Inhalt

1 Einleitung

Der Schutz personenbezogener Daten spielt in vielen Bereichen unseres täglichen Lebens eine große Rolle. Angaben über unsere Person werden beispielsweise zur Begründung und Aufrechterhaltung von Beschäftigungsverhältnissen, Liefer- und Leistungsbeziehungen, bei der Beantragung von Kunden- und Bonuskarten, Registrierungen bei Buchungen im Hotel, auf Reisen, in Verbänden und andernorts abgefordert. Die Verarbeitung dieser personenbezogenen Daten, deren Erfassung, Bearbeitung, Speicherung, Übermittlung und Archivierung, unterliegt datenschutzrechtlichen Regelungen. Wesentliche Belange für den Datenschutz sind auf europäischer Ebene und für alle Mitgliedstaaten verbindlich in der **EU-Datenschutz-Grundverordnung (DSGVO)** sowie auf nationaler Ebene in der Bundesrepublik Deutschland vorrangig im revisionierten **Bundesdatenschutzgesetz**, im Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) sowie anderen Rechtsverordnungen geregelt.

Im vorliegenden Buch sollen grundlegende **Aspekte des Datenschutzes für den nicht-öffentlichen Bereich** in einfacher und verständlicher Form erläutert werden. Wesentliche Regelungen für die betriebliche Praxis werden entweder in Beispielen oder Musterlösungen dargestellt, so dass eine einfache Adaption der Texte für eigene Belange möglich wird. Diverse Situationen aus der täglichen Unternehmenspraxis werden aus datenschutzrechtlicher Sicht beleuchtet, auf Rechtskonformität bewertet und mit Optionen für Lösungen versehen.

Obwohl für den nicht-öffentlichen Bereich verfasst, sind viele der dargestellten Situationen und Muster auch für private Zwecke anwendbar. Beispielsweise gelten die Regelungen für die Internet-, E-Mail- und Telefonnutzung, für den Umgang mit USB-Sticks, Kopier- und Faxgeräten u. a. m. auch für den privaten Umgang und dürften damit im Interesse jedes Einzelnen liegen. Die Prinzipien der Datensparsamkeit und eingeschränkten Verfügbarkeit personenbezogener Daten seien hier nur stellvertretend genannt.

Der Wert dieses Buches liegt im einführenden Charakter in die Thematik und kann damit als Grundlagenwerk für den Datenschutz bezeichnet werden. Es **unterstützt die Tätigkeit des Datenschutzbeauftragten**, der über diese Publikation Anleitung für seine praktische Arbeit und die hierfür anzuwendende Methodik erhält. Der Datenschutzbeauftragte profitiert von den in der Mediathek (www.beuth-mediathek.de) zu diesem Buch geführten Mustervereinbarungen, Musterbestellurkunden, Vorlagen für datenschutzrechtliche Regelungen sowie Fallbeispielen mit Musterlösungen. Diese können ohne großen Aufwand an die eigene Situation angepasst werden. Zur besseren Übersicht sind alle Muster, Beispiele, auch Hinweise und Zitate aus den Rechtsverordnungen am Rand des Textes als solche kenntlich gemacht.

Im vorliegenden Buch werden nach der Einleitung (Kapitel 1) zunächst Aufbau und wesentliche Inhalte und Definitionen der EU-Datenschutz-Grundverordnung und Passagen des Bundesdatenschutzgesetzes näher beleuchtet (Kapitel 2 und 3). Die Darstellung erhebt keinen Anspruch auf Vollständigkeit. Vielmehr sollen bereits am Anfang wesentliche Grundsätze, Leitlinien und Prinzipien im Datenschutz interpretiert und damit für weitere Ausführungen verständlich und anwendbar gemacht werden. Dazu zählen die Definition personenbezogener Daten, das Recht des Betroffenen auf informationelle Selbstbestimmung, die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, die Einwilligung des Betroffenen für die Nutzung seiner Daten, Auskunftsrechte sowie die Pflichten der verantwortlichen Stelle.

