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

© 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

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 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

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

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 *(Arning/Rohwedder)* 73
I. Überblick über die einschlägigen Regelungen der DSGVO 74
II. Gesetzliche Erlaubnisvorschriften 76
1. Verarbeitung personenbezogener Daten zu Zwecken der Vertragserfüllung 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

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 *(Arning)* 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

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. Vervollständigungsanspruchs (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

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 Löschungsanspruchs (Art. 12 DSGVO) 402
a) Frist bei Löschung aufgrund der in Art. 17 Abs. 1 DSGVO enthaltenen Löschungspflicht 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 Einzelfall-entscheidungen unterworfen zu werden 464
a) Voraussetzungen des Rechts, keinen automatisierten Einzelfallentscheidungen unterworfen zu werden 464

b) Rechtsfolgen aus Art. 22 Abs. 1 DSGVO ... 475
c) Ausnahmen vom Recht, keinen automatisierten Einzelfallentscheidungen unterworfen zu werden (Art. 22 Abs. 2 und 3 DSGVO) ... 475
d) Sonderfall: Verarbeitung besonderer Kategorien personenbezogener Daten ... 485
2. Modalitäten des Rechts, keinen automatisierten Einzelfallentscheidungen 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 berechtigte Interessen 624
d) Keine überwiegenden Interessen der betroffenen Person 625

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

III. Terminologie ... 648
IV. Datenschutzorganisation als Voraussetzung von Datenschutzcompliance ... 648
V. Pflicht zur Errichtung einer Datenschutzorganisation ... 649
1. Datenschutz-Grundverordnung ... 649
a) Gesetzliche Vorgaben ... 649
b) Konkrete Wertung ... 650
2. Gesellschaftsrechtliche Verpflichtung in Deutschland ... 652
3. Ordnungswidrigkeitenrecht ... 653
4. Fazit ... 654
VI. Gestaltung einer Datenschutzorganisation ... 655
1. Der Zweck einer Datenschutzorganisation ... 655
2. Aufgaben einer Datenschutzorganisation ... 655
a) Vier grundlegende Aufgaben ... 655
b) Beachtung und Anwendung des Datenschutzrechts im operativen Geschäft ... 655
c) Beratung ... 656
d) Richtlinienkompetenz ... 656
e) Auditierung und Überwachung ... 656
3. Elemente einer Datenschutzorganisation ... 656
a) Einführung ... 656
b) Die Geschäftsleitung ... 657
c) Der Datenschutzbeauftragte ... 657
d) Datenschutzberater ... 694
e) Datenschutzmanager ... 694
f) Datenschutzexperten ... 695
g) Datenschutzkoordinatoren ... 696
h) Sonstige Mitarbeiter des Unternehmens ... 696
i) (Inländischer) Vertreter ... 696
4. Entwicklung einer Datenschutzorganisation ... 697
VII. Beispiele ... 698
1. Verwendung der Beispiele ... 698
2. Datenschutzorganisation in kleinen Unternehmen ... 698
3. Datenschutzorganisation in mittleren Unternehmen ... 699
4. Datenschutzorganisation im Großkonzern ... 700

Kapitel 12: Datenschutzprozesse *(Gardyan-Eisenlohr/Cornelius)* ... 703
I. Prozessuale Umsetzung datenschutzrechtlicher Vorgaben ... 705

II. Privacy by Design und by Default, Art. 25 DSGVO 707
1. Überblick über die einschlägigen Regelungen der DSGVO 708
2. Wer ist für Privacy by Design und by Default verantwortlich? 708
3. Was bedeutet Privacy by Design und by Default? 710
a) Datenschutz durch Technikgestaltung, Art. 25 Abs. 1 DSGVO. 711
b) Datenschutz durch datenschutzfreundliche Voreinstellungen, Art. 25 Abs. 2 DSGVO 715
c) Genehmigte Zertifizierungsverfahren, Art. 25 Abs. 3 DSGVO. 718
III. Datenlöschung 718
1. Allgemeines 718
2. Geschäftliche Relevanz 721
3. Löschkonzept 722
4. Praktische Hinweise für die Implementierung 726
IV. Verzeichnis von Verarbeitungstätigkeiten 727
1. Überblick über die einschlägigen Regelungen der DSGVO 728
2. Aufzeichnungspflichten statt Meldepflicht und Verfahrensverzeichnis 729
3. Verarbeitungsverzeichnis des Verantwortlichen 729
a) Wer ist zur Führung eines Verarbeitungsverzeichnisses nach Art. 30 Abs. 1 DSGVO verpflichtet? 729
b) Inhalt des Verarbeitungsverzeichnisses 731
c) Form des Verarbeitungsverzeichnisses 735
4. Verarbeitungsverzeichnis des Auftragsverarbeiters 737
5. Praktische Hinweise zur Implementierung 738
V. Datenschutz-Folgenabschätzung 739
1. Überblick über die einschlägigen Regelungen der DSGVO 741
2. Wer ist für eine Datenschutz-Folgenabschätzung verantwortlich? . 741
3. Wann muss eine Datenschutz-Folgenabschätzung erfolgen? 742
a) Voraussichtlich hohes Risiko (Art. 35 Abs. 1 S. 1 DSGVO).... 744
b) Regelbeispiele (Art. 35 Abs. 3 DSGVO)..... 747
c) Positivliste der Aufsichtsbehörden (Art. 35 Abs. 4 DSGVO)... 748
d) Mögliche Befreiung von der Folgenabschätzung aufgrund bestimmter Verarbeitungszwecke (Art. 35 Abs. 10 DSGVO) .. 749
4. Was muss im Rahmen der Folgenabschätzung passieren? 750
a) Welche hohen Risiken sind zu adressieren (Art. 35 Abs. 1 DSGVO)? 750
b) Welche technischen und organisatorischen Maßnahmen sind geeignet, um das Risiko zu minimieren? 750

c) Welche Dokumentation der Folgenabschätzung ist erforderlich (Art. 35 Abs. 7 DSGVO)? ... 751
d) Bedarf es der Beratung durch den Datenschutzbeauftragten (Art. 35 Abs. 2 DSGVO)? ... 752
e) Müssen betroffene Personen oder Vertreter (Art. 35 Abs. 9 DSGVO) eingebunden werden? ... 753
f) Wann bedarf es der erneuten Überprüfung? ... 754
g) Welche Rolle spielt die Aufsichtsbehörde bei der Folgenabschätzung (Art. 36 Abs. 2 DSGVO)? ... 754
5. Praktische Hinweise zur Implementierung ... 755
VI. Umgang mit Datenlecks ... 758
1. Überblick über die einschlägigen Regelungen der DSGVO ... 758
2. Meldepflichten (Art. 33 DSGVO) ... 760
a) Was muss gemeldet werden? (Art. 33 Abs. 1 DSGVO) ... 760
b) Bis wann muss gemeldet werden? (Art. 33 Abs. 1 S. 1 und 2 DSGVO) ... 765
c) Wie muss gemeldet werden? (Art. 33 Abs. 3 DSGVO) ... 767
d) Was tun bei Verzögerung? (Art. 33 Abs. 4 DSGVO) ... 769
e) Was muss in jedem Fall dokumentiert werden? (Art. 33 Abs. 5 DSGVO) ... 770
f) Welche Pflichten treffen den Auftragsverarbeiter? (Art. 33 Abs. 2 DSGVO) ... 771
3. Benachrichtigungspflichten (Art. 34 DSGVO) ... 772
a) Wann müssen betroffene Personen benachrichtigt werden? (Art. 34 Abs. 1 DSGVO) ... 772
b) Bis wann müssen betroffene Personen benachrichtigt werden? (Art. 34 Abs. 1 DSGVO) ... 774
c) Was muss die Benachrichtigung beinhalten und wie muss sie erfolgen? (Art. 34 Abs. 2 DSGVO) ... 775
d) Wann kann auf eine Benachrichtigung verzichtet werden? (Art. 34 Abs. 3 DSGVO) ... 776
4. Praktische Hinweise zur Implementierung ... 778
VII. Integration des Datenschutzes in allgemeine Unternehmensprozesse ... 780
1. Aufgaben der Datenschutzorganisation – eine Chance für vielfältige Integration in die Unternehmensprozesse ... 780
a) Governance ... 780
b) Hinwirken auf den Datenschutz ... 781
c) Überwachung und Auditierung ... 782

2. Definition von Unternehmensprozessen, in denen Datenschutzprozesse integriert werden ... 783
a) Datenschutzprozesse ... 783
b) Risikobetrachtung ... 785
c) Typische Hüter der Anforderungen des Datenschutzes ... 787
3. Praktische Hinweise zur Implementierung ... 791

Kapitel 13: Technischer Datenschutz und Risikomanagement *(Heinemann)* ... 793

I. Überblick über die einschlägigen Regelungen ... 794
1. Art. 24, 32 DSGVO und Erwägungsgrund 83 ... 795
2. Art. 24, 25 DSGVO und Erwägungsgrund 78 ... 795
3. §§ 64, 65, 76 BDSG ... 796

II. Allgemeine Grundlagen des technischen Datenschutzrisikomanagements ... 797
1. Auswahl eines Vorgehensmodells ... 800
2. Anwendung etablierter Methoden und Verfahren ... 803
a) Anwendung PDCA und Eingliederung in Managementsysteme ... 803
b) Anwendung eines risikobasierten Verfahrens ... 805

III. Nutzung der Standards und Vorgehen der Informationssicherheit ... 806
1. Grundlegende Begriffe und Standards der Informationssicherheit ... 806
a) Terminologie ... 807
b) Zentrale Standards der Informationssicherheit ... 809
2. Risikobasiertes Verfahren zur Herstellung der Informationssicherheit ... 812
a) Schutzbedarfsfeststellung ... 814
b) Soll-Ist-Vergleich/Risiko-Assessment ... 816
c) Schutzmaßnahmen ... 823
d) Dokumentation und Nachweis ... 824
e) Kontrolle und Prüfung ... 824
f) Behandlung von Sicherheitsvorfällen ... 825
g) Zertifizierung ... 825
3. Zusammenfassung und Fazit ... 825

IV. Technische Maßnahmen zur datenschutzkonformen Verarbeitung ... 826
1. Datenschutzziele ... 827
a) Schutzziele der Datensicherheit nach der DSGVO ... 827
b) Weitere Schutzziele des Datenschutzes ... 831

2. Risikobasiertes Verfahren für den Datenschutz ... 833
a) Schutzbedarfsfeststellung des Datenschutzes ... 835
b) Soll-Ist-Vergleich des Datenschutzes ... 838
c) Risiko-Assessment des Datenschutzes ... 840
d) Auswahl von Datenschutzmaßnahmen ... 844
3. Dokumentation und Nachweis ... 867
4. Kontrolle und Prüfung ... 867
5. Behandlung von Datenschutzvorfällen ... 868
6. Zertifizierung ... 868
7. Zusammenfassung und Fazit ... 869
V. Privacy by Design und Privacy by Default ... 871
1. Privacy Enhancing Technologies ... 872
2. Privacy by Design/Privacy by Default als Ergänzung des IT-Sicherheits- und IT-Risikomanagements ... 874
VI. Ausblick ... 876
1. Anpassung des risikobasierten Verfahrens mit Auditierung/Zertifizierung ... 876
2. Entwicklung von Verhaltensregeln ... 876
3. Datenschutzeignung von Software ... 876
4. Datenschutzkonformes Design von Datenbeständen ... 877

Kapitel 14: Verhaltensregeln und Zertifizierungen *(Rothkegel)* ... 879
I. Einleitung ... 879
II. Grundsätzliche Unterscheidung und Komplementarität ... 882
III. Mehrwert für Unternehmen ... 883
1. Einhaltung und Nachweis datenschutzkonformen Handelns ... 884
2. Rechtskonkretisierungsfunktion ... 885
3. Absicherung von Drittlandübermittlungen ... 886
4. Berücksichtigung bei der Bemessung von Sanktionen ... 888
IV. Genehmigung von Verhaltensregeln ... 889
1. Vorlageberechtigte Stellen ... 889
2. Verhaltensregeln mit rein nationaler Wirkung ... 890
3. Verhaltensregeln mit landesübergreifender Wirkung ... 891
4. Allgemeingültigkeitserklärung ... 893
5. Gültigkeitsdauer ... 893

6. Bindungswirkung genehmigter Verhaltensregeln 894
a) Bindungswirkung gegenüber Aufsichtsbehörden 895
b) Bindungswirkung gegenüber Gerichten 896
c) Bindungswirkung gegenüber Unternehmen 897
V. Überwachung genehmigter Verhaltensregeln / Sanktionen im Falle von Verstößen 898
VI. Inhalte und Gestaltung von Verhaltensregeln 900
1. Regelungsinhalte von Verhaltensregeln 900
2. Gestaltungsprozess in der Praxis 901
a) Bedarfs- und Maßnahmenermittlung 902
b) Ausarbeitung unter Beteiligung betroffener Interessenträger . . 902
VII. Zertifizierungsverfahren 903
1. Ablauf des Zertifizierungsverfahrens / Beteiligte Stellen 903
2. Regelungsinhalte und Prüfmaßstab 904
3. Bindungswirkung 905

