

KOMMUNIKATION UND RECHT

HANDBUCH

Moos / Schefzig / Arning (Hrsg.)

Praxishandbuch DSGVO

einschließlich BDSG und
spezifischer Anwendungsfälle

2. Auflage

Kommunikation & Recht

Praxishandbuch
DSGVO
einschließlich BDSG und
spezifischer Anwendungsfälle

Herausgegeben von

Dr. Flemming Moos

Rechtsanwalt, Fachanwalt für IT-Recht, Hamburg

Dr. Jens Schefzig

Rechtsanwalt, Hamburg

Dr. Marian Alexander Arning

LL.M., Dozent, Türkisch-Deutsche Universität, Istanbul

2., komplett überarbeitete und erweiterte Auflage 2021

Bearbeitet von

Dr. Marian Alexander Arning, LL.M.; Dr. Ulrich Baumgartner, LL.M.

(King's College London); Ingo Braun; Cay Lennart Cornelius;

Eva Gardyan-Eisenlohr, D.I.A.P. (ENA, Paris);

Dr. Tina Gausling, LL.M. (Columbia University); Stephan Hansen-Oest;

Carmen Heinemann; Per Meyerdierks; Dr. Flemming Moos;

Leif Rohwedder; Dr. Tobias Rothkegel; Dr. Jens Schefzig;

Laurenz Strassemeyer; Dr. Anna Zeiter, LL.M. (Stanford)

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

I S B N 9 7 8 - 3 - 8 0 0 5 - 1 7 2 8 - 2

dfv Mediengruppe

©2021 Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft,
Frankfurt am Main
www.ruw.de

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Satzkonvertierung: Lichtsatz Michael Glaese GmbH, 69502 Hemsbach

Druck und Verarbeitung: Eberl & Koesel GmbH & Co. KG, 87452 Altusried-Krugzell

Printed in Germany

Vorwort

Die Europäische Datenschutz-Grundverordnung (DSGVO) und das „neue“ BDSG sind nunmehr seit drei Jahren in Kraft. Trotzdem bleibt ihre Umsetzung eine laufende Herausforderung für Unternehmen. Denn einerseits haben viele Unternehmen die DSGVO noch lange nicht in alle Unternehmensprozesse und -bereiche integriert. Andererseits sind laufend neue Gerichtsurteile sowie Beschlüsse und Leitlinien der Datenschutzbehörden zu berücksichtigen. Schließlich können auch andere Entwicklungen, wie beispielsweise die globale Covid-19-Pandemie, die weiter fortschreitende digitale Transformation oder auch der Brexit, neue Fragestellungen mit sich bringen, die Unternehmen auch in datenschutzrechtlicher Hinsicht lösen müssen. Auch nach drei Jahren Geltungsdauer ist der Rechtsrahmen noch nicht so konkretisiert, dass zu allen Datenschutzfragen im Unternehmen einfach ableitbare Lösungen vorliegen. Hinzu kommt, dass die Datenschutzbehörden häufig besonders strenge Positionen vertreten, denen Unternehmen nicht ohne Weiteres folgen wollen. Es bleibt aktuell also weitgehend den Unternehmen selbst überlassen, pragmatische und praxistaugliche Lösungen zur Umsetzung der DSGVO-Vorgaben zu entwickeln.

Vor diesem Hintergrund richtet sich das vorliegende Handbuch an alle Datenschutzpraktiker, also Datenschutzverantwortliche in Unternehmen, Datenschutzbeauftragte, Syndizi, Datenschutzberater, Mitarbeiter in Datenschutzbehörden sowie Rechtsanwälte. Es soll umfassende Lösungen für die Vielzahl an Fragestellungen liefern, die sich im Unternehmen ganz praktisch bei der Einhaltung der DSGVO ergeben. Das vorliegende Handbuch dient als kontinuierlicher Ratgeber bei datenschutzrechtlichen Fragestellungen, sowohl im täglichen Geschäft als auch um gewisse Themenbereiche grundsätzlich zu adressieren. Statt einer Aneinanderreihung verschiedener Beiträge war es dabei das Anliegen, eine systematische Darstellung der Rechtslage zu gewährleisten, die auch eine Einarbeitung ermöglicht. Gleichzeitig sollen die zahlreichen Praxishinweise bei der Umsetzung der abstrakten Vorgaben helfen.

Einige besondere Themenkomplexe – wie etwa Fragen des Web Trackings oder Customer Relationship Managements – haben für den Datenschutzpraktiker regelmäßig und fortwährend eine überragende Bedeutung. Sie erfordern unseres Erachtens eine in sich geschlossene Darstellung, um ihre praktischen Implikationen zu erfassen. Diese Themenkomplexe werden in Kapitel 17 erläutert. Darüber hinaus haben wir in der 2. Auflage nunmehr ein eigenes Kapitel zum Datenschutzrecht in Österreich aufgenommen, um auch diese Facette des praktischen Datenschutzes zu beleuchten.

Um der Bedeutung des Case Law für die Auslegung und Anwendung der DSGVO gerecht zu werden, haben wir einen für deutsche Praxishandbücher

Vorwort

ungewöhnlichen Teil in dieses Handbuch aufgenommen: Wir haben die relevantesten Urteile zum Datenschutzrecht in einem eigenen Kapitel aufbereitet. Der Datenschutzpraktiker hat so eine Quelle, um sich alle Leitentscheidungen zu vergegenwärtigen.

Bei den Autoren dieses Handbuchs handelt es sich ausnahmslos um erfahrene Datenschutzpraktiker, die sich in ihrer Arbeit laufend mit den adressierten Themen auseinandersetzen. Wir danken diesen Autoren, dass sie in einer durch eine Pandemie geprägten, beruflich und familiär belastenden Zeit den Enthusiasmus und Einsatz gezeigt haben, um dieses Werk zu ermöglichen. Ihre in der Praxis gewonnenen Erfahrungen stellen einen unschätzbaren Mehrwert dieses Werks dar.

Über sämtliche Anregungen zu diesem Handbuch sind wir dankbar.

Flemming Moos

Jens Schefzig

Marian Arning

im April 2021

Autorenverzeichnis

Dr. Marian Alexander Arning, LL.M., Dozent an der Türkisch-Deutschen Universität in Istanbul u.a. für Datenschutz- und IT-Recht. Zudem ist er seit 2011 als Rechtsanwalt in Deutschland zugelassen und war in der Folge im Bereich des Datenschutz- und IT-Rechts bei den internationalen Wirtschaftsprüfungskanzleien Norton Rose Fulbright und Osborne Clarke in Hamburg tätig. In diesem Zusammenhang hat er internationale Großkonzerne, Mittelständler, aber auch Start-Ups zu allen Aspekten des Datenschutzrechts beraten. Ein besonderer Schwerpunkt liegt im Bereich Life Science & Healthcare. Er hat seinen Master im IT-Recht am Institut für Rechtsinformatik der Leibniz Universität Hannover und an der Katholieke Universiteit Leuven (Belgien) absolviert. Dr. Arning hat eine Vielzahl von Buch- und Zeitschriftenbeiträgen zum Datenschutzrecht veröffentlicht.

