderen einen Richtlinien-Entwurf für den Polizei- und Justizbereich. Beide Vorschläge werden derzeit von den Mitgliedstaaten im Rat der Europäischen Union und vom Europäischen Parlament im ordentlichen Gesetz-

³⁸ Vgl. KOM(2010) 609 endgültig.

³⁹ Vgl. KOM(2012) 11 endgültig.

gebungsverfahren der EU beraten. Die dabei entstandenen mehreren tausend Änderungsanträge lassen dabei einen Rückschluss auf die Intensität zu, mit der die Vorschläge auf politischer, gesellschaftlicher und juristischer Ebene diskutiert werden. Sollte die ursprüngliche Richtlinie am Ende dieses Prozesses tatsächlich durch eine Verordnung ersetzt werden, hätte dies auch für das deutsche Datenschutzrecht drastische Auswirkungen. Im Gegensatz zu Richtlinien, die in nationales Recht transformiert werden müssen, entfalten Verordnungen in den Mitgliedsstaaten unmittelbare Wirkung. Das bedeutet, dass die Bestimmungen der Verordnung die Regelungen des BDSG und sämtlicher anderen nationalen Datenschutzgesetze ersetzen würden. Die derzeitigen Planungen auf europäischer Ebene gingen zunächst davon aus, dass der Verhandlungsbeginn zwischen Europäischem Parlament, Rat und Europäischer Kommission („Trilog“) im Herbst 2013 starten und die Richtlinie nach Abschluss dieser Gespräche – wahrscheinlich mit einer ein- oder zweijährigen Übergangsfrist – in Kraft treten könnte. Mittlerweile ist es jedoch unsicher geworden, ob es dazu noch vor den Neuwahlen des Europäischen Parlaments im Mai 2014 kommt. Bis zum Inkrafttreten des neuen Rechtsrahmens behält die EU-Datenschutzrichtlinie 95/46/EG jedoch ihre Geltung.

IV. Mit welchen Problemen muss man beim Umgang mit dem BDSG in der Praxis rechnen?

- 26 Dieser einleitende Abschnitt zeigt in knapper Form die gängigsten Probleme bei der Anwendung des BDSG auf. Er informiert darüber, warum der Datenschutz als schwieriges und unklares Thema gilt. Die nachfolgenden Kapitel zeigen dann, wie man diese Probleme in der Praxis löst und den Umgang mit dem BDSG im Unternehmen meistert.

1. Sprachliche Schwächen des BDSG

- 27 Ein wesentliches Problem beim Datenschutz ist die – auch für Juristen – gewöhnungsbedürftige Sprache des BDSG. Viele Formulierungen und Begriffe des Gesetzes sind technisch und wenig praxisgerecht. Ein Beispiel hierfür ist, dass das BDSG von der „Erhebung, Verarbeitung oder Nutzung personenbezogener Daten“ spricht. Das liest sich sperrig und erschwert das Verständnis der einzelnen Regelungen. Besser wäre es, der Gesetzgeber hätte als Oberbegriff für die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten etwa den „Umgang mit Daten“⁴⁰, die „Verwendung von Daten“ oder die „Datenverarbeitung“ verwendet, ähnlich wie dies Art. 2 lit. b) der

40 Zumal das Gesetz in § 1 Abs. 1 BDSG selbst vom „Umgang mit (...) personenbezogenen Daten“ spricht.

IV. Mit welchen Problemen muss man beim Umgang mit dem BDSG in der Praxis rechnen?

Datenschutzrichtlinie 95/46/EG⁴¹ tut. Um sprachlich verständlicher als der Gesetzestext zu sein, verwendet dieses Handbuch die Begriffe Datenumgang, Datenverwendung oder Datenverarbeitung häufig sinngemäß für das Erheben, Verarbeiten und Nutzen personenbezogener Daten.⁴²

2. Verwendung unbestimmter Rechtsbegriffe

Viele Regelungen zum Datenschutz enthalten weitgehend unbestimmte Rechtsbegriffe. Deren Auslegung ist schwierig, weil sie weite Interpretationsspielräume zulassen. Das BDSG zeichnet sich wegen dieser vielen unbestimmten Rechtsbegriffe durch viele Grauzonen aus. Da diese Begriffe keine präzise umrissenen Sachverhalte beschreiben, muss ihr Inhalt bei der Rechtsanwendung durch Auslegung im Einzelfall bestimmt werden.⁴³ 28

Wichtige Rechtsbegriffe des BDSG sind beispielsweise die „Erforderlichkeit“ (z. B. in § 28 oder § 32 BDSG) oder „Verhältnismäßigkeit“ eines Umgangs mit personenbezogenen Daten (z. B. § 3a Satz 2 BDSG), die „schutzwürdigen Interessen des Betroffenen“ (z. B. §§ 4 Abs. 2 Satz 2, 28 Abs. 1 Satz 1 Nr. 2 und Nr. 3, 32 Abs. 1 Satz 2 BDSG), der „angestrebte Schutzzweck“ (vgl. § 3a BDSG) einzelner Regelungen oder das „angemessene Datenschutzniveau“ (vgl. § 4c BDSG). Bei der praktischen Arbeit mit dem BDSG müssen Unternehmen diese Begriffe in einer Form anwenden, die einer gerichtlichen Überprüfung oder einer Kontrolle durch die zuständige Datenschutzbehörde standhält. 29

3. Fehlende Vorgaben von Gerichten und Aufsichtsbehörden

Weder Rechtsprechung noch Aufsichtsbehörden haben bislang klare Grundsätze aufgestellt, wie die Anforderungen des BDSG auszulegen sind. Dies gilt ganz besonders im Bereich des Beschäftigtendatenschutzes. Das hat auch die Politik erkannt. Das Bundesinnenministerium formuliert dies so: „Es gibt bereits heute zu vielen Fragen des Beschäftigtendatenschutzes eine einzelfallbezogene Rechtsprechung der Arbeitsgerichte. Diese ist allerdings oft uneinheitlich. Obergerichtliche Urteile sind selten. Für zahlreiche in der beruflichen Praxis vorhandene Fragen bestehen derzeit keine speziellen gesetzlichen Regelungen.“⁴⁴ 30

41 Veröffentlicht in ABl. EG 1995, L 281, 31.

42 Vgl. zum Umgang mit personenbezogenen Daten als Oberbegriff für das Erheben, Speichern, Verändern, Übermitteln, Sperren und Nutzen von Daten auch *Gola/Schomerus*, BDSG, § 1 Rn. 22.

43 Vgl. hierzu *Hilgendorf*, DTV-Atlas Recht, S. 31 f.

44 Eckpunktepapier des Bundesministeriums des Inneren zum Beschäftigtendatenschutz vom 31.3.2010.

- 31 Auch die Kontrollpraxis beim Datenschutz erschwert es Unternehmen, zu erkennen, welche Vorgaben sie beim Umgang mit Kunden- und Beschäftigendaten erfüllen müssen.⁴⁵ In Deutschland überprüfen Aufsichtsbehörden auf Landesebene die Einhaltung der Regeln des BDSG durch Unternehmen der Privatwirtschaft, § 38 Abs. 6 BDSG. Die Aufsichtsbehörden in den einzelnen Bundesländern vertreten hierbei häufig unterschiedliche Auffassungen. Was beispielsweise von einer Aufsichtsbehörde nicht beanstandet wird, kann nach Auffassung der Kontrollbehörde eines anderen Bundeslandes durchaus ein Problem darstellen. Zwar stimmen sich die Aufsichtsbehörden zu einzelnen Fragen in mehreren gemeinsamen Gremien ab, zu denen der sogenannte „Düsseldorfer Kreis“, die „Konferenz der Datenschutzbeauftragten des Bundes und der Länder“ und der „Kooperationskreis IuK“ gehören. In vielen Punkten bestehen zwischen den einzelnen Aufsichtsbehörden dennoch recht unterschiedliche Auffassungen, was weiter zur bestehenden Rechtsunsicherheit beiträgt. Verantwortliche sind deshalb gut beraten, sich bei ihrem Vorgehen an den Anforderungen der jeweils zuständigen Kontrollbehörden zu orientieren.
- 32 Der Europäische Gerichtshof hat im März 2010 die fehlende Unabhängigkeit der Aufsichtsbehörden für die Privatwirtschaft bemängelt.⁴⁶ Daher wird es voraussichtlich auch bei der organisatorischen Struktur der Aufsichtsbehörden für den Datenschutz in der Privatwirtschaft zu weiteren Veränderungen kommen. Ob es in diesem Rahmen allerdings auch zu einer nennenswerten Vereinheitlichung der Datenschutzpraxis kommt, darf bezweifelt werden.