Kapitel 15: Beschäftigtendatenschutz *(Baumgartner/Gausling)* 907
I. Überblick über die einschlägigen Regelungen der DSGVO 908
II. Handlungsoptionen des Gesetzgebers 909
1. Reichweite des Art. 88 Abs. 1 DSGVO 909
a) Spezifischere Vorschriften 909
b) Personenbezogene Beschäftigtendaten 910
c) Zwecke der Datenverarbeitung 910
2. Mindestanforderungen gem. Art. 88 Abs. 2 DSGVO 911
a) Transparenz der Verarbeitung 912
b) Datenübermittlung innerhalb einer Unternehmensgruppe 913
c) Überwachungssysteme am Arbeitsplatz 913
3. Mitteilung gem. Art. 88 Abs. 3 DSGVO 913
4. Nationale Regelungen in Deutschland 914
a) Zentrale Vorschrift zum Beschäftigtendatenschutz 914
b) Verhältnis zu den Vorgaben des Art. 88 DSGVO 917
III. Datenschutzrechtliche Erlaubnistatbestände 918
1. Einwilligung im Beschäftigungsverhältnis 918
a) Allgemeine Voraussetzungen einer wirksamen Einwilligung . . 918
b) Freiwilligkeit der Einwilligung im Beschäftigungsverhältnis . . 919
c) Form der Einwilligung im Beschäftigungsverhältnis 924
2. Gesetzliche Erlaubnistatbestände 925
a) Vertragsdurchführung (Art. 6 Abs. 1 lit. b DSGVO) 926

b) Erfüllung rechtlicher Verpflichtungen (Art. 6 Abs. 1 lit. c DSGVO) ... 926
c) Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DSGVO) ... 928
d) Besondere Kategorien von personenbezogenen Daten (Art. 9 Abs. 2 lit. b DSGVO) ... 928
3. Betriebsvereinbarungen ... 929
a) Angemessene und besondere Schutzmaßnahmen ... 929
b) Betriebsvereinbarung als Erlaubnistatbestand ... 931
c) Weitere Regelungen in Betriebsvereinbarungen ... 932
d) Bereits abgeschlossene Betriebsvereinbarungen ... 933
4. Datenaustausch in Matrixorganisationen ... 934
a) Erlaubnistatbestände ... 934
b) Gemeinsame Verantwortlichkeit ... 935
IV. Informationspflichten und Betroffenenrechte ... 935
1. Informationspflichten des Arbeitgebers ... 935
2. Betroffenenrechte ... 936
3. Automatisierte Entscheidungen einschließlich Profiling ... 939
V. Überwachungsmaßnahmen – Rechtslage in Deutschland ... 940
1. Kontrolle der Internet- und E-Mail-Nutzung ... 940
a) Erlaubnistatbestand ... 940
b) Kontrolle der dienstlichen Internet- und E-Mail-Nutzung ... 941
c) Arbeitgeber als Diensteanbieter ... 941
d) Beweisverwertungsverbote ... 944
2. Videoüberwachung ... 944
VI. Handlungsempfehlung ... 946

Kapitel 16: Behördliche und gerichtliche Verfahren
(Schefzig/Rothkegel/Cornelius) ... 949
I. Aufsichtsbehörden ... 950
1. Überblick über die einschlägigen Normen ... 950
2. Einleitung ... 951
3. Zuständigkeit innerhalb der Europäischen Union ... 952
4. Zuständigkeit innerhalb Deutschlands ... 954
5. Europäischer Datenschutzausschuss ... 955
6. Aufgaben und Befugnisse ... 956
a) Aufgaben der Aufsichtsbehörden ... 956
b) Befugnisse der Aufsichtsbehörden ... 958

II. Aufsichtsverfahren ... 965
1. Aufsichtsverfahren in Deutschland ... 965
2. Zusammenarbeit der Aufsichtsbehörden auf europäischer Ebene ... 969
a) Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und den betroffenen Aufsichtsbehörden ... 970
b) Kohärenzverfahren im Falle von Unstimmigkeiten ... 971
3. Öffentliche Äußerungen von Behörden/Mediale Aufmerksamkeit 974
a) Die namentliche Nennung des sanktionierten Unternehmens ... 974
b) Pressemitteilungen und Stellungnahmen zu aktuellen Geschehnissen ... 975
III. Umgang mit Aufsichtsbehörden ... 977
1. Gründe für den Kontakt mit Aufsichtsbehörden ... 977
a) Kontrolldichte ... 977
b) Anfragen durch Aufsichtsbehörden ... 978
2. Bedeutung von Rechtspositionen der Datenschutzbehörden ... 979
3. Erste Maßnahmen nach Anfrage einer Aufsichtsbehörde ... 980
4. Sofortige Korrektur von festgestellten Rechtsverstößen ... 981
5. Generelle Hinweise zur Interaktion mit Aufsichtsbehörden ... 982
6. Kooperation und Selbstbelastung ... 983
IV. Bußgelder ... 986
1. Überblick über die einschlägigen Normen ... 986
2. Bußgeldvorschriften der DSGVO ... 987
a) Kategorisierung der Bußgelder und Strafvorschriften ... 987
b) Referenztechnik ... 988
c) Einzelne Tatbestände ... 988
d) Bisher bekannte und nennenswerte Bußgelder ... 990
3. Bemessung des Bußgeldes ... 995
a) Allgemeine Vorgaben nach der DSGVO ... 995
b) Das Bußgeldmodell der Datenschutzkonferenz in Deutschland ... 998
4. Straf- und Bußgeldvorschriften des BDSG ... 1004
a) Strafvorschriften ... 1004
b) Bußgeldvorschriften ... 1008
5. Adressat des Bußgeldes ... 1008
a) Verantwortliche Stelle, Auftragsverarbeiter und spezielle Stellen ... 1008
b) Bußgelder gegenüber einzelnen Personen innerhalb eines Unternehmens ... 1010
c) Bußgelder gegenüber Behörden ... 1011

V. Gerichtlicher Rechtsschutz 1012
1. Überblick über die einschlägigen Normen 1012
2. Verhältnis Betroffener – Verantwortlicher bzw. Auftragsverarbeiter 1012
a) Auskunftsanspruch und weitere subjektive Rechte 1013
b) Unterlassungsanspruch 1014
c) Schadensersatzanspruch 1015
3. Verhältnis Verantwortlicher bzw. Auftragsverarbeiter – Aufsichtsbehörde 1019
a) Rechtsschutzgarantie unter der DSGVO 1019
b) Konkreter Rechtsschutz nach deutschem Verfahrensrecht 1020
4. Sonderfall: Beschlüsse des Europäischen Datenschutzausschusses 1023
5. Vorgehen gegen öffentliche Äußerungen der Datenschutzbehörden 1023
VI. Verbandsklage. 1025
1. Überblick über die einschlägigen Normen 1025
2. Verbandsklagen auf Grundlage der DSGVO (Art. 80 DSGVO) . . . 1026
a) Unter Mitwirkung des Betroffenen (Art. 80 Abs. 1 DSGVO). . . 1026
b) Ohne Mitwirkung des Betroffenen (Art. 80 Abs. 2 DSGVO) . . . 1028
3. Möglichkeiten zur Verbandsklage nach deutschem Recht 1029
a) UKlaG 1029
b) Anwendbarkeit des UWG und AGB-Rechts seit Einführung der DSGVO 1032

Kapitel 17: Besondere Themenkomplexe 1035

A. Web Tracking und Online Advertising *(Arning/Hansen-Oest/Strassemeyer)*. 1037

I. Technische Abläufe 1039
1. Der Einsatz von Cookies zum Web Tracking 1040
2. Das Ausspielen von Werbung (Online Advertising) 1041
3. Weitere Methoden zum Web Tracking 1042
a) Tracking Pixel 1042
b) Social Plugins 1043
c) Andere dynamische Websiteinhalte Dritter. 1044
d) Fingerprinting 1044
e) Server to Server Tracking 1045

II. Zulässigkeit des Web Tracking und des Online Advertising 1045
1. Anwendbare Regelungen auf das Web Tracking und Online Advertising 1046
a) Rechtsunklarheit aufgrund fehlender ePrivacy-Verordnung ... 1046
b) Das Zusammenspiel zwischen der DSGVO und der ePrivacy-Richtlinie 1048
c) Das einschlägige Regelungsregime für einzelne Trackingmethoden 1053
d) Anwendbarkeit der DSGVO für die (weitere) Verarbeitung 1056
2. Zulässigkeit des Web Tracking für einzelne Zwecke 1060
a) Zulässigkeit zu Zwecken des Online Advertising 1061
b) Zulässigkeit der Datenverarbeitung zu anderen Zwecken als dem Online Advertising 1087
III. Verantwortlichkeit für Web Tracking und Online Advertising 1095
1. Verpflichteter nach Art. 5 Abs. 3 ePrivacy-Richtlinie 1095
2. Datenschutzrechtlich Verantwortlicher nach Art. 4 Nr. 7 DSGVO 1096
IV. Zusätzliche Pflichten 1098
V. Bußgeldrahmen bei Verstößen 1100

B. Customer-Relationship-Management *(Rohwedder)* 1103
I. Überblick über die einschlägigen Regelungen 1103
II. Datenquellen 1104
III. Profiling zu Werbezwecken 1106
1. Interessenabwägung 1106
2. Zweckändernde Verarbeitung 1110
3. Keine Anwendung von Art. 22 DSGVO 1111
4. Einwilligung 1112
IV. Werbliche Kommunikation mit Kunden 1113
1. Briefwerbung 1113
a) Interessenabwägung/Zweckänderung 1113
b) Einwilligung 1114
2. Direktwerbung über elektronische Post, Anrufautomaten und Fax 1115
3. Persönliche Telefonwerbung 1116
4. Vorrang der ePrivacy-Bestimmungen 1118
5. Zusammenfassung 1118

C. E-Discovery *(Heinemann)* 1120
I. Ausgewählte Rahmenbedingungen 1121
1. Federal Rule of Civil Procedure der Vereinigten Staaten 1121
2. Sedona Konferenzen, Frameworks und Arbeitsgruppen 1123
3. Leitlinien der Artikel-29-Datenschutzgruppe 1124
II. Kollision mit dem Datenschutz im Beweissicherungsprozess 1124
1. Grundlage: Das e-Discovery Referenzmodell (EDRM) 1125
2. Grundlage: Information Management und Governance 1125
3. Durchführung des e-Discovery-Prozesses mit dem Referenzmodell 1126
a) Identifikationsphase (Identification) 1126
b) Phase der Extraktion und Sicherung (Collection and Preservation) 1127
c) Phase der Bearbeitung (Processing, Review and Analysis) 1132
d) Phase der Weitergabe und Nutzung (Production and Presentation) 1132
III. Fazit 1134

D. Cloud Computing *(Meyerdierks)* 1136
I. Eigenschaften und Terminologie 1136
II. Cloud-spezifische Problemfelder 1138

E. Big Data *(Meyerdierks)* 1141
I. Eigenschaften und Terminologie 1141
II. Big Data-spezifische Problemfelder 1142
1. Personenbezug 1142
2. Zweckbindung 1143
3. Datenminimierung 1144
4. Betroffenenrechte 1144
a) Informationspflichten 1145
b) Auskunftsrecht 1145

F. Gesundheitsdatenschutz *(Arning)* 1147
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
1. Verarbeitung von Gesundheitsdaten auf Basis einer Einwilligung (Art. 9 Abs. 2 lit. a DSGVO) 1161
a) Allgemeine Anforderungen an die Einwilligung 1161
b) Freiwilligkeit der Einwilligung gem. Art. 4 Nr. 11 und Art. 7 Abs. 4 DSGVO 1163
c) Ausschluss der Einwilligung gem. Art. 9 Abs. 2 lit. a DSGVO . 1165
2. Verarbeitung von Gesundheitsdaten zu Zwecken der Gesundheitsversorgung (Art. 9 Abs. 2 lit. h, Abs. 3 DSGVO i.V.m. § 22 Abs. 1 Nr. 1 lit. b, Abs. 2 BDSG) 1166
a) Verarbeitung von Gesundheitsdaten zu Zwecken der Gesundheitsversorgung gem. Art. 9 Abs. 2 lit. h DSGVO i.V.m. § 22 Abs. 1 lit. b BDSG 1170
b) Angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gem. Art. 9 Abs. 4 DSGVO i.V.m. § 22 Abs. 2 BDSG 1175
3. Verarbeitung von Gesundheitsdaten im Beschäftigungskontext (Art. 9 Abs. 2 lit. b DSGVO, § 26 Abs. 3 und 4 BDSG) 1178
IV. Weitere Besonderheiten nach der DSGVO/dem BDSG bei der Verarbeitung von Gesundheitsdaten 1178
V. (Berufsrechtliche) Schweigepflicht 1181
VI. Verarbeitung zu wissenschaftlichen Forschungszwecken 1189
1. Zulässigkeit der Verarbeitung von Gesundheitsdaten zu Zwecken der wissenschaftlichen Forschung 1191
a) Verarbeitung von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken gem. Art. 9 Abs. 2 lit. j DSGVO i.V.m. § 27 Abs. 1 BDSG 1191
b) Verarbeitung von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken auf Basis einer Einwilligung 1195
2. Weitere Besonderheiten bei der Verarbeitung von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken 1199

