Kommunikation & Recht

Praxisleitfaden

Tim Wybitul

# EU-Datenschutz-Grundverordnung im Unternehmen

mit Abdruck der DSGVO

dfv Mediengruppe

R&W Fachmedien Recht und Wirtschaft

Praxisleitfaden

# EU-Datenschutz-Grundverordnung im Unternehmen

von

Tim Wybitul

Rechtsanwalt, Frankfurt a. M.

unter Mitwirkung von

Jana Bruns,
Dr. Lukas Ströbel,
Lukas von Gierke

Rechtsreferendare, Frankfurt a. M.

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | 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.de abrufbar.

ISBN 978-3-8005-1634-6

dfv Mediengruppe



Satzkonvertierung: Lichtsatz Michael Glaese GmbH, 69502 Hemsbach

Druck und Verarbeitung: WIRmachenDRUCK GmbH, Mühlbachstraße 7, 71522 Backnang

Printed in Germany

# Vorwort von Jan Philipp Albrecht, MdEP*

Mit der Datenschutz-Grundverordnung der Europäischen Union ist im Frühjahr 2016 nicht nur eine umfassende EU-weit einheitliche Neuregelung des Datenschutzrechts verabschiedet worden. In schwierigen politischen Zeiten in Europa und der Welt ist sie ein wichtiger Schritt in eine globalisierte und digitalisierte Lebens- und Marktrealität, die uns alle bereits heute umgibt. Die rasante Vernetzung und die umfassende Digitalisierung in allen Wirtschaftszweigen stellen dabei nicht nur eine große Chance für Innovation und Wachstum dar. Sie werfen auch grundlegende Fragen der Regulierung in einem immer stärker grenzüberschreitend funktionierenden Markt auf. Die fragmentierte Rechtslage im digitalen Markt sorgt dabei nicht nur für Bürokratiekosten und Rechtsunsicherheit auf Seiten der Unternehmen. Auch Verbraucherinnen und Verbraucher verlieren zunehmend das Vertrauen in die Gültigkeit und Durchsetzbarkeit ihrer Rechte und Interessen. Dieser Vertrauensverlust trifft alle Marktteilnehmer, auch jene, die bereits heute einen hohen Standard befolgen. Dies gilt insbesondere beim Datenschutz, dem im Leben der Menschen eine immer größere Bedeutung zukommt. An der Schwelle zur Kompletterfassung ihres Alltags wollen sie darauf vertrauen können, dass ihre persönlichen Daten nicht zweckentfremdet werden oder zu einer negativen Ungleichbehandlung führen. Es ist daher entscheidend, dass alle Unternehmen in Zukunft den gleichen Regelsatz zum Datenschutz auf dem Binnenmarkt der EU befolgen und je nach ihrer wirtschaftlichen Bedeutung auch mit entsprechend scharfen Sanktionen bei Regelverletzungen rechnen müssen. Und zwar ganz gleich, wo ein Unternehmen seinen Sitz hat.

Immer häufiger sorgt das bisherige, fragmentierte Datenschutzrecht auch für Wettbewerbsverzerrungen. Können oder wollen doch nicht alle Unternehmen von heute auf morgen ihren Unternehmenssitz nach Irland oder Großbritannien verlegen, wo der Datenschutz lockerer geregelt und die Aufsichtsbehörden zurückhaltender sind. Hiermit wird die Datenschutz-Grundverordnung nun Schluss machen. Sie sorgt nicht nur für einheitliche unmittelbar anwendbare Bestimmungen zum Datenschutz, sondern schafft auch einen vollständig neuen Durchsetzungsmechanismus. Künftig werden die Aufsichtsbehörden aller EU-Mitgliedstaaten gemeinsam über grenzübergreifende (Streit-)Fragen des Datenschutzrechts entscheiden. Vor allem bei der Durchsetzung des Datenschutzes wird hierdurch eine höhere Kohärenz und Rechtssicherheit im gesamten Binnenmarkt der EU geschaffen. Das ist der große Erfolg der Neuregelung, die ohne Zweifel auch ein Kompromiss war. Denn 28 noch immer unterschiedliche

* Verhandlungsführer des Europäischen Parlaments für die Datenschutz-Grundverordnung.

Rechtsordnungen und -kulturen durch einen einheitlichen, verbindlichen Rechtskatalog – sowohl bei den Rechten und Pflichten zum Datenschutz als auch bei der Durchsetzung durch Behörden und Gerichte – zu ersetzen, ist eine Mammutaufgabe und erfordert von allen Beteiligten, dass sie sich von ihrem gewohnten Umfeld lösen und auf ein komplett neues Terrain einlassen müssen. Dementsprechend wird die Datenschutz-Grundverordnung auch für den Anwender – also insbesondere für die Unternehmen – neues Terrain sein. Sie sind im Zuge des Verantwortlichkeitsprinzips erster Adressat der neuen Datenschutzregeln. Hierfür werden sie Orientierung brauchen. Genau diese bringt ihnen auf kompakte und verständliche Weise das vorliegende Buch als Einführung und Praxisleitfaden.

