# Handbuch Europäisches und deutsches Datenschutzrecht

Bereichsspezifischer Datenschutz in Privatwirtschaft und öffentlichem Sektor

Bearbeitet von
Herausgegeben von Prof. Dr. Louisa Specht, und Dr. Reto Mantz, Dipl.-Inf., Richter am Landgericht, Unter Mitarbeit von Kirsten Bock, Prof. Dr. Benjamin Bodungen, LL.M., Dr. Tobias Born, Dr. Christoffer Bortz, Dr. Sebastian Bretthauer, Dr. Malte Engeler, Dr. Sebastian Golla, Dr. Dennis Heinson, LL.M., Dr. Moritz Hennemann, M.Jur. (Oxford), Dr. Gerd Kiparski, MBA, Dr. Dennis-Kenji Kipker, Dr. Stefan Krätschmer, PD Dr. Bernhard Kreße, LL.M., Prof. Dr. Anne Lauber-Rönsberg, LL.M., Johannes Marosi, Dr. Anne Paschke, Maren Pollmann, Prof. Dr. Jan Dirk Roggenkamp, Elke Sassenberg, Adrian Schneider, Dr. Jan Spittka, Prof. Dr. Eric Steinhauer, Dr. Björn Steinrötter, Dr. Lukas Ströbel, Dr. Mirko Wieczorek, und Tim Wybitul

1. Auflage 2019. Buch. XLII, 788 S. Hardcover (In Leinen)
ISBN 978 3 406 72539 5
Format (B x L): 16,0 x 24,0 cm

**b) Verbot mit Erlaubnisvorbehalt: Gesetzliche Legitimationstatbestände.** In bestimmten Fällen ist die Verarbeitung elektronischer Kommunikationsdaten auch ohne Einwilligung des Endnutzers zulässig. Im Vergleich zur DS-GVO sind die **Erlaubnissätze im KOM-Vorschlag** allerdings sehr **dürftig** ausgefallen. Nachdem das EU-Parlament[117] insoweit ebenfalls einen sehr restriktiven Kurs verfolgt hat, **sprach sich der Rat** mit Vorschlag vom 5. 12. 2017[118] für eine **Annäherung an die DS-GVO** und damit die Einführung „klassischer" Erlaubnistatbestände wie die Vertragserfüllung aus. Eine Abwägungs- bzw. Auffangklausel vergleichbar mit Art. 6 Abs. 1 S. 1 lit. f DS-GVO war hingegen auch hier und bis zuletzt[119] noch kein Thema. 32

**aa) Verarbeitung elektronischer Kommunikationsdaten.** Zu Gunsten von Betreibern elektronischer Kommunikationsnetze sowie -dienste ist die Verarbeitung zulässig, wenn und soweit es für die **Kommunikationsübermittlung** (Art. 6 Abs. 1 lit. a ePrivacy-VO E) bzw. zur **Bewahrung oder Rekonstruktion der Sicherheit der Netze/Dienste** oder zum **Erkennen technischer Defekte/Fehler beim Datentransfer „nötig"**[120] ist (Art. 6 Abs. 1 lit. b ePrivacy-VO E). Welche Dauer insoweit als „nötig" anzusehen ist, bleibt leider offen.[121] Vorstehende Erlaubnissätze stehen für sich exklusiv und sind nicht kumulativ mit den Abs. 2, 3 zu lesen, was sich bereits daran zeigt, dass teilweise unterschiedliche Verpflichtete adressiert sind.[122] Einwilligungen sind insoweit a priori nicht vorgesehen. **Kommunikationsmetadaten** dürfen Dienstebetreiber verarbeiten, wenn und soweit dies insbesondere für die Einhaltung verbindlicher Dienstqualitätsanforderungen, zur Rechnungsstellung, zum Erkennen bzw. Beenden betrügerischer oder missbräuchlicher Nutzungen „nötig"[123] ist (Art. 6 Abs. 2 lit. a, b ePrivacy-VO E). Dabei ist keineswegs klar und damit dem Rechtsanwender letztendlich zunächst über ein trial-and-error-Vorgehen überantwortet, ab wann ein derartiger Missbrauch anzunehmen ist.[124] Der Rat der EU hat hier einige Erlaubnistatbestände ergänzt, etwa für den Fall, dass die Datenverarbeitung notwendig ist, um wichtige Interessen einer natürlichen Person zu schützen oder bestimmte statistische Erhebungen durchführen zu können.[125] Hinsichtlich **Kommunikationsinhalten** bedarf es schließlich stets zwingend der Einwilligung durch den Endnutzer (Art. 6 Abs. 3 ePrivacy-VO E). Etwa bei der M2M-Kommunikation kann die Unterscheidung zwischen Metadatum (Abs. 2) und Inhalt (Abs. 3) durchaus diffizil geraten.[126] 33