Im 4. Kapitel wird explizit auf die Rolle des Datenschutzbeauftragten eingegangen. In praxisorientierter Weise und unter zur Verfügungstellung von Vorlagen und Mustertexten wird aufgezeigt, wie der Datenschutzbeauftragte seine Arbeit gestalten kann und welche Regelungen er für den betrieblichen Datenschutz aufstellen muss. Dabei steht insbesondere die Art und Weise seiner Herangehensweise an datenschutzrechtliche Belange im Fokus der Betrachtung. Mit dieser Handlungsanleitung soll versucht werden, ausgebildeten und betrieblich bestellten Datenschutzbeauftragten mehr Sicherheit im Umgang mit den Rechtsforderungen der EU-Datenschutz-Grundverordnung und des BDSG und anderer geltender Bestimmungen zu geben und Wege aufzuzeigen, wie diese in der Praxis umgesetzt werden können.

Kapitel 5 beschäftigt sich mit den technischen und organisatorischen Anforderungen im Datenschutz. Im Wesentlichen erfolgt hier die Klarstellung der Begrifflichkeiten, mit denen in den folgenden Kapiteln betriebliche Regelungen für den Datenschutz beispielhaft dargestellt und verständlich aufbereitet werden.

In Kapitel 6 wird auf das Vorgehen bei der Datenschutz-Folgenabschätzung näher eingegangen. Anhand eines Beispiels wird die Methodik zur Risikobewertung datenschutzrechtlicher Risiken (Datenschutz-Folgenabschätzung) erläutert.

Den bedeutendsten Teil dieses Buches nehmen die konkreten auf die betriebliche Praxis leicht adaptierbaren Anweisungen zum Datenschutz im Kapitel 7 wie zum Umgang mit E-Mail, Internet, Videokonferenzen und mobilem Arbeiten ein. Von ebensolcher Bedeutung sind die Themen in den Kapiteln 8 und 11 zu den datenschutzrechtlichen Vereinbarungen mit Dienstleistern und den Informationsschreiben und Anweisungen zu Notfallsituationen, Meldepflichten etc. Hier findet der Leser zahlreiche Beispiele aus der Praxis der Autorin, die er für seine Arbeit nutzen kann.

Weitere Abschnitte des Buches beleuchten die Auftragsverarbeitung (Kapitel 8) oder beschäftigen sich mit dem Spezialfall der Anwendung des Datenschutzes im Personalwesen (Kapitel 10). Auch hier werden Praxisbeispiele vermittelt und Vorlagen zur Adaption angeboten.

Einen nicht unerheblichen Teil der Arbeit des Datenschutzbeauftragten stellen innerbetriebliche Schulungen und Unterweisungen dar. Diesem Anspruch trägt vor allem Kapitel 13 Rechnung.

Letztlich könnten alle Aktivitäten des Datenschutzbeauftragten in einem Handbuch zusammengefasst werden (Kapitel 14). Sowohl der Aufbau der Dokumentation als auch das Vorgehen step by step werden hier beschrieben. Die Liste der Mindestregelungen für den Datenschutz kann als Leitlinie für den Datenschutzbeauftragten dienen.

Klare Grenzen sind von der Autorin des Buches hinsichtlich der technischen Umsetzung des Datenschutzes gezogen. Sie setzt vorrangig auf die Vermittlung datenschutzrechtlicher Grundsätze im Denken und Handeln, nur ansatzweise auf technische Lösungen. Hierfür existieren bereits zahlreiche Publikationsreihen am Markt, allerdings sind diese für den Einsteiger nicht selten kompliziert und schwer zu erschließen. So die Thematik des Datenschutzes und die Argumentation der Autorin richtig verstanden werden, fällt auch die Beurteilung und Auswahl der geeigneten technischen Lösung im Anschluss leicht.

Datenschutz ist ein sehr komplexes Thema. Trotz des Umfangs dieser Veröffentlichung war es nicht möglich, auf alle Aspekte des Datenschutzes einzugehen. In diesem Zusammenhang wird auf die vielfältigen Veröffentlichungen zu Spezialthemen verwiesen, u. a. durch den Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.

Das vorliegende Buch hilft dem Leser, Datenschutz in der Praxis zu regeln, zu organisieren und umzusetzen sowie das Bewusstsein für den Datenschutz zu fördern.

