C.F. Müller Wirtschaftsrecht

Compliance

Aufbau - Management - Risikobereiche

Bearbeitet von
Dr. Cornelia Inderst, Prof. Dr. Britta Bannenberg, Sina Poppe, Dr. Tobias Ackermann, Silvia C. Bauer, Dr. Sophie Luise Bings, Dr. Björn Demuth, Markus Eberhard, David Elshorst, Christina Fischer, Martina Flitsch, Hermann Geiger, LL.M., Anne-Catherine Hahn, Marion Hanten, Dr. Mathias Hanten, Uwe Heim, Dr. Frank M. Hülsberg, Daniel Kaiser, Sebastian Lach, Jens C. Laue, Bernd Michael Lindner, Michael Bernd Peters, Eva Racky, Dr. Torsten Reich, Markus S. Rieder, LL.M., Christoph Rieken, LL.M., Frank Romeike, Alexander von Saenger, Joachim Schrey, Burkhard Schwenker, Prof. Dr. Fabian Stancke, Michael Steiner, Annke von Tiling, Stefan Weiss, Uta Zentes, LL.M.

3., neu bearbeitete Auflage 2017. Buch. XLVII, 809 S. Gebunden
ISBN 978 3 8114 4661 8
Format (B x L): 17 x 24 cm

Wirtschaft > Management > Risikomanagement

Zu Inhaltsverzeichnis

schnell und portofrei erhältlich bei

beck-shop.de
DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung beck-shop.de ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

F. Datenschutz

I. Einführung

301 Während der Datenschutz früher ein eher bescheidenes Dasein führte, rückte er in den letzten Jahren immer mehr in den Fokus der Öffentlichkeit. Diverse medienwirksame Skandale,[341] die Globalisierung und auch der technische Fortschritt haben die Menschen für das Thema sensibilisiert. Die Angst vor dem „gläsernen Menschen", der ohne sein Wissen (video)überwacht wird oder dessen Daten im Nirvana des WorldWideWeb umherirren und für Zwecke genutzt werden, die er nicht absehen kann, wird immer größer. Daneben steigen im digitalen Zeitalter die Risiken des Missbrauchs von Daten – dies beginnt bei Risiken durch die Nutzung von Geldautomaten mittels EC-Karten und endet mit dem Abfangen von Kreditkartendaten im Internet. Cyber-Security ist ein Stichwort, das inzwischen fast wöchentlich in den Medien erwähnt wird. Dazu kommt, dass Datenschutz immer mehr als ein internationales Thema erkannt wird; die Europäische Union hat daher am 24.5.2016 nach langen Diskussionen die Europäische Datenschutzgrundverordnung („DSGVO") in Kraft gesetzt, die ab dem 25.5.2018 in allen Mitgliedstaaten der Europäischen Gemeinschaft unmittelbar anwendbar ist und das bis heute bekannte Datenschutzrecht in Deutschland weitestgehend ersetzen wird.[342]

II. Entwicklung des Datenschutzrechtes

302 Auch wenn der Datenschutz bis vor wenigen Jahren von der Öffentlichkeit nicht so wahrgenommen wurde, hat er in Deutschland bereits eine lange Tradition: Die Geschichte der Datenschutzgesetzgebung hat hier bereits im Jahr 1970 mit der Verabschiedung des ersten Landesdatenschutzgesetzes in Hessen begonnen.[343] Das erste Bundesdatenschutzgesetz folgte 1977.[344] Seitdem hat sich das Bundesdatenschutzgesetz und der Datenschutz an sich stetig weiterentwickelt. Maßgeblich für die Entwicklung waren hierbei zum einen das Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983, welches unter anderem mit der Verknüpfung des Rechts auf informationelle Selbstbestimmung mit dem Grundgesetz die Bedingungen der Verarbeitung personenbezogener Daten neu festlegte.[345] Dieses gewährleistet das Recht des Einzelnen, grundsätzlich über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Der Grundsatz lautet: So viel Freiheit wie möglich und so viel Bindung

341 Vgl. www.handelsblatt.com/politik/deutschland/nach-neuem-datenschutzskandal-neuer-datenskandal-heizt-sicherheitsdebatte-an-seite-3/3072452-3.html; www.pcwelt.de/ratgeber/Sicherheit-Die-groessten-Datenschutz-Skandale-der-IT-Geschichte-4976380.html; www.projekt-datenschutz.de/datenschutzvorfaelle.

342 *Albrecht/Jotzo* Das neue Datenschutzrecht der EU, 2017, S. 40 Rn. 11 ff.

343 Vgl. *Simitis* BDSG, 8. Aufl. 2014, Einl. Rn. 1; *Däubler/Klebe/Wedde/Weichert* BDSG, 5. Aufl. 2016, Einl. Rn. 4; GVBl. I 1970, 625; dazu *Birkelbach* IBM-Nachrichten 1974, 241 ff., 333 ff.; *Reh* Gegenstand und Aufgabe des Datenschutzes in der öffentlichen Verwaltung, Beiträge zum Datenschutz, hrsg. vom Hessischen Datenschutzbeauftragten, H.2 (1974), insbesondere S. 23 ff.; *Gola/Schomerus* BDSG, 12. Aufl. 2015, Einl. Rn. 1.