Es wird nun von entscheidender Bedeutung für den Erfolg eines Unternehmens im digitalen Markt der Zukunft sein, dass es sich zügig und umfassend auf die neuen Datenschutzregeln der EU einstellt. Als größter gemeinsamer Binnenmarkt der Welt wird die Europäische Union ihre über Jahre gewachsenen Vorstellungen des Datenschutzes auch im globalen Marktumfeld durchsetzen wollen und können. Sie setzt damit aus Sicht der Verbraucherinnen und Verbraucher, aber auch im Sinne ihrer eigenen digitalen Wirtschaft einen Datenschutz-Goldstandard für den Weltmarkt. Wer diesen bereits jetzt ins Zentrum seiner unternehmerischen Grundsätze rückt und auf einen starken Datenschutz im Unternehmen als Wettbewerbsfaktor baut, wird bereits in wenigen Jahren zur Spitzengruppe im digitalisierten Markt der Zukunft gehören. Denn Datenschutz und Innovation schließen sich keineswegs aus: Sie sind auf absehbare Zeit zwei Seiten derselben Medaille. Schon heute findet ein Wettlauf um neue Technologien statt, die einen starken Datenschutz und ein hohes Maß an Verbraucherkontrolle mit den Möglichkeiten von Big Data-Anwendungen und dem Internet der Dinge verknüpfen. Der Datenschutz gehört mit der neuen EU-Verordnung nicht nur wegen der drohenden, hohen Sanktionen ins Kerngeschäft des Unternehmensmanagements. Er wird – auch durch die gestärkte Rolle des Verbrauchers beim Datenschutz – zukünftig ein entscheidender Marktfaktor werden. Die neuen Regeln sind dabei keine Belastung. Unnötige Bürokratie wie die Vorabkontrolle wird durch sie abgeschafft und aus 28 unterschiedlichen Regeln im selben Markt wird ein einziger Standard. Es ist also genau das Gegenteil: Die Datenschutz-Grundverordnung ist eine große Chance für Unternehmen, sich im digitalisierten Markt von morgen zu positionieren.

Hamburg/Brüssel, den 11.8.2016

*Jan Philipp Albrecht, MdEP*

# Inhaltsverzeichnis und Gliederung

# Abkürzungsverzeichnis

| | |
|---|---|
| Abl. | Amtsblatt |
| Abs. | Absatz |
| ADV | Auftragsdatenverarbeitung |
| a. E. | am Ende |
| AEUV | Vertrag über die Arbeitsweise der europäischen Union |
| a. G. | auf Gegenseitigkeit |
| AG | Aktiengesellschaft |
| AGB | allgemeine Geschäftsbedingungen |
| AO | Abgabenordnung |
| Art. | Artikel |
| Aufl. | Auflage |
| BAG | Bundesarbeitsgericht |
| BB | Betriebsberater (Zeitschrift) |
| BCM | Business Continuity Management (englisch, = Betriebliches Kontinuitätsmanagement) |
| BCR | Binding Corporate Rule (englisch, = Verbindliche Unternehmensregel) |
| BDSG | Bundesdatenschutzgesetz |
| BEM | Betriebliches Eingliederungsmanagement |
| BetrVG | Betriebsverfassungsgesetz |
| BGB | Bürgerliches Gesetzbuch |
| BGH | Bundesgerichtshof |
| BKM | Betriebliches Kontinuitätsmanagement |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| BT-Drucks. | Bundestagsdrucksache |
| BZRG | Bundeszentralregistergesetz |
| Bzw. | beziehungsweise |
| C2C | Controller-to-Controller (englisch, = Verantwortlicher zu Verantwortlichem) |
| C2P | Controller-to-Processor (englisch, = Verantwortlicher zu Verarbeiter) |
| CB | Compliance Berater (Zeitschrift) |
| CERT | Computer Emergency Response Team (englisch, = Informationssicherheit-Krisenreaktionsteam |
| CMS | Compliance Management System |
| DB | Der Betrieb (Zeitschrift) |
| d. h. | das heißt |
| DIN | Deutsche Industrie Normen ? |

| | |
|---|---|
| DLP | data loss leakage (detection and) prevention (englisch, = Datenverlustprävention) |
| DMS | Datenschutz Management System |
| DÖV | Die Öffentliche Verwaltung (Zeitschrift) |
| DPA 1998 | Data Protection Act 1998 |
| DPMS | (data) privacy management system (englisch, = Datenschutz Management System) |
| Dr. | Doktor |
| DSB | Datenschutzbeauftragter |
| DSGVO | Datenschutzgrundverordnung |
| DViA | Auftragsdatenverarbeitung |
| EFTA | Europäische Freihandelsassoziation |
| EG | Europäische Gemeinschaft |
| EGMR | Europäischer Gerichtshof für Menschenrechte |
| Engl. | Englisch |
| EU | Europäische Union |
| EuGH | Europäischer Gerichtshof |
| EuZW | Europäische Zeitschrift für Wirtschaftsrecht |
| evtl. | eventuell |
| EWR | Europäischer Wirtschaftsraum |
| f. | folgend |
| ff. | folgende |
| FISA | Foreign Intelligence Surveillance Act (englisch, = Gesetz zur Überwachung in der Auslandsaufklärung) |
| FTC | Federal Trade Commission (englisch, = Bundeshandelskommission) |
| GG | Grundgesetz |
| ggf. | gegebenenfalls |
| GmbH | Gesellschaft mit beschränkter Haftung |
| HaagBewÜbK | Haager Beweisüberkommen |
| HGB | Handelsgesetzbuch |
| Hrsg. | Herausgeber |
| i. S. d. | im Sinne des/der |
| i. V. m. | in Verbindung mit |
| ICC | International Chambers of Commerce (englisch, = internationale Handelskammer) |
| IDW | Institut der Wirtschaftsprüfer in Deutschland |
| IKT | Informations- und Kommunikationstechnologie |
| IP | Internetprotokoll |
| ISO | Internationale Organisation für Normierung |
| IT | Informationtechnik |
| KVP | Kontinuierlicher Verbesserungsprozess |
| LAG | Landesarbeitsgericht |