**bb) Endeinrichtungen des Endnutzers.** Die Verwendung der Verarbeitungs- und Speicherfunktion einer Endeinrichtung durch jeden anderen als den Endnutzer selbst ist im Grundsatz ebenso rechtswidrig wie die Erhebung von Informationen aus den Endeinrichtungen (auch über deren Soft- und Hardware). Angesprochen sind damit insbesondere 34

[117] EU-Parlament C8–0009/2017, 2017/0003(COD), 56 ff.; dazu kursorisch Spindler WRP 2/2018, Die erste Seite.
[118] Council of the EU 15333/17, 42 ff.
[119] Stand: 12. 6. 2018 unter Berücksichtigung von Council of the EU 8537/18, 51 ff.
[120] Die DS-GVO verwendet in der deutschen Sprachfassung den Begriff „erforderlich" (Art. 6 Abs. 1 S. 1 lit. b-f DS-GVO). In der Sache ergeben sich insofern jedoch keine Unterschiede. Das EU-Parlament hat eine sprachliche Verschärfung beantragt: „technisch zwingend nötig", C8–0009/2017, 2017/0003(COD), 57. Das dürfte faktisch eine erhöhte Darlegungslast für Betreiber nach sich ziehen; Piltz DB 2018, 749 (750).
[121] Kritisch auch Engeler/Felber ZD 2017, 251 (254).
[122] Unsicher insoweit Härting ITRB 2017, 265 (266).
[123] Das EU-Parlament hat eine sprachliche Verschärfung beantragt: „[…] unbedingt nötig ist, für die dazu technisch erforderliche Dauer […]", C8–0009/2017, 2017/0003(COD), 58.
[124] Zutreffend Engeler/Felber ZD 2017, 251 (254): „unerfreulich vage"; ebenso Schmitz ZRP 2017, 172 (173 f.).
[125] Council of the EU 8537/18, 53.
[126] Härting ITRB 2017, 265 (266) bildet das Beispiel der Verbrauchsrohdaten („ein"/„aus") in Smart Homes.

**Cookies bzw. ganz allgemein das Online-Tracking**[127] als Basis zum Erstellen von Nutzerprofilen insbesondere für zielgenaue Werbeschaltungen. Der Regulierungsansatz des vorstehend beschriebenen Art. 8 Abs. 1 ePrivacy-VO E, ein **generelles Verarbeitungsverbot,** das sich insbesondere nicht auf personenbezogene Daten kapriziert, ist damit im Ausgangspunkt denkbar weit. Für den europäischen Normgeber war hier offenbar leitend, dass Zugriffe auf das Endgerät und damit gleichsam Eingriffe in die Endnutzerrechte über den Aufbau moderner Profiling- und Trackingtools[128] bereits über zunächst „unverdächtig" erscheinende Maschinendaten möglich sind, es mithin keineswegs nur um Cookies und IP-Adressen als Datenbasis geht.[129] Festzuhalten bleibt aber, dass der ePrivacy-VO E nicht das gesamte Webtracking, sondern allein die Datenerhebung auf dem Endgerät zum Gegenstand hat.[130]

35 **Ausnahmsweise** kann die Nutzung jener Funktionen bzw. die Informationserhebung **zulässig** geraten, wenn sie für den exklusiven Zweck der **Durchführung eines elektronischen Kommunikationsvorgangs** über ein elektronisches Kommunikationsnetz, für **die Bereitstellung eines vom Endnutzer gewünschten Dienstes der Informationsgesellschaft**[131] oder für die **Messung des Webpublikums**[132] „nötig" ist (Art. 8 Abs. 1 lit. a, c, d ePrivacy-VO E). Letzteres indes nur dann, wenn der Betreiber des vom Endnutzer gewählten Dienstes die Messung vornimmt, was auch dann anzunehmen ist, sofern er mit seinem Dienstleister wiederum einen Auftragsdatenverarbeitungsvertrag geschlossen hat[133] – dies hat der Rat nunmehr klarstellend explizit in den Text aufgenommen.[134] Wer annimmt, dass bei alledem die herrschenden technischen Kommunikationsstandards letztendlich einseitig festlegen, was „nötig" ist (zB Browserfingerprints),[135] scheint ein Stück weit vor technischen Gegebenheiten zu kapitulieren. Es kann für das Recht aber nicht Maßstab sein, was gerade herrschender technischer Standard ist, sondern vielmehr, was technischer Standard sein sollte und dabei technisch machbar und sinnvoll ist. Art. 8 Abs. 1 ePrivacy-VO schreibt bei diesem Verständnis der Norm nicht weniger vor, als die Internetarchitektur im Lichte des Gebots der Datensparsamkeit zu überarbeiten. Bis dahin käme die Teilnahme am Netzverkehr bei konsequenter Verfolgung des vorstehenden Ansatzes aber faktisch zum Erliegen.[136] Eine (eher provisorische, weil keineswegs sämtliche neuralgischen Fälle der Konturierung des Begriffs „nötig" erfassende) Lösung böte eine Lesart des Art. 8 Abs. 1 ePrivacy-VO E, wonach bei Daten, welche durch Internet- und Netzwerkprotokolle vorgeschrieben sind, allein die **Weiterverarbeitung untersagt** ist, wohingegen die **Erstverarbeitung zulässig** bleibt.[137] Eine Folge der hier skizzierten Unsicherheit mag sein, dass Website-, App- und Plattformanbieter sich sicherheitshalber die Einwilligung des Nutzers zu holen versuchen, was in eine Art „Banner-Overload" aus-