344 Vgl. *Gola/Schomerus* BDSG, 12. Aufl. 2015, Einl. Rn. 1; *Simitis* BDSG, 8. Aufl. 2014, Einl. Rn. 1; BGBl I 1977, 201; *Bull* NJW 1979, 1177 ff.; *Dammann* NJW 1978, 1931 ff.

345 Vgl. *BVerfGE* 65, 1; *Gola/Schomerus* BDSG, 12. Aufl. 2015, Einl. Rn. 3; *BVerfGE* 65, 1.

wie nötig. Neben dieser Entwicklung erfordern auch die ständigen Neuentwicklungen in der Informations- und Kommunikationstechnologie zu nicht geahnten Möglichkeiten der globalen Datenverarbeitung, die eine Modernisierung des Datenschutzes erforderlich machen.

303 Ein einheitliches Datenschutzniveau innerhalb Europas wurde durch die RL 95/46/EG vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr geschaffen.[346] Der deutsche Gesetzgeber hat diese Richtlinie durch das BDSG vom 20.12.2001 (BDSG 2001) angepasst; welches seitdem verschiedene Änderungen erfahren hat.[347]

304 Die letzte Änderung erfuhr das BDSG durch die umfassenden Novellierungen in 2009.[348] Mit der „Novelle I" regelte der Gesetzgeber die Tätigkeit von Auskunfteien und ihrer Vertragspartner, insbesondere Kreditinstituten, sowie das Scoring neu. Die „Novelle II" änderte u.a. den Beschäftigtendatenschutz, die Auftragsdatenverarbeitung, die Informationspflichten bei Datenschutzverstößen, schuf neue Befugnisse für die Aufsichtsbehörden und führte einen verstärkten Kündigungsschutz für Datenschutzbeauftragte ein. Daneben wurden die möglichen Sanktionen erheblich verschärft.[349]

305 Gleichwohl war in der Praxis zu beobachten, dass trotz der strengeren gesetzlichen Anforderungen erst dann Aktivitäten der Unternehmen zu verzeichnen waren, als tatsächlich Strafen in Millionenhöhe verhängt wurden und damit einhergehend die Reputation diverser Unternehmen erheblichen Schaden nahm. Effektiv war in diesem Zusammenhang insbesondere der mit § 42a BDSG eingeführte so genannte „Datenschutzpranger": Danach bestehen bei bestimmten Verstößen bzw. der unberechtigten Kenntnisnahme von Daten durch Dritte erweiterte Informationspflichten gegenüber den Betroffenen und den Datenschutzaufsichtsbehörden, die auch die Verpflichtung beinhalten können, in zwei bundesweit erscheinenden Tageszeitungen die entsprechenden Verstöße anzuzeigen, um die Betroffenen zu informieren. Diverse große Unternehmen nahmen diese Vorkommnisse zum Anlass, ihre Datenschutzorganisation anzupassen und Datenschutz als einen wesentlichen Bestandteil der Compliance – Organisation des Unternehmens zu installieren.

306 Durch die – wie bereits oben ausgeführt – Anpassung des Datenschutzrechts auf europäischer Ebene wird diese Entwicklung weiter Fahrt aufnehmen. Um die Umsetzungsbereitschaft der Unternehmen zu erhöhen, hat der europäische Gesetzgeber vorgesehen, dass bei Verstößen gegen das ab Mai 2018 auch in Deutschland geltende Datenschutzrecht Sanktionen in Höhe von bis zu 20 Mio. EUR bzw. 4 % des weltweiten Jahresumsatzes des Unternehmens verhängt werden können.[350] Zudem werden die Meldepflichten für Datenschutzverstöße verschärft (siehe Art. 33, 34 DSGVO).[351]

---

346 S. dazu EG-Datenschutzrichtlinie v. 24.10.1995, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html.

347 S. dazu BDSG-Novelle 2001 v. 20.12.2001.

348 S. BGBl I, 2254, 2814 und 2355.

349 S. BR-Drucks. 4/09, BT-Drucks. 16/10529, BT-Drucks. 16/12011 sowie BT-Drucks. 16/13657.

350 Plath/*Becker* BDSG/DSGVO, 2. Aufl. 2016, Art. 83, Rn. 4 ff.; *Albrecht/Jotzo* Das neue Datenschutzrecht der EU, 2017, S. 131 Rn. 36; *Gola/Jaspers/Müthlein/Schwartmann* Datenschutz-Grundverordnung im Überblick, 2017, S. 70; *Faust/Spittka/Wybitul* ZD 2016, 120.

351 *Plath/Grages* BDSG/DSGVO, 2. Aufl. 2016, Art. 33 Rn. 1; *Albrecht/Jotzo* Das neue Datenschutzrecht der EU, 2017, S. 93 Rn. 10 ff.