2 Aufbau und wesentliche Inhalte der EU-Datenschutz-Grundverordnung (EU-DSGVO)

Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 26. April 2016 (EU-DSGVO) basiert auf dem Grundrecht des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten. Mit der 1995 für alle 28 Mitgliedstaaten erlassenen europäischen Datenschutzrichtlinie wurden einheitliche Guidelines zur Umsetzung des Datenschutzes bestimmt. Alle Mitgliedstaaten veröffentlichten der europäischen Datenschutzrichtlinie folgend eigene Datenschutzgesetze. Deren praktische Umsetzung wurde jedoch auf unterschiedlichem Niveau realisiert. Mit der EU-DSGVO wird das Datenschutzrecht innerhalb der EU für den privaten und öffentlichen Bereich weitgehend vereinheitlicht. Für 500 Millionen Bürger Europas soll gleiches Recht zum Schutz der Privatsphäre gelten:

„Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden ‚Charta') sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten."

Erwägungsgrund 1, EU-DSGVO

Alle Mitgliedstaaten der EU auf ein einheitliches Vorgehen nicht nur im Grundsatz, sondern auch im Detail zu verpflichten, bedurfte etlicher Diskussionen auf inhaltlicher Ebene. Die EU-DSGVO gilt unmittelbar für jeden einzelnen Mitgliedstaat der EU. Den Mitgliedstaaten ist es grundsätzlich nicht erlaubt, die von dieser Verordnung festgeschriebenen Regelungen im Datenschutz abzuschwächen oder auch zu verstärken. Um nationale Belange dennoch berücksichtigen zu können, enthält die EU-DSGVO sogenannte Öffnungsklauseln. Diese Öffnungsklauseln erlauben es, bestimmte thematische Aspekte im Datenschutz national zu regeln. Daher spricht man im Allgemeinen von einer „Hybridlösung im Datenschutz", einem Hybrid zwischen Richtlinie und Verordnung.

Die Diskussionen um die EU-DSGVO währten mehr als 4 Jahre. Verschiedene Entwürfe der Europäischen Kommission, des Europäischen Parlaments und Rates wurden von vielen Seiten kritisiert. Auch von deutscher Seite gab es viele Einwände.

Zu den wesentlichen Kritikpunkten an den Entwürfen zur EU-DSGVO zählten:

- Bestellung von internen Datenschutzbeauftragten nur bei Unternehmen mit mehr als 250 Mitarbeitern, was eine Schwächung des Datenschutzniveaus in Deutschland und Österreich bedeutet hätte.
  - In der endgültigen Fassung der EU-DSGVO ist der verbindlich zu bestellende Datenschutzbeauftragte bei Behörden und Verantwortlichen vorgesehen, deren Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen oder in der umfangreichen Verarbeitung sensibler Daten besteht (Art. 37 Abs. 1). Gemäß Art. 37 Abs. 4 dürfen auf nationaler Ebene nun strengere Regelungen getroffen werden.
- Dokumentationspflichten nur bei Unternehmen mit mehr als 250 Mitarbeitern
  - Später wurden Dokumentationspflichten auch für kleinere Unternehmen festgelegt, sofern die Datenverarbeitung ein Risiko für die Betroffenen birgt und nicht nur gelegentlich erfolgt und die Verarbeitung sensibler Daten einschließt.
- Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) kritisierte die unkonkreten Regelungen für den Datentransfer in Drittstaaten, z. B. USA usw.

Auch nach der Verabschiedung der EU-Datenschutz-Grundverordnung blieb Kritik nicht aus, beispielsweise vom Deutschen Anwaltverein und etlichen Vertretern der Wissenschaft aus Universitäten und Hochschulen.

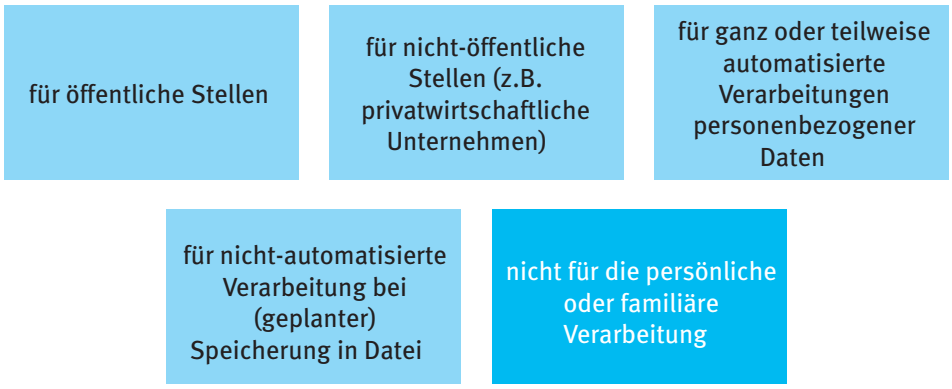
Unabhängig von allen Kontroversen in Europa erhoffen sich Datenschützer jenseits des europäischen Kontinents den sogenannten „California Effect", d. h. den Effekt des Nachahmens zumindest in den Grundsätzen. In den USA beispielsweise unterliegen lediglich Finanz- und Gesundheitsdaten dem Datenschutz. International agierende Konzerne sind hier die Treiber des Geschehens.