Kapitel 18: Österreichisches Datenschutzrecht *(Braun)* 1203
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
1. Verarbeitung von Bilddaten (Bildaufnahmen) 1215
2. Verarbeitung von Strafdaten 1220
3. Back-Up-Privileg 1222
4. Verwarnung durch die Datenschutzbehörde 1222
5. Datengeheimnis 1223
6. Datenschutz-Folgenabschätzungen 1226
7. Regelungen in Materiengesetzen 1228
VI. Arbeitnehmer-Datenschutz 1229
1. Einwilligungen im Arbeitsverhältnis, Tracking von Mitarbeitern 1229
2. Betriebsverfassungsrecht und DSGVO 1231
3. Betriebsrat 1235
VII. Österreichische Entscheidungen 1235
1. Anwendbarkeit der DSGVO 1235
2. Sensible Daten 1236
3. Verwendung öffentlich zugänglicher Registerdaten 1237
4. Automatische Erfassung von Daten 1238
5. Speicherung von Daten 1238
6. Datenschutzbeauftragter 1240
7. Einwilligung 1240
8. Informationsrecht 1243
9. Auskunftsrecht 1244
10. Löschung 1245
11. Kreditauskunft 1247
12. Datensicherheitsmaßnahmen gemäß Art. 32 DSGVO 1249
VIII. Rechtsdurchsetzung und Verfahrensrecht 1250
1. Verwaltungsverfahren 1250
a) Beschwerde an die Datenschutzbehörde 1250
b) Amtswegiges Prüfungsverfahren der Datenschutzbehörde 1253
c) Rechtsmittel und Rechtsbehelfe gegen Entscheidungen der Datenschutzbehörde 1253
d) Vollstreckung von Entscheidungen im Verwaltungsverfahren 1254
2. Verwaltungsstrafverfahren 1254
3. Verfahren vor ordentlichen Gerichten und parallele Verfahrensführung 1258

Kapitel 19: Leitentscheidungen des EuGH zur DSGVO
(Strassemeyer/Schefzig/Moos) 1263

I. Einleitung 1264

II. Leitentscheidungen des EuGH 1265

1. Anwendungsbereich des europäischen Datenschutzrechts
(EuGH, Urt. v. 13.5.2014 – C-131/12 – *Google Spain*) 1265
a) Sachverhalt 1265
b) Entscheidungsgründe 1265
c) Implikationen für die Unternehmenspraxis 1267

2. Personenbezug von Daten
(EuGH, Urt. v. 6.12.2016 – C-582/14 – *Breyer*) 1271
a) Sachverhalt 1271
b) Entscheidungsgründe – der Personenbezug dynamischer IP-Adressen 1272
c) Implikationen für die Unternehmenspraxis 1273

3. Gemeinsame Verantwortlichkeit I
(EuGH, Urt. v. 5.6.2018 – C-210/16 – *Facebook Fanpages*) 1274
a) Sachverhalt 1274
b) Entscheidungsgründe 1275
c) Implikationen für die Unternehmenspraxis 1276

4. Gemeinsame Verantwortlichkeit II
(EuGH, Urt. v. 10.7.2018 – C-25/17 – *Zeugen Jehovas*) 1277
a) Sachverhalt 1277
b) Entscheidungsgründe 1278
c) Implikationen für die Unternehmenspraxis 1279

5. Gemeinsame Verantwortlichkeit III
(EuGH, Urt. v. 29.7.2019 – C-40/17 – *Fashion ID*) 1280
a) Sachverhalt 1280
b) Entscheidungsgründe 1281
c) Implikationen für die Unternehmenspraxis 1282

6. Verlinkung auf besondere personenbezogene Daten
(EuGH, Urt. v. 14.9.2019 – C-136/17) 1284
a) Sachverhalt 1285
b) Entscheidungsgründe 1285
c) Implikationen für die Unternehmenspraxis 1286

7. Keine extraterritoriale Auslistung
(EuGH, Urt. v. 14.9.2019 – C-507/17) 1287
a) Sachverhalt 1287
b) Entscheidungsgründe 1287
c) Implikationen für die Unternehmenspraxis 1288

8. Anforderungen an eine wirksame Einwilligung (EuGH, Urt. v. 1.10.2019 – C-673/17 – *Planet49*) ... 1288
a) Sachverhalt ... 1289
b) Entscheidungsgründe ... 1289
c) Implikationen für die Unternehmenspraxis ... 1290
9. Die Rechtfertigung von Drittlandtransfers (EuGH, Urt. v 16.7.2020 – C-311/18 – *Schrems II*) ... 1295
a) Sachverhalt ... 1295
b) Entscheidungsgründe ... 1295
c) Implikationen für die Unternehmenspraxis ... 1297

Kapitel 20: Vorgehensweise zur Umsetzung von DSGVO-Anforderungen im Unternehmen *(Zeiter/Moos)* ... 1303

I. Anpassungsbedarf im Unternehmen ... 1303

II. Leitbild zur Umsetzung der DSGVO im Unternehmen ... 1305

III. Ausgestaltung eines Umsetzungsprojekts ... 1305
1. Vorbereitung ... 1305
a) Welche Abteilung bzw. welche Person ist unternehmensintern für die Umstellung auf die DSGVO verantwortlich? ... 1306
b) Welche datenschutzrechtlichen Vorschriften sollen konkret umgesetzt werden? ... 1306
c) Auf welche verantwortlichen Stellen bezieht sich das Umsetzungsprojekt genau? ... 1307
d) Sollte die DSGVO im Unternehmen global umgesetzt werden? 1308
e) Welche Ressourcen stehen zur Verfügung? ... 1308
f) Soll die Implementierung durch interne oder externe Ressourcen erfolgen? ... 1309
g) Welche Abteilungen sollten involviert bzw. informiert werden? 1309
h) Bis wann sollte die DSGVO im Unternehmen umgesetzt sein? . 1309
i) Kann die Umsetzung der DSGVO im Unternehmen auch als Chance wahrgenommen werden? ... 1310
2. Anforderungsspezifizierung ... 1311
3. Gap-Analyse ... 1312
a) Vorbereitung der Gap-Analyse ... 1312
b) Durchführung der Gap-Analyse ... 1312
c) Ergebnis der Gap-Analyse ... 1314
4. Planung von Ressourcen ... 1314
a) Planung von Budget ... 1314
b) Planung von Mitarbeitern ... 1315
c) Zeitplan ... 1315

5. Implementierung ... 1315
a) Definition von Unterprojekten ... 1316
b) Bestimmung von Meilensteinen und Abhängigkeiten ... 1316
c) Durchführung der Unterprojekte ... 1317
6. Testing und Monitoring ... 1317
7. Kommunikation und Training ... 1318
a) Interne Unternehmenskommunikation ... 1319
b) Mitarbeiterschulungen ... 1319
IV. Erste Erfahrungen aus der Umsetzungspraxis ... 1319
V. Fazit ... 1321

Kapitel 21: Weitere rechtliche Entwicklungen und Ausblick *(Moos/Schefzig)* ... 1323
I. Datenschutzrecht als dynamisches Rechtsgebiet ... 1323
II. Gesetzgeber ... 1324
1. Rechtsakte der Europäischen Kommission ... 1324
a) Delegierte Rechtsakte ... 1325
b) Durchführungsrechtsakte ... 1325
2. Begleitgesetze der Mitgliedstaaten ... 1328
3. ePrivacy ... 1328
III. Datenschutzbehörden ... 1330
1. Europäischer Datenschutzausschuss ... 1330
2. Black- und Whitelists für Datenschutz-Folgenabschätzung ... 1331
3. Musterverträge ... 1331
4. Konkretisierung von Pflichten nach der DSGVO ... 1332
IV. Rechtsprechung ... 1334
V. Entwicklung der Datenschutzpraxis ... 1334
VI. Ausblick ... 1335

Sachregister ... 1337

Abkürzungsverzeichnis

a. A.	anderer Ansicht
ABl.	Amtsblatt
ABl. EG	Amtsblatt der Europäischen Gemeinschaft
ABl. EU	Amtsblatt der Europäischen Union
Abs.	Absatz
AES	Advanced Encryption Standard
AEUV	Vertrag über die Arbeitsweise der Europäischen Union (EU-Arbeitsweisevertrag)
AGB	Allgemeine Geschäftsbedingungen
AiB	Arbeitsrecht im Betrieb
AktG	Aktiengesetz
Alt.	Alternative
AMGuaÄndG	Gesetz zur Änderung arzneimittelrechtlicher und anderer Vorschriften
Anm.	Anmerkung
AO	Abgabenordnung
API	Advance Passenger Information
ArbG	Arbeitsgericht
ArbRB	Arbeitsrechtsberater (Zeitschrift)
Art.	Artikel
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAG	Bundesarbeitsgericht
BAGE	Entscheidungen des Bundesarbeitsgerichts
BayDSG	Bayerisches Datenschutzgesetz
BayLDA	Bayerisches Landesamt für Datenschutzaufsicht
BB	Betriebs-Berater (Zeitschrift)
BCR	Binding Corporate Rules
BDIU	Bundesverband Deutscher Inkasso-Unternehmen
BDSG	Bundesdatenschutzgesetz
BeckOK	Beck'scher Onlinekommentar
BeckOK-DS	Wolff/Brink (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht, 35. Edition, 2021
BeckOK-OWiG	Graf (Hrsg.), Beck'scher Online-Kommentar OWiG, 29. Edition, 2021
BeckOK-StGB	von Heintschel-Heinegg (Hrsg.), Beck'scher Online-Kommentar StGB, 48. Edition, 2020
Begr.	Begründung
BetrVG	Betriebsverfassungsgesetz

BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BlnBDI	Berliner Beauftragte für Datenschutz und Informationsfreiheit
BNotO	Bundesnotarordnung
BORA	Berufsordnung der Rechtsanwälte
BOStB	Satzung über die Rechte und Pflichten bei der Ausübung der Berufe der Steuerberater und der Steuerbevollmächtigten (Berufsordnung)
BRAO	Bundesrechtsanwaltsordnung
BR-Drs.	Drucksache des Deutschen Bundesrates
BSG	Bundessozialgericht
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT	Bundestag
BT-Drs.	Drucksache des Deutschen Bundestages
BVDW	Bundesverband Digitale Wirtschaft e. V.
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
CR	Computer und Recht (Zeitschrift)
Cri	Computer und Recht International (Zeitschrift)
CRM	Customer Relationship Management
DB	Der Betrieb (Zeitschrift)
d. h.	das heißt
Drs.	Drucksache
DSB	Datenschutzberater (Zeitschrift)
DSB	Datenschutzbeauftragter
DSRL	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 (Datenschutzrichtlinie)
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DV	Datenverarbeitung
e. V.	Eingetragener Verein
EDV	Elektronische Datenverarbeitung

EG	Europäische Gemeinschaft
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten (Europäische Menschenrechtskonvention)
ENISA	European Union Agency for Network and Information Security
ER	Europäischer Rat
EuGH	Europäischer Gerichtshof
EU-Komm	Europäische Kommission
EWR	Europäischer Wirtschaftsraum
FAQ	Frequently Asked Questions
f.	folgende
ff.	fortfolgende
Fn.	Fußnote
FS	Festschrift
GDD	Gesellschaft für Datenschutz und Datensicherheit
GenDG	Gendiagnostikgesetz
GewO	Gewerbeordnung
GG	Grundgesetz
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GrCh	Europäische Grundrechtecharta
GVG	Gerichtsverfassungsgesetz
h. M.	herrschende Meinung
Hs.	Halbsatz
HBÜ	Haager Übereinkommen vom 18.3.1970 über die Beweisaufnahme im Ausland in Zivil- und Handelssachen
HGB	Handelsgesetzbuch
HR	Human Resources
ico	Information Commissioner's Office
i. d. R.	in der Regel
i. S. d.	im Sinne des/der
i. S. v.	im Sinne von
ID	Identity
IHK	Industrie- und Handelskammer
IKS	Internes Kontrollsystem
IP	Intellectual Property
ISMS	IT-Sicherheitsmanagement-System

ISO	Internationale Organisation für Normung
IoT	Internet of things
i. S. d.	im Sinne des/der
i. S. v.	im Sinne von
IT	Informationstechnologie
ITRB	Der IT-Rechts-Berater (Zeitschrift)
i. V. m.	in Verbindung mit
Kap.	Kapitel
K&R	Kommunikation und Recht (Zeitschrift)
KWG	Gesetz über das Kreditwesen (Kreditwesengesetz)
LAG	Landesarbeitsgericht
LDI NRW	Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
LfD	Landesbeauftragte/Landesbeauftragter für den Datenschutz
LfDI M-V	Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern
LG	Landgericht
lit.	littera (= Buchstabe)
LT-Drs.	Landtags-Drucksache
MaRisk	Mindestanforderungen an das Risikomanagement
MDR	Monatsschrift für Deutsches Recht (Zeitschrift)
MedR	Medizinrecht (Zeitschrift)
Mio.	Millionen
MMR	Multimedia und Recht (Zeitschrift)
Mrd.	Milliarden
MüKo-BGB	Münchener Kommentar zum Bürgerlichen Gesetzbuch (BGB), Band 2, Schuldrecht – Allgemeiner Teil I, 8. Aufl. 2019
MüKo-GmbHG	Münchener Kommentar zum Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG), Band 2, §§ 35–52, 3. Aufl. 2019
MüKo-StGB	Münchener Kommentar zum Strafgesetzbuch (StGB), Band 4, §§ 185–262, 3. Aufl. 2017
m. w. N.	mit weiteren Nachweisen
NJW	Neue Juristische Wochenschrift (Zeitschrift)
NJW-RR	NJW-Rechtsprechungsreport (Zeitschrift)
Nr.	Nummer
Nrn.	Nummern