Dr. Ulrich Baumgartner, LL.M. (King's College London), Partner der Kanzlei BAUMGARTNER BAUMANN am Standort München, zuvor Partner der Kanzleien Allen & Overy und Osborne Clarke. Er berät seit 2003 im deutschen und europäischen Datenschutzrecht sowie im IT-Recht. Einen Schwerpunkt seiner Beratung bildet die Onlinebranche sowie der Sektor Digital Business. Neben seiner Anwaltstätigkeit leitet Ulrich Baumgartner als Region Leader die Aktivitäten der International Association of Privacy Professionals (IAPP) in Deutschland, Österreich und der Schweiz und ist Co-Chair der lokalen Münchener Gruppe der IAPP. Er ist regelmäßiger Referent zu Datenschutzthemen und Autor verschiedener Kommentare, Fachbücher und Beiträge zum Datenschutzrecht.

Ingo Braun, Rechtsanwalt und Partner in der Kanzlei bpv Hügel in Österreich. Er ist seit 2004 als Rechtsanwalt in Österreich zugelassen und war seither mit einem Schwerpunkt im Bereich des IT- und Datenschutzrechts in unterschiedlichen internationalen Kanzleien tätig. Er hält Vorträge und verfasst Beiträge zum Datenschutzrecht.

Cay Lennart Cornelius, Justiziar und Referent insbesondere im Bereich Sanktionen bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI). Vor dem Wechsel zur Aufsichtsbehörde war er unter anderem als selbstständiger externer Datenschutzbeauftragter und mehrere Jahre als wissenschaftlicher Mitarbeiter im IT- und Datenschutzrecht im Team von Dr. Fleming Moos in der Kanzlei Osborne Clarke an den Standorten Berlin und Hamburg tätig. Die International Association of Privacy Professionals (IAPP) verlieh ihm die Zertifikate des Certified Information Privacy Professional/Europe (CIPP/E) und des Certified Information Privacy Manager (CIPM).

Eva Gardyan-Eisenlohr, Rechtsanwältin und Absolventin der Ecole Nationale d'Administration, Frankreich. Nach langjähriger Tätigkeit als in-house counsel

in der AgroScience und Pharmaindustrie, leitete sie als General Counsel und Compliance Officer von 2009–2015 die Rechtsfunktion der Bayer Pharma AG und verantwortete von 2016–2020 als Group Data Privacy Officer die weltweite Datenschutzfunktion der Bayer AG. Für die Rechtsfunktion war sie Mitglied im Bayer Digital Excellence Council. Zum 1. Januar 2021 wechselte Eva Gardyan-Eisenlohr zur Olympus Corporation, Tokio. Seit dem 1. April 2021 ist sie für das Unternehmen Global Chief Compliance Officer und verantwortet die Bereiche Compliance, Ethics und Data Privacy berichtend an den Vorstandsvorsitzenden.

Dr. Tina Gausling, LL.M. (Columbia University), Fachanwältin für IT-Recht und zertifizierte Datenschutzexpertin (CIPP/E) in der Kanzlei Allen & Overy LLP am Standort München. Nach einem Masterstudium an der Columbia Law School in New York war sie in führenden internationalen Wirtschaftskanzleien in Berlin, Hamburg und München tätig. Sie berät nationale und internationale Unternehmen im IT- und Datenschutzrecht vorrangig zu grenzüberschreitenden Fragestellungen und mit einem besonderen Fokus auf aktuellen technologischen Entwicklungen, u. a. in den Bereichen Online-Marketing und AdTech, IoT und Künstliche Intelligenz. Dr. Gausling wirkt als Mitglied des European Advisory Board der IAPP (International Association of Privacy Professionals) intensiv an der rechtlichen Weiterentwicklung dieser Themen mit, publiziert regelmäßig in Fachzeitschriften und internationalen Journals und tritt als Referentin auf fachspezifischen Tagungen, Konferenzen und in Seminaren auf.

Stephan Hansen-Oest, Rechtsanwalt und Fachanwalt für IT-Recht in Flensburg. Er ist seit 2002 Rechtsanwalt und Inhaber einer Kanzlei für Datenschutzrecht. Neben der anwaltlichen Beratung ist Rechtsanwalt Hansen-Oest zudem auch als rechtlicher Sachverständiger für das Gütesiegel für IT-Produkte des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein und auch als Legal Expert für das European Privacy Seal (EuroPriSe) akkreditiert gewesen. Er ist Certified Information Privacy Professional/Europe (CIPP/E) und Geschäftsführer der Datenschutz-Guru GmbH.

Carmen Heinemann, Diplom-Informationsjuristin (FH), arbeitet als Beraterin für IT-Compliance, Prozessmanagement, Business Intelligence und Digitalisierung in der Hessischen Landesbank an der Schnittstelle zwischen IT, Informationssicherheit und Datenschutz. Neben ihrer langjährigen Tätigkeit als IT-Projektmanagerin, u. a. bei der Deutschen Bank, IBM und Microsoft, hat Frau Heinemann Informationsrecht studiert, um die zunehmenden Compliance-Anforderungen bei der Einführung von IT-Lösungen optimal berücksichtigen zu können. Nebenberuflich lehrt und schreibt Frau Heinemann zu Praxisfragen des IT-Rechts und des IT-Projektmanagements. Frau Heinemann ist zertifizierte IT-Security Beauftragte (TÜV) und zertifizierte IT-Compliance Managerin (TÜV).

Per Meyerdierks, Senior Privacy Counsel und Syndikusrechtsanwalt bei Google in Hamburg. Er ist seit 2005 als Rechtsanwalt und seit 2017 als Syndikusrechtsanwalt zugelassen. Nachdem er zunächst in der Rechtsabteilung der Lycos Europe GmbH tätig war, berät er seit 2007 Google in allen Fragen des Datenschutzrechts mit Fokus auf die an Unternehmen gerichteten Cloud-Dienste. Er ist zudem Ansprechpartner für die Datenschutzaufsichtsbehörden in mehreren Ländern einschließlich Deutschlands. Per Meyerdierks hat diverse Fachbeiträge zum Datenschutzrecht verfasst und tritt regelmäßig als Referent zu diesem Thema auf.

Dr. Flemming Moos, Fachanwalt für IT-Recht und Partner in der Kanzlei Osborne Clarke am Standort Hamburg. Er ist seit 2001 als Rechtsanwalt zugelassen und war seither im Bereich des IT- und Datenschutzrechts in unterschiedlichen internationalen Kanzleien tätig. Dr. Moos leitet die internationale Data Privacy Service Line bei Osborne Clarke und hat im Datenschutzrecht einen Branchenfokus in den Bereichen Retail, Digital Business sowie Life Science & Healthcare. Schwerpunkte seiner Beratung liegen in Datenschutz-Complianceprojekten, in der Vertretung in komplexen Gerichts- und Behördenverfahren und in der Begleitung datengetriebener Digitalisierungsvorhaben. Er ist Mitglied der International Association of Privacy Professionals (IAPP) und leitet aktuell deren Hamburg KnowledgeNet. Dr. Moos hat diverse Bücher und Fachbeiträge zum Datenschutzrecht verfasst; er tritt regelmäßig als Referent auf den führenden Datenschutzkongressen auf.

Leif Rohwedder, Rechtsanwalt und Senior Legal Counsel in der Konzernrechtsabteilung von Telefónica Deutschland am Standort Hamburg. Er ist seit 2001 als Rechtsanwalt zugelassen und schwerpunktmäßig im Gewerblichen Rechtsschutz, Datenschutzrecht und Vertragsrecht tätig. Bei Telefónica zählt die Vertragsgestaltung und rechtliche Beratung bei der Konzeption von Werbemaßnahmen für die Marke O₂ zu seinen Aufgaben. Daneben doziert er seit 2009 als Referent für Lehrgänge zum Datenschutz in den Gebieten Permission-Management und Datenschutz bei Telemedien. Leif Rohwedder ist außerdem Mitautor eines Formularhandbuchs für Datennutzungs- und Datenschutzverträge.