Die letzten Schritte im zeitlichen Verlauf der Vorbereitung der EU-DSGVO werden im Folgenden dargestellt:

Seit dem 25. Mai 2018 gilt nun die EU-DSGVO für alle europäischen Staaten gleichermaßen, wenn auch sogenannte Öffnungsklauseln Möglichkeiten der nationalen Ergänzung und Vertiefung boten, die in unterschiedlichem Maße genutzt wurden.

2.1 Anwendungsbereich der EU-DSGVO

Die EU-DSGVO kann auf folgende Sachverhalte angewendet werden:



Aufgrund des Risikos der Umgehung des Datenschutzes gelten die Vorschriften technologieneutral und unabhängig von jeglichem Technikzwang. Nicht der Datenschutz soll sich nach der Technik richten, sondern umgekehrt.

Weiterhin ist der Datenschutz, wie schon in der Abbildung dargestellt, sowohl auf automatisierte als auch manuelle Systeme anzuwenden.

Wenn Verarbeitungen personenbezogener Daten für private Zwecke ausgeschlossen werden, so meint die EU-DSGVO Zwecke ohne beruflichen oder wirtschaftlichen Hintergrund. Das private Tätigwerden in sozialen Netzwerken unterliegt damit nicht der EU-DSGVO. Allerdings sind die Regelungen der EU-DSGVO durch die Verantwortlichen für soziale Netzwerke oder deren Auftragsverarbeiter einzuhalten, die die Instrumente zur Verfügung stellen (EG 18). Betroffen davon sind unter anderem auch US-amerikanische Unternehmen wie Google und Facebook.

Die EU-DSGVO ist von allen Mitgliedstaaten der EU verbindlich und vorrangig anzuwenden. Sie ist nicht subsidiär, also nicht unterstützend gemeint. Sie kann durch nationales Recht flankiert werden. Die nationalen Regelungen dürfen jedoch nicht der EU-DSGVO widersprechen. In Zweifelsfällen wird das Recht durch den EuGH ausgelegt.

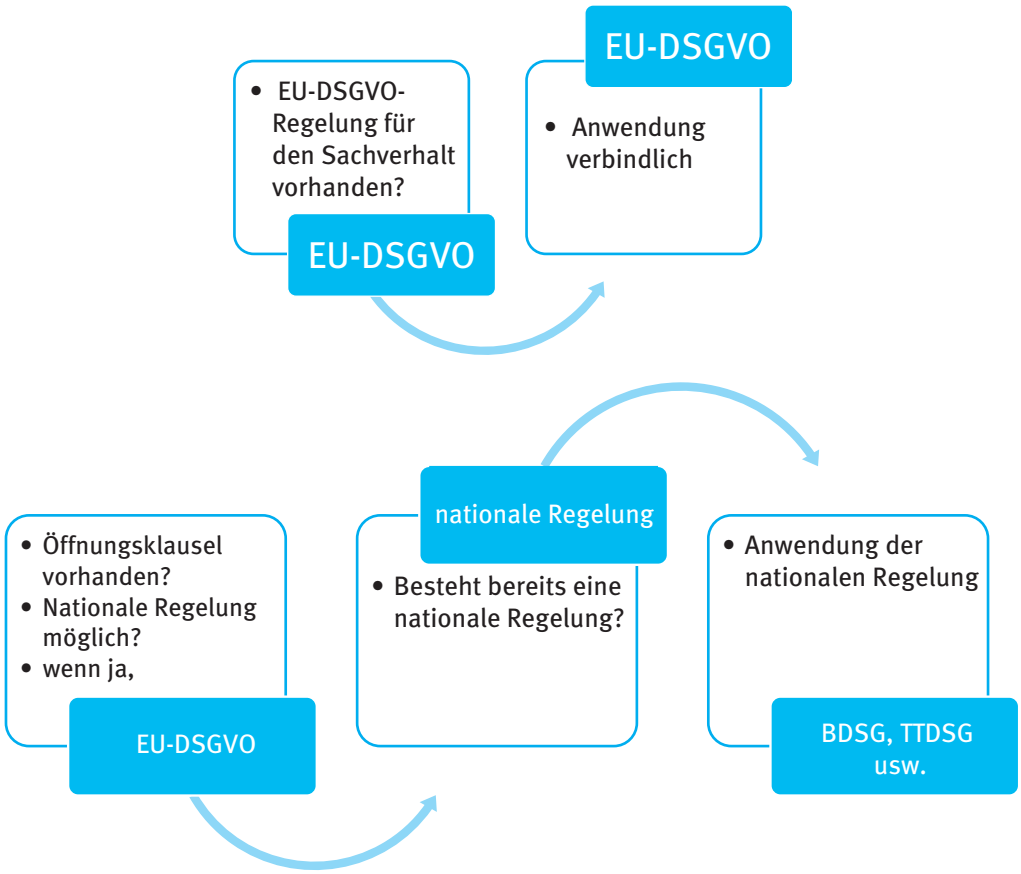
Um zu erkennen, welche Regelungen im Datenschutz anzuwenden sind, empfiehlt es sich, die unten abgebildete Vorgehensweise zu nutzen.

