Kommunikation und Recht

Handbuch

Moos / Schefzig / Arning (Hrsg.)

Praxishandbuch DSGVO

einschließlich BDSG und spezifischer Anwendungsfälle

2. Auflage

dfv Mediengruppe

R&W Fachmedien Recht und Wirtschaft

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)

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.d-nb.de abrufbar.

ISBN 978-3-8005-1728-2

dfv Mediengruppe

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

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 Wirtschaftsrechtskanzleien 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. Flemming 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 O_2 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 7: Auftragsverarbeitung

Kapitel 8: Verarbeitungen in gemeinsamer, getrennter und alleiniger Verantwortlichkeit

Kapitel 9: Internationale Datenübermittlungen

Kapitel 10: Datenschutzmanagement

Kapitel 11: Datenschutzorganisation

Kapitel 12: Datenschutzprozesse

Kapitel 13: Technischer Datenschutz und Risikomanagement

Kapitel 14: Verhaltensregeln und Zertifizierungen

Kapitel 15: Beschäftigtendatenschutz

Kapitel 16: Behördliche und gerichtliche Verfahren

Kapitel 17: Besondere Themenkomplexe

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

Kapitel 21: Weitere rechtliche Entwicklungen und Ausblick

Inhaltsverzeichnis