Dr. Tobias Rothkegel, Rechtsanwalt in der Kanzlei Osborne Clarke am Standort Hamburg. Er ist seit 2016 als Rechtsanwalt zugelassen und im Bereich des IT- und Datenschutzrechts tätig. Ferner berät er zu den rechtlichen Aspekten von Cyber-Security und Blockchain. Herr Rothkegel hat einen Branchenfokus in den Bereichen Life Science und Financial Services und berät dabei internationale Großkonzerne, mittelständische Unternehmen als auch Start-Ups zu sämtlichen Aspekten des Datenschutzrechts und -managements und der Datennutzung sowie rechtlichen Fragenstellungen rund um Cyber-Security und Blockchain. Er hat an zahlreichen Veröffentlichungen im Bereich des Daten-

schutzrechts sowohl in führenden Fachzeitschriften als auch in juristischen Handbüchern und Kommentaren mitgewirkt.

Dr. Jens Schefzig, Rechtsanwalt und Partner in der Kanzlei Osborne Clarke am Standort Hamburg. Nachdem er zuvor für eine andere internationale Kanzlei tätig war, ist er seit 2014 Rechtsanwalt bei Osborne Clarke. Er berät ausschließlich zu Rechtsfragen rund um Daten. Vor seiner Tätigkeit als Rechtsanwalt war Dr. Schefzig als Unternehmensberater bei McKinsey & Company tätig. Er befasst sich deshalb insbesondere auch mit Fragen des Datenschutzmanagements. Dr. Schefzig hat zahlreiche Buch- und Zeitschriftenbeiträge zum Datenschutzrecht verfasst und ist regelmäßiger Referent auf Fachtagungen und -kongressen.

Laurenz Strassemeyer, Diplom-Jurist und Doktorand an der Universität Bonn. Er lässt sich zur datenschutzrechtlichen Regulierung von Künstlicher Intelligenz von Prof. Dr. Specht-Riemenschneider promovieren. Seit Januar 2021 ist er Visiting Student Researcher an der UC Berkeley School of Law am Berkeley Center for Law & Technology. Zuvor arbeitete Herr Strassemeyer zwei Jahre als wissenschaftlicher Mitarbeiter bei Osborne Clarke in der Praxisgruppe IT-Recht & Datenschutz in Hamburg. Nach Abschluss seines Studiums 2018 absolvierte er ein mehrmonatiges Client Secondment für eine Boutique-Kanzlei für Datenschutz und IT-Recht bei einem weltweit führenden Textildiscounter, den er bei der Umsetzung der DSGVO-Vorgaben unterstützte. Herr Strassemeyer ist seit August 2019 zudem Mitglied der Redaktion der Fachzeitschrift Datenschutz-Berater (DSB).

Dr. Anna Zeiter, LL.M. (Stanford), ist Associate General Counsel und Chief Privacy Officer von eBay Inc. Vor ihrer Tätigkeit bei eBay hat Anna Zeiter in Hamburg im Bereich Medienrecht promoviert und war anschließend als Rechtsanwältin bei zwei internationalen Großkanzleien im Bereich Datenschutz-, IT- und eCommerce-Recht tätig. Anschließend hat sie das LL.M.-Programm in Law, Science and Technology Recht an der der Stanford Law School absolviert. Neben ihrer beruflichen Tätigkeit ist Anna Zeiter regelmäßig Referentin bei internationalen Datenschutzkonferenzen und unterrichtet als Dozentin an verschiedenen Universitäten, u. a. in Bern, St. Gallen und Göttingen. Daneben veröffentlicht Frau Dr. Zeiter regelmäßig Beiträge zu datenschutzrechtlichen Themen, beispielsweise im Stanford Transatlantic Technology Law Forum sowie im European Data Protection Law Review. Darüber hinaus ist Anna Zeiter Board Member der International Association of Privacy Professionals (IAPP), Committee Member des Data Protection Officer Networks in Dublin sowie Mitglied des World Economic Forums (WEF).

Die Beiträge geben die persönlichen Meinungen der Autoren wieder.

Inhaltsübersicht

Kapitel 1: Grundlagen des Umgangs mit der DSGVO

I.	Die Anwendung der DSGVO und der nationalen Begleitgesetze	1
II.	Parallelität von DSGVO und „Altgesetzen“	6
III.	Auslegung der DSGVO und der Begleitgesetze	7

Kapitel 2: Grundlagen des Datenschutzrechts

I.	Datenschutz im Anwendungsbereich des EU-Rechts	17
II.	Schutzgut des Datenschutzrechts	18
III.	Grundbegriffe des Datenschutzrechts	20
IV.	Zusammenspiel mit anderen Rechtsmaterien	23

Kapitel 3: Anwendungsbereich des Datenschutzrechts

I.	Überblick über die einschlägigen Regelungen der DSGVO	33
II.	Sachlicher Anwendungsbereich	35
III.	Räumlicher Anwendungsbereich, Art. 3 DSGVO	43
IV.	Anwendungsbereich mitgliedstaatlicher Regelungen	56
V.	Anwendungsbereich sonstiger ausfüllender Normen	60

Kapitel 4: Datenschutzrechtliche Grundsätze

I.	Bedeutung und Funktion der Datenschutzgrundsätze	61
II.	Die Grundsätze im Einzelnen	62
III.	Die Rechenschaftspflicht	70

Kapitel 5: Zulässigkeit der Verarbeitung personenbezogener Daten

I.	Überblick über die einschlägigen Regelungen der DSGVO	74
II.	Gesetzliche Erlaubnisvorschriften	76
III.	Einwilligung der Betroffenen	173

Kapitel 6: Umgang mit Betroffenen

I.	Einführung	211
II.	Systematischer Überblick über die Betroffenenrechte gem. Art. 12–23 DSGVO und Art. 77 ff. DSGVO	212
III.	Informationspflichten (Art. 13 und 14 DSGVO)	214
IV.	Recht auf Auskunft (Art. 15 DSGVO)	277
V.	Recht auf Berichtigung (Art. 16 DSGVO)	358

Inhaltsübersicht

VI. Recht auf Löschung/Recht auf Vergessenwerden (Art. 17 DSGVO) .	367
VII. Recht auf Einschränkung der Datenverarbeitung (Art. 18 DSGVO)..	410
VIII. Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung (Art. 19 DSGVO)	420
IX. Recht auf Datenübertragbarkeit (Art. 20 DSGVO)	429
X. Widerspruchsrecht (Art. 21 DSGVO)	447
XI. Automatisierte Entscheidungen im Einzelfall einschließlich Profiling (Art. 22 DSGVO)	462
XII. Sanktionierung	487

Kapitel 7: Auftragsverarbeitung

I. Begriff und Gegenstand der Auftragsverarbeitung	490
II. Abgrenzung zum Verantwortlichen und zur gemeinsamen Verantwortlichkeit	493
III. Rechtsnatur der Auftragsverarbeitung	498
IV. Typische Fallkonstellationen einer Auftragsverarbeitung	500
V. Rechte und Pflichten aus einer Auftragsverarbeitung	502
VI. Begründung einer Auftragsverarbeitung	506
VII. Auftragsverarbeitung innerhalb von Unternehmensgruppen.	517
VIII. Unterbeauftragungen.	518
IX. Haftung von Auftragsverarbeitern.	522
X. Kontrolle von Auftragsverarbeitern.	526
XI. Dokumentation der Kontrollen	529
XII. Kontrollergebnis	529