[127] Zu Einsatzzwecken und Phasen des Webtracking siehe Schleipfer ZD 2017, 460 (461).
[128] ErwGr 20 S. 3 ePrivacy-VO E: „unerwünschte Verfolgungswerkzeuge wie zB Spyware, Webbugs, versteckte Kennungen und Verfolgungs-Cookies".
[129] Engeler/Felber ZD 2017, 251 (254 f.).
[130] Schleipfer ZD 2017, 460 (464).
[131] Beispiele: Aufruf einer Internetseite, für die ua der Transfer der IP-Adresse, der URL und von Konfigurationsdaten nötig erscheint, s. dazu Schleipfer ZD 2017, 460 (464), Warenkorbfunktion eines Online-Shops, s. dazu Herbrich jurisPR-ITR 23/2017 Anm. 2; kritisch Piltz DB 2018, 749 (751): „völlig unklar".
[132] Beispiel: Webanalyse und Reichweitenmessung, Schleipfer ZD 2017, 460 (464). Beachte auch die weitaus detailliertere Fassung des EU-Parlaments A8–0324/2017 v. 20.10.2017, 63.
[133] Beispiel: Adope Analytics, Google Analytics, INFOnline, Schleipfer ZD 2017, 460 (464). Zum diffizilen Verhältnis des ePrivacy-VO E zu Art. 28 DS-GVO Herbrich jurisPR-ITR 18/2017 Anm. 2; siehe auch Rauer/Ettig ZD 2018, 255 (257).
[134] Council of the EU Examination of the Presidency discussion paper 7207/18 v. 22.3.2018, 14.
[135] So Engeler/Felber ZD 2017, 251 (255).
[136] Engeler/Felber ZD 2017, 251 (255).
[137] IE überzeugend Engeler/Felber ZD 2017, 251 (255).

ufern könnte.[138] Ergänzt hat der Rat der EU einen Erlaubnistatbestand hinsichtlich der Notwendigkeit der Datenverarbeitung mit Blick auf bestimmte Sicherheitsupdates.[139]

Ausnahmsweise ist die Erhebung von solchen Informationen, die Endeinrichtungen zur Verbindung mit anderen Geräten oder Netzanlagen aussenden, dann zulässig, wenn und soweit sie gerade **ausschließlich zum Verbindungsaufbau** erfolgt (Art. 8 Abs. 2 lit. a ePrivacy-VO E). Derlei Informationen dürfen auch dann erhoben werden, wenn in transparenter Weise insbesondere auf die nach Art. 13 DS-GVO verlangten Informationen (ggf. in Kombination mit standardisierten Bildsymbolen) hingewiesen und geeignete technische und organisatorische Maßnahmen („TOMs") nach Art. 32 DS-GVO Anwendung finden (näher Art. 8 Abs. 2 lit. b, Abs. 3, 4 ePrivacy-VO E).[140] Es geht um **M2M-Kommunikation** als Basis für **IoT- und Industrie 4.0-Anwendungsfälle** sowie **Offline-Tracking.**[141] Ob der Entwurf das Offline-Tracking auf diese Weise wirksam zu regulieren vermag, erscheint jedoch nicht nur hinsichtlich der konkreten Umsetzung,[142] sondern ebenso mit Blick auf die im Gegensatz zu den Informationsgeboten datenschutzrechtlicher Provenienz stehenden technischen Realitäten zweifelhaft. Diese Realitäten zeichnen sich eben dadurch aus, über WLAN/Bluetooth in möglichst zuverlässiger und effektiver Weise eine Verbindung aufzubauen.[143] Auch hier bedürfte es zur Umsetzung der Norm daher im Grunde der Umgestaltung der technischen Standards.[144] Ob es insoweit sinnvoll erscheint, in die aktive Einwilligung zu flüchten, welche die Ratsfassung nunmehr (ebenso wie die Informationsgewinnung bei der Notwendigkeit iRv bestimmten statistischen Erhebungen) zulässt,[145] ist fraglich. 36