NRW	Nordrhein-Westfalen
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZA	Neue Zeitschrift für Arbeitsrecht
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (Organisation for Economic Co-operation and Development)
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
OWiG	Gesetz über Ordnungswidrigkeiten
PIN	Persönliche Identifikationsnummer
PostG	Postgesetz
RDV	Recht der Datenverarbeitung (Zeitschrift)
RegE	Regierungsentwurf
Rn.	Randnummer
Rs.	Rechtssache (EuGH)
RSA	Asymmetrisches Verschlüsselungssystem nach Rivest, Shamir und Adleman
S.	Seite, Satz (bei Rechtsnormen)
SaaS	Software as a Service
Schufa	Schutzgemeinschaft für allgemeine Kreditsicherung
SGB I	Sozialgesetzbuch Erstes Buch
SGB V	Sozialgesetzbuch Fünftes Buch
SGB X	Sozialgesetzbuch Zehntes Buch
SIM	Subscriber Identity Module
SMS	Short Message Service
StBerG	Steuerberatungsgesetz
StGB	Strafgesetzbuch
st. Rspr.	ständige Rechtsprechung
StPO	Strafprozessordnung
TB	Tätigkeitsbericht
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TTDSG	Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien
u. a.	unter anderem

UKlaG	Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen (Unterlassungsklagengesetz)
ULD SH	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
UrhG	Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz)
USA	United States of America
USB	Universal Serial Bus
usw.	und so weiter
UWG	Gesetz gegen den unlauteren Wettbewerb
Var.	Variante
VG	Verwaltungsgericht
vgl.	vergleiche
VoIP	Voice over IP
Vol.	Volume
VPN	Virtual private Network
VuR	Verbraucher und Recht (Zeitschrift)
VVG	Gesetz über den Versicherungsvertrag (Versicherungsvertragsgesetz)
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
WLAN	Wireless Local Area Network
WP	Working Paper
WRP	Wettbewerb in Recht und Praxis (Zeitschrift)
ZAfTDa	Zentralarchiv für Tätigkeitsberichte des Bundes- und der Landesdatenschutzbeauftragten und der Aufsichtsbehörden für den Datenschutz
z. B.	zum Beispiel
Ziff.	Ziffer
ZPO	Zivilprozessordnung
ZUM	Zeitschrift für Urheber- und Medienrecht

Literaturverzeichnis

Adam, Azad	Implementing electronic document and record management systems, Boca Raton 2007 (zit.: *Adam*)
Albrecht, Jan Philipp/ Jotzo, Florian	Das neue Datenschutzrecht der EU, Baden-Baden 2017 (zit.: *Albrecht*/*Jotzo*)
Auer-Reinsdorff, Astrid/ Conrad, Isabell	Handbuch IT- und Datenschutzrecht, 3. Aufl., München 2019 (zit.: Auer-Reinsdorff/Conrad/ *Bearbeiter*)
Auernhammer, Herbert	(herausgegeben von Eßer, Martin/Kramer, Philipp/v. Lewinski, Kai) DSGVO BDSG, 7. Aufl., Köln 2020 (zit. Auernhammer/*Bearbeiter*)
Bader, Johann/ Ronellenfitsch, Michael	Beck'scher Online-Kommentar VwVfG, 51. Edition, München 2020 (zit.: BeckOK-VwVfG/*Bearbeiter*)
Behling, Thorsten B./ Abel, Ralf B.	Praxishandbuch Datenschutz im Unternehmen, Berlin 2014 (zit.: Behling/Abel/*Bearbeiter*)
Bergmann, Jan	Handlexikon der Europäischen Union, 5. Aufl., Baden-Baden 2015 (zit.: Bergmann/*Bearbeiter*)
Beyvers, Eva	Privatheit in der Waagschale, Berlin 2018
Bresich, Ronald/Dopplinger, Lorenz/Dörnhöfer, Stefanie/ Kunnert, Gerhard/Riedl, Eckhard	DSG: Datenschutzgesetz Kommentar, Wien 2018 (zit.: *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl*)
Bretz, Jörg/Hinssen, Johannes/Kolb, Andreas/ Martin, Gerd/Peltier, Georges/Rosenberger, Peter	IT-Sicherheitsmanagement in Banken und Sparkassen, Heidelberg 2007 (zit.: Bretz et al./*Bearbeiter*)
von dem Bussche, Axel/ Voigt, Paul	Konzerndatenschutz, 2. Aufl., München 2019 (zit.: von dem Bussche/Voigt/*Bearbeiter*)
Calliess, Christian/ Ruffert, Matthias	EUV/AEUV, 5. Aufl., München 2016 (zit.: Calliess/Ruffert/*Bearbeiter*)

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/ Weichert, Thilo	Bundesdatenschutzgesetz, 5. Aufl., Frankfurt/ Main 2016 (zit.: Däubler/Klebe/Wedde/Weichert/*Bearbeiter*)
Däubler, Wolfgang/Wedde, Peter/Weichert, Thilo/ Sommer, Imke	EU-DSGVO und BDSG, 2. Aufl., Frankfurt/ Main 2020 (zit.: Däubler/Wedde/Weichert/Sommer/*Bearbeiter*)
Dauses, Manfred A./ Ludwigs, Markus	Handbuch des EU-Wirtschaftsrechts, 52. Aufl., München 2021 (zit.: Dauses/Ludwigs/*Bearbeiter*)
Dochow, Carsten/Dörfer, Bert-Sebastian/Halbe, Bernd/ Hübner, Marlis/Ippach, Jan/ Schröder, Jürgen/Schütz, Joachim/Strüve, Jakob	Datenschutz in der ärztlichen Praxis, Köln 2019 (zit.: Dochow/Dörfer/Halbe/Hübner/Ippach/Schröder/Schütz/Strüve/*Bearbeiter*)
Dreier, Thomas/Schulze, Gernot	Urheberrechtsgesetz, 6. Aufl., München 2018 (zit.: Dreier/Schulze/*Bearbeiter*)
Ehmann, Eugen/Schonschek, Oliver	Prozessorientierte Datenschutzpraxis, 2. Aufl., Kissing 2011 (zit.: *Ehmann*/*Schonschek*)
Ehmann, Eugen/Selmayr, Martin	Datenschutz-Grundverordnung, 2. Aufl., München 2018 (zit.: Ehmann/Selmayr/*Bearbeiter*)
Falta, Roman P./Dueblin, Christian	Praxishandbuch Legal Operations Management, Berlin/Heidelberg 2017 (zit.: Falta/Dueblin/*Bearbeiter*)
Forgó, Nikolaus/Helfrich, Marcus/Schneider, Jochen	Betrieblicher Datenschutz, 3. Aufl., München 2019 (zit.: Forgó/Helfrich/Schneider/*Bearbeiter*)
Forgó, Nikolaus/Kollek, Regine/Arning, Marian/ Krügel, Tina/Petersen, Imme	Ethical and Legal Requirements of Transnational Genetic Research, München/Oxford/Baden-Baden 2010 (zit.: *Forgó*/*Kollek*/*Arning*/*Krügel*/*Petersen*)
Friedewald, Michael/Obersteller, Hannah/Nebel, Maxi/ Bieker, Felix/Rost, Martin	White Paper Datenschutz-Folgenabschätzung (zit.: *Friedewald*/*Obersteller/Nebel/Bieker/Rost*)
Gierschmann, Sibylle/ Schlender, Katharina/ Stentzel, Rainer/ Veil, Winfried	Kommentar Datenschutz-Grundverordnung, Köln 2018 (zit. Gierschmann/Schlender/Stentzel/ Veil/*Bearbeiter*)

Gola, Peter	Datenschutz-Grundverordnung, 2. Aufl., München 2018 (zit.: Gola/*Bearbeiter*)
Gola, Peter/Heckmann, Dirk	Bundesdatenschutzgesetz, 13. Aufl., München 2019 (zit.: Gola/Heckmann/*Bearbeiter*)
Gola, Peter/Jaspers, Andreas/ Müthlein, Thomas/ Schwartmann, Rolf	DS-GVO/BDSG im Überblick, 3. Aufl., Frechen 2018 (zit. *Gola/Jaspers/Müthlein/Schwartmann*)
Gola, Peter/Schomerus, Rudolf	Bundesdatenschutzgesetz, 12. Aufl., München 2015 (zit.: Gola/Schomerus/*Bearbeiter*)
Golland, Alexander	Datenverarbeitung in sozialen Netzwerken, Frankfurt/Main 2019 (zit.: *Golland*)
Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin	Das Recht der Europäischen Union, Band 1, 71. Aufl., München 2020 (zit.: Grabitz/Hilf/Nettesheim/*Bearbeiter*)
Graf, Peter	Beck'scher Online-Kommentar OWiG, 29. Edition, München 2021 (zit.: BeckOK-OWiG/*Bearbeiter*)
Griller, Stefan/Rill, Heinz Peter	Rechtstheorie: Rechtsbegriff – Dynamik – Auslegung, Wien 2011 (zit.: Griller/Rill/*Bearbeiter*)
Hänlein, Andreas/Schuler, Rolf	Sozialgesetzbuch V: Gesetzliche Krankenversicherung, 5. Aufl., Baden-Baden 2016 (zit.: Hänlein/Schuler/*Bearbeiter*)
Härting, Niko	Datenschutz-Grundverordnung, Köln 2016 (zit.: *Härting*)
Hansen-Oest, Stephan	Datenschutzbeauftragte, Frankfurt a. M. 2020
Hartmann, Matthias H.	Internationale E-Discovery und Information Governance, Berlin 2011 (zit.: Hartmann/*Bearbeiter*)
Hauschka, Christoph E./ Moosmayer, Klaus/Lösler, Thomas	Corporate Compliance, 3. Aufl., München 2016 (zit.: Hauschka/Moosmayer/Lösler/*Bearbeiter*)
Heidrich, Jörg/Forgó, Nikolaus/Feldmann, Thorsten	Heise Online-Recht, 3. EL, Hannover 2011 (zit.: Heidrich/Forgó/Feldmann/*Bearbeiter*)
von Heintschel-Heinegg, Bernd	Beck'scher Online-Kommentar StGB, 48. Edition, München 2020 (zit.: BeckOK-StGB/*Bearbeiter*)

Hoffmann-Becking, Michael	Münchener Handbuch des Gesellschaftsrechts Band 4, Aktiengesellschaft, 5. Aufl., München 2020 (zit.: Münchener Handbuch des Gesellschaftsrechts/*Bearbeiter*)
Hunzinger, Sven	Das Löschen im Datenschutzrecht, Baden-Baden 2018
Jahnel, Dietmar	Datenschutzrecht – Jahrbuch 2018, Wien 2018 (zit.: Jahnel/*Bearbeiter*, Datenschutzrecht – Jahrbuch 2018)
Jarass, Hans D.	Charta der Grundrechte der Europäischen Union, 3. Aufl., München 2016 (zit.: Jarass/*Bearbeiter*)
Johlen, Heribert	Münchener Prozessformularbuch, Band 7 Verwaltungsrecht, 5. Aufl., München 2018 (zit.: Johlen/*Bearbeiter*)
Junker, Abbo	Electronic Discovery gegen deutsche Unternehmen, Frankfurt/Main 2008 (zit.: *Junker*)
Katzenmeier, Christian/ Ratzel, Rudolf	Festschrift für Franz-Josef Dahm, Berlin 2017 (zit.: Katzenmeier/Ratzel/*Bearbeiter*)
Kersten, Heinrich/Klett, Gerhard/Reuter, Jürgen/ Schröder, Klaus-Werner	IT-Sicherheitsmanagement nach der neuen ISO 27001, 2. Aufl., Wiesbaden 2020 (zit.: *Kersten/ Klett/Reuter/Schröder*)
Kilian, Wolfgang/Heussen, Benno	(herausgegeben von Taeger, Jürgen/Pohle, Jan) Computerrechts-Handbuch, 35. Aufl., München 2020 (zit.: Kilian/Heussen/*Bearbeiter*)
Knoll, Matthias	IT-Prüfung und IT-Revision, Heidelberg 2013 (zit.: Knoll/*Bearbeiter*)
Knyrim, Rainer	Datenschutz-Grundverordnung, Wien 2016 (zit.: Knyrim/*Bearbeiter*)
Knyrim, Rainer	Der DatKomm Praxiskommentar zum Datenschutzrecht – DSGVO und DSG, Stand: 7.5.2020, Wien 2020 (zit.: Knyrim/*Bearbeiter*, Der DatKomm Praxiskommentar zum Datenschutzrecht – DSGVO und DSG)
Köhler, Helmut/Bornkamm, Joachim/Feddersen, Jörn	Gesetz gegen den unlauteren Wettbewerb UWG, 39. Aufl., München 2021 (zit.: Köhler/ Bornkamm/Feddersen/*Bearbeiter*)

Körber-Risak, Katharina/ Brodil, Wolfgang	Datenschutz und Arbeitsrecht, Wien 2018 (zit.: Körber-Risak/Brodil/*Bearbeiter*, Datenschutz und Arbeitsrecht)
Koreng, Ansgar/Lachenmann, Matthias	Formularhandbuch Datenschutzrecht, 2. Aufl., München 2018 (zit.: Koreng/Lachenmann/*Bearbeiter*)
Kotschy, Waltraud	RdW Spezial: DSGVO, Wien 2019 (zit.: Kotschy/*Bearbeiter*, RdW Spezial: DSGVO)
Kühling, Jürgen/Buchner, Benedikt	Datenschutz-Grundverordnung BDSG, 3. Aufl., München 2020 (zit.: Kühling/Buchner/*Bearbeiter*)
Kühling, Jürgen/Martini, Mario/Heberlein, Johanna/ Kühl, Benjamin/Nink, David/ Weinzierl, Quirin/Wenzel, Michael	Die Datenschutz-Grundverordnung und das nationale Recht, Münster 2016 (zit.: *Kühling/Martini et al.*)
Laue, Philip/Kremer, Sascha	Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl., Baden-Baden 2019 (zit.: Laue/Kremer/*Bearbeiter*)
Laue, Philip/Nink, Judith/ Kremer, Sascha	Das neue Datenschutzrecht in der betrieblichen Praxis, Baden-Baden 2016 (zit.: *Laue/Nink/Kremer*)
Laufs, Adolf/Kern, Bernd-Rüdiger/Rehborn, Martin	Handbuch des Arztrechts, 5. Aufl., München 2019 (zit.: Laufs/Kern/Rehborn/*Bearbeiter*)
Loomans, Dirk/Matz, Manuela/Wiedemann, Michael	Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, Wiesbaden 2014 (zit.: *Loomans/Matz/Wiedemann*)
von Mangoldt, Hermann/ Klein, Friedrich/Starck, Christian	Kommentar zum Grundgesetz, Band 2, 7. Aufl., München 2018 (zit.: v. Mangold/Klein/Starck/*Bearbeiter*)
Mazal, Wolfgang/ Risak, Martin E.	Das Arbeitsrecht – System und Praxiskommentar, 33. Lieferung, Wien 2019 (zit.: Mazal/Risak/*Bearbeiter*, Arbeitsrecht – System und Praxiskommentar)