Kapitel 8: Verarbeitungen in gemeinsamer, getrennter und alleiniger Verantwortlichkeit

I. Überblick über die einschlägigen Regelungen der DSGVO.	532
II. Gemeinsam für die Verarbeitung Verantwortliche	532
III. Getrennte Verantwortlichkeiten	552
IV. Niederlassungsübergreifende Verarbeitungen	557

Kapitel 9: Internationale Datenübermittlungen

I. Überblick über die einschlägigen Regelungen der DSGVO.	565
II. Einführung in den Regelungsbereich	565
III. Länder mit angemessenem Schutzniveau.	575
IV. Geeignete Garantien für Drittlandtransfers	582
V. Ausnahmen für bestimmte Fälle	614

Kapitel 10: Datenschutzmanagement

I.	Überblick über die einschlägigen Regelungen der DSGVO	627
II.	Terminologie	628
III.	Anforderungen an das Datenschutzmanagement	629
IV.	Risikoadäquates Datenschutzmanagement	630
V.	Konkrete Maßnahmen hängen vom Einzelfall ab	633
VI.	Grundlegende Maßnahmen des Datenschutzmanagements	634
VII.	Datenschutzmanagementsystem	640

Kapitel 11: Datenschutzorganisation

I.	Überblick über die einschlägigen Regelungen der DSGVO	647
II.	Ergänzende Regelungen des BDSG	648
III.	Terminologie	648
IV.	Datenschutzorganisation als Voraussetzung von Datenschutzcompliance	648
V.	Pflicht zur Errichtung einer Datenschutzorganisation	649
VI.	Gestaltung einer Datenschutzorganisation	655
VII.	Beispiele	698

Kapitel 12: Datenschutzprozesse

I.	Prozessuale Umsetzung datenschutzrechtlicher Vorgaben	705
II.	Privacy by Design und by Default, Art. 25 DSGVO	707
III.	Datenlöschung	718
IV.	Verzeichnis von Verarbeitungstätigkeiten	727
V.	Datenschutz-Folgenabschätzung	739
VI.	Umgang mit Datenlecks	758
VII.	Integration des Datenschutzes in allgemeine Unternehmensprozesse	780

Kapitel 13: Technischer Datenschutz und Risikomanagement

I.	Überblick über die einschlägigen Regelungen	794
II.	Allgemeine Grundlagen des technischen Datenschutzrisiko- managements	797
III.	Nutzung der Standards und Vorgehen der Informationssicherheit	806
IV.	Technische Maßnahmen zur datenschutzkonformen Verarbeitung	826
V.	Privacy by Design und Privacy by Default	871
VI.	Ausblick	876

Kapitel 14: Verhaltensregeln und Zertifizierungen

I.	Einleitung	879
II.	Grundsätzliche Unterscheidung und Komplementarität	882
III.	Mehrwert für Unternehmen	883
IV.	Genehmigung von Verhaltensregeln	889
V.	Überwachung genehmigter Verhaltensregeln/Sanktionen im Falle von Verstößen	898
VI.	Inhalte und Gestaltung von Verhaltensregeln	900
VII.	Zertifizierungsverfahren	903

Kapitel 15: Beschäftigtendatenschutz

I.	Überblick über die einschlägigen Regelungen der DSGVO	908
II.	Handlungsoptionen des Gesetzgebers	909
III.	Datenschutzrechtliche Erlaubnistatbestände	918
IV.	Informationspflichten und Betroffenenrechte	935
V.	Überwachungsmaßnahmen – Rechtslage in Deutschland	940
VI.	Handlungsempfehlung	946

Kapitel 16: Behördliche und gerichtliche Verfahren

I.	Aufsichtsbehörden	950
II.	Aufsichtsverfahren	965
III.	Umgang mit Aufsichtsbehörden	977
IV.	Bußgelder	986
V.	Gerichtlicher Rechtsschutz	1012
VI.	Verbandsklage	1025

Kapitel 17: Besondere Themenkomplexe

A. Web Tracking und Online Advertising

I.	Technische Abläufe	1039
II.	Zulässigkeit des Web Tracking und des Online Advertising	1045
III.	Verantwortlichkeit für Web Tracking und Online Advertising	1095
IV.	Zusätzliche Pflichten	1098
V.	Bußgeldrahmen bei Verstößen	1100

B. Customer-Relationship-Management

I.	Überblick über die einschlägigen Regelungen	1103
II.	Datenquellen	1104
III.	Profiling zu Werbezwecken	1106
IV.	Werbliche Kommunikation mit Kunden	1113

C. E-Discovery	
I. Ausgewählte Rahmenbedingungen	1121
II. Kollision mit dem Datenschutz im Beweissicherungsprozess	1124
III. Fazit	1134
D. Cloud Computing	
I. Eigenschaften und Terminologie	1136
II. Cloud-spezifische Problemfelder	1138
E. Big Data	
I. Eigenschaften und Terminologie	1141
II. Big Data-spezifische Problemfelder	1142
F. Gesundheitsdatenschutz	
I. Definition „Gesundheitsdaten“	1148
II. Systematik der datenschutzrechtlichen Regelungen im Gesundheitsbereich	1151
III. Zulässigkeit der Verarbeitung von Gesundheitsdaten auf Basis von Vorschriften aus der DSGVO/dem BDSG	1159
IV. Weitere Besonderheiten nach der DSGVO/dem BDSG bei der Verarbeitung von Gesundheitsdaten	1178
V. (Berufsrechtliche) Schweigepflicht	1181
VI. Verarbeitung zu wissenschaftlichen Forschungszwecken	1189

Kapitel 18: Österreichisches Datenschutzrecht

I. Gesetzliche Grundlagen	1204
II. Nutzung von Öffnungsklauseln	1205
III. Grundrecht auf Datenschutz	1209
IV. Marketing und Kontaktaufnahme zu Werbezwecken	1212
V. Österreichische Spezialregelungen	1215
VI. Arbeitnehmer-Datenschutz	1229
VII. Österreichische Entscheidungen	1235
VIII. Rechtsdurchsetzung und Verfahrensrecht	1250

Kapitel 19: Leitentscheidungen des EuGH zur DSGVO

I. Einleitung	1264
II. Leitentscheidungen des EuGH	1265

**Kapitel 20: Vorgehensweise zur Umsetzung von
DSGVO-Anforderungen im Unternehmen**

I.	Anpassungsbedarf im Unternehmen	1303
II.	Leitbild zur Umsetzung der DSGVO im Unternehmen	1305
III.	Ausgestaltung eines Umsetzungsprojekts	1305
IV.	Erste Erfahrungen aus der Umsetzungspraxis	1319
V.	Fazit	1321

Kapitel 21: Weitere rechtliche Entwicklungen und Ausblick

I.	Datenschutzrecht als dynamisches Rechtsgebiet.	1323
II.	Gesetzgeber	1324
III.	Datenschutzbehörden	1330
IV.	Rechtsprechung	1334
V.	Entwicklung der Datenschutzpraxis	1334
VI.	Ausblick	1335