Der Parlamentsbericht[146] sieht weitere Legitimationstatbestände vor, etwa für die Erfüllung von aus Arbeitsverhältnissen resultierenden Pflichten des Arbeitnehmers. Der Rat[147] hat sich zwischenzeitlich dafür ausgesprochen, dass der Endnutzer regelmäßig über die Verfügbarkeit der Privatsphäre-Einstellungen zu unterrichten ist und die jeweilige Software die Änderungen klar und leicht ermöglicht. 37



**c) Löschungs- und Anonymisierungsgebote.** Werden Kommunikationsdaten nicht mehr benötigt, sieht Art. 7 ePrivacy-VO E weitgehende Löschungs- bzw. Anonymisierungspflichten vor.[148] 38

### 4. Aufsichtsarchitektur und Durchsetzungsmechanismen

Für die mitgliedstaatlichen Aufsichtsbehörden sowie den Europäischen Datenschutzausschuss (EDA) gelten mutatis mutandis weithin die Zuständigkeiten und Befugnisse, welche bereits die DS-GVO vorgibt (→ § 3 Rn. 198 ff.), Art. 18–20 ePrivacy-VO E. Für Deutschland bedeutet das im Ergebnis, dass es zu einem **Zusammenspiel von BNetzA und Datenschutzbehörden** kommt.[149] 39

Der Endnutzer kann die Rechtsbehelfe geltend machen, die dem Betroffenen nach Art. 77 ff. DS-GVO (dazu → § 3 Rn. 236 ff.) zustehen (Art. 21 Abs. 1 ePrivacy-VO). Zusätzlich hat jede durch Verstöße gegen die ePrivacy-VO beeinträchtigte und ein berechtigtes Interesse an der Unterlassung bzw. dem Verbot solcher Verstöße aufweisende natür- 40

[138] Engeler/Felber ZD 2017, 251 (255).
[139] Council of the EU 8537/18, 57.
[140] Die Kommission kann nach Art. 8 Abs. 4 iVm Art. 25 ePrivacy-VO E delegierte Rechtsakte hinsichtlich der standardisierten Bildsymbole erlassen.
[141] Herbrich jurisPR-ITR 23/2017 Anm. 2; vgl. auch Lurtz ZD-Aktuell 2017, 05707.
[142] Wo genau sollen etwa Hinweisschilder angebracht werden, damit diese effektiv wirken?
[143] Engeler/Felber ZD 2017, 251 (255 f.).
[144] Engeler/Felber ZD 2017, 251 (256).
[145] Council of the EU 8537/18, 57.
[146] EU-Parlament A8–0324/2017 v. 20.10.2017, 64 ff.
[147] Council of the EU Examination of the Presidency discussion paper 7207/18 v. 22.3.2018, 16.
[148] Kritisch zu Existenz und Ausgestaltung des Art. 7 ePrivacy-VO E Härting ITRB 2017, 265 (266).
[149] Eingehend Engeler/Felber ZD 2017, 251 (257).

liche oder juristische Person nach Maßgabe von Art. 21 Abs. 2 ePrivacy-VO E das Recht, gerichtlichen Schutz zu erlangen.

41 Die Regeln für Schadensersatz zu Gunsten der Endnutzer (Art. 22 ePrivacy-VO E), für die Verhängung der – auch hier drakonischen – Geldbußen (Art. 23 ePrivacy-VO E) sowie anderer Sanktionen (Art. 24 ePrivacy-VO E) folgen weitgehend denen der DS-GVO (→ § 3 Rn. 236 ff.).[150] **Private enforcement** einerseits und **effektuierte Bußgeldandrohungen** andererseits bilden damit auch im Bereich der elektronischen Kommunikation grundsätzlich ein scharfes Schwert.[151]

42 Weshalb die Kapitel IV und V des Entwurfs explizit Anordnungen bezüglich der Anwendbarkeit bestimmter Normen oder Kapitel der DS-GVO beinhalten anstatt das Zusammenspiel – wie an anderen Stellen – systematisch dem übergeordneten „Einbettungsprinzip" zu überlassen, bleibt an vielen Stellen unklar.

### 5. Unerwünschte Anrufe

43 Die Regelungen insbesondere zu (unerwünschten) Anrufen in den Art. 12–15, ErwGr 27 ff. ePrivacy-VO E bleiben vorliegend ausgespart.[152]

### 6. Direktwerbung

44 Die Vorschrift des Art. 16 ePrivacy-VO E zur „unerbetenen Kommunikation" erfasst sämtliche Formen der Direktwerbung,[153] inklusive des nichtkommerziellen[154] Bereichs.[155] Beispielsweise sind Bewertungsanfragen sowie iBeacons als Direktwerbung zu qualifizieren.[156]