Meyer-Ladewig, Jens/ Nettesheim, Martin/ von Raumer, Stefan	EMRK, 4. Aufl., Baden-Baden 2017 (zit.: Meyer-Ladewig/Nettesheim/von Raumer/*Bearbeiter*)
Moos, Flemming	Datenschutz und Datennutzung, 3. Aufl., Köln 2021 (zit.: Moos/*Bearbeiter*)
Münchener Kommentar zum Aktiengesetz (AktG)	Band 2, §§ 76–117, MitbestG, DrittelbG, 5. Aufl., München 2019 (MüKo-AktG/*Bearbeiter*)
Münchener Kommentar zum Bürgerlichen Gesetzbuch (BGB)	Band 2, Schuldrecht – Allgemeiner Teil I, 8. Aufl., München 2019 (zit.: MüKo-BGB/*Bearbeiter*)
Münchener Kommentar zum Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG)	Band 2, §§ 35–52, 3. Aufl., München 2019 (zit.: MüKo-GmbHG/*Bearbeiter*)
Münchener Kommentar zum Strafgesetzbuch (StGB)	Band 4, §§ 185–262, 3. Aufl., München 2017 (zit.: MüKo-StGB/*Bearbeiter*)
Paal, Boris P./ Pauly, Daniel A.	Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Aufl., München 2018 (zit.: Paal/Pauly/*Bearbeiter*)
Piltz, Carlo	BDSG, Frankfurt a. M. 2018 (zit.: *Piltz*)
Plath, Kai-Uwe	DSGVO/BDSG, 3. Aufl., Köln 2018 (zit.: Plath/ *Bearbeiter*)
Pollirer, Hans J./Weiss, Ernst M./Knyrim, Rainer/ Haidinger, Viktoria	DSG, 4. Aufl., Wien 2019 (zit.: *Pollirer/Weiss/ Knyrim/Haidinger*, DSG)
Riesenhuber, Karl	Europäische Methodenlehre, 3. Aufl., Berlin 2015 (zit.: Riesenhuber/*Bearbeiter*)
Riesz, Thomas/Schilchegger, Michael	TKG: Telekommunikationsgesetz, Wien 2016 (zit.: Riesz/Schilchegger/*Bearbeiter*, Telekommunikationsgesetz)
Rolfs, Christian/Giesen, Richard/Kreikebohm, Ralf/ Meßling, Miriam/Udsching, Peter	Beck'scher Online-Kommentar Sozialrecht, 59. Edition, München 2020 (zit.: BeckOK-Sozialrecht/*Bearbeiter*)

Roßnagel, Alexander	Europäische Datenschutz-Grundverordnung, Baden-Baden 2017 (zit.: Roßnagel/*Bearbeiter*)
Roßnagel, Alexander/ Hornung, Gerrit/Jandt, Silke	Teil-Rechtsgutachten zu den datenschutzrechtlichen Fragen der medizinischen Forschung, Stand 12/2009 (zit.: *Roßnagel*/*Hornung*/*Jandt*, Teil-Rechtsgutachten zu den datenschutzrechtlichen Fragen der medizinischen Forschung)
Rücker, Daniel/Kugler, Tobias	New European General Data Protection Regulation, München, Oxford, Baden-Baden 2018 (zit.: Rücker/Kugler/*Bearbeiter*)
Schaffland, Hans-Jürgen/ Wiltfang, Noeme	Datenschutz-Grundverordnung (DS-GVO)/Bundesdatenschutzgesetz (BDSG), Stand 2021, Berlin (zit.: Schaffland/Wiltfang/*Bearbeiter*)
Schantz, Peter/Wolff, Heinrich Amadeus	Das neue Datenschutzrecht, München 2017 (zit.: Schantz/Wolff/*Bearbeiter*)
Schmeh, Klaus	Kryptografie, 6. Aufl., Heidelberg 2016 (zit.: *Schmeh*)
Schönke, Adolf/Schröder, Horst	Strafgesetzbuch (StGB), 30. Aufl., München 2019 (zit.: Schönke/Schröder/*Bearbeiter*)
Schrems, Max	Kämpf um deine Daten, Wien 2014 (zit.: *Schrems*)
Schwartmann, Rolf/Jaspers, Andreas/Thüsing, Gregor/ Kugelmann, Dieter	DS-GVO/BDSG, 2. Aufl, Heidelberg 2020 (zit.: Schwartmann/Jaspers/Thüsing/Kugelmann/*Bearbeiter*)
Schwarze, Jürgen/Becker, Ulrich/Hatje, Armin/Schoo, Johann	EU-Kommentar, 4. Aufl., Baden-Baden 2019 (zit.: Schwarze/Becker/Hatje/Schoo/*Bearbeiter*)
Simitis, Spiros	Bundesdatenschutzgesetz, 8. Aufl., Baden-Baden 2014 (zit.: Simitis/*Bearbeiter*)
Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra	Datenschutzrecht: DSGVO mit BDSG, Baden-Baden 2019 (zit. Simitis/Hornung/Spiecker gen. Döhmann/*Bearbeiter*)
Specht, Louisa	Diktat der Technik, Baden-Baden 2019
Specht, Louisa/Mantz, Reto	Handbuch Europäisches und deutsches Datenschutzrecht, München 2019 (zit.: Specht/Mantz/ *Bearbeiter*)

Specht-Riemenschneider, Louisa/Buchner, Benedikt/ Heinze, Christian/Thomsen, Oliver	Festschrift für Jürgen Taeger: IT-Recht in Wissenschaft und Praxis, Frankfurt a. M. 2020 (zit.: FS Taeger/*Bearbeiter*)
Specht-Riemenschneider, Louisa/Werry, Nikola/Werry, Susanne	Datenrecht in der Digitalisierung, Berlin 2020 (zit.: Specht-Riemenschneider/Werry/Werry/*Bearbeiter*)
Spickhoff, Andreas	Medizinrecht, 3. Aufl., München 2018 (zit.: Spickhoff/*Bearbeiter*)
Spindler, Gerald/Schuster, Fabian	Recht der elektronischen Medien, 4. Aufl., München 2019 (zit.: Spindler/Schuster/*Bearbeiter*)
Sydow, Gernot	Europäische Datenschutzgrundverordnung, 2. Aufl., Baden-Baden 2018 (zit.: Sydow/*Bearbeiter*)
Sydow, Gernot	Bundesdatenschutzgesetz, Baden-Baden 2020 (zit.: Sydow/*Bearbeiter*)
Taeger, Jürgen	Smart World – Smart Law?, Tagungsband DSRI-Herbstakademie, Edewecht 2016 (zit.: Taeger/*Bearbeiter*, DSRITB 2016)
Taeger, Jürgen	Recht 4.0 – Innovationen aus den rechtswissenschaftlichen Laboren, Tagungsband DSRI-Herbstakademie, Edewecht 2017 (zit.: Taeger/*Bearbeiter*, DSRITB 2017)
Taeger, Jürgen	Rechtsfragen digitaler Transformationen – Gestaltung digitaler Veränderungsprozesse durch Recht, Tagungsband DSRI-Herbstakademie, Edewecht 2018 (zit.: Taeger/*Bearbeiter*, Rechtsfragen digitaler Transformationen)
Taeger, Jürgen	Die Macht der Daten und der Algorithmen – Regulierung von IT, IoT und KI, Tagungsband DSRI-Herbstakademie, Edewecht 2019 (zit.: Taeger/*Bearbeiter*, DSRITB 2019)
Taeger, Jürgen	Den Wandel begleiten – IT-rechtliche Herausforderungen der Digitalisierung, Tagungsband DSRI-Herbstakademie, Edewecht 2020 (zit.: Taeger/*Bearbeiter*, DSRITB 2020)

Taeger, Jürgen/Gabel, Detlev	DSGVO BDSG, 3. Aufl., Frankfurt/Main 2019 (zit.: Taeger/Gabel/*Bearbeiter*)
Thome, Günter/Sollbach, Wolfgang	Grundlagen und Modelle des Information Lifecycle Management, Heidelberg 2007 (zit.: *Thome/Sollbach)*
Thüsing, Gregor	Beschäftigtendatenschutz und Compliance, 3. Aufl., München 2021 (zit.: *Thüsing*)
Vedder, Christoph/Heintschel von Heinegg, Wolff	Europäisches Unionsrecht, 2. Aufl., München 2018 (zit.: Vedder/Heintschel/v. Heinegg/*Bearbeiter*)
Weber, Wolfgang/Kabst, Rüdiger/Baum, Matthias	Einführung in die Betriebswirtschaftslehre, 10. Aufl., Wiesbaden 2017 (zit.: *Weber/Kabst/Baum*)
Wenhold, Céline	Nutzerprofilbildung durch Webtracking, Baden-Baden 2018
Weth, Stephan/Herberger, Maximilian/Wächter, Michael/Sorge, Christoph	Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl., München 2019 (zit.: Weth/Herberger/Wächter/Sorge/*Bearbeiter*)
Wiedemann, Gerhard	Handbuch des Kartellrechts, 4. Aufl., München 2020 (zit.: Wiedemann/*Bearbeiter*)
Wolff, Heinrich Amadeus/Brink, Stefan	Beck'scher Online-Kommentar Datenschutzrecht, 35. Edition, München 2021 (zit.: BeckOK-DS/*Bearbeiter*)
Wybitul, Tim	EU-Datenschutz-Grundverordnung im Unternehmen, Frankfurt/Main 2016 (zit.: Wybitul/*Bearbeiter*)
Zippelius, Reinhold	Juristische Methodenlehre, 12. Aufl., München 2021 (zit.: *Zippelius*)

Kapitel 1

Grundlagen des Umgangs mit der DSGVO

Übersicht

Rn.

I. Die Anwendung der DSGVO und der nationalen Begleitgesetze 1
1. Stand der Umsetzung in den Unternehmen 3
2. Zeitliche Geltung 4
3. Unmittelbare Geltung 6
4. Zusammenspiel mit anderen Regelwerken 7
a) Begleitgesetze auf Basis von Öffnungsklauseln 8
b) Spezialgesetzliche Datenschutzregelungen in Richtlinien und Gesetzen 12
c) Datenschutzregelungen außerhalb des Anwendungsbereichs der DSGVO 14
d) Zwischenergebnis 16

Rn.

II. Parallelität von DSGVO und „Altgesetzen“ 17

III. Auslegung der DSGVO und der Begleitgesetze 20
1. Auslegung der DSGVO 23
a) Autonome Auslegung des Unionsrechts 23
b) Auslegungsmethoden 24
c) Relevanz existierender Rechtsprechung 38
2. Auslegung der Begleitgesetze . . 41
a) Auslegungsmethoden 41
b) Relevanz existierender Rechtsprechung 45

I. Die Anwendung der DSGVO und der nationalen Begleitgesetze

Die DSGVO wurde häufig in einem Satz dadurch charakterisiert, dass sie keine Revolution, sondern eher eine **Evolution des Datenschutzrechts** mit sich gebracht habe. Das stimmt in vielen Bereichen, z. B. weil die der DSGVO zugrundeliegenden Datenschutzprinzipien[1] bereits aus der DSRL bekannt waren und weil u. a. einige Zulässigkeitsvorschriften[2] fast wortgleich aus der DSRL übernommen worden waren. **1**

Es ist aber auch richtig, dass die DSGVO in mehreren Bereichen **bedeutsame Änderungen** bewirkt hat. Zwei prominente Beispiele hierfür sind die signifikant erhöhten Bußgelder[3] und die starke Ausprägung der Verpflichtungen zur Implementierung eines Datenschutz-Managementsystems,[4] das in dem von der **2**

1 Siehe Kap. 4 Rn. 3 ff.
2 Siehe Kap. 5 Rn. 10 ff.
3 Siehe Kap. 16 Rn. 87 ff.
4 Siehe Kap. 10 Rn. 10 ff.

DSGVO verlangten Reifegrad vorher nur in sehr wenigen Unternehmen konsequent umgesetzt war.