Inhaltsverzeichnis

Vorwort	V
Autorenverzeichnis	VII
Inhaltsübersicht	XI
Abkürzungsverzeichnis.....	XLVII
Literaturverzeichnis.....	LIII
Kapitel 1: Grundlagen des Umgangs mit der DSGVO (Moos/Schefzig).	1
I. Die Anwendung der DSGVO und der nationalen Begleitgesetze	1
1. Stand der Umsetzung in den Unternehmen	2
2. Zeitliche Geltung	2
3. Unmittelbare Geltung	3
4. Zusammenspiel mit anderen Regelwerken.....	3
a) Begleitgesetze auf Basis von Öffnungsklauseln.....	3
b) Spezialgesetzliche Datenschutzregelungen in Richtlinien und Gesetzen.	4
c) Datenschutzregelungen außerhalb des Anwendungsbereichs der DSGVO	5
d) Zwischenergebnis.....	5
II. Parallelität von DSGVO und „Altgesetzen“	6
III. Auslegung der DSGVO und der Begleitgesetze	7
1. Auslegung der DSGVO.....	8
a) Autonome Auslegung des Unionsrechts	8
b) Auslegungsmethoden.....	8
c) Relevanz existierender Rechtsprechung	14
2. Auslegung der Begleitgesetze	15
a) Auslegungsmethoden.....	15
b) Relevanz existierender Rechtsprechung	16
Kapitel 2: Grundlagen des Datenschutzrechts (Moos)	17
I. Datenschutz im Anwendungsbereich des EU-Rechts	17
II. Schutzgut des Datenschutzrechts	18
1. Schutz der natürlichen Personen	18
2. Schutz des freien Datenverkehrs	19

Inhaltsverzeichnis

III. Grundbegriffe des Datenschutzrechts	20
1. Personenbezug	20
2. Datenverarbeitung	21
3. Verantwortlicher	22
IV. Zusammenspiel mit anderen Rechtsmaterien	23
1. Wettbewerbsrecht	23
2. Kartellrecht	24
a) Missbräuchliche Nutzung von Kundendaten	24
b) Missbräuchliche Zugangsverweigerung zu Daten	25
c) AGB-Recht	26
3. Besonderer Geheimnisschutz	27
a) Berufsrechtliche Schweigepflichten	27
b) Strafrechtliche Schweigepflichten	28
c) Fernmeldegeheimnis	28
d) Schutz von Geschäftsgeheimnissen	29
4. Arbeits- und Mitbestimmungsrecht	30
a) Umfang von Datenerhebungen im Bewerbungsgespräch	30
b) Betriebsvereinbarungen als datenschutzrechtliche Erlaubnisvorschrift	31
c) Einsicht in Personalakten	31
d) Kündigungsschutz für Datenschutzbeauftragte	32
Kapitel 3: Anwendungsbereich des Datenschutzrechts (Meyerdierks)	33
I. Überblick über die einschlägigen Regelungen der DSGVO	33
II. Sachlicher Anwendungsbereich	35
1. Verarbeitung personenbezogener Daten, Art. 2 Abs. 1 DSGVO	35
2. Ausnahmetatbestände, Art. 2 Abs. 2 bis 4 DSGVO	37
III. Räumlicher Anwendungsbereich, Art. 3 DSGVO	43
1. Niederlassungsprinzip, Art. 3 Abs. 1 DSGVO	43
a) Verarbeitung im Rahmen der Tätigkeiten der Niederlassung eines Verantwortlichen	44
b) Verarbeitung im Rahmen der Tätigkeiten der Niederlassung eines Auftragsverarbeiters	45
2. Marktortprinzip, Art. 3 Abs. 2 DSGVO	46
a) Anbieten von Waren oder Dienstleistungen, Art. 3 Abs. 2 lit. a DSGVO	47
b) Verhaltensbeobachtung, Art. 3 Abs. 2 lit. b DSGVO	51
c) Betroffene Person in der EU	53

3. Räumlicher Anwendungsbereich bei mehreren Beteiligten	54
4. Räumliche Reichweite der Betroffenenrechte	56
5. Geltung der DSGVO im EWR	56
IV. Anwendungsbereich mitgliedstaatlicher Regelungen	56
V. Anwendungsbereich sonstiger ausfüllender Normen	60
Kapitel 4: Datenschutzrechtliche Grundsätze (Moos)	61
I. Bedeutung und Funktion der Datenschutzgrundsätze	61
II. Die Grundsätze im Einzelnen	62
1. Rechtmäßigkeit und Verarbeitung nach Treu und Glauben	62
2. Transparenz	64
3. Zweckbindung	64
4. Datenminimierung	66
5. Datenrichtigkeit	66
6. Speicherbegrenzung	68
7. Integrität und Vertraulichkeit	69
III. Die Rechenschaftspflicht	70
Kapitel 5: Zulässigkeit der Verarbeitung personenbezogener Daten <i>(Arning/Rohwedder)</i>	73
I. Überblick über die einschlägigen Regelungen der DSGVO	74
II. Gesetzliche Erlaubnisvorschriften	76
1. Verarbeitung personenbezogener Daten zu Zwecken der Vertrags- erfüllung oder zur Durchführung vorvertraglicher Maßnahmen	77
a) Verarbeitung personenbezogener Daten zu Zwecken der Vertragserfüllung	78
b) Verarbeitung personenbezogener Daten zu Zwecken der Durchführung vorvertraglicher Maßnahmen	84
c) Erforderlichkeit der Datenverarbeitung für die genannten Zwecke	85
2. Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung	98
3. Verarbeitung personenbezogener Daten auf Basis einer Interessenabwägung	101
a) Berechtigte Interessen des Verantwortlichen oder eines Dritten	102
b) Erforderlichkeit einer Datenverarbeitung zur Wahrung der berechtigten Interessen	104

Inhaltsverzeichnis

c) Keine überwiegenden Interessen/Rechte der betroffenen Person am Ausschluss der Datenverarbeitung	105
4. Verarbeitung personenbezogener Daten zu Zwecken der Werbung	111
5. Verhältnis der Alternativen des Art. 6 Abs. 1 DSGVO zueinander.	116
6. Verhältnis zwischen besonders praxisrelevanten nationalen Vorschriften und der DSGVO	118
a) Videoüberwachung öffentlich zugänglicher Räume gem. § 4 BDSG	119
b) Scoring und Bonitätsauskünfte gem. § 31 BDSG	122
c) Verhältnis zwischen dem Kunsturhebergesetz und der DSGVO	125
7. Zweckänderung – Verarbeitung personenbezogener Daten zu einem anderen Zweck	129
a) Zweckänderung auf Basis einer Rechtsvorschrift	129
b) Zweckänderung auf Basis einer Einwilligung	133
c) Zweckänderung auf Basis des Kompatibilitätstests gem. Art. 6 Abs. 4 DSGVO	133
d) Weitere datenschutzrechtliche Pflichten im Fall der Zweckänderung	135
8. Verarbeitung besonderer Kategorien personenbezogener Daten . .	136
a) Besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO)	136
b) Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten	142
c) Voraussetzungen für die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 2 DSGVO)	144
9. Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten – Art. 10 DSGVO	160
10. Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist – Art. 11 DSGVO	163
a) Keine Pflicht zur Verarbeitung von identifizierenden Merkmalen	163
b) Pflichten und Privilegierung des Verantwortlichen gem. Art. 11 Abs. 2 DSGVO	165
11. Besondere Verarbeitungssituationen	172
12. Zulässigkeit der Verarbeitung personenbezogener Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden	173
13. Sanktionierung	173
III. Einwilligung der Betroffenen	173
1. Überblick über die einschlägigen Regelungen	174