45 Während im Ausgangspunkt die Direktwerbung über elektronische Kommunikationsdienste (traditionell sowie aus dem OTT-Bereich)[157] nur mit Einwilligung des Endnutzers zulässig ist (Abs. 1), gilt für Bestandskunden bei Direktwerbung für ähnliche Produkte/Dienstleistungen lediglich eine Widerspruchslösung (Abs. 2). Wer Direktwerbung qua elektronischer Kommunikationsdienste betreibt, unterliegt nach Art. 16 Abs. 6 ePrivacy-VO E bestimmten Informationspflichten. So muss der Werbecharakter der Nachricht und die Identität desjenigen, in dessen Namen die Übermittlung erfolgt, herausgestrichen[158] sowie darüber informiert werden, wie der Empfänger in einfacher Weise sein Widerrufsrecht bezüglich künftiger Werbenachrichten ausüben kann. Letzteres kann über die Angabe eines Links oder einer gültigen Mail-Adresse erfolgen.[159]

46 Für Direktwerbeanrufe gelten die besonderen Bestimmungen des Art. 16 Abs. 3, 4, 7 ePrivacy-VO E. Siehe allgemein zur Direktwerbung → § 9 Rn. 78 ff.



[150] Beachtung verdient, dass die Mitgliedstaaten die Sanktionen für Verstöße gegen die Art. 12–14, 17 ePrivacy-VO E (Telefonwerbung) selbst festsetzen können (Art. 23 Abs. 4 ePrivacy-VO E).
[151] Zur DS-GVO Steinrötter EWS 2018, 61 (71).
[152] Dazu Herbrich jurisPR-ITR 25/2017 Anm. 2.
[153] Art. 4 Abs. 3 lit. f ePrivacy-VO E: „jede Art der Werbung in schriftlicher oder mündlicher Form, die an einen oder mehrere bestimmte oder bestimmbare Endnutzer elektronischer Kommunikationsdienste gerichtet wird, auch mittels automatischer Anruf- und Kommunikationssysteme mit oder ohne menschliche(r) Beteiligung, mittels E-Mail [Art. 4 Abs. 3 lit. e ePrivacy-VO E], SMS-Nachrichten usw."
[154] Vgl. ErwGr 32 ePrivacy-VO E.
[155] Zu den Auswirkungen auf das UWG Köhler WRP 2017, 1291 (1295 ff.).
[156] Herbrich jurisPR-ITR 25/2017 Anm. 2.
[157] ErwGr 33 ePrivacy-VO E.
[158] ErwGr 34 ePrivacy-VO E.
[159] ErwGr 35, 1 ePrivacy-VO E.

# § 6 Compliance

## Übersicht





**Literatur:**

*Behling,* Die datenschutzrechtliche Compliance-Verantwortung der Geschäftsleitung, ZIP 2017, 697; *Jung,* Datenschutz-(Compliance-)Management-Systeme – Nachweis- und Rechenschaftspflichten nach der DS-GVO, ZD 2018, 208; *Lantwin,* Risikoberuf Datenschutzbeauftragter? Die Haftung nach der neuen DS-GVO, ArbRAktuell 2017, 508; *Veil,* Accountability – Wie weit reicht die Rechenschaftspflicht der DS-GVO, ZD 2018, 9; *Wybitul,* Welche Folgen hat die EU-Datenschutz-Grundverordnung für Compliance?, CCZ 2016, 194.

## I. Einleitung

Bei Betrachtung der umfänglichen Anforderungen der Verordnung haben Unternehmen zu entscheiden, wie diese am effektivsten umgesetzt werden, um eine „DS-GVO Compliance“ im Unternehmen sicherzustellen. Dies kann dadurch erfolgen, dass die Anforderungen in ein bestehendes Compliance-Management-System des Unternehmens integriert werden. Sofern dieses nicht besteht, stellt sich die Frage, ob aufgrund der DS-GVO ein solches System aufzubauen ist. In jedem Fall sollten dabei die wesentlichen Elemente eines Compliance-Management-Systems verstanden werden und darauf aufbauend die Art und Weise, wie diese sich in der DS-GVO als Mindestanforderungen wiederfinden. Zudem ist im Rahmen der praktischen Umsetzung dieser Anforderungen zu überlegen, wie diese strukturiert – idealerweise mittels einer Compliance-Methodik – umgesetzt werden können. 1

Darauf soll in diesem Kapitel detaillierter eingegangen werden, wobei das Thema Compliance unter dem Blickwinkel von Unternehmen betrachtet wird. Die Ausführungen gelten allerdings sinngemäß auch für Behörden.