1. Stand der Umsetzung in den Unternehmen

3 Jedes Unternehmen, das in relevantem Umfang personenbezogene Daten verarbeitet, musste und muss sich deshalb intensiv mit den Regelungen befassen und in spezifischen DSGVO-Umsetzungsprojekten oder im Rahmen laufender Kontrollen die Relevanz für die eigene Datenverarbeitung ermitteln und notwendige Anpassungsmaßnahmen ableiten und ergreifen.[5] Nach unseren Erfahrungen ist es zwar so, dass die allermeisten Unternehmen ihre DSGVO-Umsetzungsprojekte mittlerweile abgeschlossen haben. Es ist aber auch nicht zu verkennen, dass bei weitem nicht alle Unternehmen bereits eine 100%ige DSGVO-Konformität erreicht haben. Nach einer Umfrage des Branchenverbandes Bitkom aus dem September 2019 hätten zwar 67% der Unternehmen Maßnahmen zur Umsetzung der DSGVO ergriffen; es seien eineinhalb Jahre nach Inkrafttreten der neuen Regelungen aber nur 25% der Unternehmen vollständig DSGVO-konform.[6] Darüber hinaus muss aus einem statischen Datenschutz-Managementsystem, das im Rahmen eines DSGVO-Umsetzungsprojekts entsteht, ein dynamisches System werden, das sich laufend optimiert. Anderenfalls ist eine nachhaltige DSGVO-Compliance gerade nicht gewährleistet.[7] Es ist daher wichtig, sich fortwährend zu vergegenwärtigen, dass der Übergang zur DSGVO auch einen **systematischen Schwenk** mit sich gebracht hat, der in zeitlicher und in inhaltlicher Hinsicht ebenfalls fortwährend bewältigt werden muss.

2. Zeitliche Geltung

4 In zeitlicher Hinsicht war der Übergang weniger problematisch, weil es eine klare **Stichtagsregelung** gibt: Bis zum 24.5.2018 war das alte Recht vollumfänglich anwendbar; erst seit dem **25.5.2018** gilt die DSGVO. Dort wo die DSGVO also Erleichterungen gegenüber der ehemaligen Rechtslage bewirkt hat, z. B. durch den Verzicht auf das ehemals in § 11 Abs. 2 S. 2 BDSG a. F. normierte Schriftformerfordernis, dürfen diese erst seit dem Stichtag in rechtssicherer Weise in Anspruch genommen werden.

5 Ungeachtet dessen bedeutet dies nicht, dass das alte Recht ab sofort keine Rolle mehr spielt. Gerade in derzeit noch laufenden Gerichtsverfahren müssen Sachverhalte häufig noch nach altem Recht – und ggf. parallel auch nach der DSGVO –

5 Siehe hierzu Kap. 20.

6 Umfrage des Bitkom e. V.; Ergebnisse abrufbar unter: https://www.bitkom.org/Presse/Presseinformation/Zwei-Drittel-Unternehmen-DS-GVO-groesstenteils-umgesetzt, zuletzt abgerufen am 2.3.2021.

7 Siehe Kap. 10 Rn. 56.

beurteilt werden. Ein aktuelles Beispiel bildet das Gerichtsverfahren in Sachen *Planet49*: Der EuGH hat in seiner Entscheidung[8] einleitend festgestellt, dass der Ausgangsrechtsstreit nach der Zurückverweisung an den vorlegenden BGH u. U. auf Grundlage der nach der letzten mündlichen Verhandlung zur Geltung gekommenen DSGVO entschieden werden müsse und die Vorlagefragen daher sowohl nach Maßgabe der DSRL als auch der DSGVO zu beantworten waren.

3. Unmittelbare Geltung

Ein ganz maßgeblicher Unterschied des „neuen Datenschutzrechts" gegenüber den alten Regelungen ergibt sich aus dem Rechtscharakter der DSGVO als einer Verordnung: Sie gilt als Verordnung gemäß Art. 288 Abs. 2 AEUV unmittelbar in jedem Mitgliedstaat und bedarf deshalb keiner Umsetzung durch die Mitgliedstaaten. Bei den zusätzlich erlassenen nationalen Datenschutzgesetzen handelt es sich deshalb auch nicht um Umsetzungsakte, sondern um (freiwillige) Begleitgesetze, die den direkten und unmittelbaren Geltungsanspruch der DSGVO unberührt lassen. Die Adressaten der DSGVO einschließlich der mit personenbezogenen Daten umgehenden Unternehmen sind direkt an die Pflichten aus der DSGVO gebunden. **6**

4. Zusammenspiel mit anderen Regelwerken

Die DSGVO verfolgt dabei aber keinen Vollharmonisierungsansatz in dem Sinne, dass es keinerlei Datenschutzvorschriften in anderen Regelwerken auf europäischer oder nationaler Ebene mehr geben kann und soll. Zwar wurde die **DSRL** gemäß Art. 94 Abs. 1 DSGVO zeitlich zum 25.5.2018 **aufgehoben**, damit sind aber keineswegs alle Parallelgesetze beseitigt. Im Gegenteil bettet sich die DSGVO in ein **Regelungsgeflecht** aus manchen neuen und manchen **weitergeltenden Datenschutzregelungen** ein. Hieraus entsteht eine nicht zu unterschätzende Komplexität. **7**

a) Begleitgesetze auf Basis von Öffnungsklauseln

Zunächst enthält die DSGVO selbst eine Reihe sogenannter „**Öffnungsklauseln**", in denen sie den Mitgliedstaaten gestattet, spezifizierende oder abweichende Regelungen zu treffen. Beispiele hierfür sind Art. 8 Abs. 1 UAbs. 2 DSGVO, wonach die Mitgliedstaaten eine Absenkung der Altersgrenze für Einwilligungen von Minderjährigen von 16 auf bis zu 13 Jahren vorsehen dürfen; und Art. 37 Abs. 4 S. 1, 2. HS DSGVO, der es den Mitgliedstaaten gestattet, von Art. 37 Abs. 1 DSGVO abweichende Voraussetzungen für die Pflicht zur Bestellung eines Datenschutzbeauftragten vorzusehen. **8**

8 EuGH, Urt. v. 1.10.2019 – Rs. C-673/17, MMR 2019, 732, 734 m. Anm *Moos/Rothkegel.*

9 In vielen Mitgliedstaaten sind entsprechende Gesetzgebungsverfahren bereits abgeschlossen, die der Inanspruchnahme dieser insgesamt ca. 80 Öffnungsklauseln dienen. Der deutsche Gesetzgeber war hierbei besonders schnell: Das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (**Datenschutz-Anpassungs- und -Umsetzungsgesetz EU** – DSAnpUG-EU vom 30.6.2017) war bereits am 5.7.2017 im Bundesgesetzblatt verkündet worden.[9]

10 Das Artikelgesetz enthält unter anderem als Art. 1 das **BDSG**, welches die Begleitvorschriften zur DSGVO enthält, die auf deren Öffnungsklauseln gestützt sind.[10] Gemäß Art. 8 Abs. 1 DSAnpUG-EU trat das BDSG parallel zur DSGVO am 25.5.2018 in Kraft.

11 Am 29.11.2019 ist in Deutschland das Zweite Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (**Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU** – 2. DSAnpUG-EU) in Kraft getreten. Es handelt sich ebenfalls um ein Artikelgesetz, durch das – allerdings überwiegend nur terminologische – Änderungen an diversen Einzelgesetzen vorgenommen wurden, um so die Datenschutzregelungen in diesen Gesetzen mit den Begrifflichkeiten der DSGVO zu harmonisieren.

b) Spezialgesetzliche Datenschutzregelungen in Richtlinien und Gesetzen

12 Explizit nicht durch die DSGVO abgelöst wurde die **RL 2002/58/EG**.[11] In Art. 95 DSGVO wird folgerichtig das Verhältnis der Regelungswerke zueinander geregelt, und zwar in dem Sinne, dass die RL 2002/58/EG vorrangig vor der DSGVO gilt, soweit sie besondere Pflichten enthält, die dasselbe Ziel wie die DSGVO-Pflichten verfolgen. Die RL 2002/58/EG ist also in ihrem Anwendungsbereich **lex specialis zur DSGVO**.

13 Daraus folgt, dass auch die mitgliedstaatlichen **Vorschriften zur Umsetzung der RL 2002/58/EG** Vorrang haben vor der DSGVO; in Deutschland sind dies einige – aber nicht alle – Datenschutzregelungen im TKG, manche Datenschutzvorschriften im TMG und die Regelung in § 7 Abs. 2 und 3 UWG. Problematisch hierbei ist, dass die Datenschutzvorschriften in TKG und TMG keine 1:1-Umsetzungen der Richtlinienvorgaben sind. Sie enthalten vielmehr auch Regeln mit datenschutzrechtlicher Natur, die in der RL 2002/58/EG nicht vorgesehen sind

9 BGBl. I 1944 v. 5.7.2017, S. 2097; vgl. zur Rechtslage in Österreich außerdem ausführlich Kap. 18.

10 Vgl. *Kremer*, CR 2017, 367, 371 ff.

11 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 v. 31.7.2002, S. 37.

oder möglicherweise gerade keine Umsetzung der entsprechenden Vorschriften in der RL 2002/58/EG sind. Soweit dies der Fall ist, partizipieren solche überschießenden Regelungen nicht am Anwendungsvorrang und werden prinzipiell von der DSGVO verdrängt.

Praxishinweis

Aktuell ergibt sich hieraus eine besondere Problematik bei der Frage des rechtmäßigen Einsatzes von **Cookies** auf Unternehmens-Webseiten. Es bestehen unterschiedliche Ansichten darüber, ob die Regelungen im TMG eine ordnungsgemäße Umsetzung von Art. 5 Abs. 3 der RL 2002/58/EG darstellen. Die deutschen Datenschutzaufsichtsbehörden verneinen dies mit der Folge, dass sie insbesondere § 15 Abs. 3 TMG für unanwendbar halten und die Zulässigkeit am Maßstab der DSGVO messen.[12]

c) Datenschutzregelungen außerhalb des Anwendungsbereichs der DSGVO

Außerdem regelt die DSGVO auch im Übrigen den Datenschutz in der EU und den Mitgliedstaaten nicht vollständig. Teil des EU-Legislativpakets zum Datenschutz war nicht nur die DSGVO, sondern auch die RL 2016/680/EU[13] im Bereich der Strafverfolgung. Die Vorgaben dieser Richtlinie bedürfen wiederum der Umsetzung ins nationale Recht; in Deutschland ist dies in Teil 3 des BDSG bereits erfolgt. Diese Regelungen stehen unbeeinflusst neben der DSGVO. **14**

Der Vollständigkeit halber sei abschließend erwähnt, dass es auch datenschutzrechtliche Regelungsmaterien gibt, die weder in die Anwendungsbereiche der DSGVO noch der RL 2016/680/EU fallen, wie etwa im Bereich der Landesverteidigung. Für die Datenverarbeitung durch Unternehmen spielen diese Regelungen freilich allenfalls eine Nebenrolle. **15**

d) Zwischenergebnis

Der vorstehende Überblick zeigt, dass es nunmehr ein schwieriger zu bewältigendes Regelungsgeflecht von DSGVO, Richtlinien und nationalen Begleit- und **16**

12 Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, Stand März 2019, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf, zuletzt abgerufen am 8.10.2020.

13 Richtlinie (EU) 2016/680 vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. EU L 119 v. 4.5.2016, S. 89.

Umsetzungsgesetzen gibt. Gerade dort, wo nationale Datenschutzvorschriften nicht eindeutig und trennscharf einer Öffnungsklausel der DSGVO oder einer umzusetzenden Richtlinienvorgabe zugewiesen werden können, besteht eine **unsichere Rechtslage**.

II. Parallelität von DSGVO und „Altgesetzen"

17 Eine jedenfalls für eine längere Dauer fast noch komplexere Problematik besteht im Hinblick auf die nationalen Datenschutzregeln und Gesetze, die nach wie vor **nicht an die DSGVO angepasst** worden sind. Soweit solche nationalen Regelungen nicht entweder außerhalb des Anwendungsbereichs der DSGVO liegen oder spezialgesetzliche Richtlinienvorgaben umsetzen, sind sie nur noch in dem Umfang zugelassen und anwendbar, wie sie von Öffnungsklauseln der DSGVO gedeckt sind.

18 Auch wenn in Deutschland durch das 1. und das 2. DSAnpUG und das BDSG viele Datenschutzvorschriften in Spezialgesetzen bereits angepasst worden sind, stehen manche Anpassungen noch aus (wie z. B. beim TMG, welches durch das 2. DSAnpUG nicht geändert worden ist). Das führt dazu, dass weiterhin nationale Rechtsvorschriften fortbestehen, die nicht an die neue europäische Rechtslage angeglichen sind.

Beispiel

In seinem Urteil vom 14.2.2019 hat sich der EuGH u. a. mit der datenschutzrechtlichen Bereichsausnahme für die Medien befasst und Hinweise zur **Vereinbarkeit des Medienprivilegs** nach nationalem Recht **mit dem europäischen Datenschutzrecht** gegeben.[14] Art. 85 DSGVO sieht analog der RL 95/46/EG zwar generell eine datenschutzrechtliche Privilegierung der Medien vor, soweit personenbezogene Daten „zu journalistischen Zwecken" verarbeitet werden. Nach Art. 85 Abs. 2 DSGVO dürfen die Mitgliedstaaten hiernach Abweichungen oder Ausnahmen von Kapitel II (Grundsätze) aber nur vorsehen, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen. Aus den Ausführungen des EuGH lässt sich ableiten, dass er eine umfassende Bereichsausnahme für zu weitgehend halten könnte, wenn dadurch z. B. sämtliche Rechte der betroffenen Personen ausgeschlossen sind.