Praxistipp: Oft steht für Unternehmen im Hinblick auf den Datenschutz nicht allein die Frage im Vordergrund, ob ein konkretes Verhalten oder eine geplante Vorgehensweise bei wissenschaftlicher Betrachtung zulässig ist. Denn wie bei vielen anderen Compliance-Themen geht es weniger um die Beurteilung von „Erlaubt“ oder „Verboten“. Eine solche Abgrenzung ist bei vielen Fragen des Datenschutzes praktisch auch gar nicht möglich.

Vielmehr müssen sich die für den Datenschutz im Unternehmen Verantwortlichen vor allem fragen, was genau die möglichen Risiken eines bestimmten Vorgehens sind. Droht bei einer Kontrolle durch die Aufsichtsbehörden ein Bußgeld oder allenfalls eine Änderungsanordnung? Wie wäre die Öffentlichkeitswirkung, falls der fragliche Datenumgang bekannt würde? Muss man sich vor Einführung eines konkret geplanten Prozesses mit Arbeitnehmervertretern abstimmen, weil Mitbestimmungsrechte des Be-

⁴⁵ Vgl. *Seiffert*, Datenschutzprüfung durch die Aufsichtsbehörden, S. 14.

⁴⁶ Urt. v. 9.3.2010 – C 518/07, NJW 2010, 1265 ff. = RDV 2010, 121 ff., vgl. Rn. 21.

IV. Mit welchen Problemen muss man beim Umgang mit dem BDSG in der Praxis rechnen?

etriebsrats berührt sind?⁴⁷ Wie reagiert die Belegschaft auf einen geplanten Datenumgang?

In der Praxis kommt es beim Datenschutz im Unternehmen daher oft darauf an, neben der rechtlichen Zulässigkeit und den möglichen Folgen beispielsweise auch Fragen der technischen Machbarkeit, Kosten, Abstimmung mit den Beschäftigten, deren Vertretern und gegebenenfalls den Aufsichtsbehörden im Auge zu behalten.

4. Verschachtelter Aufbau des BDSG

Der Einstieg in die Materie des Datenschutzrechts wird durch den verschachtelten Aufbau des BDSG nicht erleichtert. Beschäftigt man sich allerdings mit der Struktur des Gesetzes, kann man durchaus verstehen, wie die einzelnen Regelungen des BDSG funktionieren und was man beim Umgang mit personenbezogenen Daten beachten muss. **33**

Das BDSG ist in sechs Abschnitte unterteilt, für Wirtschaftsunternehmen sind vor allem der erste (§§ 1–11 BDSG, Allgemeine und gemeinsame Bestimmungen) und der dritte Abschnitt (§§ 27–38a BDSG, Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen) wichtig. Der erste Abschnitt des Gesetzes enthält die allgemeinen Regeln des BDSG, also grundlegende Bestimmungen, die beispielsweise auch für öffentlich-rechtliche Stellen gelten. Wenn man das System der im ersten Abschnitt des Gesetzes enthaltenen Grundregeln kennt, hat man bereits einen großen Schritt zum rechtskonformen Umgang mit dem BDSG gemacht. Die wichtigste Norm des ersten Abschnitts ist § 4 Abs. 1 BDSG, der die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten grundsätzlich verbietet – es sei denn, dass eine Rechtsvorschrift dies erlaubt oder dass der Betroffene⁴⁸ eingewilligt hat. Aus diesem Verbot ergibt sich bereits ein allgemeiner Ablaufplan für den zulässigen Umgang mit personenbezogenen Daten. **34**

Checkliste zum Umgang mit dem BDSG

Da § 4 Abs. 1 BDSG den Umgang mit personenbezogenen Daten grundsätzlich verbietet, falls nicht einer der gesetzlich geregelten Ausnahmefälle (Erlaubnisnorm oder Einwilligung) vorliegt, kann man die Frage nach der Zulässigkeit eines Umgangs mit Daten oft nach folgendem groben Muster beantworten:

47 Erfahrungsgemäß ist es in der Praxis in einem solchen Fall der zwingenden Mitbestimmung (z. B. nach § 87 Betriebsverfassungsgesetz) deutlich wahrscheinlicher, dass das fragliche Vorhaben auch außerhalb des Unternehmens publik wird.

48 Mit „Betroffener“ meint das BDSG die natürliche Person, auf die sich die fraglichen Daten beziehen, vgl. § 3 Abs. 1 BDSG.

- Sind von dem geplanten Vorhaben personenbezogene Daten gem. § 3 Abs. 1 BDSG betroffen oder ausschließlich Informationen, die nicht dem BDSG unterliegen, z. B. statistische Informationen, Angaben über Wirtschaftsunternehmen oder Verstorbene?
- Falls personenbezogene Daten betroffen sind, werden diese bei dem geplanten Vorhaben erhoben, verarbeitet oder genutzt? Dies ist eine weitere Voraussetzung für die Anwendbarkeit des BDSG.
- Werden die Daten unter Einsatz von Datenverarbeitungsanlagen, für den Einsatz in Datenverarbeitungsanlagen oder nicht-automatisierten Dateien erhoben? In der Praxis ist das übrigens heutzutage fast immer der Fall.
- Falls es tatsächlich um das automatisierte oder dateimäßige Erheben, Verarbeiten oder Nutzen von personenbezogenen Daten geht, muss man sich auf einer zweiten Stufe fragen, ob dieser Datenumgang vorliegend erlaubt ist; entweder weil eine Einwilligung des Betroffenen vorliegt oder eine Rechtsvorschrift dies erlaubt oder vorschreibt.

In der Praxis liegt ein Schwerpunkt bei der Arbeit mit dem BDSG häufig darauf, eine geeignete Erlaubnisnorm zu finden und ein geplantes Vorhaben an den Anforderungen dieser Erlaubnisnorm (und an den allgemeinen Regeln des BDSG) auszurichten. Zudem kann man das so ermittelte Ergebnis mit einer einfachen Kontrollüberlegung überprüfen. Wenn man von dem geplanten Datenumgang durch das eigene Unternehmen nur ungern in der Zeitung lesen würde, sollte man sich auf jeden Fall fragen, ob eine weitere juristische Prüfung oder eine Abstimmung mit den Aufsichtsbehörden nicht zweckmäßig wäre.

- 35** Der zweite Abschnitt des BDSG enthält Regeln für öffentliche Stellen. Der dritte Abschnitt ist für Wirtschaftsunternehmen maßgeblich; er regelt die Beschränkungen für Personen und Unternehmen, die in der Privatwirtschaft tätig sind sowie für öffentlich-rechtliche Unternehmen, die am privaten Wettbewerb teilnehmen.⁴⁹ Der vierte Abschnitt des BDSG enthält einige Sondervorschriften, wie etwa § 42a BDSG, der die Voraussetzungen und Rechtsfolgen von sogenannten Datenpannen regelt. Der fünfte Abschnitt besteht aus Vorschriften über die Verhängung von Bußgeldern sowie Geld- und Haftstrafen, der sechste Abschnitt enthält Übergangsvorschriften.
- 36** Für die praktische Arbeit von Unternehmen im Bereich Datenschutz ist es daher zumeist zweckmäßig, sich auf den ersten (§§ 1–11 BDSG) und den dritten Abschnitt (§§ 27–38a BDSG) des Gesetzes zu konzentrieren. Ist man

⁴⁹ Vgl. hierzu § 27 Abs. 1 Satz 1 Nr. 2 BDSG sowie die weitergehenden Erläuterungen von *Kühling/Seidel/Sivridis*, Datenschutzrecht, S. 161.

mit den maßgeblichen Regelungen dieser beiden Abschnitte in groben Zügen vertraut, so hat man bereits eine gute Grundlage für den Umgang mit dem BDSG.