## II. Allgemeine Compliance-Anforderungen

### 1. Der Begriff der „Compliance"

2 Der Begriff „Compliance" im unternehmerischen, also im betriebswirtschaftlichen Sinne hat sich ursprünglich in der US-Finanzbranche im Zusammenhang mit Risikobereichen im Bankenwesen entwickelt. Aufgrund gesetzlicher Vorgaben für **Banken- und Versicherungen** (→ Rn. 6) sind in der Folge auch in Deutschland in den 1990er Jahren unternehmerische Compliance-Strukturen aufgebaut worden, bis nach der Jahrtausendwende durch Korruptionsaffären das Thema „Compliance" auch außerhalb der Finanzbranche zu einer zentralen Aufgabe für Unternehmen geworden ist.[1] Aufgrund von internationalen Vorgaben[2] und des verstärkten Fokus auf der Verfolgung von Korruption hatten in der Folge auch einzelne europäische Länder ihre Antikorruptionsgesetze verschärft.[3]

Neben den branchenspezifischen Regelungen und der Korruptionsbekämpfung haben Compliance-Aspekte nach der Jahrtausendwende vor allem im Bereich des **Kartellrechts** an Bedeutung gewonnen. Dies nicht zuletzt wegen der hohen Strafen, die Unternehmen im Rahmen des Kartellrechts nicht nur drohen, sondern die auch verhängt wurden, sowohl in Deutschland[4] als auch in Europa[5] als auch in den USA[6]. Insgesamt ist der Begriff der „Compliance" allerdings weiter zu verstehen und umschreibt einfach ausgedrückt die Einhaltung von Normen durch Unternehmen, unabhängig davon ob es sich dabei um gesetzliche oder auch unternehmensinterne Vorschriften handelt.

3 Darüber hinaus ist in den letzten zehn Jahren auch der **Datenschutz** verstärkt zu einem Compliance-Thema geworden, in Deutschland nicht zuletzt ausgelöst durch die in den Jahren 2008–2010 aufgedeckten Datenschutzschutzskandale.[7] Auch wenn die in diesem Zusammenhang verhängten Geldbußen – gemessen an Geldbußen im Bereich des Kartellrechts und der Schwere der Verstöße – verhältnismäßig gering ausfielen,[8] so darf nicht vergessen werden, dass diese Skandale nicht zuletzt auch zu Rücktritten auf höchster Managementebene der Unternehmen geführt haben.[9] In der Folge wurden nicht nur die Datenschutzteams von Unternehmen erheblich aufgewertet, sondern auch – zumindest in Großunternehmen – der Datenschutz als eigenständiger (Rechts-)Bereich im Un-



[1] Im Bereich von Unternehmen ist dabei als prominentestes Beispiel die Korruptionsaffäre bei Siemens in den Jahren 2006–2008 zu nennen.

[2] Siehe dazu innerhalb der EU der „Rahmenbeschluss 2003/568/JI des Rates vom 22.7.2003 zur Bekämpfung der Bestechung im privaten Sektor", abrufbar unter https://db.eurocrim.org/db/de/doc/187.pdf, zuletzt abgerufen am 24.6.2018.

[3] Das bekannteste Beispiel ist der UK Bribery Act von 2010, abrufbar unter http://www.legislation.gov.uk/ukpga/2010/23/contents, zuletzt abgerufen am 24.6.2018; zur Verschärfung der Korruptionsvorschriften in Deutschland siehe das „Gesetz zur Bekämpfung der Korruption",, BGBl I 2025. Neben dem UK Bribery Act wird vor allem das französische „Sapin II Gesetz" vom Dezember 2016 (Law n° 2016–1691 of 9 December 2016) als eines der strengsten Antikorruptionsgesetze weltweit angesehen.

[4] Zur Statistik der vom Bundeskartellamt bis 2016 in Deutschland verhängten Geldbußen siehe https://de.statista.com/statistik/daten/studie/158809/umfrage/vom-bundeskartellamt-verhaengte-bussgelder/, zuletzt abgerufen am 24.6.2018.

[5] Zur Übersicht der von der EU Kommission verhängten Geldbußen siehe http://ec.europa.eu/competition/cartels/statistics/statistics.pdf, zuletzt abgerufen am 24.6.2018.

[6] Zu einer Übersicht des US Justizministeriums zu Strafen, die unter dem Sherman Act verhängt wurden, siehe https://www.justice.gov/atr/sherman-act-violations-yielding-corporate-fine-10-million-or-more, zuletzt abgerufen am 24.6.2018.

[7] Siehe dazu die Datenschutzskandale der Telekom (2008), bei Lidl (2008) und der Deutschen Bahn (2009). Die Jahresangaben in Klammern bezeichnen das Jahr der Aufdeckung der Skandale.

[8] Im Falle der Deutschen Bahn wurde gegen das Unternehmen eine Geldbuße in Höhe von ca. EUR 1,1 Mio. und im Falle von Lidl in Höhe von ca. EUR 1,5 Mio. verhängt. Eine vergleichbar hohe Geldbuße in Höhe von EUR 1,3 Mio. hat im Jahre 2014 auch die Debeka akzeptiert und sich bereit erklärt, zusätzlich mit EUR 600.000 eine Stiftungsprofessur für Datenschutz zu finanzieren. Als Folge der sog Spitzelaffäre der Deutsche Telekom ist ein Abteilungsleiter im Bereich Konzernsicherheit des Unternehmens zu 3 1/2 Jahren Gefängnis verurteilt worden.

