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

Fachmedien Recht und Wirtschaft I dfv Mediengruppe I Frankfurt am Main

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

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 verwerten, 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 Vorauflage 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 praxisgerecht 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 Kurzkommentierung 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 Paragrafen des BDSG. Die Kurzkommentierung 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 Wybitul*

Inhaltsverzeichnis

Zweiter Abschnitt: Datenverarbeitung der öffentlichen Stellen

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

Vierter Abschnitt: Sondervorschriften

Fünfter Abschnitt: Schlussvorschriften

Sechster Abschnitt: Übergangsvorschriften

Anhang

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] **1**

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- **2**

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 Unternehmen[10] 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 *Taeger/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 *Taeger*, 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 Paragrafen 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 1977[12] 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 berücksichtigen[19] 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/EG[25] 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 *Taeger/Schmidt*, in: Taeger/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 ABl. 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

12 In erster Linie als Reaktion auf Datenschutzskandale bei einer Reihe von Großunternehmen[28] 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]

6. Entwurf eines „Gesetzes zur Regelung des Beschäftigtendatenschutzes"

13 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]

14 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-

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)

18 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".

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

19 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.

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

20 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,

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 Effizienzgesichtspunkt. 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 zugänglich 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 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. **23**

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. **24**

Dazu gehörte nach der Überzeugung der Kommission insbesondere die zu steigernde 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- **25**

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.

Datenschutzrichtlinie 95/46/EG[41] 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

28 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]

29 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.

3. Fehlende Vorgaben von Gerichten und Aufsichtsbehörden

30 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]

---

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 Beschäftigtendaten 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.