| | |
|---|---|
| lit. | litera (lateinisch, = Buchstabe) |
| LLP | Limited Liability Partnership |
| NJW | Neue Juristische Wochenschrift (Zeitschrift) |
| Nr. | Nummer |
| NVwZ | Neue Zeitschrift für Verwaltungsrecht |
| NZA | Neue Zeitschrift für Arbeitsrecht |
| OECD | Organisation für wirtschaftliche Zusammenarbeit und Entwicklung |
| OWiG | Ordnungswidrigkeitengesetz |
| PERT | Privacy Emergency Response Team (englisch, = Datenschutz-Krisenreaktionsteam) |
| PIA | Privacy Impact Assessment (englisch, = Datenschutz-Folgenabschätzung) |
| PKPI | Privacy Key Performance Indicators (englisch, = Datenschutzleistungskennzahlen) |
| PKRI | Privacy Key Risk Indicators (englisch, = Datenschutzrisikoindikatoren) |
| PM | Pressemitteilung |
| PRE | Privacy Risk Exposure (englisch, = Datenschutzgefährdungsmaßstab) |
| PS | Prüfungsstandard (z. B. des IDW) |
| RDV | Recht der Datenverarbeitung (Zeitschrift) |
| RL | Richtlinie |
| Rn. | Randnummer |
| ROI | Return of Investment (englisch, = Kapitalrendite) |
| ROPI | return on (Privacy) Investments (englisch, = Rentabilität der Datenschutzinvestitionen) |
| ROSI | Returns on Security Investments (englisch, = Rentabilität der Sicherheitsinvestitionen) |
| Rs. | Rechtssache |
| S. | Seite |
| SCC | EU Standard Contractual Clauses (englisch, = EU-Standardvertragsklauseln) |
| SLA | Service Level Agreement (englisch, = Dienstgütevereinbarung) |
| sog. | sogenannt |
| StGB | Strafgesetzbuch |
| TKG | Telekommunikationsgesetz |
| TOM | technische und organisatorische Maßnahmen |
| u. U. | unter Umständen |
| UAbs. | Unterabsatz |
| Urt. | Urteil |
| US | United States (of America) |

| | |
|---|---|
| USA | United States of America (englisch, = Vereinigte Staaten von Amerika) |
| v. | von/vom |
| Vgl. | Vergleiche |
| VIP | Very important persons (englisch, = sehr wichtige Personen) |
| WP | working papers |
| z. B. | zum Beispiel |
| ZD | Zeitschrift für Datenschutz |
| ZD-Aktuell | Newsdienst. ZD aktuell |

# Einleitung

Ab dem 25.5.2018 regelt die Datenschutz-Grundverordnung (DSGVO)[1] die Verarbeitung personenbezogener Daten einheitlich für die gesamte Europäische Union. Das neue europäische Datenschutzrecht bringt eine Reihe neuer Anforderungen mit sich. Viele Unternehmen haben erkannt, dass die verbleibende Zeit bis zur verbindlichen Anwendung der DSGVO eher knapp bemessen ist, und haben damit begonnen, erste Schritte zur Umsetzung der Vorgaben der Verordnung einzuführen. Dieses Buch fasst bisherige Erfahrungen aus der Implementierung der Verordnung[2] bei einer Reihe von Wirtschaftsunternehmen zusammen. Es beschreibt die für Unternehmen relevanten Anforderungen des Datenschutzes an die Verarbeitung personenbezogener Daten in klarer und einfacher Sprache. Zur besseren Verständlichkeit bietet das Buch viele Beispiele, Schaubilder und Praxistipps. Dabei werden viele in der DSGVO vorgesehene Prozesse und Strukturen durch Checklisten oder Ablaufpläne anschaulich beschrieben. Ein abschließender Teil dieses Buches beschreibt die erforderlichen Projektschritte zur Umsetzung der Vorgaben der DSGVO und fasst diese Planungsschritte in Form einer Checkliste zusammen. Das Buch enthält auch einen Praktiker-Glossar zur DSGVO, der anhand von Stichworten wichtige Begriffe und Zusammenhänge aus der Datenschutz-Praxis erläutert. Dabei werden auch Besonderheiten beziehungsweise Veränderungen durch die DSGVO beschrieben. Die praktische Arbeit mit dem vorliegenden Buch soll dadurch weiter erleichtert werden, dass auch die Artikel der Verordnung abgedruckt sind. Der Leser kann einzelne Vorschriften der DSGVO so nachschlagen, ohne ein weiteres Buch zur Hand nehmen zu müssen. Auf den Abdruck der Erwägungsgründe wird dagegen aus Platzgründen verzichtet. Teilweise werden für die Praxis wichtige Passagen aus den Erwägungsgründen allerdings in den Fußnoten wiedergegeben, sofern dies für die Anwendung der Verordnung hilfreich ist. **1**

Die vorliegende Einführung in den kommenden EU-Datenschutz ist eine an den Bedürfnissen der Wirtschaft orientierte Gebrauchsanweisung für einen einfachen Einstieg in die DSGVO – und für die praktische Umsetzung der Anfor- **2**

1 Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) im Amtsblatt der Europäischen Union, Abl. L 119/1.

2 Soweit in diesem Buch von der „Verordnung" die Rede ist, bezieht sich dies ebenso wie die Abkürzung „DSGVO" auf die Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) im Amtsblatt der Europäischen Union, Abl. L 119/1.

derungen des neuen Datenschutzrechts. Dieses Buch soll dem Leser einen unkomplizierten Überblick über die ab Mai 2018 geltende EU-Verordnung zum Datenschutz geben. Es richtet sich an den Praktiker im Unternehmen und verzichtet dabei bewusst auf eine wissenschaftliche Bewertung der Regelungskomplexe der Verordnung. Für die Praxis wichtige Fragen wie die Auswirkungen des zwischen der EU-Kommission und den USA vereinbarten Privacy Shield oder die datenschutzrechtlichen Folgen des Brexit werden in knapper Form dargestellt.

**3** Diese Einführung enthält Checklisten, Beispiele, Ablaufpläne, Schaubilder und Praxistipps, die die konkrete Anwendung des neuen Datenschutzrechts erleichtern. Dabei steht die praktische Umsetzung der DSGVO im Unternehmen im Vordergrund.