Die EU-DSGVO lässt an definierten Stellen ganz bewusst regelungsbedürftige Sachverhalte offen (Öffnungsklauseln), um dem nationalen Gesetzgeber Gestaltungsraum zu geben. Damit wird sowohl ein verbindlich einheitliches Vorgehen im Datenschutz innerhalb der EU umgesetzt als auch der Individualität und dem Freiheitsgrad der Mitglieder Rechnung getragen. Wörtlich heißt es dazu im EG 10:

„Diesbezüglich schließt diese Verordnung nicht Rechtsvorschriften aus, in denen die Umstände besonderer Verarbeitungssituationen festgelegt werden, einschließlich einer genaueren Bestimmung der Voraussetzungen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist.“

EG 10, EU-DSGVO

Zur Bestimmung, wann nationale Regelungen anwendbar sind, steht folgendes Tableau zur Verfügung.



Artikel 3 der EU-DSGVO regelt den räumlichen Anwendungsbereich der EU-DSGVO. Sie gilt für alle in der EU niedergelassenen Unternehmen (Art. 3 Abs. 1), auch wenn sie keine Verarbeitung personenbezogener Daten in der EU vornehmen. Weiterhin gilt sie für alle im EU-Raum anbietenden Unternehmen, die personenbezogene Daten von Betroffenen in der EU halten bzw. verarbeiten. Somit ist die Anwendung der EU-DSGVO bereits verpflichtend, wenn ausländische Unternehmen in der EU Offerten unterbreiten (Marktortprinzip). Dies wird im Artikel 3 Absatz 2 davon abhängig gemacht, ob das ausländische Unternehmen

- das Angebot an EU-Bürger richtet,
- eine Bestellung in einer der EU-Sprachen vorsieht,
- die Bezahlung in der Währung der EU-Bürger zulässt.

Des Weiteren ist die EU-DSGVO anzuwenden, so ein ausländisches Unternehmen das Verhalten von betroffenen Personen in der EU beobachtet.

Damit trifft der einzuhaltende Datenschutz auch viele im EU-Raum operierende ausländische Unternehmen, die sich in ihren AGB und datenschutzrechtlichen Vorgehensweisen zwingend anpassen müssen.

Im Artikel 3 Absatz 3 wird geregelt, dass die EU-DSGVO für alle Unternehmen anzuwenden ist, sofern die Verarbeitung personenbezogener Daten durch einen nicht in der EU niedergelassenen Verantwortlichen an einem Ort erfolgt, der aufgrund des Völkerrechts dem Recht eines der Mitgliedstaaten unterliegt.

2.2 Ausschlüsse aus dem Anwendungsbereich

Wie bereits dargestellt, gilt die EU-DSGVO nicht für die Anwendung im privaten und familiären Bereich. Weiterhin gilt sie gemäß EG 14 nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristisch gegründete Unternehmen einschließlich Name, Rechtsform und Kontaktdaten der juristischen Person. Sind jedoch Kontaktdaten von Ansprechpartnern, deren private Rufnummern o. Ä. angegeben, so unterliegen diese dem Datenschutzrecht.