2. Allgemeine Voraussetzungen der Einwilligung	176
a) Form der Willensbekundung	176
b) Freiwilligkeit	182
c) Erteilung für den bestimmten Fall	189
d) Transparenzgebot	189
e) Einwilligungen als Gegenstand von AGB	192
f) Widerruflichkeit	195
g) Nachweisbarkeit	197
h) Gültigkeitsdauer	200
3. Einwilligung von Kindern	201
a) Voraussetzungen bei direkten Angeboten von Fernabsatzdiensten	201
b) Vergewisserungspflicht des Verantwortlichen	203
4. Einwilligung bei sensiblen Datenkategorien	204
5. Wirksamkeit von Alt-Einwilligungen	205
Kapitel 6: Umgang mit Betroffenen (<i>Arning</i>)	207
I. Einführung	211
II. Systematischer Überblick über die Betroffenenrechte gem. Art. 12–23 DSGVO und Art. 77 ff. DSGVO	212
III. Informationspflichten (Art. 13 und 14 DSGVO)	214
1. Informationspflichten bei der Direkterhebung von Daten von der betroffenen Person (Art. 13 DSGVO)	216
a) Voraussetzungen der Informationspflicht nach Art. 13 DSGVO	216
b) Systematik von Art. 13 DSGVO	216
c) Inhalte der Informationspflichten nach Art. 13 Abs. 1 DSGVO	218
d) Inhalte der Informationspflichten nach Art. 13 Abs. 2 DSGVO	224
e) Zeitpunkt der Information	234
f) Information im Fall der Zweckänderung (Art. 13 Abs. 3 DSGVO)	235
g) Information im Fall der Änderung der Datenverarbeitung	238
h) Ausnahmen von der Informationspflicht (Art. 13 Abs. 4 DSGVO)	241
i) Keine Pflicht zur „Nachinformation“ im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden	244
j) Erfüllung der Informationspflichten als Zulässigkeits- voraussetzung?	244
2. Informationspflichten bei der Erhebung von Daten aus anderen Quellen als von der betroffenen Person (Art. 14)	246
a) Voraussetzungen der Informationspflicht nach Art. 14 DSGVO	246

Inhaltsverzeichnis

b) Inhalte der Informationspflichten nach Art. 14 Abs. 1 DSGVO	246
c) Inhalte der Informationspflichten nach Art. 14 Abs. 2 DSGVO	247
d) Weitere Informationen, die nicht in Art. 14 Abs. 1 und Abs. 2 DSGVO genannt werden	248
e) Zeitpunkt der Informationserteilung nach Art. 14 Abs. 3 DSGVO	249
f) Information im Fall der Zweckänderung (Art. 14 Abs. 4 DSGVO) und im Fall der Änderung der Datenverarbeitung	250
g) Ausnahmen von der Informationspflicht nach Art. 14 DSGVO	250
h) „Nachinformation“ und keine Zulässigkeitsvoraussetzung	259
3. Modalitäten der Information der betroffenen Personen (Art. 12 DSGVO)	259
a) Formulierung der Information	259
b) Information in leicht zugänglicher Form	262
c) Form	262
d) Unentgeltlichkeit	267
e) Kombination mit standardisierten Bildsymbolen	268
4. Rechenschaftspflicht	269
5. Beispiele für Möglichkeiten zur Darstellung der Informationen	269
a) Gestaltung als Checkliste	270
b) Gruppierung von Informationen	271
c) Gestaltung als „Story“/nach dem geschichtlichen Ablauf der Datenverarbeitung	271
d) Gestaltung unter Einsatz von Tabellen	272
e) Multilayered notice/Mehrebenenansatz	274
IV. Recht auf Auskunft (Art. 15 DSGVO)	277
1. Auskunftsrecht nach Art. 15 Abs. 1 und 2 DSGVO	279
a) Voraussetzungen des Auskunftsrechts nach Art. 15 Abs. 1 und 2 DSGVO	279
b) Inhalte des Auskunftsrechts nach Art. 15 Abs. 1 und 2 DSGVO	279
c) Umfang des Auskunftsrechts nach Art. 15 Abs. 1 und 2 DSGVO	287
2. Ausnahmen vom Auskunftsrecht	289
a) Ausnahmen vom Auskunftsrecht gem. Art. 15 Abs. 1 und Abs. 2 DSGVO in der DSGVO	293
b) Ausnahmen vom Auskunftsrecht gem. Art. 15 Abs. 1 und Abs. 2 DSGVO im nationalen Recht	303
3. Modalitäten der Auskunftserteilung (Art. 12 DSGVO)	309
a) Antragserfordernis	309
b) Erleichterung der Rechtsausübung (Art. 12 Abs. 2 S. 1 DSGVO)	311

c) Identifizierung des Antragstellers (Art. 12 Abs. 6 DSGVO) . . .	312
d) Formulierung der Auskunft (Art. 12 Abs. 1 DSGVO)	319
e) Form der Auskunft	320
f) Unentgeltlichkeit (Art. 12 Abs. 5 S. 2 lit. a DSGVO)	321
g) Frist zur Erteilung der Auskunft sowie von Informationen über das Auskunftsverlangen und ggf. über dessen Ablehnung (Art. 12 Abs. 3 und Abs. 4 DSGVO)	323
h) Zweckbindung von Daten im Zusammenhang mit der Auskunftserteilung	330
4. Recht der betroffenen Person, eine Kopie ihrer Daten zu erhalten (Art. 15 Abs. 3 und 4 DSGVO)	330
a) Inhalte und Umfang der Kopie nach Art. 15 Abs. 3 DSGVO . . .	330
b) Ausnahmen vom Recht auf Erhalt einer Kopie in der DSGVO . .	341
c) Modalitäten im Hinblick auf die Aushändigung der Kopie gem. Art. 15 Abs. 3 DSGVO	349
d) Praktischer Umgang mit Anträgen auf Erhalt einer Kopie	353
5. Auskunft im Hinblick auf Daten bzw. Erhalt von Kopien von Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden . .	358
V. Recht auf Berichtigung (Art. 16 DSGVO)	358
1. Inhalte des Berichtigungsrechts nach Art. 16 DSGVO	358
a) Berichtigung unrichtiger personenbezogener Daten (S. 1)	359
b) Vervollständigung unvollständiger personenbezogener Daten (S. 2)	359
c) Darlegungs- und Beweislast	360
2. Ausnahmen vom Berichtigungsrecht	364
3. Modalitäten des Berichtigungs- bzw. Vervollständigungs- anspruchs (Art. 12 DSGVO)	365
4. Mitteilungspflicht nach Art. 19 DSGVO	367
5. Berichtigung/Vervollständigung im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden	367
VI. Recht auf Löschung/Recht auf Vergessenwerden (Art. 17 DSGVO) . .	367
1. Voraussetzungen des Rechts der betroffenen Person auf Löschung sowie der Löschpflicht des Verantwortlichen (Art. 17 Abs. 1 DSGVO)	368
a) Recht der betroffenen Person auf Löschung ihrer Daten	368
b) Pflicht des Verantwortlichen zur Datenlöschung	369
c) Löschungsgründe: Tatbestandsalternativen des Art. 17 Abs. 1 DSGVO	376
2. Rechtsfolge: Löschen i. S. d. Art. 17 Abs. 1 DSGVO	383