Über die DSGVO als gemeinsame Rechtsgrundlage innerhalb der Europäischen Union wurde seit 2011 im Rahmen eines Trilogs zwischen dem Rat, dem Parlament und der Europäischen Kommission gerungen. Am 14.4.2016 war es dann soweit: Das EU-Parlament nahm die DSGVO an. Am 24.5.2016 ist sie in Kraft getreten. Sie besteht aus Artikeln und einer Reihe Erwägungsgründen, die zur Auslegung der jeweiligen Artikel herangezogen werden können. Die Erwägungsgründe ergänzen sozusagen die gesetzlichen Grundlagen. **307**

Ziel der DSGVO ist es innerhalb der EU ein einheitliches Datenschutzrecht zu schaffen und so u.a. die Wettbewerbsfähigkeit der europäischen Unternehmen im internationalen Umfeld zu verbessern. Zudem gilt das auf der europäischen RL 95/46 EG basierende Datenschutzrecht als veraltet, da es nicht mehr die neuesten technischen Entwicklungen reflektiert. Es wird vollständig durch die DSGVO abgelöst. Durch ein zeitgemäßes Datenschutzrecht sollen die Rechte der Betroffenen, insbesondere deren Kontrolle über ihre eigenen Daten sowohl im Online- als auch im Offline-Bereich gestärkt werden. Weiterhin soll eine möglichst einheitliche Rechtsauslegung durch das sog. One-Stop-Shop-Verfahren gewährleistet werden. Durch einen komplexen Kooperations- und Kohärenzmechanismus soll u.a. die Zusammenarbeit der nationalen Datenschutzaufsichtsbehörden sichergestellt werden und für Unternehmen werden Erleichterungen eingeführt, da sie unter bestimmten Umständen insbesondere als Konzerngruppe mit Tochterunternehmen mit Sitz in verschiedenen Mitgliedsstaaten der EU nur noch eine Aufsichtsbehörde in der EU als Ansprechpartner haben.[352]

Die DSGVO gilt unmittelbar in den Mitgliedsstaaten der EU, so dass grundsätzlich kein nationaler Umsetzungsakt erforderlich ist. Innerstaatliche Rechtsnormen werden verdrängt. In manchen Bereichen – wie z.B. dem Beschäftigtendatenschutz (Art. 88 DSGVO) oder der Bestellung des Datenschutzbeauftragten, (Art. 37 Abs. 4 DSGVO) – kann der nationale Gesetzgeber gleichwohl eigene gesetzliche Grundlagen schaffen. Voraussetzung ist u.a., dass diese die Mindestanforderungen der DSGVO umsetzen. Damit sind die in Deutschland zurzeit geltenden Bundes- und Landesgesetze entsprechend anzupassen bzw. werden ihre Gültigkeit verlieren. **308**

Deutschland hat von dieser Möglichkeit auf Bundesebene bereits Gebrauch gemacht. Am 1.2.2017 hat die Bundesregierung einen „Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die VO (EU) 2016/679 und zur Umsetzung der RL (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)“ vorgelegt, über den im März/April 2017 sowohl der Bundestag als auch der Bundesrat beraten haben und zu dem Sachverständige im Innenausschuss des Bundestags angehört wurden.[353] Am 27.3.2017 gab es zudem eine Anhörung von Sachverständigen im Innenausschuss des Bundestags. Der Bundestag nahm den Gesetzentwurf am 27.4.2017 auf Empfehlung des Innenausschusses[354] und gegen das Votum der Opposition in 2./3. Lesung an. **309**

352 S. zur zuständigen Aufsichtsbehörde das WP 244 der Art. 29-Gruppe, der Zusammenschluss der europäischen Aufsichtsbehörde auf europäischer Ebene; abrufbar unter: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf.

353 Vgl. BT-Drucks. 18/11325, 18/11655, 18/11822 Nr. 10, BR-Drucks. 110/17(B). Am 27.3.2017 gab es zudem eine Anhörung von Sachverständigen im Innenausschuss des Bundestags; siehe auch den Änderungsantrag der Regierungsfraktionen, Ausschussdrucksache 18(4)842).

354 Vgl. BT-Drucks. 18/12084 und 18/12144.

310 Trotz der vielen Kritikpunkte – unter anderem wurde moniert, dass das DSAnpUG den Datenschutz verwässern, den Vorgaben der DSGVO nicht entsprechen und die Harmonisierung des Datenschutzes in der EU konterkarieren würde – hat der Bundesrat im Mai 2017 den Weg für das DSAnpUG freigemacht, so dass es im Mai 2018 in Kraft treten wird.[355] Ob ggf. einige Regelungen durch den Europäischen Gerichtshof als nicht europarechtskonform in der Zukunft für unzulässig erklärt werden, ist zurzeit nicht absehbar. Wann zudem die Landesdatenschutzgesetze oder die bestehenden bereichsspezifischen Vorschriften, die datenschutzrechtliche Vorgaben enthalten, wie z.B. die Melde- oder IHK-Gesetze, angepasst werden, ist noch offen.

311 Viele der Regelungen der DSGVO ähneln dem zurzeit geltenden deutschen Datenschutzrecht; gleichwohl wird sich auch für deutsche Unternehmen erheblicher Änderungsbedarf u.a. bei den bestehenden Prozessen oder auch Dokumentationspflichten ergeben. Nachfolgend wird daher auch ein erster Überblick über wesentliche Inhalte des künftigen Rechts und den möglichen Handlungsbedarf gegeben.