Mit der EU-DSGVO sollte mehr Transparenz und Rechtssicherheit für kleine und mittelständische Unternehmen geschaffen werden. Die EU-DSGVO sieht in Anrechnung der Größe vieler Unternehmen eine Ausnahmeregelung für Kleinstunternehmen im Hinblick auf die Führung von Verzeichnissen vor. Ein Kleinstunternehmen ist, wer nach Art. 2 des Anhangs Empfehlung 2003/361/EG der Kommission den dort genannten Kriterien entspricht.

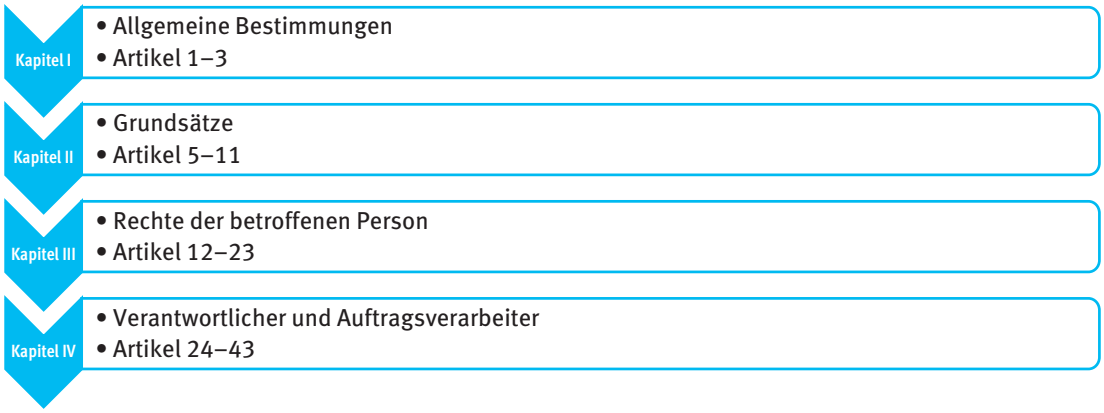
Unternehmenskategorie	Zahl der Mitarbeiter	Umsatz oder	Bilanzsumme
mittelgroß	unter 250	höchstens 50 Mio. €	höchstens 43 Mio. €
klein	unter 50	höchstens 10 Mio. €	höchstens 10 Mio. €
mikro	unter 10	höchstens 2 Mio. €	höchstens 2 Mio. €

Die EU-DSGVO gilt nicht für die Verarbeitung personenbezogener Daten Verstorbener. Hier lässt die EU-DSGVO eine Öffnung für nationale Regelungen (EG 27).

2.3 Struktur der EU-DSGVO

Die EU-DSGVO besteht aus 173 Erwägungsgründen (EG) und 99 Artikeln. Die Erwägungsgründe stellen Erläuterungen zu den einzelnen Artikeln dar, bilden Zusammenhänge ab und sind damit für die Anwendung der Artikel unerlässlich. Sie gehören zum Rechtstext und sind gleichermaßen verbindlich.

Die einzelnen Artikel der EU-DSGVO sind sachbezogen Kapiteln zugeordnet, so dass eine Auffindbarkeit von Rechtsregelungen zu bestimmten Sachthemen erleichtert wird. Hier eine Übersicht:



Kapitel V	• Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen • Artikel 44–50
Kapitel VI	• Unabhängige Aufsichtsbehörden • Artikel 51–59
Kapitel VII	• Zusammenarbeit und Kohärenz • Artikel 60–76
Kapitel VIII	• Rechtsbehelf, Haftung und Sanktionen • Artikel 77–84
Kapitel IX	• Vorschriften für besondere Verarbeitungssituationen • Artikel 85–91
Kapitel X	• Delegierte Rechtsakte und Durchführungsrechtsakte • Artikel 92–93
Kapitel XI	• Schlussbestimmungen • Artikel 94–99