**4** Dieses Buch ist nicht allein das Ergebnis meiner eigenen Arbeit. Auch Jana Bruns, Dr. Lukas Ströbel und Lukas von Gierke, alle Hogan Lovells International LLP, haben daran intensiv mitgewirkt. Daher möchte ich ihnen, aber auch Dr. Wolf-Tassilo Böhm, Marlien Telöken und vielen anderen Anwälten des deutschen Arbeitsrechtsteams und auch des globalen Datenschutzteams unserer Sozietät danken. Sie haben mich mit Rat und wertvollen Anregungen unterstützt. Insbesondere der stetige Austausch mit meinen Partnern Harriet Pearson, Christopher Wolf, Eduardo Ustaran, Julie Brill, Tim Tobin, Winston Maxwell und Scott Loughlin war bei der täglichen Arbeit im internationalen Datenschutz enorm hilfreich. Dr. Jyn Schultze-Melling und Thorsten Sörup danke ich für ihre Mitarbeit an dem Praktiker-Glossar und den stets wertvollen Austausch und Rat zu aktuellen Fragen des Datenschutzes. Auch Dr. Stefan Brink, Philipp Zikesch und Dr. Oliver Draf haben wertvolle Denkanstöße und Ideen beigesteuert. Gerade Dr. Oliver Draf und Juliane Kraska verdanke ich auch ausgesprochen hilfreiche Hinweise zur Planung von Implementierung von Umsetzungsprojekten zur DSGVO. Abschließend danke ich Frau Anja Eiserfey für die professionelle, geduldige und unermüdliche Koordination unserer Arbeit an diesem Buch.

# I. Ziele, Umsetzung und Anwendung der DSGVO

Am 4.5.2016 veröffentlichte die Europäische Union (EU) die Endfassung der seit 2012 verhandelten DSGVO.[3] Sie gilt nach einer gut zweijährigen Übergangsfrist ab dem 25.5.2018 und hebt die Richtlinie 95/46/EG[4] (Datenschutzrichtlinie) auf.[5] Die DSGVO wirkt dann in der gesamten Europäischen Union unmittelbar und direkt. Anders als bei einer EU-Richtlinie ist eine Umsetzung in das nationale Recht der Mitgliedstaaten nicht mehr erforderlich. Dies soll zu einer erheblichen Vereinheitlichung beim Datenschutz in der EU führen und einheitliche Wirtschaftsbedingungen schaffen, die den Binnenmarkt stärken sollen.[6] **5**

Für Unternehmen hat die Verordnung[7] gravierende Folgen: Neben Schadensersatzklagen drohen bei Fehlern Bußgelder von bis zu vier Prozent des globalen (Konzern-)Umsatzes. Beteiligte Manager, Datenschützer und sonstige Entscheidungsträger müssen bei Verstößen mit Geldbußen bis zu 20 Millionen Euro rechnen. Zudem sind die inhaltlichen Anforderungen beim neuen Datenschutz sehr hoch. Sie betreffen viele Unternehmensbereiche, etwa IT, Personal, Compliance, interne Revision und Vertrieb. **6**

Dieser Teil des Buches zeigt, welche Ziele der EU-Gesetzgeber mit der Einführung der DSGVO verfolgt. Es beschreibt zudem, für welche Anwendungsfälle das neue Datenschutzrecht gilt. Der Schwerpunkt liegt dabei auf der Frage, bei welchen Datenverarbeitungen Unternehmen[8] die Vorgaben der Verordnung beachten müssen. **7**

---

3 Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) im Amtsblatt der Europäischen Union, Abl. L 119/1.

4 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

5 Art. 94 Abs. 1 DSGVO.

6 Vgl. Erwägungsgrund 7.

7 Soweit in der vorliegenden Einführung die Begriffe „Verordnung" oder „DSGVO" in Bezug genommen werden, bezieht sich dies auf die deutsche Endfassung der EU-Datenschutz-Grundverordnung, abrufbar etwa unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

8 Vgl. zum Begriff des Unternehmens Art. 4 Nr. 18 DSGVO.

### 1. Ziele der Verordnung

**8** Die Verordnung soll das Datenschutzrecht EU-weit vereinheitlichen.[9] Das Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung ihrer personenbezogenen Daten soll in der gesamten Union gleichmäßig hoch und einheitlich sein.[10] Die Anwendung einer einzigen EU-Verordnung zum Datenschutz soll es Unternehmen ermöglichen, die Datenverarbeitung in allen 28 Mitgliedstaaten gleich zu regeln. Diese Vereinheitlichung soll auch den Binnenmarkt in der Union stärken.[11]

**9** Allerdings enthält die Verordnung auch eine Reihe von sogenannten „Öffnungsklauseln". Diese Vorschriften erlauben es den Mitgliedstaaten, in gewissen Umfang für einzelne Datenverarbeitungen oder Anforderungen nationale Spezialgesetze zu schaffen, etwa beim Beschäftigtendatenschutz gemäß Art. 88 DSGVO. Dabei legt Erwägungsgrund 155 fest, dass diese Öffnungsklausel es den Mitgliedstaaten vor allem erlaubt, Vorschriften über die Bedingungen vorzusehen, unter denen personenbezogene Daten im Beschäftigungsverhältnis auf der Einwilligung[12] eines Beschäftigten verarbeitet werden dürfen.[13]

**10** Solche Ausnahmevorschriften müssen aber den grundsätzlichen Vorgaben der DSGVO entsprechen.[14] Im Ergebnis beschränken die Öffnungsklauseln das Maß an EU-weiter Vereinheitlichung. Daher bleibt in vielen Bereichen abzuwarten, ob und in welcher Form die Mitgliedstaaten nationale Regelungen zum Beschäftigtendatenschutz erlassen werden – und welchen Spielraum der Europäische Gerichtshof (EuGH) ihnen hierfür letztlich zubilligen wird.[15] Allerdings legt Erwägungsgrund 8 nahe, dass einzelstaatliche Regelungen nur in eingeschränktem Umfang möglich sind: „Wenn in dieser Verordnung Präzisierungen oder Einschränkungen ihrer Vorschriften durch das Recht der Mitgliedstaaten vorgesehen sind, können die Mitgliedstaaten Teile dieser Verordnung in ihr nationales Recht aufnehmen, soweit dies erforderlich ist, um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen."