III. Anwendungsbereich des Datenschutzrechts

1. Heutige gesetzliche Grundlagen

312 Das BDSG gilt für Unternehmen der Privatwirtschaft, öffentliche Stellen des Bundes und öffentliche Stellen der Länder soweit diese bspw. Bundesrecht ausführen, § 1 Abs. 2 BDSG. Der Umgang mit personenbezogenen Daten durch öffentliche Stellen der Länder wird nicht durch das BDSG, sondern durch die einzelnen Landesdatenschutzgesetze geregelt, die in diesem Fall vorrangig gelten. Soweit daneben für einzelne Bereiche Spezialgesetze bestehen, sind diese ebenfalls vorrangig zu beachten. Dazu zählen bspw. die Verarbeitung von Daten, die in einem Online-Shop erhoben werden, da hier das Telemediengesetz vorrangig anwendbar ist oder der Umgang mit Sozialdaten, der u.a. in den Sozialgesetzbüchern geregelt ist.[356]

2. Anwendungsbereich der DSGVO

313 Die DSGVO gilt nach Art. 3 für u.a. juristische Personen, Behörden, Auftragsverarbeiter oder deren Niederlassungen mit Sitz in der EU. Es ist dabei unerheblich, wo die Verarbeitung erfolgt; maßgeblich ist der Sitz des Verarbeiters.[357] Zudem findet die DSGVO künftig auch Anwendung, wenn Unternehmen mit Sitz außerhalb der EU europäischen Betroffenen Waren oder Dienstleistungen (auch kostenlos) anbieten oder deren Verhalten beobachten (sog. „Marktortprinzip“).[358] Erstellt daher ein Anbieter mit Sitz in den USA im Internet Profile über Konsumenten für Zwecke der Absatzförderung, muss er die DSGVO beachten. Damit sollen Betroffene mehr Kontrolle über ihre Daten erlangen und es soll sichergestellt werden, dass konkret an EU-Bürger gerichtete Angebote dem europäischen Recht unterliegen (siehe Erwägungsgrund 23).[359]

355 Vgl. BR-Drucks. 332/17.
356 S. dazu: *Bauer* Marketing und Vertrieb in: Rechtshandbuch Onlineshop, 2. Aufl. 2016, 449 ff.
357 Plath/*Plath* BDSG/DSGVO, 2. Aufl. 2016, Art. 3 Rn. 1 ff.
358 Plath/*Plath* BDSG/DSGVO, 2. Aufl. 2016, Art. 3 Rn. 11 ff.
359 Plath/*Plath* BDSG/DSGVO, 2. Aufl. 2016, Art. 3 Rn. 21.

Die DSGVO soll zudem technologieneutral sein und unterscheidet grundsätzlich nicht zwischen dem Online- und dem Offline-Bereich.[360] Allerdings wird zurzeit im Online-Bereich die bereichsspezifische ePrivacy-Richtlinie verhandelt. Hier ist davon auszugehen, dass diese u.a. Anpassungen des zurzeit z.B. für den Umgang mit Daten im World-Wide-Web geltenden Regelungen des Telemediengesetzes („TMG") erfolgen müssen. Bislang hat der deutsche Gesetzgeber jedoch nicht konkret Stellung genommen, auf welche Art und Weise er das nationale Recht anpassen wird, so dass es hier abzuwarten gilt. **314**

3. Personenbezogene Daten

Das BDSG gilt grundsätzlich nur für die Erhebung etc. personenbezogener Daten **natürlicher Personen** (sog. Betroffene). Allerdings vertritt die überwiegende Meinung inzwischen die Auffassung, dass immer dann, wenn Informationen über eine juristische Person einen Rückschluss auf eine natürliche Person zulassen, auch der Anwendungsbereich des BDSG eröffnet sein soll. So kann bspw. aus dem Umstand, dass eine 1-Mann-GmbH insolvent ist, ein Rückschluss auf die Vermögenslage des Gesellschafters gezogen werden.[361] Das gleiche gilt für Ansprechpartner von Unternehmen: Grundsätzlich ist das eine Unternehmen (und damit die juristische Person) zwar der Kunde des anderen Unternehmens; gleichwohl werden die Daten des Ansprechpartners des Kunden (und damit einer natürlichen Person) ebenfalls gespeichert. Diese dürfen nicht ohne weiteres bspw. für Marketingzwecke genutzt werden. **315**

Der Begriff des **Personenbezugs** ist weit zu fassen: Personenbezogene Daten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, z.B. Name, Geburtsdatum, Gehalt, Arbeitgeber, Zeugnisse oder Aktienbesitz.

- „**Bestimmt**" ist eine Person dann, wenn sie in einer Personengruppe eindeutig zu identifizieren ist; in der Regel ist sie durch ihren Namen zu identifizieren. **316**
- „**Bestimmbarkeit**" setzt voraus, dass grundsätzlich die Möglichkeit besteht, die Person zu identifizieren; z.B. dann, wenn der Personenbezug durch eine Kombination von Informationen mit auch nur zufällig vorhandenem Zusatzwissen hergestellt werden kann. Für die Bestimmbarkeit kommt es auf die Möglichkeit der Kenntnisermittlung durch denjenigen, der für die Erhebung etc. der Daten gegenüber dem Betroffenen verantwortlich ist. In der Regel ist dies ein Unternehmen. Innerhalb des Unternehmens muss der Bezug zu dem Betroffenen mit den dort normalerweise zur Verfügung stehenden Hilfsmitteln ohne unverhältnismäßig großen Aufwand hergestellt werden können.[362]