2.4 Akteure im Datenschutz

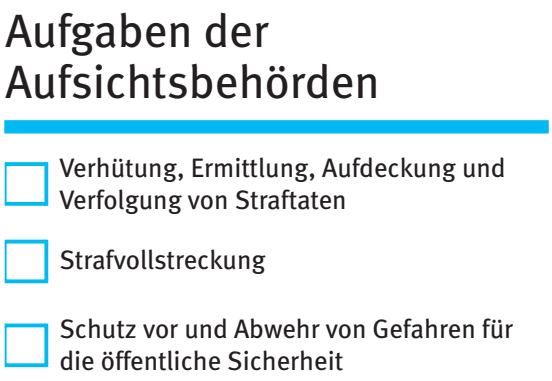
Die EU-DSGVO benennt und definiert unterschiedliche Personengruppen als Akteure im Datenschutz:

Der Verantwortliche für Datenverarbeitung personenbezogener Daten kann unter verschiedenen Bezeichnungen auftreten:

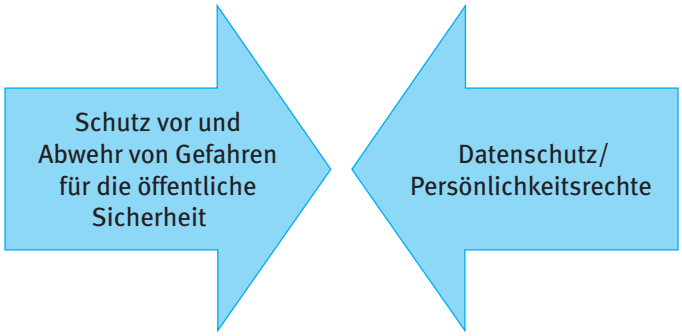
- die Hauptniederlassung
- die Niederlassung
- der (Handels-)Vertreter
- die Unternehmensgruppe (national/international)
- das Unternehmen

Sie werden durch den Inhaber oder durch die Geschäftsleitung oder den Vorstand repräsentiert.

Die Aufsichtsbehörde erfüllt im Datenschutz vorwiegend folgende Aufgaben:



Der Konflikt zwischen dem Schutz öffentlicher Interessen und dem Datenschutz ist vorprogrammiert. Auch hier bleibt von Fall zu Fall abzuwägen, welches Interesse überwiegt.



Die EU-DSGVO lässt eine Öffnungsklausel für die Verarbeitung personenbezogener Daten bei Gerichten und Justizbehörden, die einer nationalen Regelung obliegen.

2.5 Ziele der EU-Datenschutz-Grundverordnung

Der Erlass einer EU-weiten Regelung zur Verarbeitung personenbezogener Daten in Form einer Verordnung wurde aufgrund des deutlich angestiegenen Austauschs personenbezogener Daten im gewachsenen und gut funktionierenden Binnenmarkt EU notwendig. Das Unionsrecht verpflichtet die Mitgliedstaaten, immer enger zusammenzuarbeiten und damit auch Informationen gegenseitig zugänglich zu machen. Im Erwägungsgrund (EG) 6 heißt es, dass die rasche technologische Entwicklung den Datenschutz vor neue Herausforderungen gestellt hat. Angesichts des World Wide Web haben die Verarbeitung und die Verarbeitungsintensität personenbezogener Daten immens zugenommen. Dem müssen datenschutzrechtliche Regelungen auf aktualisiertem Niveau folgen. Die EU-DSGVO wurde verabschiedet, um Hemmnisse im EU-Binnenmarkt abzubauen und ein einheitlich hohes Datenschutzniveau bei allen Mitgliedstaaten zu sichern.

Ziele der EU-DSGVO sind vor allem:

- Wahrung der Grundrechte und Grundfreiheiten
- insbesondere Wahrung des Rechts auf Schutz personenbezogener Daten ungeachtet der Staatsangehörigkeit oder des Aufenthaltsorts
- Vollendung eines Raums für
  - Freiheit
  - Sicherheit
  - Recht

- eine Wirtschaftsunion zwecks
  - wirtschaftlichen und sozialen Fortschritts
  - Stärke und Zusammenwachsens der Volkswirtschaften im Binnenmarkt EU
- freien Verkehr personenbezogener Daten zwischen den Mitgliedstaaten
- Verarbeitung personenbezogener Daten im Dienste der Menschheit

Die in der Charta verbrieften Grundrechte sind u. a.:

Der Schutz personenbezogener Daten ist indes kein uneingeschränktes Recht.

Das Recht auf Schutz personenbezogener Daten wird durch das Verhältnismäßigkeitsprinzip gebrochen. Die Verarbeitung personenbezogener Daten ist gegen andere Grundrechte abzuwägen, beispielsweise das Recht der Unversehrtheit der Person.