14 EuGH, Urt. v. 14.2.2019 – C-345/17, ECLI:EU:C:2019:122.

Nationale Vorschriften können seit dem 25.5.2018 somit nicht mehr bedenkenlos weiter angewendet werden, so dass für die Unternehmen eine gewisse Rechtsunsicherheit entsteht. Sie müssen in jedem Einzelfall prüfen, ob und in welchem Umfang die Regelung **von einer Öffnungsklausel der DSGVO oder einer spezialgesetzlichen EU-Richtlinie gedeckt** ist. Nur in diesem Rahmen kann die jeweilige Vorschrift weiter angewendet werden. Außerhalb dieses Rahmens gilt der **Anwendungsvorrang des EU-Rechts**, so dass dann ggf. auf die Vorschriften der **DSGVO** zurückgegriffen werden muss. **19**

Praxishinweis

Sobald für eine konkrete Rechtsfrage Normen verschiedener Gesetze relevant sind, sollte in einem ersten Schritt die Wirksamkeit dieser Normen und ihr Verhältnis zueinander anhand der vorstehend aufgeführten Maßstäbe geprüft werden.

III. Auslegung der DSGVO und der Begleitgesetze

Neben der Ermittlung der Anwendbarkeit der einschlägigen Datenschutzvorschriften besteht eine Herausforderung in ihrer richtigen Auslegung. **20**

Sowohl die DSGVO als auch die ePrivacy-Richtlinie sind europäische Rechtsakte. Nur die europäischen Gerichte legen sie verbindlich aus. Nach Art. 267 Abs. 1 lit. a AEUV entscheidet der EuGH z. B. im Wege der Vorabentscheidung über die Auslegung der Verträge. Hingegen sind das BDSG, das TMG, das TKG und sonstige deutsche Gesetze mit datenschutzrechtlichem Regelungsgehalt nationale Rechtsakte, die primär von den deutschen Gerichten ausgelegt werden. Europäische Gerichte legen diese deutschen Gesetze nur dann aus, wenn es für europarechtliche Fragen relevant ist.[15] **21**

Diese scheinbar trivialen Feststellungen haben spätestens seit Geltung der DSGVO erhebliche Implikationen für den Datenschutzpraktiker. Denn regelmäßig hängt die konkrete Ausgestaltung datenschutzrechtlich getriebener Maßnahmen von der Auslegung eines der oben genannten Gesetze ab. Dabei darf die deutsche **Auslegungsmethodologie** – wie es auch in der Literatur häufig passiert – nicht unreflektiert auf die DSGVO angewendet werden. Stattdessen sind die europäischen Vorgaben entsprechend der Methoden der europäischen Gerichte auszulegen. **22**

15 Siehe beispielsweise zur Reichweite von Öffnungsklauseln oben Rn. 8 ff.

Praxishinweis

Das Datenschutzrecht ist eine komplexe Materie. Nichtsdestoweniger sollte sich auch der Datenschutzpraktiker eine eigene Meinung dazu bilden, wie bestimmte Normen auszulegen sind. Denn weder die Datenschutzbehörden noch besonders profilierte Rechtswissenschaftler haben eine Deutungshoheit bezüglich der Auslegung von Normen.[16] Zwar sollte das Unternehmen schon aus Haftungsgründen die entsprechenden Stellungnahmen seiner zuständigen Aufsichtsbehörde kennen und in Entscheidungen einbeziehen, doch muss der Anwender im Unternehmen nichtsdestoweniger eine **eigene Wertung** treffen. Diese Wertung sollte – jedenfalls bei wichtigen Fragestellungen – im Hinblick auf die **Rechenschaftspflicht** gemäß Art. 5 DSGVO[17] auch dokumentiert werden.

1. Auslegung der DSGVO

a) Autonome Auslegung des Unionsrechts

23 Aus den Anforderungen sowohl der einheitlichen Anwendung des Unionsrechts als auch des Gleichheitsgrundsatzes hat der EuGH seit jeher gefolgert, dass die Begriffe einer Vorschrift des Unionsrechts, die für die Ermittlung ihres Sinnes und ihrer Tragweite nicht ausdrücklich auf das Recht der Mitgliedstaaten verweist, in der Regel in der gesamten Union eine **autonome und einheitliche Auslegung** erhalten müssen.[18] Eine schlichte Übernahme bestimmter, im nationalen Recht etablierter Interpretationen verbietet sich also.

b) Auslegungsmethoden

24 Grundsätzlich wenden die europäischen Gerichte die gleichen Auslegungsmethoden an wie die deutsche Rechtswissenschaft. Neben der Auslegung auf Grundlage des Wortlauts finden also die systematische, die teleologische und die historische Auslegung Anwendung. Allerdings unterscheiden sich die Gewichtung und konkrete Anwendung dieser Methoden nennenswert von der deutschen Vorgehensweise. Darüber hinaus spielt regelmäßig das „**effet-utile-Prinzip**“ im Europarecht eine große Rolle.

16 Siehe zur Bedeutung von Stellungnahmen der Datenschutzbehörden Kap. 16 Rn. 62 ff.
17 Siehe zur Rechenschaftspflicht Kap. 4 Rn. 27 ff.
18 EuGH, Urt. v. 1.10.2019 – Rs. C-673/17, MMR 2019, 732, 734, Rn. 47 m. Anm *Moos/Rothkegel*.

aa) Wortlaut

Auch im europäischen Recht stellt die **Interpretation des Wortlauts** einer Norm die grundlegende Auslegungsmethode dar. Allerdings ist schon umstritten, ob sie auch die wichtigste ist.[19] Jedenfalls stellt der Wortlaut prinzipiell den Ausgangspunkt und die Grenze der Auslegung von Normen dar.[20] Nichtsdestoweniger hat der EuGH in einzelnen Entscheidungen Auslegungen entwickelt, die die Rechtswissenschaft eher als Rechtsfortbildung denn als Rechtsauslegung bewertet hat.[21] **25**

Darüber hinaus sind bei der Auslegung des Wortlauts einer Norm des Unionsrechts die Besonderheiten des europäischen Rechts als **supranationales und multilinguales Rechtssystem** zu berücksichtigen. Die verschiedenen sprachlichen Versionen der europäischen Gesetze sind gleichrangig.[22] Weder aus der Zahl der Bevölkerung, die eine gewisse Sprache spricht, noch aus sonstigen Umständen lässt sich herleiten, dass eine Sprachfassung gültiger ist als eine andere. Darüber hinaus legt der EuGH die unionsrechtlichen Begriffe unabhängig von der Verwendung dieser Begriffe in einzelnen Mitgliedstaaten aus.[23] **26**

Praxishinweis

Bei der Auslegung der DSGVO sollten auch **andere Sprachfassungen** Berücksichtigung finden. Im Fall von Unstimmigkeiten sind beide Versionen gleich gültig. Der Wortlaut ist dann unstimmig. Widersprüche lassen sich nicht durch eine Auslegung der verschiedenen Sprachfassungen auflösen, sondern nur durch die Anwendung der anderen Auslegungsmethoden. Obwohl die Trilogverhandlungen auf Englisch geführt wurden, geht also die englische den anderen Sprachfassungen bei der Auslegung des Wortlauts nicht vor. Diese Tatsache kann alleine im Rahmen der teleologischen oder systematischen Auslegung Berücksichtigung finden.

19 Dauses/Ludwigs/*Pieper*, Teil B I Rn. 11, hält sie auch für die wichtigste; Bergmann/*Bergmann*, Begriff „Auslegung von Unionsrecht"; Calliess/Ruffert/*Wegener*, Art. 19 EUV (Lissabon) Rn. 13, und Schwarze/Becker/Hatje/Schoo/*Schwarze/Wunderlich*, Art. 19 EUV Rn. 36 m. w. N., halten hingegen die teleologische Auslegungsmethode für wichtiger.

20 Dauses/Ludwigs/*Pieper*, Teil B I Rn. 12; Calliess/Ruffert/*Wegener*, Art. 19 EUV (Lissabon) Rn. 13.

21 Bergmann/*Bergmann*, Begriff „Auslegung von Unionsrecht".

22 Griller/Rill/*Streinz*, S. 223, 243.

23 Vgl. Calliess/Ruffert/*Wegener*, Art. 19 EUV (Lissabon) Rn. 13 mit zahlreichen Nachweisen.

bb) Teleologische Auslegung

27 Eine besonders wichtige Auslegungsmethode der europäischen Gerichtsbarkeit ist die Auslegung von Normen anhand des **Gesetzeszwecks**. Diese Auslegungsmethode hat in der europäischen Rechtsprechung eine weitaus größere Bedeutung als in der deutschen und sie wird teilweise auch als bei Weitem wichtigste Auslegungsmethode gesehen.[24]

28 Zur Bestimmung des Ziels einer Norm greift der EuGH insbesondere auf die entsprechenden **Erwägungsgründe** zurück.[25] Dabei leitet der EuGH aus diesen Erwägungsgründen vereinzelt sogar selbstständige Rechtssätze ab.[26] Punktuell korrigiert oder ergänzt der EuGH die Erwägungsgründe auch anhand der relevanten Regelungen der Verträge.[27]

29 Falls die Erwägungsgründe unergiebig sind, stellt der Gerichtshof hinsichtlich des Zwecks einer Norm auch auf den **Zusammenhang des Textes** ab. Er bezieht dabei weitere Normen des jeweiligen Gesetzes in seine Auslegung mit ein und identifiziert deren Ziele und die Auswirkungen des Gesamtsystems. Diese Auswirkungen sieht er grundsätzlich als vom Gesetzgeber intendiert an und verbindet auf diese Weise eine teleologische mit einer systematischen Auslegung.[28]

30 Auch in **datenschutzrechtlichen Leitentscheidungen** hat die teleologische Auslegung bereits eine wichtige Rolle gespielt. So hat der Gerichtshof z. B. in seiner **„Safe Harbor"-Entscheidung** entscheidend auf den Zweck der Art. 25 und 28 RL 95/46/EG abgestellt, um sein Ergebnis zu begründen.[29] Dabei hat er auch auf Art. 8 GRCh zurückgegriffen, um diesen Zweck herzuleiten.[30] Auch für

---

24 *Schwarze*/*Wunderlich*, Art. 19 EUV Rn. 36 m. w. N.; Griller/Rill/*Streinz*, S. 223, 243.

25 Dauses/Ludwigs/*Pieper*, Teil B I Rn. 35 unter Verweis auf EuGH, Urt. v. 17.6.1971 – 3/71, ECLI:EU:C:1971:70, S. 588; EuGH, Urt. v. 4.10.1972 – 9–72, ECLI:EU:C:1972:81, S. 969; EuGH, Urt. v. 4.4.1974 – 167–73, ECLI:EU:C:1974:35, S. 378; EuGH, Urt. v. 10.10.1974 – 25–74, ECLI:EU:C:1974:102, S. 1023; EuGH, Urt. v. 30.1.1974 – 159–73, ECLI:EU:C:1974:9, S. 1230; EuGH, Urt. v. 28.6.1979 – verb. Rs. 233, 234 und 235/78, ECLI:EU:C:1979:174; EuGH, Urt. v. 12.7.1979 – 244/78, ECLI:EU:C:1979:198, S. 2682; EuGH, Urt. v. 7.7.1981 – 158/80, ECLI:EU:C:1981:163, S. 1869; EuGH, Urt. v. 29.3.1979 – 118/77, ECLI:EU:C:1979:92; EuGH, Urt. v. 6.10.1981 – 246/80, ECLI:EU:C:1981:218, S. 2330; *GA Roemer*, EuGH, Urt. v. 16.3.1971 – 67/69, ECLI:EU:C:1971:26, S. 222; speziell zum Datenschutzrecht EuGH, Urt. v. 6.10.2015 – C-362/14 Rn. 46, BeckEuRS 2015, 447115.

26 EuGH, Urt. v. 24.5.2011 – C-54/08, ECLI:EU:C:2011:339, S. 1870.

27 Dauses/Ludwigs/*Pieper*,Teil B I Rn. 44.

28 Dauses/Ludwig/*Pieper*, Teil B I Rn. 44 f.

29 EuGH, Urt. v. 6.10.2015 – C-362/14, BeckEuRS 2015, 447115, Rn. 56 f. u. Rn. 72.

30 EuGH, Urt. v. 6.10.2015 – C-362/14, BeckEuRS 2015, 447115 Rn. 72 f.

die Auslegung des Begriffs „personenbezogenes Datum" war eine Auslegung auf Grundlage des entsprechenden Erwägungsgrunds entscheidend.[31]

cc) Systematische Auslegung

Die **systematische Auslegung** erschließt den Regelungsgehalt einer Norm durch ihre Position und ihre Funktion innerhalb der Normen und des Systems des jeweiligen Textes.[32] Innerhalb der DSGVO wäre beispielsweise die Auslegung eines Begriffs in einem Artikel anhand der entsprechenden Begriffsdefinition in Art. 4 DSGVO ein Fall der systematischen Auslegung. **31**

Ein besonderer Fall der systematischen Auslegung des Unionsrechts ist die **vertragskonforme Auslegung des Sekundärrechts**.[33]

Insbesondere im Hinblick auf die RL 95/46/EG hat der Gerichtshof bei seiner Auslegung auch bereits auf **Art. 8 GRCh** zurückgegriffen und aus dieser die Zwecke einer Norm hergeleitet.[34] Er sprach insoweit von einer Auslegung „im Lichte der Charta".[35] Es handelte sich wohl um eine systematische Auslegung, die darauf abzielte, den Gesetzeszweck für eine teleologische Auslegung herzuleiten. **32**

Beispiel

Ein aktuelles Beispiel, in dem die systematische Auslegung eine große Rolle spielt, betrifft die Bestimmung der datenschutzrechtlichen Anforderungen an den **Einsatz von Cookies**. Im Zusammenhang mit der Auslegung der Anforderungen nach Art. 5 Abs. 3 RL 2002/58/EG hat der EuGH in seinem Urteil in Sachen *Planet49* konstatiert, dass bei der Auslegung einer Vorschrift des Gemeinschaftsrechts neben Wortlaut und Zielen auch der Kontext und **das gesamte Unionsrecht** zu berücksichtigen seien.[36] Das könnte zur Folge haben, dass bei der Frage der Anwendung von Art. 6 DSGVO durchaus auch dem Umstand Rechnung zu tragen ist, dass in Art. 5 Abs. 3 RL 2002/58/EG ein explizites Einwilligungserfordernis enthalten ist.