V. Warum sollten Unternehmen das BDSG beachten?

Unternehmen müssen sich mit den Anforderungen des Datenschutzes umfassend auseinandersetzen. Tun sie das nicht, drohen Bußgelder, Schadensersatz und vor allem erhebliche Rufschäden. Bei besonders schweren Verstößen drohen sogar Haft- oder Geldstrafen. Wenn man betrachtet, welche Beträge große Unternehmen jährlich für Öffentlichkeitsarbeit ausgeben, kann man erfassen, welche tatsächlichen Kosten sogenannte Datenskandale insgesamt verursachen. Unbedachtes Vorgehen beim Datenschutz im Unternehmen kann die Wirkung von Werbeausgaben in Millionenhöhe in kurzer Zeit entwerten. 37

Bis vor wenigen Jahren sahen Unternehmen den Datenschutz teilweise als „zahnlosen Tiger“⁵⁰ an. Dies hat sich in Folge der Datenschutzaffären der letzten Jahre grundlegend geändert. Die Intensität und Anzahl der Kontrollen der Einhaltung der Vorschriften zum Datenschutz nimmt zu.⁵¹ So gibt allein die Bundesregierung in ihrem Haushalt 2010 den Betrag von 1,8 Milliarden mehr für Datenschutz als im Vorjahr aus.⁵² Mittlerweile haben deutsche Aufsichtsbehörden eine Vielzahl von Bußgeldern – teilweise in empfindlicher Höhe – gegen Unternehmen verhängt. Heute zählt die Einhaltung von Datenschutzregeln, ebenso wie die Korruptionsbekämpfung oder das Kartellrecht, zu den ernst zu nehmenden Anforderungen für deutsche Unternehmen. Werden flächendeckende Verstöße gegen das BDSG bekannt, kann dies für Unternehmen zu enormen Imageschäden führen. Hinzu kommt das Risiko hoher Bußgelder und von Gewinnabschöpfung durch Aufsichtsbehörden. Zudem haftet die Unternehmensleitung selbst für Verstöße (vgl. hierzu etwa Rn. 469, 504 ff.). 38

Die möglichen Folgen von Verstößen sind gravierend – nicht nur für die betroffenen Unternehmen, sondern auch für die handelnden Personen selbst. Bei Fehlern können Beteiligte schnell den Arbeitsplatz verlieren. Ihnen drohen zudem Geldbußen und Schadensersatzansprüche. Schwere Datenschutzverstöße sind gemäß § 44 BDSG sogar strafbar.⁵³ Diese Regelung sieht für besonders erhebliche Verstöße Freiheitsstrafe von bis zu zwei Jahren oder Geldstrafen vor. Dieser Sanktionsrahmen könnte sich mit Inkrafttreten der 39

50 Vgl. zum Begriff des „zahnlosen Tigers“ im Zusammenhang mit Datenschutzstrafrecht, *Weichert*, NStZ 1999, 490 ff.

51 *Würz/Markatou*, Ratgeber Arbeitnehmerdatenschutz, S. 5.

52 Vgl. Plenarprotokoll des Deutschen Bundestages, 17. Wahlperiode, 59. Sitzung vom 16.9.2010, S. 6255.

53 Vgl. BGH, ZD 2013, 509 ff. m. Anm. *Wybitul*.

EU-Datenschutzgrundverordnung noch erheblich verschlimmern. Artikel 79 des Verordnungsentwurfs der Europäischen Kommission sieht derzeit ein gestaffeltes System von Sanktionen vor, das Geldbußen von bis zu 1 Million Euro oder – bei Unternehmen – 2% ihres weltweiten Jahresumsatzes vorsieht. Das EU-Parlament setzt derzeit sogar 5% an.

Praxistipp: Kennt man hingegen die Regeln des BDSG, kann man die geschilderten Risiken beim Umgang mit Daten im Unternehmen durchaus vermeiden – und dennoch die wesentlichen Unternehmensziele erreichen. Denn beim Datenschutz entscheidet in der Regel die Art und Weise, in der man eine Maßnahme gestaltet, ganz wesentlich über deren Zulässigkeit. Daher stellt sich oftmals nicht allein die Frage, ob ein einzelner Datenumgang erlaubt ist, sondern wie man ihn ausgestalten muss, um unangenehme Folgen zu vermeiden. Zudem muss man stets den Zweck eines Datenumgangs angemessen gegen die Eingriffe in Persönlichkeitsrechte Betroffener abwägen.⁵⁴

54 Vgl. etwa BAG, 20.6.2013 – 2 AZR 546/12, BB 2014, 179 (Ls.) = NZA 2014, 143.

Kapitel 2: Welche Grundprinzipien des BDSG sollte man kennen?

I. Was bedeuten Begriffe wie Verhältnismäßigkeitsgrundsatz, Datenvermeidung oder Datensparsamkeit?

Ein wesentliches Ziel des gesetzlichen Datenschutzes ist es, den Umgang mit personenbezogenen Daten nur dann zu erlauben, wenn dieser Umgang verhältnismäßig ist⁵⁵ – wenn also der Zweck des Datenumgangs in einem angemessenen Verhältnis zum Eingriff in die betroffenen Persönlichkeitsrechte steht.⁵⁶ 40

§ 1 Abs. 1 BDSG: „Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.“

Der datenschutzrechtliche Verhältnismäßigkeitsgrundsatz ist das wichtigste Prinzip des BDSG.⁵⁷ Dies ermöglicht eine einfache Kontrollüberlegung zur Überprüfung der Zulässigkeit einer datenschutzrechtlich relevanten Maßnahme. Wenn der Umgang eines Unternehmens mit den personenbezogenen Daten Dritter keine angemessene Abwägung der betroffenen Interessen und Persönlichkeitsrechte erkennen lässt, spricht sehr vieles dafür, dass es auch den strengen Anforderungen des BDSG nicht genügen wird. Durch die nachstehend geschilderten Punkte wird der datenschutzrechtliche Verhältnismäßigkeitsgrundsatz in der Praxis näher konkretisiert. 41

1. Recht auf informationelle Selbstbestimmung

Das BDSG zielt darauf ab, Menschen davor zu schützen, dass ihre Persönlichkeitsrechte durch den Umgang mit ihren personenbezogenen Daten beeinträchtigt werden. Grundsätzlich soll jeder Bürger selbst bestimmen können, was mit seinen Daten geschieht. Allerdings gilt dieser gesetzliche Schutz nicht grenzenlos, sondern nur in einem gewissen Umfang.⁵⁸ Das Bundesverfassungsgericht (BVerfG) beschreibt das in seinem sogenannten Volkszäh- 42

55 BVerfGE 65, 1, 45.

56 Vgl. *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 1 Rn. 8.

57 Zur Bedeutung des Verhältnismäßigkeitsgrundsatz insbesondere beim Beschäftigtendatenschutz: *Wybitul*, BB 2010, 1085, 1086 f.