Auch die **DSGVO** gilt für den Umgang mit personenbezogenen Daten natürlicher Personen, d.h. für Daten, die sich auf eine identifizierte oder identifizierbare Person beziehen, Art. 4 Abs. 1 DSGVO. Da die DSGVO sich ausdrücklich nur auf natürliche Personen und nicht – wie heute von einigen deutschen Datenschutzaufsichtsbehörden vertreten – auch auf juristische Personen bezieht, wird hier wohl künftig der Anwendungsbereich limitiert sein.[363] Dies führt zu Erleichterungen im Umgang mit Daten **317**

360 Plath/*Plath* BDSG/DSGVO, 2. Aufl. 2016, Art. 2 Rn. 7.
361 Vgl. *Taeger/Gabel/Buchner* BDSG, 2. Aufl. 2013, § 3 Rn. 8.
362 Vgl. *Gola/Schomerus* BDSG, 12. Aufl. 2015, § 3 Rn. 10.
363 Plath/*Schreiber* BDSG/DSGVO, 2. Aufl. 2016, Art. 4 Rn. 5.

von B2B-Kunden; allerdings ist hier zu berücksichtigen, dass auf Daten von z.B. Ansprechpartnern, die in Customer Relationship Management-Systemen gespeichert werden, die DSGVO sehr wohl Anwendung finden wird. Zudem stellt die DSGVO klar, dass sie sich nur auf die Daten lebender Personen bezieht. Hier kann allerdings der nationale Gesetzgeber abweichende Regelungen treffen (Erwägungsgrund 27).

Personenbezogen sind nach Erwägungsgrund 30 der DGSGVO – neben z.B. dem Namen, der Adresse oder Standortdaten – auch IP-Adressen oder Cookies. Damit wurde klargestellt, dass auch diese dem Anwendungsbereich der DSGVO unterfallen.

318 Identifizierbar sind nach Erwägungsgrund 26 ff. grundsätzlich auch Betroffene, deren Daten **pseudonymisiert** wurden. Im Rahmen der Pseudonymisierung wird das Identifizierungsmerkmal wie z.B. der Name durch ein Kennzeichen ersetzt. Der Schlüssel zur Reidentifizierung wird gesondert aufbewahrt, so dass der verantwortlichen Stelle nur in engen Grenzen eine Reidentifizierung möglich ist. Pseudonymisierte Daten sollen künftig – bis auf wenige enge Ausnahmen – dem Datenschutzrecht unterliegen.[364] Dies ist eine durchaus erhebliche Umstellung zur heutigen Rechtslage nach der pseudonymisierte Daten jedenfalls nach dem BDSG nicht als personenbezogene Daten gelten.[365] Künftig wird dies z.B. zu einem Umdenken bei der Nutzung von Patientendaten führen, die in der Regel pseudonymisiert verarbeitet werden.

4. Besondere personenbezogene Daten

319 Neben den personenbezogenen Daten findet das BDSG auch Anwendung auf die so genannten „**besonderen personenbezogenen Daten**“, die Angaben über die rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Besondere Arten personenbezogener Daten unterliegen bei der Verarbeitung besonderen Schutzvorschriften da ihre Kenntnisnahme etc. besondere Risiken für den Einzelnen birgt.[366]

320 Die DSGVO sieht – im Gegensatz zum BDSG – mit Art. 9 eine eigene Rechtsgrundlage zum Umgang mit besonderen personenbezogenen Daten vor.[367] Zudem erweitert sie den Begriff um „genetische Daten“ und „biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person“.[368]

5. Automatisierte und manuelle Verarbeitung etc. von Daten

321 Das BDSG gilt zunächst für die automatisierte Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten mittels entsprechender IT-Systeme. Verarbeitung umfasst dabei u.a. die Speicherung, Veränderung, Übermittlung, Sperrung und Löschung von Daten. Werden die Daten daneben in einer organisierten Struktur erhoben (bspw. Aktenordner), findet das BDSG ebenfalls Anwendung. Im Bereich des Beschäftigtendatenschutzrechts ist es unerheblich, ob Daten automatisiert oder manuell erhoben etc. werden; hier findet jedenfalls das BDSG Anwendung, § 32 Abs. 1 BDSG.

---

364 A.A. Plath/*Schreiber* BDSG/DSGVO, 2. Aufl. 2016, Art. 4 Rn. 10, 20.

365 Siehe zur Rechtslage nach BDSG und den verschiedenen Ansichten zum Personenbezug von Pseudonymen: *Härting* NJW 2013, 2065.

366 Siehe dazu unten, Rn. 423.

367 Siehe dazu unten Rn. 409, 424 ff.

368 Plath/*Plath* BDSG/DSGVO, 2. Aufl. 2016, Art. 9 Rn. 3 ff.

Der Anwendungsbereich der DSGVO erstreckt sich sowohl auf die automatisierte (d.h. unter Einsatz von IT-Systemen) als auch auf die nicht-automatisierte Verarbeitung (d.h. Daten werden manuell unter Berücksichtigung einer gewissen Systematik in einem Dateisystem abgelegt) von personenbezogenen Daten, Art. 2 DSGVO.[369] Damit unterliegen z.B. der Umgang mit Daten unter Nutzung von HR-Systemen, aber auch die Ablage von Daten in Personalakten, die in Papierform geführt werden, dem Anwendungsbereich der DSGVO. Das BDSG sieht entsprechende Regelungen vor, so dass dies keine wesentliche Änderung zu den bisherigen Regelungen darstellt. **322**