---

9 Vgl. Erwägungsgründe 10 ff.
10 Vgl. Erwägungsgrund 10.
11 Vgl. Erwägungsgründe 2 und 13.
12 Vgl. zum Begriff der Einwilligung Art. 4 Nr. 11 DSGVO.
13 Vgl. auch *Kort*, DB 2016, 711, 715.
14 Vgl. zum Regelungsrahmen bei Präzisierungen zum Beschäftigtendatenschutz etwa Art. 88 Abs. 2 DSGVO. Ausführlich hierzu auch Rn. 308 ff.
15 Vgl. Erwägungsgrund 8, der lediglich „Präzisierungen oder Einschränkungen (…) durch das Recht der Mitgliedstaaten" erlaubt.

## 2. Inkrafttreten der DSGVO

Die DSGVO wurde am 14.5.2016 vom EU-Parlament verabschiedet. Die Verordnung wurde am 4.5.2016 im Amtsblatt der Europäischen Union veröffentlicht und trat am 20. Tag nach der Veröffentlichung in Kraft.[16] Nach einer zweijährigen Umsetzungsfrist wird die DSGVO ab dem 25.5.2018 geltendes Recht.[17] Sie hebt die EU-Datenschutzrichtlinie 95/46/EG auf.[18] Die DSGVO verdrängt die deckungsgleichen Vorschriften des Bundesdatenschutzgesetzes (BDSG). Der Verordnung kommt ein sogenannter „Anwendungsvorrang“[19] zu. **11**

Die Anforderungen der Verordnung gehen in einigen Bereichen weit über die Vorgaben des BDSG hinaus. Zudem erfordern sie zahlreiche neue Prozesse, welche die Unternehmen erst implementieren müssen. Gerade die Vorschriften zur Information betroffener Personen, zur Dokumentation von Datenschutzprozessen, zur Datenübertragbarkeit, zur Datenlöschung, zum Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen oder zur Datenschutz-Folgenabschätzung erfordern einigen Umsetzungsaufwand. **12**

Das Bundesinnenministerium plant derzeit ein Ausführungsgesetz zur DSGVO. Ob und in welcher Form das geplante Gesetz Änderungen für die Wirtschaft mit sich bringen wird, ist noch offen. Die laufende Legislaturperiode dauert nur noch bis September 2017 an. Es besteht Handlungsbedarf. Ein mögliches Ausführungsgesetz sollte im Hinblick auf den nach bisherigem Stand dann beginnenden Wahlkampf jedenfalls bis Mitte 2017 ausgearbeitet und beschlossen sein.[20] **13**

**Praxistipp**: Die Umsetzungsfrist von zwei Jahren ist für eine effektive Implementierung der notwendigen Prozesse und Strukturen zur Umsetzung der DSGVO knapp bemessen. Gerade die für den Datenschutz verantwortlichen Unternehmensfunktionen sollten möglichst bald einen Ist-Soll-Vergleich beginnen. Zudem sollten sie auch zügig mit den erforderlichen Budget-Planungen beginnen. **14**

In diesem Zusammenhang kann eine zeitige und gut vorbereitete Unterrichtung des Managements über die neuen Anforderungen und Haftungsrisiken durch die Vorordnung zweckmäßig sein. Auch viele andere Unternehmensfunktionen außerhalb des Datenschutzes sind von den Anforderungen der DSGVO in erheblicher Weise betroffen. Unternehmen sollten grundsätzlich prüfen, welche

16 Vgl. Art. 99 Abs. 1 DSGVO.
17 Vgl. Art. 99 Abs. 2 DSGVO.
18 Vgl. Art. 94 Abs. 1 DSGVO.
19 Vgl. Art. 288 Abs. 2 AEUV.
20 Vgl. hierzu etwa *Kühling/Martini*, EuZW 2016, 448, 450.

Folgen das neue EU-Datenschutzrecht für ihre Arbeit hat und wie sie die neuen Anforderungen effektiv und ohne unnötige Risiken und Aufwände umsetzen. Kapitel VI dieses Buchs gibt dem Leser einen an den Bedürfnissen der Praxis orientierten Überblick über erforderliche Projektschritte zur Umsetzung der Vorgaben der DSGVO.

### 3. Von der DSGVO verwendete Begriffe

**15** Die DSGVO verwendet grundsätzlich sehr ähnliche Begriffe wie das BDSG. Allerdings gibt es einige Unterschiede, die der Anwender kennen sollte, um die Verordnung rechtssicher anwenden zu können.

**16** Der für die „Verarbeitung personenbezogener Daten Verantwortliche“[21] (oder kurz: „Verantwortlicher“) ist diejenige Stelle, die die Entscheidung über die Verarbeitung von personenbezogenen Daten trifft.[22] Bei einem Unternehmen ist dies die rechtliche Person, mittels derer das Unternehmen betrieben wird, z. B. eine GmbH oder Aktiengesellschaft. Dies entspricht der bereits aus § 3 Abs. 7 BDSG bekannten Definition der „verantwortlichen Stelle“.

**17** Ebenso wie das BDSG definiert die DSGVO den Begriff der „personenbezogenen Daten“.[23] Die Verordnung bezeichnet damit alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.[24] Diese Person bezeichnet die DSGVO als „betroffene Person“. Dieser Begriff entspricht weitgehend dem aus § 3 Abs. 1 BDSG bekannten „Betroffenen“.