58 Zum Spannungsfeld zwischen dem Recht des Einzelnen auf informationelle Selbstbestimmung und den Interessen seiner Umwelt an der Nutzung seiner Daten, *Taeger/Schmidt*, in: *Taeger/Gabel*, BDSG, Einf. Rn. 33 ff.

lungsurteil so: „Das Recht auf informationelle Selbstbestimmung ist nicht schrankenlos.“⁵⁹

2. Interessenabwägung

- 43 Für den Umgang mit Daten durch Unternehmen bedeutet der Verhältnismäßigkeitsgrundsatz vor allem Folgendes: Man muss die schutzwürdigen Interessen derjenigen, deren personenbezogene Daten verarbeitet werden, fortwährend gegen die berechtigten Interessen des Unternehmens abwägen. Das BDSG nennt die Person, um deren Daten es geht, den „Betroffenen“.⁶⁰ Wenn man sich beim Umgang mit personenbezogenen Daten stets fragt, welche Interessen der Betroffenen und des Unternehmens berührt sind, ist der erste Schritt zur Einhaltung des BDSG bereits getan. Bringt man diese Interessen nun noch in einen angemessenen Ausgleich, so braucht man spätere Kontrollen durch Datenschutzaufsichtsbehörden in der Regel nicht zu fürchten.
- 44 Auch bei der Anwendung der einzelnen Normen des Datenschutzrechts sind die verfassungsmäßigen Rechte der Betroffenen hinreichend zu berücksichtigen. Die sogenannte mittelbare Drittwirkung der Grundrechte⁶¹ kommt zum Tragen. Unternehmen müssen also ähnliche Kriterien beachten wie der Gesetzgeber, wenn dieser Gesetze zum Umgang mit den personenbezogenen Daten seiner Bürger erlässt.⁶²
- 45 Beim Umgang mit personenbezogenen Daten müssen Unternehmen die Vorgaben des BDSG befolgen. Das BDSG enthält allerdings wenig klare Vorgaben und arbeitet mit unbestimmten Rechtsbegriffen,⁶³ insbesondere muss die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Unternehmen oftmals „erforderlich“ sein. Wie auch jede andere einfachgesetzliche Regelung ist das BDSG stets verfassungskonform auszulegen.⁶⁴ Die Gesetzesbegründung zur BDSG-Novelle 2009 besagt sogar ausdrücklich, dass beispielsweise § 32 BDSG die von der Rechtsprechung nach den Vorgaben der Verfassung erarbeiteten Grundsätze nicht ändern, sondern lediglich zusammenfassen solle.⁶⁵

59 BVerfGE 65,1, 43 f.

60 § 3 Abs. 1 BDSG: „Personenbezogene Daten sind Einzelangaben über natürliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).“

61 Vgl. zur Drittwirkung der Grundrechte bei der Auslegung des BDSG: *Wybitul*, BB 2010, 889 ff.; *Rath/Karner*, K&R 2010, 469, 472.

62 Vgl. zum Umfang der Übertragbarkeit der Entscheidungen des BVerfG auf die betriebliche Praxis: *Thüsing*, NZA 2009, 865, 868.

63 Vgl. hierzu bereits Rn. 28.

64 Vgl. *Bergmann/Möhrle/Herb*, Datenschutzrecht, §1 Rn. 8.

65 Zur Bedeutung des Verhältnismäßigkeitsgrundsatzes insbesondere beim Beschäftigtendatenschutz: *Wybitul*, BB 2010, 1085, 1086 ff.; *Brink/Wybitul*, ZD 2014, 225 ff.

Beispiel: Will ein Unternehmen etwa feststellen, ob ein bestimmter Umgang mit personenbezogenen Daten „erforderlich“ im Sinne des § 32 BDSG und damit zulässig ist, sollte es sich an den Vorgaben des Grundgesetzes orientieren. Und diese werden im Einzelnen durch das Bundesverfassungsgericht festgestellt und konkretisiert.

3. Datenvermeidung und Datensparsamkeit, § 3a BDSG

Eine Grundregel beim Datenschutz im Unternehmen lautet: So viel personenbezogene Datenverarbeitung wie nötig, so wenig wie möglich. Dieser allgemeine Grundsatz ist eine Ausprägung des datenschutzrechtlichen Verhältnismäßigkeitsgrundsatzes und zeigt sich besonders deutlich in § 3a BDSG, aber auch an vielen anderen Stellen im BDSG, die Abwägungen zwischen dem angestrebten Zweck des Datenumgangs und den schutzwürdigen Interessen der hiervon Betroffenen vorsehen.⁶⁶ 46

§ 3a BDSG: *„Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.“*

§ 3a BDSG konkretisiert den allgemeinen Verhältnismäßigkeitsgrundsatz, indem er Datenvermeidung und Datensparsamkeit vorschreibt. Unternehmen müssen sowohl den Umgang mit Daten als auch Datenverarbeitungssystemen daher stets so ausrichten, dass sie so wenig personenbezogene Daten wie möglich erheben, verarbeiten oder nutzen. Soweit dies machbar und praktikabel ist, müssen Unternehmen diese Daten zudem anonymisieren oder pseudonymisieren.⁶⁷ 47

⁶⁶ Die für die Praxis relevantesten Beispiele sind wohl § 28 Abs. 1 Satz 1 Nr. 2 BDSG und § 32 Abs. 1 Satz 2 BDSG.

⁶⁷ Durch das Anonymisieren wird Daten der Personenbezug genommen; dieser Vorgang entzieht die anonymisierten Daten der Anwendbarkeit des BDSG. Beim Pseudonymisieren werden Erkennungsmerkmale (z. B. Name, Geburtsdatum, Adresse) verschlüsselt oder durch Kennzeichen ersetzt. Dies erschwert die Zuordnung einzelner Datensätze. Beide Begriffe werden nachstehend noch im Einzelnen erläutert.

4. Prüfung der Verhältnismäßigkeit einer konkreten Maßnahme

- 48 Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten muss stets verhältnismäßig sein.⁶⁸ In der Praxis kann man die Frage nach der Verhältnismäßigkeit eines bestimmten Datenumgangs auf wenige Prüfungsschritte reduzieren.
- 49 Zunächst muss ein Daten verarbeitendes Unternehmen den Zweck des beabsichtigten Erhebens, Verarbeitens oder Nutzes von Daten genau festlegen. Diese zentrale Verpflichtung regelt das Gesetz recht versteckt in § 28 Abs. 1 Satz 2 BDSG: „Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.“
- 50 Wenn das Unternehmen den Zweck der vorgesehenen Datenverarbeitung festgelegt hat, muss es entscheiden, ob dieser Zweck eine ausreichende Rechtsgrundlage für den vorgegebenen Umgang mit den Daten der Personen gibt, die von der vorgesehenen Datenverarbeitung betroffen sind. Es geht also um eine Interessenabwägung.
- 51 Im Einzelnen muss das handelnde Unternehmen zwischen seinem Interesse an der Erreichung des fraglichen Zwecks und dem Interesse der Betroffenen am Schutz ihrer Persönlichkeitsrechte abwägen. Der konkrete Umgang mit personenbezogenen Daten ist dann verhältnismäßig, wenn er zur Erreichung des angestrebten Zwecks geeignet, erforderlich und angemessen ist. Die Rechtsprechung hat die Begriffe Geeignetheit, Erforderlichkeit und Angemessenheit so genau bestimmt, dass man hieraus in der Praxis durchaus konkrete Vorgaben für erlaubtes Handeln ableiten kann.

a) Geeignetheit

- 52 Bei der Überprüfung der Verhältnismäßigkeit eines Datenumgangs ist stets der geplante Zweck des Erhebens, Verarbeitens oder Nutzens von Daten entscheidend.
- 53 Eine Maßnahme ist dann geeignet, wenn sie der Erreichung des angestrebten Zwecks objektiv förderlich ist.⁶⁹ Wenn der Umgang mit den Daten einen solchen Zweck tatsächlich verwirklichen kann, ist die Maßnahme geeignet. Falls die geplante Maßnahme diesen Zweck dagegen gar nicht verwirklichen kann oder falls der Zweck nicht legitim ist, ist der Datenumgang bereits nicht geeignet und damit verboten. Zudem ist das Erheben, Verarbeiten oder Nutzen personenbezogener Daten prinzipiell nur für von der Rechtsordnung gebilligte Zwecke geeignet.

68 BAG, 20.6.2013 – 2 AZR 546/12, BB 2014, 179 (Ls.) = NZA 2014, 143; so beispielsweise auch Wybitul/Pötters, BB 2014, 437 ff.; Thüsing, NZA 2009, 865, 867; Heinson/Schmidt, CR 2010, 540 ff. mit weiteren Nachweisen.