Inhaltsverzeichnis

3. Informationspflichten im Fall der Öffentlichmachung der Daten (Art. 17 Abs. 2 DSGVO)	389
a) Voraussetzungen des Rechts auf Vergessenwerden	390
b) Vom Verantwortlichen zur Erfüllung des Rechts auf Vergessenwerden zu ergreifende Maßnahmen	391
4. Ausnahmen vom Recht auf Löschung gem. Art. 17 Abs. 1 DSGVO und von den Informationspflichten gem. Art. 17 Abs. 2 DSGVO (Art. 17 Abs. 3, Art. 12 DSGVO)	393
a) Ausnahmen nach Art. 17 Abs. 3 DSGVO	393
b) Weitere Ausnahmen in der DSGVO	396
c) Ausnahmen im nationalen Recht	397
5. Modalitäten des Lösungsanspruchs (Art. 12 DSGVO)	402
a) Frist bei Löschung aufgrund der in Art. 17 Abs. 1 DSGVO enthaltenen Löschungsspflicht	403
b) Frist bei Löschung gem. Art. 17 Abs. 1 DSGVO infolge eines Antrags der betroffenen Person	406
c) Frist für die Information nach Art. 17 Abs. 2 DSGVO	408
6. Mitteilungspflicht nach Art. 19 DSGVO/Verhältnis zu Art. 17 Abs. 2 DSGVO	409
7. Recht auf Löschung im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden	410
VII. Recht auf Einschränkung der Datenverarbeitung (Art. 18 DSGVO) . .	410
1. Inhalte des Rechts auf Einschränkung der Datenverarbeitung . . .	411
a) Voraussetzungen (Art. 18 Abs. 1 DSGVO)	411
b) Rechtsfolge: Einschränkung der Datenverarbeitung	416
c) Bedingungen für die Weiterverarbeitung der Daten (Art. 18 Abs. 2 DSGVO, Erwägungsgrund 67 DSGVO)	416
d) Informationspflichten für den Fall, dass die Daten wieder uneingeschränkt verarbeitet werden (Art. 18 Abs. 3 DSGVO) . .	417
2. Ausnahmen vom Recht auf Einschränkung der Datenverarbeitung	418
3. Modalitäten des Rechts auf Einschränkung der Datenverarbeitung (Art. 12 DSGVO)	419
4. Mitteilungspflicht nach Art. 19 DSGVO	420
5. Recht auf Einschränkung der Datenverarbeitung im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden . .	420
VIII. Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung (Art. 19 DSGVO)	420
1. Voraussetzungen der Mitteilungspflicht	421

2. Mitteilung der Berichtigung, Löschung oder Einschränkung der Verarbeitung	424
3. Unterrichtungspflicht gegenüber der betroffenen Person (Art. 19 S. 2 DSGVO)	425
4. Weitere Ausnahmen von der Mitteilungspflicht	427
5. Modalitäten der Mitteilungspflicht (Art. 12 DSGVO)	428
6. Mitteilungspflicht im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden	429
IX. Recht auf Datenübertragbarkeit (Art. 20 DSGVO)	429
1. Inhalte des Rechts auf Datenübertragbarkeit	431
a) Voraussetzungen des Rechts auf Datenübertragbarkeit (Art. 20 Abs. 1 DSGVO)	431
b) Rechtsfolgen: Bereitstellung (Abs. 1) bzw. Übermittlung (Abs. 2) von Daten durch den Verantwortlichen	434
c) Verhältnis zu Art. 17 DSGVO (Art. 20 Abs. 3 S. 1 DSGVO) ..	438
2. Ausnahmen vom Recht auf Datenübertragbarkeit (Art. 20 Abs. 4, Art. 12 DSGVO)	439
a) Beeinträchtigung von Rechten und Freiheiten anderer Personen (Art. 20 Abs. 4 DSGVO)	439
b) Weitere Ausnahmen	445
3. Modalitäten des Rechts auf Datenübertragbarkeit	445
4. Recht auf Datenübertragbarkeit im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden	447
X. Widerspruchsrecht (Art. 21 DSGVO)	447
1. Inhalte des Widerspruchsrechts	448
a) Allgemeines Widerspruchsrecht gem. Art. 21 Abs. 1 DSGVO ..	448
b) Widerspruchsrecht bei der Datenverarbeitung zu Zwecken der Direktwerbung gem. Art. 21 Abs. 2 und 3 DSGVO	453
c) Informationspflichten nach Art. 21 Abs. 4 DSGVO	456
2. Weitere Ausnahmen vom Widerspruchsrecht	459
3. Modalitäten des Widerspruchsrechts	460
4. Widerspruchsrecht im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden	462
XI. Automatisierte Entscheidungen im Einzelfall einschließlich Profiling (Art. 22 DSGVO)	462
1. Inhalte des Rechts, keinen automatisierten Einzelfallentscheidungen unterworfen zu werden	464
a) Voraussetzungen des Rechts, keinen automatisierten Einzelfallentscheidungen unterworfen zu werden	464

Inhaltsverzeichnis

b) Rechtsfolgen aus Art. 22 Abs. 1 DSGVO	475
c) Ausnahmen vom Recht, keinen automatisierten Einzelfall- entscheidungen unterworfen zu werden (Art. 22 Abs. 2 und 3 DSGVO)	475
d) Sonderfall: Verarbeitung besonderer Kategorien personen- bezogener Daten.	485
2. Modalitäten des Rechts, keinen automatisierten Einzelfall- entscheidungen unterworfen zu werden	486
3. Das Recht, keinen automatisierten Einzelfallentscheidungen unterworfen zu werden, im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden	486
XII. Sanktionierung.	487
Kapitel 7: Auftragsverarbeitung (Moos/Cornelius)	489
I. Begriff und Gegenstand der Auftragsverarbeitung	490
II. Abgrenzung zum Verantwortlichen und zur gemeinsamen Verantwortlichkeit	493
1. Abgrenzung zum Verantwortlichen	493
a) Entscheidungsbefugnis über Zwecke	494
b) Entscheidungsbefugnis über Mittel	495
2. Abgrenzung zur gemeinsamen Verantwortlichkeit.	497
III. Rechtsnatur der Auftragsverarbeitung	498
IV. Typische Fallkonstellationen einer Auftragsverarbeitung	500
V. Rechte und Pflichten aus einer Auftragsverarbeitung	502
1. Pflichten des Auftragsverarbeiters	502
2. Rechte und Pflichten des Verantwortlichen	504
a) Erteilung von Weisungen	505
b) Dokumentation der Weisungen	506
VI. Begründung einer Auftragsverarbeitung	506
1. Auswahl des Auftragsverarbeiters	506
2. Abschluss eines Auftragsverarbeitungsvertrages	508
a) Form des Auftragsverarbeitungsvertrages	509
b) Inhalt des Auftragsverarbeitungsvertrages	510
c) Umstellung von alten Auftragsverarbeitungsverträgen auf die DSGVO	514
VII. Auftragsverarbeitung innerhalb von Unternehmensgruppen.	517

VIII. Unterbeauftragungen	518
1. Zustimmungspflicht des Verantwortlichen.	518
a) Art der Erteilung.	519
b) Einspruchsrecht bei Allgemeinzustimmung.	520
2. Begründung des Unterauftragsverhältnisses	521
IX. Haftung von Auftragsverarbeitern	522
1. Haftung auf Schadensersatz	522
a) Haftung für eigenes Verschulden	523
b) Haftung von Unterauftragsverarbeitern.	523
c) Beweislastumkehr.	523
d) Gesamtschuldnerische Haftung	524
2. Sanktionen gegen Auftragsverarbeiter	524
X. Kontrolle von Auftragsverarbeitern	526
1. Recht zur Kontrolle	526
2. Pflicht zur Kontrolle	527
3. Art und Häufigkeit der Kontrolle.	527
a) Art der Kontrolle.	528
b) Häufigkeit der Kontrolle	529
XI. Dokumentation der Kontrollen.	529
XII. Kontrollergebnis.	529