**18** An Stelle der aus dem BDSG bekannten „Erhebung, Verarbeitung oder Nutzung“[25] personenbezogener Daten tritt im Rahmen der DSGVO die „Verarbeitung“. Diese bezieht sich auf jede Verwendung personenbezogener Daten.[26] Beide Begriffe sind im Wesentlichen deckungsgleich. Allerdings ist die sprachliche Vereinfachung gegenüber der „Erhebung, Verarbeitung und Nutzung per-

21 Auch als „Verantwortlicher“ bezeichnet.

22 Vgl. Art. 4 Nr. 7 DSGVO.

23 Siehe ausführlich zur Definition der „personenbezogenen Daten“: *Herbst*, NVwZ 2016, 902; sowie das Schlussplädoyer des Generalanwalts am EuGH, Manuel Campos Sánchez-Bordona, im Vorabentscheidungsverfahren Patrick Breyer/ Bundesrepublik Deutschland (Rs. C-582/2014), *Knoke*, ZD-Aktuell 2016, 05206, der dynamische IP-Adressen als personenbezogene Daten qualifiziert.

24 Vgl. Art. 4 Nr. 1 DSGVO.

25 Vgl. § 3 Abs. 2 bis 5 BDSG.

26 Vgl. Art. 4 Nr. 2 DSGVO.

sonenbezogener Daten“[27] nach dem BDSG zu begrüßen. Als Verarbeitung bestimmt Art. 4 Nr. 2 DSGVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten.

An Stelle des „Auftragsdatenverarbeiters“ nach § 11 BDSG tritt der in Art. 4 Nr. 8 DSGVO näher bestimmte „Auftragsverarbeiter“.[28] Dieser bezeichnet jede natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet.[29] **19**

## 4. Anwendungsbereich der DSGVO

Die Verordnung gilt zunächst für die Verarbeitung personenbezogener Daten durch Verantwortliche und Auftragsverarbeiter, die im Rahmen von Tätigkeiten von Niederlassungen in der EU erfolgen.[30] Zudem finden die Vorschriften der DSGVO in bestimmten Fällen auch auf Verantwortliche oder Auftragsverarbeiter außerhalb der Union[31] Anwendung.[32] **20**

### *a) Sachlicher Anwendungsbereich: Welche Datenverarbeitungen sind betroffen?*

Die Verordnung gilt in sachlicher Hinsicht für die automatisierte Verarbeitung personenbezogener Daten, Art. 2 Abs. 1 DSGVO. Hierbei ist es unerheblich, ob die Verarbeitung vollständig oder nur teilweise automatisiert stattfindet.[33] Zu- **21**

27 Vgl. etwa § 3 Abs. 2 Satz 1 BDSG.

28 Vgl. zu den Anforderungen an Auftragsverarbeiter auch Erwägungsgrund 81.

29 Vgl. zu den Einzelheiten der Auftragsverarbeitung nach der Verordnung Art. 28 f. DSGVO.

30 Vgl. Art. 3 Abs. 1 DSGVO.

31 Soweit in der vorliegenden Einführung von der „Union“ oder der „EU“ die Rede ist, bezieht sich dies auf die Europäische Union und den Europäischen Wirtschaftsraum (EWR). Von einer jeweils gesonderten Nennung des EWR sieht die vorliegende Darstellung aus Gründen der sprachlichen Vereinfachung bewusst ab.

32 Vgl. das in Art. 3 Abs. 2 DSGVO geregelte sog. „Marktortprinzip“.

33 So der Wortlaut von Art. 2 Abs. 1 DSGVO. Vgl. auch Erwägungsgrund 15: „Um ein ernsthaftes Risiko einer Umgehung der Vorschriften zu vermeiden, sollte der Schutz natürlicher Personen technologieneutral sein und nicht von den verwendeten Techniken abhängen. Der Schutz natürlicher Personen sollte für die automatisierte Verarbeitung personenbezogener Daten ebenso gelten wie für die manuelle Verarbeitung von personenbezogenen Daten, wenn die personenbezogenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind, sollten nicht in den Anwendungsbereich dieser Verordnung fallen.“

dem findet die Verordnung auf die nichtautomatisierte Verarbeitung von personenbezogenen Daten Anwendung, die bereits in einer Datei gespeichert sind oder noch gespeichert werden sollen.

**22** Damit ist der sachliche Anwendungsbereich der Verordnung in der Praxis weit gefasst. Unternehmen werden selten Daten erheben, die sie nicht im Anschluss speichern oder in sonstiger Weise weiterverarbeiten. Selbst eine zunächst nicht automatisierte Datenerhebung (z. B. durch Beobachten, Befragen, Mithören oder andere nicht technikgestützte Wahrnehmungsvorgänge) wird bei wirtschaftlich relevanten Vorgängen erfahrungsgemäß schnell Gegenstand einer späteren Speicherung.

**23** Art. 2 Abs. 2 DSGVO regelt einige Ausnahmen, bei deren Vorliegen die Verordnung keine Anwendung findet. Für die Unternehmenspraxis relevant kann vor allem Art. 2 Abs. 2 lit. (c) DSGVO sein. Danach findet die Verordnung keine Anwendung, wenn natürliche Personen personenbezogene Daten ausschließlich zur Ausübung persönlicher oder familiärer Tätigkeiten erheben. Im Vergleich zum BDSG ändert sich der sachliche Geltungsbereich für Unternehmen insofern nicht wesentlich. Dies gilt auch in Bezug auf Daten, die erst später gespeichert werden sollen. Bereits im bisherigen Recht sieht § 29 Abs. 1 Satz 1 BDSG vor, dass die Vorgaben dieses Gesetzes auch gelten, soweit personenbezogene Daten für den Einsatz in Datenverarbeitungsanlagen erhoben werden sollen.

**24** **Beispiel 1:** Wenn ein Unternehmen Mitarbeiter befragt und die Ergebnisse dieser Befragungen im Anschluss mit einem Textverarbeitungsprogramm dokumentiert oder auch nur in einer E-Mail zusammenfasst, ist der sachliche Geltungsbereich der Verordnung nach Art. 2 Abs. 1 Alt. 2 DSGVO eröffnet.