69 Vgl. Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 147.

Beispiel: Grundsätzlich darf ein Unternehmen Daten sammeln, um die Kündigung einzelner Mitarbeiter vorzubereiten.⁷⁰ Beispielsweise ist das Zusammenstellen von Sozialdaten für die im Rahmen einer betriebsbedingten Kündigung erforderliche Sozialauswahl nicht verboten. Auch das Zusammentragen von Informationen zur Vorbereitung einer Kündigung wegen Fehlverhaltens ist normalerweise unproblematisch.

Als Faustregel kann man davon ausgehen, dass jedes Verhalten zur Erreichung eines von der Rechtsordnung gebilligten Zwecks geeignet ist, wenn es der Verwirklichung eines der Zwecke dient, die das BDSG oder andere Gesetze in Erlaubnistatbeständen ausdrücklich nennen, z. B. in §§ 28 oder 32 BDSG.

Anders ist es hingegen, wenn ein Vorgesetzter einen Mitarbeiter allein aus persönlicher Abneigung „loswerden“ will und dessen Privatleben und Vergangenheit durchleuchten lässt, um Gründe für eine mögliche Kündigung zu finden. Hier fehlt es an einem von der Rechtsordnung gebilligtem Zweck der Datenerhebung. Der Datenumgang ist unzulässig.

b) Erforderlichkeit

Die Erforderlichkeit im Rahmen einer Verhältnismäßigkeitsprüfung ist nicht identisch mit dem im BDSG häufig (z. B. in §§ 28 oder 32 BDSG) verwendeten Begriff „erforderlich“. Vielmehr ist dort, wo das Gesetz von „erforderlich“ spricht, in der Regel eine vollständige Verhältnismäßigkeitsprüfung vorzunehmen, bei der die hier beschriebene Erforderlichkeit nur ein Teil der anzustellenden Überlegungen ist. **54**

Im Rahmen der Überprüfung der Verhältnismäßigkeit einer Maßnahme ist diese dann erforderlich, wenn der fragliche Zweck des Datenumgangs nicht mit milderem Mitteln ebenso effektiv erreicht werden kann.⁷¹ Ein Mittel ist dann milder, wenn es weniger in Persönlichkeitsrechte eingreift.⁷² Ein geringerer Eingriff in Persönlichkeitsrechte ist beispielsweise dann gegeben, wenn eine Maßnahme weniger eingriffsintensiv, weniger lang andauernd oder etwa weniger flächendeckend ist, sich also anders ausgedrückt weniger auf die Betroffenen auswirkt. Bei der Erforderlichkeit geht es letztlich darum, von allen gleich zweckmäßigen Maßnahmen diejenige zu wählen, welche die informationelle Selbstbestimmung der Betroffenen am wenigsten berührt. Hierbei ist auch zu fragen, ob tatsächlich alle Daten, die erhoben, verwendet oder genutzt werden, tatsächlich zur Erreichung des (geeigneten) Verarbeitungszwecks notwendig sind. **55**

⁷⁰ Die Erlaubnis für diesen Datenumgang ergibt sich aus § 32 Abs. 1 Satz 1 BDSG.

⁷¹ *Wybitul*, BB 2010, 1085, 1086 f.

⁷² *Wybitul*, BB 2010, 1085, 1086.

c) Angemessenheit

- 56 Hat man die mildeste geeignete Maßnahme zur Erreichung des vorgesehenen Zwecks identifiziert, so muss man fragen, ob der angestrebte Zweck die geplanten Eingriffe in die Persönlichkeitsrechte der Betroffenen rechtfertigt, ob der fragliche Datenumgang also angemessen ist. Diese Angemessenheit wird auch als „Verhältnismäßigkeit im engeren Sinne“⁷³ bezeichnet. An dieser Stelle muss das Unternehmen zwischen den eigenen wirtschaftlichen Interessen und dem Recht der Betroffenen auf informationelle Selbstbestimmung abwägen. Es geht um eine Zweck-Mittel-Relation der betroffenen schutzwürdigen Belange. In der Praxis liegt an dieser Stelle oft der Schwerpunkt der Prüfung der datenschutzrechtlichen Zulässigkeit eines Vorhabens. Obgleich diese Prüfung regelmäßig komplexe juristische Abwägungen erfordert, zeigt sich in der alltäglichen Anwendung meist, dass sich die so gefundenen Argumentationen auch durch Anwendung gesunden Menschenverstandes und einer objektiven, ausgewogenen Herangehensweise bestätigen lassen.
- 57 Abschließend sei noch darauf hingewiesen, dass nicht zuletzt auch die Üblichkeit einer Vorgehensweise und ihre Akzeptanz in der Fachliteratur Indizien für die Verhältnismäßigkeit einer Maßnahme sein können.⁷⁴ Wenn beispielsweise die zuständigen Aufsichtsbehörden eine bestimmte Maßnahme oder Kategorien von Datenverarbeitungen bei unveränderter Gesetzeslage in der Vergangenheit nicht beanstandet hatten, spricht einiges dafür, dass dieser Datenumgang nicht völlig unverhältnismäßig sein kann. Schon von daher lohnt es sich, aufmerksam die regelmäßig erscheinenden Tätigkeitsberichte der Datenschutzaufsichtsbehörden zu studieren. Dies erleichtert es den Verantwortlichen, ein Gefühl dafür zu bekommen, was dort noch als verhältnismäßig angesehen wird und wo möglicherweise im Einzelfall die Grenzen dieser Verhältnismäßigkeit gezogen werden.

II. Was hat es mit dem Verbot mit Erlaubnisvorbehalt auf sich?

- 58 Das BDSG geht von einem schlichten Prinzip aus: Der Umgang mit personenbezogenen Daten ist grundsätzlich verboten. Dies gilt nur dann nicht, wenn eine Erlaubnis des Betroffenen vorliegt oder eine Rechtsvorschrift den Datenumgang erlaubt.

⁷³ Vgl. BVerfG, NJW 2010, 833, 838, Abs. 209 ff.

⁷⁴ *Thüsing*, Arbeitnehmerdatenschutz und Compliance, Rn. 156.

§ 4 Abs. 1 BDSG: „Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder vorschreibt oder der Betroffene eingewilligt hat.“

Dieses so genannte Verbot mit Erlaubnisvorbehalt führt dazu, dass man vor dem Umgang mit personenbezogenen Daten stets prüfen muss, ob eine Regelung diesen Datenumgang erlaubt. Ausnahmen von dem grundsätzlichen Verbot gelten etwa dann, wenn das BDSG selbst die Erhebung, Verarbeitung oder Nutzung erlaubt, z. B. in § 32 BDSG oder § 28 BDSG. Zudem können die Einwilligungen Betroffener, Betriebsvereinbarungen oder Tarifverträge den Umgang mit personenbezogenen Daten erlauben. **59**

Neben dem BDSG gibt es jedoch noch eine Vielzahl weiterer Gesetze, die den Umgang mit personenbezogenen Daten in bestimmten Konstellationen ausdrücklich erlauben. Dazu gehören beispielsweise das Telemediengesetz (TMG) für die Verwendung von personenbezogenen Daten im Rahmen von Online-Diensten, das Sozialgesetzbuch (SGB) im Rahmen der Arbeit von Schwerbehindertenvertretungen im Unternehmen und mitunter sogar die Strafprozessordnung (StPO), in der die Datennutzung der Staatsanwaltschaft und der Polizei im Rahmen der Verbrechensbekämpfung geregelt ist. Bevor also zur Legitimation einer Datenverarbeitung vorschnell auf die Einwilligung der Betroffenen abgestellt wird, macht es immer Sinn, die im Einzelfall einschlägigen Gesetze auf entsprechende datenschutzrechtliche Erlaubnistatbestände hin zu durchsuchen. **60**

III. Was besagt der Grundsatz der Zweckbindung bei der Verarbeitung personenbezogener Daten?

Nach dem Grundsatz der Zweckbindung dürfen personenbezogene Daten nur für vorher festgelegte eindeutige (und rechtmäßige) Zwecke erhoben werden. **61**

Diese nächste essenzielle Grundregel soll die unkontrollierte Erhebung oder Speicherung personenbezogener Daten verbieten. Eine Datenerhebung „ins Blaue hinein“⁷⁵ ist folglich genauso verboten wie eine Datenspeicherung auf Vorrat – also für zum Zeitpunkt der Erhebung noch nicht näher bestimmte Zwecke. Dies hat das Bundesverfassungsgericht auch in seinem Urteil vom 2.3.2010 zur Nichtigkeit der Vorratsdatenspeicherung durch Telekommunikationsunternehmen noch einmal eindringlich betont.⁷⁶ **62**

⁷⁵ Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 74.