Die DSGVO unterscheidet künftig – im Gegensatz zum BDSG – nicht mehr zwischen z.B. der Erhebung, Verarbeitung und Nutzung von Daten. Der Begriff „Verarbeitung" erfasst sämtlichen Umgang mit Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung, gem. Art. 4 Ziff. 2 DSGVO. **323**

IV. Rollen nach BDSG und DSGVO

1. Verantwortliche Stelle nach BDSG

Gemäß § 3 Abs. 7 BDSG ist jede Person oder Stelle, die personenbezogene Daten für sich selbst, erhebt, verarbeitet oder nutzt bzw. dies durch andere im Auftrag vornehmen lässt, für die Zulässigkeit der Datenerhebung, -verarbeitung oder Nutzung verantwortlich. Sie muss dafür Sorge tragen, dass nicht nur innerhalb des eigenen Unternehmens sondern auch bei dem von ihr ggf. eingesetzten Auftragnehmer die datenschutzrechtlichen Vorgaben eingehalten werden. Die Verantwortung obliegt dabei dem jeweiligen Unternehmen als juristische Person und nicht nur der betrieblichen Einheit, die in der Praxis mit den Daten umgeht.[370] **324**

Daraus leitet sich auch eine besondere Verantwortung der Geschäftsführung des Unternehmens ab: Sie hat dafür Sorge zu tragen, dass im Unternehmen die erforderlichen organisatorischen Strukturen eingeführt werden, die datenschutzrechtliche Compliance sicherstellen. **325**

2. Neue Rollen nach DSGVO

Die DSGVO definiert in Art. 4 Ziff. 7 als „**Verantwortlichen**" jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet.[371] Damit wird der Anwendungsbereich zum Einen u.a. auch auf sämtliche Behörden ausgeweitet und zum Anderen der sog. „**Joint Controller**" (Art. 26 DSGVO) als ein für deutsche Unternehmen neues Instrument eingeführt. Nach Art. 26 DSGVO können künftig zwei Verantwortliche auch gemeinsam Zweck und Mittel im Umgang mit den Daten bestimmen und sind auch gemeinsam haftbar.[372] **326**

369 Plath/*Plath* BDSG/DSGVO, 2. Aufl. 2016, Art. 2 Rn. 5.
370 Vgl. *Simitis/Dammann* BDSG, 8. Aufl. 2014, § 3 Rn. 224 ff.
371 Plath/*Schreiber* BDSG/DSGVO, 2. Aufl. 2016, Art. 4 Rn. 25 ff.
372 Plath/*Plath* BDSG/DSGVO, 2. Aufl. 2016, Art. 27 Rn. 9.

327 Neu ist zudem, dass auch der **Auftragsverarbeiter** (vormals „Auftragsdatenverarbeiter" nach BDSG) neben dem Verantwortlichen haftet: Hier ist in Art. 82 DSGVO explizit vorgesehen, dass auch dieser vom Betroffenen in Anspruch genommen werden kann bzw. gegen diesen – neben dem Verantwortlichen – eigenständig Bußgelder verhängt werden können.[373] Dies ist im Vergleich zum BDSG eine erhebliche Änderung und wird es erforderlich machen, die bis dato bestehenden Verträge mit Auftragsverarbeitern entsprechend anzupassen.[374]

328 Verantwortliche oder Auftragsverarbeiter, die nicht in der EU ihren Sitz haben und auf die die DSGVO nach dem Marktortprinzip Anwendung findet, müssen einen **Vertreter** innerhalb der EU benennen, der als Ansprechpartner und Repräsentant fungiert, Art. 27 DSGVO.[375]

V. Datenschutzrechtliche Pflichten von privaten Unternehmen

329 Datenschutzrechtliche Compliance setzt u.a. die Einhaltung der Vorgaben des Datenschutzrechtsvoraus. In der Praxis sind sich viele Unternehmen dieser Vorgaben nicht bewusst oder haben sie bislang als eher lästigen Bestandteil der IT-Compliance unter technischen Aspekten betrachtet. Durch die Datenschutzskandale der Vergangenheit und nicht zuletzt durch die Einführung der DSGVO beginnt sich dieses Bewusstsein zu ändern: Der Gesetzgeber hat in der Vergangenheit mit Verschärfungen des BDSG reagiert, auf deren Grundlage die deutschen Datenschutzaufsichtsbehörden empfindliche Sanktionen in Form von Geldbußen verhängt und auch ihre Kontrollen von Unternehmen verschärft haben.[376] Zudem drohen auf Grundlage der DSGVO kartellrechtsähnliche Strafen, die zu einem Umdenken führen. Nicht zuletzt beobachtet die Öffentlichkeit mit Argwohn Unternehmen, denen Datenmissbrauch zur Last gelegt wird und entzieht diesen ihr Vertrauen. Datenschutz wird damit zunehmend als Wettbewerbsvorteil im Kampf um Kunden erachtet.