**Beispiel 2:** Wenn ein Vorgesetzter auf der Arbeit einen Mitarbeiter zur Begrüßung fragt, wie es diesem Mitarbeiter geht, wird dies nicht als ausschließlich persönlicher Vorgang zu bewerten sein. Denn der Vorgesetzte stellt diese Frage erkennbar in einem Kontext zum Beschäftigungsverhältnis. Allerdings bleibt die Frage nach dem Wohlbefinden auch am Arbeitsplatz richtigerweise nach Art. 9 Abs. 2 lit. (b) oder lit. (h) DSGVO zulässig.

*b) Räumlicher Anwendungsbereich: Wo gilt die Verordnung?*

**25** Die Verordnung gilt nach Art. 3 Abs. 1 DSGVO für die Datenverarbeitung im Rahmen der Tätigkeit einer Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der EU. Dabei ist unerheblich, ob die Verarbeitung in der Union stattfindet oder nicht. Entscheidend ist zunächst, ob sich die Niederlas-

sung des Verantwortlichen oder Auftragsverarbeiters in der EU befindet (sogenanntes „Niederlassungsprinzip“).

Zudem kann die Verordnung nach Art. 3 Abs. 2 DSGVO auch für Verantwortliche oder Auftragsverarbeiter außerhalb der EU gelten (sogenanntes „Marktortprinzip“). Dies ist zum einen der Fall, wenn die Datenverarbeitung dazu dient, betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten.[34] Ob dies entgeltlich oder unentgeltlich geschieht, ist unerheblich. Die Verordnung gilt zudem auch dann, wenn Verantwortliche oder Auftragsverarbeiter das Verhalten betroffener Personen in der EU beobachten.[35] **26**

**Praxistipp**: Der erweiterte räumliche Anwendungsbereich der Verordnung ist eine der wesentlichen Änderungen gegenüber dem bisherigen Recht. Sofern ausländische Datenverarbeitungen „in die EU hineinreichen“, gelten die hohen Anforderungen der DSGVO. In diesem Fall müssen auch Unternehmen ohne Niederlassung in der Union die Grundprinzipien der DSGVO beachten und prüfen, ob eine Datenverarbeitung nach Art. 6 DSGVO erlaubt ist. Zudem müssen sie in Bezug auf solche grenzüberschreitend wirkenden Datenverarbeitungen[36] nach Art. 3 Abs. 2 DSGVO unter anderem auch sicherstellen, dass sie die in Art. 12 bis Art. 39 DSGVO vorgeschriebenen Anforderungen und Prozesse umsetzen. Sofern in solchen Fallkonstellationen Daten in der EU erhoben und in einem Drittstaat gespeichert werden, können zudem die Vorgaben für die Übermittlung personenbezogener Daten in Drittländer nach Art. 44 ff. DSGVO einschlägig sein. Entscheidungsträger in Unternehmen sollten genau beobachten, wie sich europäische Aufsichtsbehörden und Gerichte zu diesen Fragen künftig positionieren. **27**

International operierende Unternehmen sollten genau prüfen, ob und in welchem Umfang sie auch bei Verarbeitungen im Rahmen von Niederlassungen außerhalb der EU gemäß Art. 3 Abs. 2 DSGVO den Vorgaben der Verordnung unterliegen. Gegebenenfalls können Haftungsrisiken und andere Nachteile auch durch getrennte Datenverarbeitungen vermieden werden.

34 Vgl. Art. 3 Abs. 2 lit. (a) DSGVO.

35 Vgl. Art. 3 Abs. 2 lit. (b) DSGVO.

36 Vgl. zum Begriff der (innerhalb der EU) grenzüberschreitenden Verarbeitung Art. 4 Nr. 23 DSGVO.

**28** **Fazit:**

- **EU-weite Vereinheitlichung des Datenschutzrechts bei Öffnungsklauseln.**
- **Kurze Umsetzungsfrist von nur zwei Jahren.**
- **Verbindliche Geltung der DSGVO ab dem 25.5.2018.**
- **DSGVO verwendet ähnliche Begriffe wie das BDSG.**
- **Weiter sachlicher Anwendungsbereich der Verordnung.**
- **Exterritoriale Wirkung der DSGVO.**

# II. Überblick über die Vorschriften der DSGVO – Was steht wo?

Dieses Kapitel soll dem Leser vor allem den ersten Einstieg in die DSGVO erleichtern. Es gibt einen Überblick darüber, welche Regelungen an welcher Stelle in der Verordnung zu finden sind. Die neuen Vorschriften zum EU-weiten Datenschutzrecht sind teilweise schwer verständlich formuliert. Auch die Struktur der DSGVO ist nicht gerade übersichtlich. Umso wichtiger ist es für den Anwender, sich zunächst ein Bild darüber zu verschaffen, welche Vorgaben der Verordnung in welchen Abschnitten und in welchen Artikeln zu finden sind. **29**