⁷⁶ BVerfG, NJW 2010, 833, 841, Abs. 226 ff.

- 63** Der Grundsatz der Zweckbindung personenbezogener Daten gilt bei allen Phasen des Datenumgangs und bei allen Arten von personenbezogenen Daten, also nach richtiger Auffassung auch bei Beschäftigtendaten.⁷⁷

§ 28 Abs. 1 Satz 2 BDSG: „Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.“

- 64** Die Übermittlung oder Nutzung für einen anderen Zweck als den bei der Erhebung festgelegten ist nur ausnahmsweise zulässig, z. B. „soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt“, § 28 Abs. 2 Nr. 1 in Verbindung mit § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Auch wenn personenbezogene Daten an einen Dritten übermittelt werden, bleibt es bei der vorher festgelegten Zweckbestimmung dieser Daten, vgl. § 28 Abs. 5 Satz 1 BDSG. Damit ist eine Zweckänderung grundsätzlich ein neuer Grundrechtseingriff und benötigt nach der Konzeption des Datenschutzrechts eine eigene Erlaubnisnorm,⁷⁸ beispielsweise § 28 Abs. 1 Satz 1 Nr. 2 BDSG.
- 65** Wenn Unternehmen personenbezogene Daten beim Betroffenen selbst erheben, müssen sie den Betroffenen nach § 4 Abs. 3 Satz 1 Nr. 2 BDSG auf die Zweckbestimmungen der Erhebung, Verarbeitung und Nutzung hinweisen.

IV. Was bedeutet Transparenz gegenüber dem Betroffenen im deutschen Datenschutzrecht?

- 66** Ein weiterer wesentlicher Grundgedanke des Datenschutzes ist die Transparenz der Verwendung personenbezogener Daten. Um sein Recht auf informationelle Selbstbestimmung ausüben zu können, muss der Betroffene darüber informiert sein, wer über seine personenbezogenen Daten verfügt und was damit konkret gemacht wird. Ein Datenumgang ohne Kenntnis des Betroffenen ist nur in Ausnahmefällen erlaubt. Das dient nicht zuletzt auch der Wahrung der Betroffenenrechte. Erst wenn derjenige, dessen Daten verarbeitet werden, hiervon weiß, kann er gegebenenfalls dagegen vorgehen. Damit ermöglicht der Grundsatz der Transparenz auch nicht zuletzt die Gewährleistung eines effektiven Rechtsschutzes gegen unzulässige Formen der Datennutzung.⁷⁹
- 67** Ein wesentliches Mittel zur Sicherstellung der nötigen Transparenz beim Umgang mit personenbezogenen Daten ist der sogenannte Direkterhebungs-

⁷⁷ Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 74; Wedde, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 63; Gola/Schomerus, BDSG, § 32 Rn. 36 ff.

⁷⁸ Vgl. § 4 Abs. 1 BDSG.

⁷⁹ Vgl. BVerfG, NJW 2010, 833, 843, Rn. 239 ff. (sog. Vorratsdaten-Entscheidung).

grundsatz des § 4 Abs. 2 BDSG. Er sieht vor, dass man personenbezogene Daten in der Regel beim Betroffenen selbst erheben muss, so dass dieser schon hierdurch vom Umgang mit seinen Daten erfährt.

§ 4 Abs. 2 Satz 1 BDSG: „*Personenbezogene Daten sind grundsätzlich beim Betroffenen zu erheben.*“

Im Rahmen der Direkterhebung muss man den Betroffenen zudem auch über die näheren Umstände des Umgangs mit seinen Daten informieren, § 4 Abs. 3 BDSG. Diese Hinweispflicht soll bei der Direkterhebung sicherstellen, dass der Betroffene weiß, wer die Daten für welchen Zweck erhebt und an wen diese weitergegeben werden sollen.⁸⁰ **68**

Checkliste zur Informationspflicht bei der Direkterhebung (§ 4 Abs. 3 BDSG):

- Ist der Betroffene hinreichend über die Identität der verantwortlichen Stelle informiert (z. B. Name und Anschrift des Unternehmens, Ansprechpartner, Telefonnummer, E-Mail-Adresse)?
- Ist der Betroffene hinreichend von den beabsichtigten Zwecken der Datenerhebung informiert?
- Bei geplanten Übermittlungen an Dritte: Ist der Betroffene hinreichend von den Kategorien der Empfänger seiner Daten informiert?

Unternehmen dürfen gemäß § 4 Abs. 2 Satz 2 BDSG nur dann von einer Direkterhebung beim Betroffenen selbst absehen, wenn Rechtsvorschriften dies vorsehen, der jeweilige Geschäftszweck dies erforderlich macht oder die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde. Aber auch beim erstmaligen Speichern von personenbezogenen Daten, die nicht direkt beim Betroffenen selbst erhoben wurden, muss man den Betroffenen informieren: **69**

§ 33 Abs. 1 Satz 1 BDSG: „*Werden erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu benachrichtigen.*“

§ 33 BDSG sieht keine bestimmte Form der Benachrichtigung des Betroffenen vor. Allerdings empfiehlt sich aus Gründen der Beweissicherung die Schriftform.⁸¹ Neben diesen allgemeinen Benachrichtigungspflichten bestehen noch weitere Informationspflichten für Unternehmen, z. B. bei Datenverlusten (§ 42a BDSG) oder auf Verlangen des Betroffenen (§ 34 BDSG). **70**

⁸⁰ Weichert, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 4 BDSG Rn. 11.

⁸¹ Meents/Hinzpeter, in: Taeger/Gabel, BDSG, § 33 Rn. 19.

Kapitel 3: Was gehört zum Basiswissen bei der praktischen Anwendung des BDSG?

- 71 Dieses Kapitel erläutert die grundlegenden Fragestellungen und die wesentlichen Begrifflichkeiten, die man kennen muss, um die Regelungen des BDSG zu verstehen und mit ihnen in der Praxis arbeiten zu können. Der Leser erfährt hier etwa, welche Informationen das Gesetz als personenbezogene Daten bezeichnet und was man unter deren Erheben, Verarbeiten oder Nutzen im Einzelnen versteht.

I. Wer ist für die Einhaltung der Regeln des BDSG verantwortlich?

- 72 Das BDSG richtet sich in erster Linie nicht an einzelne Personen im Unternehmen, sondern an das Unternehmen als Ganzes. Denn Adressat der Vorschriften des BDSG ist in erster Linie die „verantwortliche Stelle“, also die (natürliche oder juristische) Person, die über die Daten verfügt und über den Umgang mit den betroffenen personenbezogenen Daten entscheidet.⁸²

§ 3 Abs. 7 BDSG: „*Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.*“

- 73 Im Wirtschaftsleben gilt das BDSG damit vor allem für Unternehmen und deren Vertreter. Verantwortlich im Unternehmen für die Einhaltung der datenschutzrechtlichen Vorgaben ist damit in erster Linie die Geschäftsleitung (z. B. der Vorstand einer Aktiengesellschaft oder Geschäftsführer einer Gesellschaft mit beschränkter Haftung). Es darf aber nicht übersehen werden, dass es letztlich die Mitarbeiter des Unternehmens sind, die tagtäglich mit den personenbezogenen Daten arbeiten und dabei diese Vorgaben mit Leben erfüllen. Die Ausbildung und kontinuierliche Schulung der betroffenen Mitarbeiter ist damit eine wichtige Aufgabe des Unternehmens im Rahmen seiner Organisationspflichten.
- 74 Rechtlich selbstständige Unternehmen sind stets eigene verantwortliche Stellen, auch wenn sie in einem Konzernverbund stehen. Das BDSG kennt – anders als etwa das Abgaben-, das Kartell- oder das Aktienrecht – keine

82 Da sich das vorliegende Handbuch mit dem Datenschutz in Unternehmen befasst, verwendet es die Begriffe „Unternehmen“ und „verantwortliche Stelle“ oft synonym.