Kapitel 8: Verarbeitungen in gemeinsamer, getrennter und alleiniger Verantwortlichkeit (Moos)	531
I. Überblick über die einschlägigen Regelungen der DSGVO.	532
II. Gemeinsam für die Verarbeitung Verantwortliche.	532
1. Der Begriff der gemeinsamen Verantwortlichkeit (Art. 4 Nr. 7 DSGVO)	533
a) Gemeinsame Entscheidung mehrerer Stellen	535
b) Entscheidung über Zwecke und Mittel der Verarbeitung	536
c) Entscheidungshilfen für die Unternehmenspraxis	538
d) Abgrenzung von der Auftragsverarbeitung.	541
2. Reichweite der gemeinsamen Verantwortlichkeit	541
3. Zulässigkeit der Verarbeitungen durch gemeinsam Verantwortliche	542
4. Rechte und Pflichten der gemeinsam Verantwortlichen	543
a) Abschluss einer Vereinbarung über die gemeinsame Verantwortlichkeit	544
b) Geltendmachung der Rechte der Betroffenen.	548

c) Zurverfügungstellung der wesentlichen Teile der Vereinbarung	549
d) Mitteilung der erforderlichen Informationen nach Art. 13 und Art. 14 DSGVO	550
5. Haftung und Sanktionen	551
III. Getrennte Verantwortlichkeiten	552
1. Begriff der Übermittlung	553
2. Zulässigkeit von Datenübermittlungen an Dritte	554
3. Typische Fallkonstellationen getrennter Verantwortlichkeiten	554
4. Besondere Aspekte von Datenübermittlungen im Konzern	554
a) Fehlendes Konzernprivileg	555
b) Erlaubnis durch Interessenabwägung	555
c) Öffnungsklausel für nationale Sonderregelungen	557
d) Internationale Datenübermittlungen	557
IV. Niederlassungsübergreifende Verarbeitungen	557
1. Die Bestimmung einer Hauptniederlassung für eine niederlassungsübergreifende Verantwortlichkeit	558
2. Die Spezifizierung der Verarbeitungsverfahren	561
Kapitel 9: Internationale Datenübermittlungen (Moos/Zeiter)	563
I. Überblick über die einschlägigen Regelungen der DSGVO	565
II. Einführung in den Regelungsbereich	565
1. Sonderregelungen für „Drittlands-Übermittlungen“	565
a) Begriff des Drittlands	565
b) Geltung auch für internationale Organisationen	569
c) Begriff der „Übermittlung“	570
d) Geltung auch für Weiterübermittlungen	571
2. Anforderungen an Drittlands-Übermittlungen	571
a) Einhaltung der allgemeinen DSGVO-Anforderungen	572
b) Gewährleistung eines angemessenen Schutzniveaus	572
c) Verantwortlicher und Auftragsverarbeiter als Regelungsadressat	574
3. Fortgeltung etablierter Sicherungsinstrumente	574
III. Länder mit angemessenem Schutzniveau	575
1. Bestehende Angemessenheitsbeschlüsse	576
a) Einschränkungen bei Datentransfers nach Kanada	577
b) Einschränkungen bei Datentransfers nach Israel	578
c) Der Sonderfall USA: Ungültigkeit des EU-US Privacy Shield	578

2. Neue Angemessenheitsentscheidungen unter der DSGVO	579
a) Anforderungen an Angemessenheitsfeststellungen der Kommission	581
b) Das Verfahren der Angemessenheitsfeststellung	581
3. Fortlaufende Überwachung der Angemessenheit	581
IV. Geeignete Garantien für Drittlandtransfers.	582
1. Standarddatenschutzklauseln.	584
a) Existierende Standardvertragsklauseln nach Maßgabe der RL 95/46/EG.	584
b) Neue Standarddatenschutzklauseln nach DSGVO.	587
c) Standarddatenschutzklauseln einer Aufsichtsbehörde	587
d) Verwendung der Standarddatenschutzklauseln	587
2. Verbindliche interne Datenschutzvorschriften (BCRs)	596
a) Anforderungen an BCRs	598
b) Arbeitsdokumente der Artikel-29-Datenschutzgruppe	600
c) Existierende BCR.	604
d) Genehmigungsverfahren für BCR	605
e) Integration von BCR in ein Datenschutz-Managementsystem nach DSGVO.	609
3. Genehmigte Verhaltensregeln	612
4. Zertifizierungen.	613
5. Sonstige behördlich genehmigte Vertragsklauseln	613
V. Ausnahmen für bestimmte Fälle.	614
1. Einwilligung der Betroffenen.	615
a) Ausdrückliche Erteilung der Einwilligung	615
b) Notwendigkeit gesonderter Erteilung	616
c) Informiertheit der Einwilligung	616
2. Erforderlichkeit für die Vertragserfüllung	618
3. Sonstige Ausnahmefälle	618
a) Im Interesse der betroffenen Person geschlossener Vertrag	618
b) Wichtige Gründe des öffentlichen Interesses	619
c) Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen.	620
d) Schutz lebenswichtiger Interessen	622
e) Übermittlungen aus einem Register.	622
4. Auffangregelung für Einzelübermittlungen.	623
a) Keine wiederholte Übermittlung	624
b) Begrenzte Zahl betroffener Personen.	624
c) Zwingende berechnete Interessen	624
d) Keine überwiegenden Interessen der betroffenen Person	625

Inhaltsverzeichnis

e) Umfassende Beurteilung und angemessene Garantien	625
f) Information der Aufsichtsbehörde	625
Kapitel 10: Datenschutzmanagement (Schefzig)	627
I. Überblick über die einschlägigen Regelungen der DSGVO	627
II. Terminologie	628
III. Anforderungen an das Datenschutzmanagement	629
IV. Risikoadäquates Datenschutzmanagement	630
1. Risikobewertung grundlegend.	630
2. Risikoprofil eines Unternehmens	631
3. Konkrete Maßnahmen hängen vom Einzelfall ab	632
V. Konkrete Maßnahmen hängen vom Einzelfall ab	633
VI. Grundlegende Maßnahmen des Datenschutzmanagements	634
1. Einführung	634
2. Unternehmensrichtlinie zum Datenschutz	634
3. Datenschutzorganisation	637
4. Datenschutzstrategie	637
5. Meldewege und Whistleblowing	637
6. Auditierungen	638
7. Einzelfallprüfungen und -beratung	638
8. Schulungen	638
9. Sonstige Maßnahmen	639
VII. Datenschutzmanagementsystem	640
1. Sinn eines Datenschutzmanagementsystems	640
2. Gestaltung eines Datenschutzmanagementsystems	640
a) Orientierung an ähnlichen Systemen bzw. Standards	640
b) Drei Säulen	641
c) Schematische Darstellung eines Datenschutzmanagement- systems	642
3. Aufbau eines Datenschutzmanagementsystems	643
4. Messung des Erfolgs eines Datenschutzmanagementsystems	643
Kapitel 11: Datenschutzorganisation (Schefzig)	647
I. Überblick über die einschlägigen Regelungen der DSGVO	647
II. Ergänzende Regelungen des BDSG	648