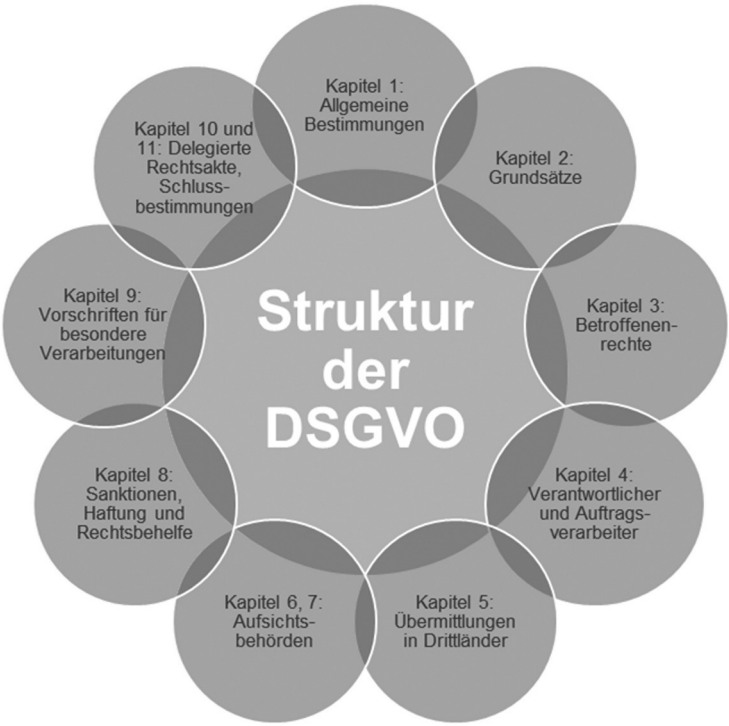


*Abbildung 1: Struktur der DSGVO*

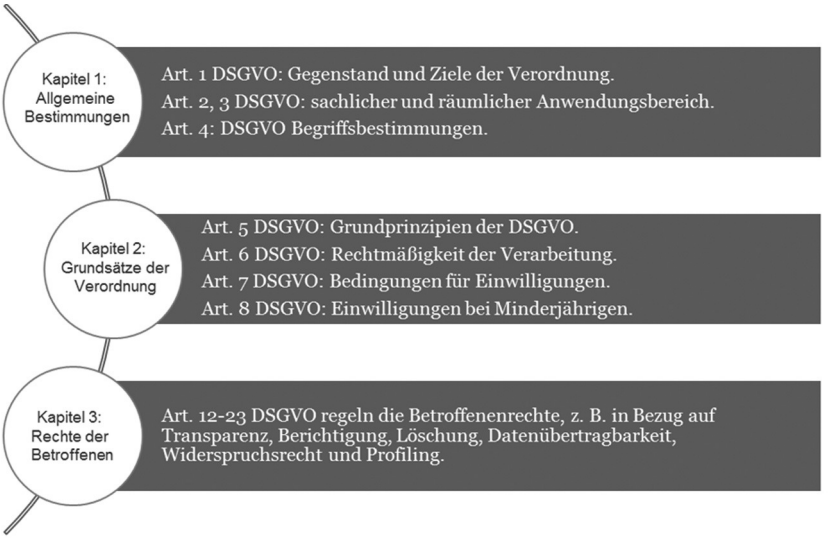


*Abbildung 2: Überblick und Aufbau der DSGVO (Kap. 1–3)*

**30** **Praxistipp**: Wer sich die Grundstrukturen der Verordnung verdeutlichen möchte, kann anhand des vorstehenden Schaubilds die einzelnen Kapitel der DSGVO nachschlagen und sich einen ersten Überblick über die Gliederung der jeweiligen Kapitel verschaffen. In einem zweiten Schritt kann man dann den nachstehenden Überblick durchgehen und die einzelnen genannten Artikel nachschlagen.

### 1. Allgemeine Bestimmungen, Kapitel 1, Art. 1 bis Art. 4 DSGVO

**31** Das erste Kapitel der Verordnung regelt Gegenstand und Ziele sowie den sachlichen und räumlichen Anwendungsbereich der DSGVO. Es enthält auch die wesentlichen Begriffsbestimmungen.

**32** Art. 1 DSGVO bestimmt Gegenstand und Ziele des neuen EU-Datenschutzrechts.[37] Die Verordnung soll das Recht natürlicher Personen auf den Schutz

37 Vgl. zu den Zielen der DSGVO Rn. 8 ff.

ihrer personenbezogenen Daten umsetzen, ohne dabei den freien Verkehr personenbezogener Daten in der EU übermäßig einzuschränken.

Art. 2 und 3 DSGVO regeln den sachlichen und räumlichen Anwendungsbereich der Verordnung.[38] Sie gilt für die automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die noch in Dateien gespeichert werden sollen. Die DSGVO gilt zunächst für Datenverarbeitungen im Rahmen der Tätigkeiten von Niederlassungen in der EU.[39] Zudem gilt sie für Datenverarbeitungen in Bezug auf Personen in der EU durch nicht in der EU niedergelassene Verantwortliche, wenn diese betroffenen Personen in der EU Waren oder Dienstleistungen anbieten oder deren Verhalten beobachten.[40] **33**

Art. 4 DSGVO enthält die wichtigsten Begriffsbestimmungen für die Anwendung der Verordnung.[41] **34**

## 2. Grundsätze der Verordnung, Kapitel 2, Art. 5 bis Art. 11 DSGVO

Art. 5 DSGVO regelt die wichtigsten Grundsätze der Verordnung.[42] Die Vorschrift enthält die wesentlichsten inhaltlichen Vorgaben der DSGVO. Sie ist damit vor allem für die Auslegung der unbestimmten Rechtsbegriffe der Verordnung maßgeblich, etwa für das unter anderem in Art. 6 und Art. 9 DSGVO vorausgesetzte Kriterium der Erforderlichkeit. **35**

Art. 5 DSGVO gibt folgende Prinzipien vor: **36**

- Rechtmäßigkeit (Verbot mit Erlaubnisvorbehalt),
- Treu und Glauben (Verhältnismäßigkeit),
- Transparenz,
- Zweckbindung,
- Datenminimierung,
- Richtigkeit,
- Speicherbegrenzung,
- Integrität und Vertraulichkeit,
- Rechenschaftspflicht.

Art. 6 DSGVO erlaubt den Umgang mit personenbezogenen Daten nur, wenn diese oder eine andere anwendbare Rechtsvorschrift dies vorsieht. Art. 6 DSGVO enthält die wichtigsten allgemeinen Erlaubnistatbestände der Verord- **37**

38 Vgl. zum sachlichen und räumlichen Anwendungsbereich der DSGVO Rn. 21 ff.
39 Vgl. Art. 3 Abs. 1 DSGVO.
40 Vgl. Art. 3 Abs. 2 lit. (a) und (b) DSGVO.
41 Vgl. zu den Begriffsbestimmungen der DSGVO Rn. 15 ff.
42 Vgl. zu den Grundsätzen der Verordnung Rn. 61 ff.