Konzerne und Unternehmensgruppen.⁸³ Das bedeutet in der Praxis, dass der Transfer personenbezogener Daten zwischen einzelnen Unternehmen eines Konzerns eine Datenübermittlung darstellt und damit stets einer Erlaubnisnorm bedarf.⁸⁴ Vor allem die Datenschutzaufsichtsbehörden wiederholen bei jeder sich bietenden Gelegenheit das Dogma vom fehlenden Konzernprivileg und weisen dabei regelmäßig darauf hin, dass dies auf einer absichtlichen Entscheidung des Gesetzgebers beruhe und daher auch nicht durch entsprechend phantasievolle Konstruktionen der Konzerndatenschützer unterminiert werden dürfe. In der Praxis sind Datenübermittlungen zwischen Konzerngesellschaften oder verbundenen Unternehmen jedoch die absolute Regel und lassen sich – aller dogmatischen Diskussionen zum Trotz – nicht selten unter Berufung auf die Wahrung berechtigter wirtschaftlicher Interessen gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG rechtfertigen.⁸⁵ Hierbei ist jedoch Vorsicht geboten. Meist rein wirtschaftlich getriebene Konzerninteressen für sich alleine sind zwar durchaus auch berechnete Interessen der verantwortlichen Stelle im Konzern. Im Rahmen der Abwägung gegen die immerhin grundrechtsrelevanten Interessen des Betroffenen stehen sie aber häufig zurück, wenn sie nicht durch entsprechende Ausgleichsmaßnahmen flankiert werden.⁸⁶

Das BDSG gilt gemäß § 1 Abs. 5 BDSG grundsätzlich für alle Unternehmen, die ihren Sitz in Deutschland haben.⁸⁷ Maßgeblich ist zunächst nicht der Ort der Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten, sondern der Sitz des Unternehmens, das diesen Datenumgang vornimmt. Dieses sogenannte Sitzprinzip gilt innerhalb aller Mitgliedstaaten der Europäischen Union (sowie anderer Vertragsstaaten des Europäischen Wirtschaftsraums). Wenn also ein deutsches Unternehmen, das in England keine Niederlassung unterhält, in London Daten erhebt und speichert, so gilt für diesen Datenumgang dennoch deutsches Datenschutzrecht. Diese Regelung soll den grenzüberschreitenden Wirtschaftsverkehr zwischen EU- und EWR-Staaten dadurch vereinfachen, dass sie es Unternehmen ermöglicht, ihr eigenes nationales Datenschutzrecht in gewissem Umfang zu „exportieren“.

75

83 *Gola/Schomerus*, BDSG, § 2 Rn. 21; *Simitis*, in: *Simitis*, BDSG, § 2 Rn. 143 mit ausdrücklichem Hinweis auf entsprechende Normen im Betriebsverfassungs- (§§ 54 ff. BetrVG), Aktien- (§§ 15 ff. AktG) oder Steuerrecht.

84 Allgemein zur Behandlung von Konzernunternehmen im Datenschutz sehr ausführlich und vergleichsweise ausgewogen *Simitis*, in: *Simitis*, BDSG, § 2 Rn. 142 ff.

85 Vgl. *Simitis*, in: *Simitis*, BDSG, § 2 Rn. 156: „Die eindeutige Weigerung des Gesetzgebers, Konzerne als verantwortliche Stellen anzusehen, zwingt auch dazu, ebenso klar jeden Versuch abzulehnen, § 28 Abs. 1 Satz 1 Nr. 2 in einer Weise zu interpretieren, die letztlich doch einen möglichst uneingeschränkten konzerninternen Informationsaustausch rechtlich absichern würde.“

86 Vgl. hierzu etwa *Plath*, in: *Plath*, BDSG, § 28 Rn. 73 mit Verweis auf *Schulz*, BB 2011, 2552, 2554.

87 Vgl. zum sog. Sitzprinzip des Art. 4 der Richtlinie beim EU-grenzüberschreitenden Datenverkehr: *Gola/Schomerus*, BDSG, § 1 Rn. 27 ff.

- 76 Eine Ausnahme von diesem Sitzprinzip gilt allerdings nach § 1 Abs. 5 BDSG dann, wenn ein ausländisches Unternehmen mit Sitz in einem EU- oder EWR-Staat nicht nur gelegentliches Geschäft, sondern eine Niederlassung in Deutschland betreibt. In diesem Falle gilt das deutsche BDSG. Eine Niederlassung setzt die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung voraus.⁸⁸ Die Rechtsform ist dabei nicht maßgeblich.
- 77 Unternehmen mit Sitz im nicht-europäischen Ausland unterliegen nach § 1 Abs. 5 Satz 2 BDSG grundsätzlich deutschem Datenschutzrecht, sofern sie personenbezogene Daten im Inland erheben, verarbeiten oder nutzen.

II. Für welche Formen der Datenverarbeitung gilt das BDSG?

- 78 Das BDSG soll Menschen vor Eingriffen in ihre Persönlichkeitsrechte schützen.⁸⁹ Das Gesetz gilt für Unternehmen vor allem dann, wenn diese beim Erheben, Verarbeiten oder Nutzen personenbezogener Daten „Datenverarbeitungsanlagen“ einsetzen.⁹⁰

§ 1 Abs. 2 BDSG: *„Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch (...) nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht-automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.“*

1. Einsatz von Datenverarbeitungsanlagen oder dateimäßige Verarbeitung

- 79 Unternehmen müssen das BDSG unter anderem dann beachten, wenn sie Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben, § 27 Abs. 1 Satz 1 BDSG. Auch die Erhebung von personenbezogenen Daten mit dem Ziel, diese später mittels Datenverarbeitungsanlagen zu verarbeiten oder zu nutzen, unterliegt also den Beschränkungen des BDSG.

⁸⁸ *Gola/Schomerus*, BDSG, § 1 Rn. 28 mit Verweis auf *Dammann*, RDV 2002, 70 u. a. zur heranziehbaren Regelung des § 42 Abs. 2 GewO.

⁸⁹ Vgl. § 1 Abs. 1 BDSG.

⁹⁰ Das BDSG gilt auch dann, wenn Unternehmen Daten auf der Grundlage einer Betriebsvereinbarung erheben, verarbeiten oder nutzen. Regelungen in Tarifverträgen oder Betriebsvereinbarungen verdrängen die Anwendbarkeit des BDSG nicht, da es sich trotz ihrer zwingenden Wirkung nicht um Rechtsvorschriften des Bundes (vgl. § 1 Abs. 3 Satz 1 BDSG) handelt, vgl. *Taeger*, in: *Taeger/Gabel*, BDSG, § 4 Rn. 35.