330 Nachfolgend wird ein kurzer Überblick über die wesentlichsten Pflichten gegeben, die von Unternehmen zu erfüllen sind, um datenschutzrechtliche Compliance sicherzustellen.[377] Compliance erfordert dabei ein abgestimmtes Vorgehen zwischen den verschiedensten Stellen im Unternehmen: Der Aufbau einer funktionierenden Datenschutzorganisation stellt Anforderungen an die Geschäftsführung, den Datenschutzbeauftragten, die IT, die Revision und nicht zuletzt an die mit der Datenverarbeitung beschäftigten Mitarbeiter. Insbesondere letztere müssen durch ihr eigenes Verhalten im Umgang mit personenbezogenen Daten sicherstellen, dass im Unternehmen Daten entsprechend den gesetzlichen Vorgaben erhoben etc. werden. Insofern zählt es auch

373 Plath/*Becker* BDSG/DSGVO, 2. Aufl. 2016, Art. 82 Rn. 6.

374 Siehe dazu unten Rn. 455 ff.

375 Plath/*Plath* BDSG/DSGVO, 2. Aufl. 2016, Art. 27 Rn. 1 ff.

376 S. dazu bspw. die Pressemitteilung über den Beschluss des Innenministerium Baden-Württemberg – Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich – v. 11.9.2008, abrufbar unter www.baden-wuerttemberg.de/fm7/2028/Lidl%20%20Bu%DFgeldverfahren%20abgeschlossen. 470204.pdf; s. dazu auch als Beispiel die Tätigkeitsberichte des hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, abrufbar unter www.Datenschutz-hamburg.de/publikationen-taetigkeitsberichte/taetigkeitsberichte.html; s. in diesem Zusammenhang zur Historie der BDSG-Novellen BR-Drucks. 4/09, BT-Drucks. 16/10529, BT-Drucks. 16/12011.

377 Vgl. dazu bspw. *Bauer/Wesselmann* WISU 8-9/08, 1128; *Bauer* Datenschutzpraxis 9/2008, 2.

zu den wesentlichen Pflichten des Unternehmens, Mitarbeiter im Bereich Datenschutz zu sensibilisieren bzw. entsprechende Schulungen durch den Datenschutzbeauftragten durchführen zu lassen.

Ab 2018 wird ein entsprechendes Vorgehen zwingend erforderlich: Nach der DSGVO trifft Unternehmen eine erhöhte **Rechenschaftspflicht (Accountability**), Art. 5 Abs. 2 DSGVO und Art. 24 DSGVO. Verantwortliche i.S.d. DSGVO müssen durch die Vorlage geeigneter Dokumente etc. nachweisen, dass der Umgang mit den Daten im Einklang mit den in Art. 5 DSGVO dargestellten Grundsätzen erfolgt (siehe auch Erwägungsgrund 85). Art. 5 fordert die Einhaltung der datenschutzrechtlichen Prinzipien wie Transparenz, Zweckbindung oder Datenminimierung, die durch die Grundsätze der „Richtigkeit", „Speicherbegrenzung" sowie „Integrität und Vertraulichkeit" ergänzt werden. Zudem ist die verantwortliche Stelle nach Art. 5 Abs. 1 DSGVO explizit verpflichtet, die Rechtmäßigkeit des Umgangs mit den Daten sicherzustellen. Kann sie diesen Nachweis nicht führen, haftet sie z.B. im Fall von Datenschutzverstöße.[378] Im Ergebnis führt die Rechenschaftspflicht zu einer Beweislastumkehr zu Lasten des Verantwortlichen, so dass bereits die fehlerhafte Dokumentation der Einhaltung des Datenschutzrechts zu wirtschaftlichen Folgen für Unternehmen führen kann.[379] Hier sollten Unternehmen ihre Compliance-Organisation um entsprechende geeignete interne Maßnahmen ergänzen. Ein Datenschutzmanagement wird künftig unumgänglich, wenn Compliance sichergestellt werden soll. **331**

1. Formelle Anforderungen

1.1 Bestellung von Datenschutzbeauftragten

1.1.1 Anforderungen nach BDSG

Der Datenschutzbeauftragte ist u.a. für die Kontrolle der Zulässigkeit der Datenverarbeitung im Unternehmen zuständig und gilt als verlängerter Arm der Datenschutzaufsichtsbehörden. Das Unterlassen der Bestellung kann als Ordnungswidrigkeit gem. § 43 Abs. 1 Nr. 2 BDSG geahndet werden.[380] **332**

Ob ein Datenschutzbeauftragter bestellt werden muss,[381] richtet sich entweder **333**

- nach der **Anzahl** der mit der Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten **beschäftigen Personen** im Unternehmen, wobei dazu sämtliche Beschäftigte, die in einem arbeitnehmerähnlichen Status stehen, zählen.[382]

Der Datenschutzbeauftragte ist zu bestellen, sofern das Unternehmen

- **mindestens zehn Personen** wenigstens vorübergehend mit **automatisierter** Datenerhebung, -verarbeitung oder -nutzung beschäftigt (§ 4f Abs. 1 S. 4 BDSG) oder
- **mindestens zwanzig Personen** wenigstens vorübergehend mit **nichtautomatisierter** Datenerhebung, -verarbeitung oder -nutzung beschäftigt (§ 4f Abs. 1 S. 3 BDSG).

---

378 S. dazu auch Plath/*Plath* BDSG/DSGVO, 2. Aufl. 2016, Art. 5 Rn. 3 ff, Rn. 24.

379 Plath/*Becker* BDSG/DSGVO, 2. Aufl. 2016, Art. 82 Rn. 5.

380 Vgl. dazu die Pressemitteilung über den Beschluss des Innenministerium Baden-Württemberg – Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich – v. 11.9.2008, a.a.O., nach der 10 000 EUR als Geldbuße für die Nichtbestellung verhängt wurden.