[9] Beispiele dafür sind der Vorstandsvorsitzende Hartmut Mehdorn im Falle der Deutschen Bahn und der Deutschlandchef Frank-Michael Mros im Fall von Lidl.

ternehmen entwickelt. Dies führt bereits heute vielfach zu einer Dreiteilung der unternehmerischen Rechtsbereiche in Abteilungen für (allgemeine) Compliance und Datenschutz auf der einen und der klassischen Rechtsabteilung für allgemeine Rechtsthemen auf der anderen Seite. Damit wurde nicht nur der gesetzlich geregelten Unabhängigkeit des Datenschutzbeauftragten und seiner Überwachungsfunktion Rechnung getragen (→ Rn. 8 ff.), sondern auch – im Sinne der allgemeinen Compliance – Interessenkonflikten vorgebeugt. Entsprechende Konflikte können insbesondere bei der fehlenden Trennung zwischen (allgemeinen) Compliance- und Datenschutzabteilungen entstehen, da es zur Kernaufgabe einer Compliance-Organisation gehört, interne Untersuchungen durchzuführen und als Folge davon ggf. in Persönlichkeitsrechte von Mitarbeitern und auch von Externen, wie zB Geschäftspartnern oder Journalisten, einzugreifen.

Dieser Trend dürfte sich durch die DS-GVO verstärken, zum einen, weil durch die Verordnung die Compliance-Anforderungen an Unternehmen erheblich gestiegen sind, zum anderen, weil die Obergrenze für Geldbußen von bisher EUR 300.000 pro Verstoß (§ 43 Abs. 3 BDSG aF) auf bis zu EUR 20 Mio. bzw. 4% des weltweiten Umsatzes erhöht wurde (Art. 83 DS-GVO). 4

### 2. Verantwortung für Compliance im Unternehmen

Die DS-GVO regelt – ebenso wie das bisherige Datenschutzrecht – nicht ausdrücklich, wer im Unternehmen die Verantwortung für die Datenschutz-Compliance trägt. Die Verordnung legt lediglich fest, wie die Verantwortung zwischen dem Verantwortlichen und dem Auftragsverarbeiter als Unternehmen verteilt ist, (→ Rn. 12, 13) sowie dass innerhalb des Unternehmens die Verantwortung nicht beim Datenschutzbeauftragten liegt (→ Rn. 8–11). Die Grundsätze des bisherigen Rechts bleiben dabei weitestgehend unverändert. 5

Mangels einer expliziten Regelung kommen damit auch im Datenschutzrecht die allgemeinen Vorschriften zur Compliance-Verantwortung im Unternehmen zur Anwendung. Die Verantwortung obliegt damit in der AG dem Vorstand und dem Aufsichtsrat aufgrund ihrer allgemeinen Sorgfalts- und Aufsichtspflichten (§§ 93, 111 Abs. 1 AktG, § 130 OWiG) sowie in der GmbH – durch entsprechende Anwendung der aktienrechtlichen Grundsätze – der Geschäftsführung und dem Aufsichtsrat (§§ 43, 52 Abs. 1 GmbHG, § 111 Abs. 1 AktG). Darüber hinaus haftet selbstverständlich auch jeder Mitarbeiter für Pflichtverstöße im Rahmen seines Arbeitsverhältnisses und seiner Verantwortlichkeit im Unternehmen (zur Verantwortung des Datenschutzbeauftragten → Rn. 11).



### 3. Compliance-Pflichten und Compliance-Management-System

Im Rahmen der vorgenannten Sorgfalts- und Aufsichtspflichten stellt sich insofern die Frage, was die Geschäftsleitung allgemein – also unabhängig von den Vorschriften der DS-GVO – zu unternehmen hat, um die Compliance im Unternehmen sicherzustellen. Dabei ist insbesondere zu klären, ob und in welchem Umfang eine Compliance-Organisation und ein Compliance-Management-System einzurichten sind. 6

Aus den vorgenannten Vorschriften des **Gesellschafts- und Ordnungswidrigkeitenrechts** allein lässt sich noch nicht ableiten, dass Unternehmen ein Compliance-Management-System errichten müssen. Aufgrund ihrer Sorgfaltspflicht sind Unternehmen allerdings in jedem Fall verpflichtet, Rechtsverstöße zu verhindern und zu verfolgen (Legalitätskontrolle).[10] Die Frage, wie sie dieser Verpflichtung nachkommen, liegt grundsätzlich im Ermessen der Geschäftsleitung. Je nachdem, welchen Compliance-Risiken das Unternehmen ausgesetzt ist (zB aufgrund seiner Größe oder seines Geschäfts-

[10] Siehe dazu Behling ZIP 2017, 698.

modells),[11] kann sich dieses Ermessen jedoch auf Null reduzieren und zu einer Pflicht zur Einrichtung eines Compliance-Management-Systems führen. Ein Überwachungssystem ist jedoch zumindest dann einzurichten, soweit der Fortbestand des Unternehmens gefährdet ist (§ 91 Abs. 2 AktG). Auf Grund der Höhe der iRd DS-GVO drohenden Geldbußen kann diese Schwelle seit Inkrafttreten der Verordnung deutlich schneller überschritten werden.