II. Für welche Formen der Datenverarbeitung gilt das BDSG?

Der Begriff der Datenverarbeitungsanlage wird dabei weit verstanden und umfasst nicht nur stationäre wie mobile Computer, sondern auch Kamera-Überwachungssysteme, Smartphones und unter Umständen sogar reine Chip-Karten, wenn diese nicht nur zum Speichern von Informationen verwendet werden, sondern mit einem eigenen Prozessor ausgestattet sind.⁹¹ **80**

Auch das Verarbeiten oder Nutzen mittels sogenannter nicht-automatisierter Dateien fällt ebenso unter das BDSG wie die Erhebung von Daten für einen späteren Einsatz in nicht-automatisierten Dateien. **81**

Unter nicht-automatisierten Dateien versteht das Gesetz Sammlungen personenbezogener Daten, die gleichartig aufgebaut und nach bestimmten Merkmalen zugänglich sind und ausgewertet werden können, §3 Abs. 2 Satz 2 BDSG. Mit dieser Formulierung meint der Gesetzgeber beispielsweise physische Personalakten, alphabetisch nach Personennamen geordnete Aktensammlungen⁹² oder auch strukturierte Karteikartensammlungen von personenbezogenen Daten. Auch bei solchen nicht-automatisierten Dateien unterliegt das Erheben von personenbezogenen Daten mit dem Ziel, diese später in einer nicht-automatisierten Datei zu verwenden, den Anforderungen des BDSG, § 1 Abs. 2 Nr. 3 BDSG. **82**

Eine ähnliche Regelung enthält auch §27 BDSG. Danach sind die Vorschriften der §§27–38a BDSG unter anderem für Unternehmen der Privatwirtschaft anwendbar, soweit diese personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder für einen solchen automatisierten Einsatz erheben. Dies gilt auch für den Einsatz von personenbezogenen Daten, die nicht-automatisierten Dateien entstammen oder in nicht-automatisierten Dateien verarbeitet oder genutzt oder hierfür erhoben werden. **83**

Bei Arbeitnehmern und anderen Beschäftigten gilt das Erfordernis der automatisierten oder dateimäßigen Verarbeitung oder Nutzung nicht. Arbeitgeber müssen gemäß § 32 Abs. 2 BDSG alle Beschäftigtendaten grundsätzlich nach den Regeln des BDSG behandeln – unabhängig davon, für welche Einsatzmöglichkeiten sie erhoben oder mittels welcher Systeme sie verarbeitet oder genutzt werden. **84**

Praxistipp: Die geschilderte Unterscheidung der automatisierten und nicht-automatisierten Datenverarbeitung wirkt sich im Wirtschaftsleben weniger stark aus als man vermuten könnte. In der Praxis ist das BDSG ohnehin bereits auf fast alle Formen des Umgangs mit personenbezogenen Daten anwendbar. Jede Benutzung von Internet oder E-Mail impliziert in

⁹¹ Vgl. hierzu Teil 2, § 6c Rn. 1 ff.

⁹² *Gola/Klug*, Grundzüge des Datenschutzrechts, S. 43.

der Praxis regelmäßig schon eine automatisierte Erhebung, Verarbeitung oder Nutzung personenbezogener Daten.⁹³

Zudem unterliegen Unternehmen bereits dann dem BDSG, wenn sie personenbezogene Daten (beispielsweise Kundendaten) für eine spätere Verarbeitung oder Nutzung mittels Datenverarbeitungsanlagen erheben. Schon die Erhebung von Daten für den späteren Einsatz in IT-Systemen muss sich an den Regeln des BDSG messen lassen. Im modernen Geschäftsleben erfolgt erfahrungsgemäß fast jeder Umgang mit personenbezogenen Daten mittels IT-Systemen oder mit dem Ziel einer späteren automatisierten Datenverarbeitung oder Datennutzung.

2. Keine Anwendung des BDSG für ausschließlich persönliche oder familiäre Tätigkeiten

- 85 Wenn jemand personenbezogene Daten ausschließlich für persönliche oder familiäre Tätigkeiten erhebt, verarbeitet oder nutzt, gilt das BDSG nach § 1 Abs. 2 Nr. 3 BDSG nicht.⁹⁴ Hat der Umgang mit den Daten allerdings sowohl einen geschäftlichen als auch einen persönlichen bzw. familiären Hintergrund, so bleibt das BDSG anwendbar.

Beispiel: Bringt man aus dem firmeninternen Intranet den Geburtstag einer Kollegin oder eines Kollegen in Erfahrung, weil man Blumen schenken möchte, so unterliegt dieser Vorgang nicht dem BDSG.⁹⁵ Sammelt man hingegen Informationen über die Geburtstage von Geschäftskontakten, um diesen mit einer Karte oder E-Mail zu gratulieren, handelt es sich nicht um eine ausschließlich persönliche Tätigkeit. Allerdings kann ein solches Vorgehen nach § 28 Abs. 3 BDSG zur Wahrung berechtigter geschäftlicher Interessen erlaubt sein, falls es sich nicht um einen Eingriff handelt, bei dem schutzwürdige Interessen des Betroffenen daran überwiegen, keine Geburtstagsgrüße zu erhalten.

93 Scheja, in: Taeger/Gabel, BDSG, § 4f Rn. 12.

94 Vgl. für Wirtschaftsunternehmen auch § 27 Abs. 1 Satz 2 BDSG.

95 Allerdings wird sich der Arbeitgeber in diesem Beispielfall fragen lassen müssen, auf welcher Rechtsgrundlage er personenbezogene Daten seiner Mitarbeiter in dieser Form betriebsintern zugänglich macht. In der Praxis arbeiten Unternehmen bei solchen internen Mitarbeiterprofilen oft auf der Grundlage von Einwilligungen.

3. Keine Anwendung des BDSG, wenn es durch Spezialgesetze verdrängt wird

Die Regelungen des BDSG haben Auffangfunktion. Wenn also ein anderes Bundesgesetz eine Spezialmaterie abschließend regelt, gilt das BDSG insoweit nicht. 86

§ 1 Abs. 3 Satz 1 BDSG: „Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor.“

Speziellere Gesetze, die das BDSG verdrängen, findet man in einer Vielzahl von Regelungsbereichen, etwa dem Sozialrecht,⁹⁶ dem Steuerrecht⁹⁷ oder dem Versicherungsrecht.⁹⁸ 87

Beispiele: § 147 Abs. 1 Abgabenordnung (AO) schreibt vor, dass Steuerpflichtige steuerlich relevante Unterlagen für bis zu zehn Jahre aufbewahren müssen, z. B. Buchungsbelege oder Handels- und Geschäftsbriefe. Auch wenn diese Unterlagen personenbezogene Daten enthalten, sind die Vorschriften des BDSG über die Löschung von Daten erst anwendbar, wenn die in der AO geregelten Fristen abgelaufen sind.

Personen oder Unternehmen, die nach dem Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (GwG) zur Vornahme von Maßnahmen gegen Geldwäsche verpflichtet sind, dürfen sich gegenseitig nach § 12 Abs. 3 GwG Informationen über Sachverhalte übermitteln, die in Bezug auf Geldwäsche oder Terrorismusfinanzierung auffällig oder ungewöhnlich sind. Sofern und soweit die Voraussetzungen von § 12 Abs. 3 GwG also vorliegen, dürfen sich die betroffenen Unternehmen (z. B. Banken, Versicherungen oder Personen, die gewerbsmäßig mit Gütern handeln) auch personenbezogene Daten übermitteln, ohne dass die Voraussetzungen des BDSG vorliegen.⁹⁹

Hierbei muss man allerdings beachten, dass speziellere Gesetze dem BDSG nur vorgehen, „soweit“ sie auf den Umgang mit personenbezogenen Daten im Einzelfall Anwendung finden. 88

96 Z. B. §§ 67 ff. des Zehnten Sozialgesetzbuchs (SGB X).

97 Z. B. § 147 Abs. 6 AO, der sogar automatisierte Datenabgleiche von Steuerdaten vorsieht. Vgl. hierzu im Einzelnen *Thüsing*, Arbeitnehmerdatenschutz und Compliance, Rn. 160 ff.

98 Z. B. § 80d Abs. 1 Satz 3 Versicherungsaufsichtsgesetz (VAG), der Versicherungsunternehmen erlaubt, personenbezogene Daten zur Abwehr von Geldwäsche und Terrorismusfinanzierung zu nutzen.

99 Vgl. z. B. zur datenschutzrechtlichen Zulässigkeit von Maßnahmen zur Verhinderung der Geldwäsche: *Brisch*, in: *Renz/Hense*, Wertpapier-Compliance in der Praxis, S. 852 ff.