381 Vgl. zu den seit 2006 geltenden Neuregelungen zusammenfassend *Gola/Klug* NJW 2007, 118 ff.

382 Damit zählen neben Arbeitnehmern u.a. auch Telearbeitnehmer oder an die IT angebundene Handelsvertreter dazu; siehe *Däubler/Klebe/Wedde/Weichert/Däubler* BDSG, 5. Aufl. 2016, § 4f Rn. 15 ff.

oder

– nach der **Art der vorgenommenen Datenverarbeitung**, § 4f BDSG.

Der Datenschutzbeauftragte ist zu bestellen, sofern das Unternehmen

– personenbezogene Daten **geschäftsmäßig** zum Zweck der Übermittlung oder der anonymisierten Übermittlung erhebt, verarbeitet oder nutzt (beispielsweise Auskunfteien, Adressverlage, Markt- und Meinungsforschungsunternehmen; § 4f Abs. 1 S. 6 BDSG) oder
– automatisierte Datenverarbeitungsvorgänge durchführt, die eine **Vorabkontrolle** gem. § 4d Abs. 5 BDSG verlangen (z.B. Systeme zur Bewertung der Kreditwürdigkeit, Einsatz von Videoüberwachung, Einführung von Personalinformationssystemen, die eine Persönlichkeitsüberwachung zulassen,[383] § 4f Abs. 1 S. 6 BDSG).

334 Der Datenschutzbeauftragte ist spätestens **binnen eines Monats** nach Eintritt der obigen Voraussetzungen schriftlich zu bestellen. Es empfiehlt sich, dabei seine Aufgaben klarstellend zu definieren (siehe §§ 4f, 4g BDSG).[384] Bestellt werden können Mitarbeiter aus dem Unternehmen (interne Datenschutzbeauftragte) oder auch externe Dienstleister. Die Bestellung muss nicht gegenüber den Datenschutzaufsichtsbehörden angezeigt werden.

335 Wird ein interner Datenschutzbeauftragter bestellt, ist zu beachten, dass dieser nach § 4f Abs. 3 S. 5 und 6 BDSG einem **besonderen Kündigungsschutz** unterliegt, der dem von Betriebsräten ähnelt. Ziel des Kündigungsschutzes ist es, die Unabhängigkeit des Datenschutzbeauftragten und dessen Weisungsfreiheit gegenüber der verantwortlichen Stelle zu stärken. Das Arbeitsverhältnis eines internen Datenschutzbeauftragten darf danach nur gekündigt werden, wenn dem internen Datenschutzbeauftragten eine Tat zur Last gelegt werden kann, die das Unternehmen zu einer Kündigung aus wichtigem Grund berechtigen würden. Auch die Bestellung darf nur widerrufen werden, wenn entsprechende wichtige Gründe vorliegen (vgl. dazu auch § 626 BGB). Nach seiner Abbestellung gilt sein Kündigungsschutz im Übrigen für die Zeitdauer von einem Jahr weiter. In der Konsequenz ist ein interner Datenschutzbeauftragter kaum kündbar.[385]

336 Als Datenschutzbeauftragter sollte im Übrigen nicht jeder beliebige Mitarbeiter benannt werden; der Datenschutzbeauftragte muss u.a. die notwendige **Sach- und Fachkunde** zur Ausübung der Tätigkeit aufweisen. Dies setzt u.a. die Kenntnis des geltenden Rechts oder auch der Grundlagen der IT-Sicherheit voraus.[386] Die Datenschutzaufsichtsbehörden können die Abberufung ungeeigneter Personen verlangen, § 38 Abs. 5 S. 3 BDSG.

337 Um die Unabhängigkeit des Datenschutzbeauftragten sicherzustellen, sollte kein Mitarbeiter benannt werden, der in **Interessenkonflikte** geraten könnte, wie beispielsweise ein Mitglied der Geschäftsführung, der Leiter der IT, Personalabteilung oder

383 Vgl. *Bergmann/Möhrle/Herb* Datenschutzrecht, 2011, § 4d Rn. 34 ff.; *Simitis/Petri* BDSG, 8. Aufl. 2014, § 4d Rn. 32.

384 Vgl. zum Berufsbild des Datenschutzbeauftragten *LG Ulm* CR 1991, 103, mit Anm. *Ehmann*; *Koch/Haag/Borchardt* Anlagenüberwachung im Umweltrecht – zum Verhältnis von staatlicher Überwachung und Eigenkontrolle, 1998, S. 131 ff.; *Rudolf* NZA 1996, 296 ff.

385 Vgl. *Wagner* DUD 2008, 660 ff.; *BAG* NZA 2011, 1063; insbesondere ist die Bestellung nicht widerrufbar weil bspw. aus Kostengründen ein externer Datenschutzbeauftragter bestellt werden soll.

386 S. dazu die Ausführungen des Berufsverbands der Datenschutzbeauftragten Deutschland e.V.: Das berufliche Leitbild der Datenschutzbeauftragten, abrufbar unter http://bvdnet.eu/wp-content/uploads/2016/12/BeBi_DE_2016.pdf.