Darüber hinaus sind Unternehmen selbstverständlich verpflichtet, ein angemessenes Risikomanagement zu implementieren, soweit dies **gesetzlich vorgeschrieben** ist, wie im Bereich der Finanz- und Versicherungsbranche (§ 25a KWG für Kredit- und Finanzdienstleister, §§ 23–34 VAG für Versicherungen).[12] Diese gesetzlichen Regelungen bestätigen jedoch im Umkehrschluss, dass eine entsprechende Pflicht nicht für Unternehmen aller Größen und Branchen besteht. Unternehmen haben daher im Einzelfall zu bewerten, ob unter Berücksichtigung der Unternehmensstruktur, des Geschäftsmodell oder weiterer Risikokriterien – wie zB der Häufung von Rechtsverletzungen in der Vergangenheit – der Pflicht zur Verfolgung von Rechtsverletzung auf andere Weise nachgekommen werden kann als durch die Einrichtung eines unternehmensinternen Compliance-Management-Systems. Davon unberührt bleibt die Möglichkeit für Unternehmen, sich zur Einrichtung eines Compliance-Management-System zu verpflichten[13] und dieses gegebenenfalls auch zertifizieren zu lassen.[14]

7 Die **wesentlichen Elemente eines Compliance-Management-Systems** können dabei vereinfacht wie folgt beschrieben werden:

- Organisationspflicht:
  Ziel der Organisationspflicht ist es, unternehmensinterne Strukturen und Prozesse zu schaffen, um damit Regelverstöße zu verhindern. Dazu gehören ein Compliance-Regelwerk (interne Richtlinien), eine Compliance-Governance (Compliance-Organisation) sowie die Auswahl von Mitarbeitern, Geschäftspartnern und Lieferanten unter Compliance-Gesichtspunkten, also im Hinblick auf ausreichende Verlässlichkeit und Qualifikation. Basierend darauf sind Unternehmensprozesse auf Compliance-Risiken zu überprüfen und entsprechend ihrer Risiken zu gestalten.
- Informationspflicht:
  Ziel der Informationspflicht ist es, eine Compliance-Kultur zu schaffen („Tone from the Top") und Mitarbeiter im Hinblick auf Compliance-Regeln zu schulen. Zudem müssen Mitarbeiter die Möglichkeit haben, sich selbst über diese Regeln zu informieren (Intranet, Hotline etc).
- Überprüfungspflicht:
  Ziel der Überprüfungspflicht ist es, die Wirksamkeit der Compliance-Organisation sowie die Einhaltung der Normen durch unternehmensinterne Prozesse auch fortlau-

[11] Zu den Kriterien bei der Frage der Ausgestaltung eines Compliance-Management-Systems siehe § 25a KWG: „Die Ausgestaltung des Risikomanagements hängt von Art, Umfang, Komplexität und Risikogehalt der Geschäftstätigkeit ab."

[12] Im Bereich des Versicherungswesens wurde zur Umsetzung der Solvency-II-Richtlinie die bisherige Regelung des § 64a VAG aF mit Wirkung zum 1.1.2016 durch einen neuen Abschnitt des VAG zur Geschäftsorganisation ersetzt (§§ 23–34 VAG). Zur vorgenannten Richtlinie 2009/138/EG vom 25.11.2009 betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II) siehe ABl. EU 2009 L 335, 1.

[13] Siehe dazu den Deutschen Corporate Governance Kodex (abgekürzt DCGK) als „Best Practice" für börsennotierte Unternehmen, in dessen Ziffer 4.1.3 sich Unternehmen zur Einrichtung eines Compliance-Management-Systems verpflichten. Zum DCGK siehe http://www.dcgk.de/de/, zuletzt abgerufen am 24.6.2018.

[14] Siehe dazu die im Jahre 2011 vom IDW bzw. dem TÜV veröffentlichten nationalen Compliance-Management-Systems-Standards IDW PS 980 und TR CMS 101:2011 (TÜV). Als internationale Standards wurde im Dezember 2014 der ISO 19600 Standard für Compliance-Management-Systeme im Allgemeinen sowie im Oktober 2016 der ISO 37001 für Antikorruption-Systeme im Speziellen verabschiedet. Zu den Standards sa Jung ZD 2018, 210 f.