31 EuGH, Urt. v. 19.10.2016 – C-582/14, MMR 2016, 842, Rn. 42 ff. m. Anm. *Moos/Rothkegel*.
32 Riesenhuber/*Pechstein*/*Drechsler*, § 7 Rn. 22 ff.
33 Calliess/Ruffert/*Wegener*, Art. 19 EUV (Lissabon) Rn. 15.
34 EuGH, Urt. v. 6.10.2015 – C-362/14, BeckEuRS 2015, 447115, Rn. 47, 58, 66.
35 EuGH, Urt. v. 6.10.2015 – C-362/14, BeckEuRS 2015, 447115, Rn. 73 f.
36 EuGH, Urt. v. 1.10.2019 – Rs. C-673/17, MMR 2019, 732, 734, Rn. 48 m. Anm *Moos/Rothkegel*.

dd) Historische Auslegung

33 Die historische Auslegung sucht den **wahren Willen des Gesetzgebers** (subjektiv-historische Auslegung) oder die historische Funktion einer Norm unter Betrachtung ihrer Entstehungsgeschichte zu ergründen (objektiv-historische Auslegung).[37] Jedenfalls im Falle des Sekundärrechts, also auch der DSGVO, wenden die europäischen Gerichte auch diese Auslegungsmethode an.[38]

34 Allerdings hat die historische Auslegung nur eine **stark untergeordnete Bedeutung**.[39] Primär findet sie bei verschiedenen veröffentlichten Fassungen aufeinander folgender Rechtsakte oder bei mehreren Entwürfen eines Rechtsakts Anwendung.[40] Insbesondere nutzt der Gerichtshof die historische Auslegung, um gefundene Auslegungsergebnisse durch die historische Auslegung als Hilfsbegründung zu bestätigen.[41]

Praxishinweis

Angesichts der geringen Bedeutung der historischen Auslegungsmethode in der Rechtsprechung des Gerichtshofs ist bei der Auslegung der DSGVO Vorsicht geboten, sofern ein Auslegungsergebnis primär mit einem Verweis auf die Änderungen des Entwurfs der DSGVO im Rahmen der **Trilogverhandlungen** gestützt wird. Es ist fraglich, ob der Gerichtshof den Trilogverhandlungen eine entscheidende Bedeutung beimessen wird.

ee) „Effet-utile-Prinzip"

35 In der europäischen Rechtsprechung hat das „**Effet-utile-Prinzip**" eine besondere Bedeutung. Normen sind danach so auszulegen, dass sie ihrem Ziel am wirksamsten entsprechen.[42] Unter mehreren Auslegungsergebnissen wäre also das Ergebnis zu wählen, mit dem das Ziel der jeweiligen Norm möglichst effektiv erreicht wird.[43]

---

37 Riesenhuber/*Pechstein*/*Drechsler*, § 7 Rn. 33.

38 Dauses/Ludwigs/*Pieper*, Teil B I Rn. 46; EuGH, Urt. v. 1.10.2019 – Rs. C-673/17, MMR 2019, 732, 734, Rn. 48 m. Anm *Moos/Rothkegel*.

39 Calliess/Ruffert/*Wegener*, Art. 19 EUV (Lissabon) Rn. 14.

40 Dauses/Ludwigs/*Pieper*, Teil B I Rn. 46.

41 Calliess/Ruffert/*Wegener*, Art. 19 EUV (Lissabon) Rn. 14; Dauses/Ludwig/*Pieper*, Teil B I Rn. 46.

42 Vgl. Dauses/Ludwigs/*Pieper*, Teil B I Rn. 46 mit zahlreichen Nachweisen.

43 Calliess/Ruffert/*Wegener*, Art. 19 EUV (Lissabon) Rn. 16.

Das „Effet-utile-Prinzip" kann sowohl als eine Variante einer systematischen[44] als auch einer teleologischen[45] Auslegung gesehen werden. **36**

Praxishinweis

Gerade im **Datenschutzrecht** ist das „Effet-utile-Prinzip" häufig relevant. Bei sämtlichen Normen, die bestimmte Verhaltensweisen untersagen sollen, streitet das „Effet-utile-Prinzip" für diejenige Auslegung, die dem jeweiligen Verbot zu einer besonders hohen Wirksamkeit verhilft. Allerdings ist nicht jegliches „Mehr an Datenschutz" immer besonders wirksam im Sinne des „Effet-utile-Prinzips". Vielmehr muss der spezifische Zweck der jeweiligen Norm besonders wirksam verwirklicht werden.

ff) Mischung verschiedener Auslegungsmethoden

Weder in der Rechtsprechung des Gerichtshofs noch generell ist es möglich, die Auslegungsmethoden eindeutig zu trennen. Ein Rückgriff auf die Erwägungsgründe kann einerseits einer teleologischen Auslegung dienen, um den Zweck einer Norm zu identifizieren, er mag aber auch Teil einer historischen Auslegung sein, um den historischen Willen des Gesetzgebers zu ermitteln. Darüber hinaus stellt der Gerichtshof seine methodologische Vorgehensweise regelmäßig kaum dar und konzentriert sich stattdessen auf die **Ergebnisse der Auslegung**.[46] Vor diesem Hintergrund bleibt eine wertende Gesamtschau der Ergebnisse der verschiedenen Auslegungsmethoden zwangsläufig notwendig, weshalb es derart schwierig ist, Urteile des Gerichtshofs vorherzusagen. **37**

Praxishinweis

In seinen jüngeren Entscheidungen hat der Gerichtshof durchgehend eine **datenschutzfreundliche Linie** verfolgt.[47] Bei unklaren Auslegungsergebnissen mag es also für Unternehmen ratsam sein, eher der strengeren Auslegung zu folgen. Allerdings ist es wirtschaftlich manchmal nicht sinnvoll, der strengsten Rechtsansicht zu folgen. Die Entscheidungsfindung ist also schwierig und sollte jedenfalls in grundlegenden Fragen durch die Leitungsebene erfolgen.

44 So z. B. wohl Dauses/Ludwigs/*Pieper*, Teil B I Rn. 30.
45 So Calliess/Ruffert/*Wegener*, Art. 19 EUV (Lissabon) Rn. 16.
46 Dauses/Ludwigs/*Pieper*, Teil B I Rn. 10.
47 Für eine überblicksartige Zusammenstellung: *Skouris*, NVwZ 2016, 1359; eingehend zum „Safe Harbor"-Urteil: *Moos*/*Schefzig*, CR 2015, 625; zum „Breyer-Urteil": MMR 2016, 842 m. Anm. *Moos*/*Rothkegel;* siehe auch Kap. 19.

Deshalb sollten Unternehmen **eigene Positionen zu rechtlichen Fragestellungen** entwickeln und diese im eigenen Datenschutzmanagement entsprechend umsetzen.[48] Beispielsweise sollten jedenfalls große Unternehmen intern definieren, welche Daten als personenbezogene Daten behandelt werden.

c) Relevanz existierender Rechtsprechung

38 Die **Rechtsprechung** des Gerichtshofs **zur DSRL** kann nicht unreflektiert auf die DSGVO übertragen werden.

Beispiel

In kurzer Folge hat der EuGH drei viel beachtete Entscheidungen zur **gemeinsamen Verantwortlichkeit** gefällt[49]; und zwar bzgl. eines Fanpage-Betreibers und des dazugehörigen sozialen Netzwerks, bzgl. einer Glaubensgemeinschaft und ihren jeweiligen Mitgliedern sowie bzgl. eines Webseitenbetreibers und des Begünstigten eines sog. „Like-Buttons". Sämtliche Urteile beziehen sich aber noch auf die Rechtslage nach der Datenschutzrichtlinie. Es ist durchaus umstritten, ob die Feststellungen des EuGH ohne weiteres zur Auslegung des Art. 26 DSGVO herangezogen werden können.[50]

39 Allerdings haben die Urteile in vielen Fällen trotzdem eine starke **Indikationswirkung** dahingehend, dass der Gerichtshof ähnliche Fragestellungen auf gleiche Art und Weise lösen wird. Insbesondere sind Entscheidungen des Gerichtshofs (bzw. EuGH) insoweit übertragbar, wie sie Normen der DSRL betreffen, die sich in identischer oder sehr ähnlicher Weise auch in der DSGVO wiederfinden. Beispielsweise dürften die Ausführungen des Gerichtshofs in seinem „Safe Harbor"-Urteil auch unter der DSGVO weitgehend Gültigkeit bewahren.[51]

40 Auch die bereits dargestellten Referenzen auf die **Charta der Grundrechte der Europäischen Union** in der jüngeren Rechtsprechung des Gerichtshofs[52] haben zur Folge, dass die entsprechenden Urteile grundlegende Erwägungen enthalten, die auch für die DSGVO fortgelten dürften.

---

48 Siehe zum Datenschutzmanagement Kap. 10.

49 Siehe im Einzelnen Kap. 19 Rn. 30 ff.

50 EuGH, Urt. v. 29.7.2019 – Rs. C-40/17, MMR 2019, 579, 586 m. Anm. *Moos/Rothkegel*.

51 Siehe zur Fragestellung internationaler Datenübermittlungen und die „Safe Harbor"-Entscheidung Kap. 9 Rn. 23 ff.

52 Vgl. oben Rn. 30, 32; siehe auch Kap. 9 Rn. 26 zum Einfluss d. EGRC im Schrems I-Urteil.

2. Auslegung der Begleitgesetze

a) Auslegungsmethoden

aa) Klassische Auslegungsmethoden

Bezüglich der klassischen Auslegungsmethoden der deutschen Gerichtsbarkeit – nämlich **Wortlaut**, **Systematik**, **teleologische Auslegung** und **historische Auslegung** – sei auf die existierenden ausführlichen Darstellungen verwiesen.[53] Der Kern der Auslegungsmethoden lässt sich unter Ausklammerung der europäischen Besonderheiten auch aus den oben stehenden Ausführungen entnehmen.[54] **41**

bb) Europarechtskonforme Auslegung

Im Datenschutzrecht ist außerdem die **europarechtskonforme Auslegung** von besonderer Bedeutung. Nach ihr sind nationale Gesetze der Mitgliedstaaten derart auszulegen, dass sie dem Unionsrecht nicht widersprechen.[55] Diese Auslegungsmethode ist eine Ausprägung des **Anwendungsvorrangs des Unionsrechts**. **42**

Im datenschutzrechtlichen Kontext sind die nationalen Datenschutzgesetze stets kritisch darauf zu prüfen, inwiefern sie unionsrechtlichen Vorgaben entsprechen. Das gilt sowohl für das BDSG als auch für Spezialgesetze wie z. B. TKG und TMG. **43**

Wie allein der Umfang des BDSG veranschaulicht, sieht der deutsche Gesetzgeber neben der DSGVO noch viel Raum für nationale Regelungen. Abgesehen von der Tatsache, dass diese Vorgehensweise das Ziel einer Rechtsharmonisierung in einem derart internationalen Feld wie dem Datenschutz konterkariert und damit volkswirtschaftlich bedenklich ist, bestehen bei diversen Normen auch Zweifel, ob sie europarechtskonform ausgelegt werden können. Schon unter der Datenschutzrichtlinie hat der Gerichtshof deutsche Sonderwege für europarechtswidrig erklärt.[56] Es ist zu erwarten, dass der Gerichtshof den neuen Sonderwegen nach Geltung der DSGVO genauso kritisch gegenübersteht. **44**

---

53 Z. B. *Zippelius*, Juristische Methodenlehre.

54 Siehe Rn. 24 ff.

55 Calliess/Ruffert/*Ruffert*, Art. 1 AEUV Rn. 24.

56 Siehe EuGH, Urt. v. 19.10.2016 – C-582/14, MMR 2016, 842, Rn. 62 ff. m. Anm. *Moos*/*Rothkegel*.

Beispiel

Ein erstes sehr praxisrelevantes Beispiel ergibt sich hierfür schon aus der Rechtsprechung des Bundesverwaltungsgerichts: Mit Urteil vom 27.3.2019 hat das BVerwG die **Videoüberwachung** öffentlicher Flächen in einer Zahnarztpraxis für unzulässig befunden.[57] Hierbei wenden die Richter i.E. § 4 BDSG nicht an, weil er europarechtskonform teleologisch zu reduzieren sei.[58] Dem Wortlaut nach gilt § 4 BDSG für die Videoüberwachung durch öffentliche und private Stellen gleichermaßen. Da die Mitgliedstaaten in Art. 6 Abs. 2, Abs. 3 DSGVO jedoch nur über Öffnungsklauseln verfügen, die sich auf Art. 6 Abs. 1 lit. c DSGVO (rechtliche Verpflichtung) oder Art. 6 Abs. 1 lit. e DSGVO (Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde) beziehen, verneinte das BVerwG das Vorliegen einer einschlägigen Öffnungsklausel für den Privatbereich. Die Zulässigkeit von Videoüberwachungen durch Private bestimmt sich deshalb nach Art. 6 Abs. 1 lit. f DSGVO.

b) Relevanz existierender Rechtsprechung

45 Die zum BDSG a. F. **existierende nationale Rechtsprechung** kann praktisch **nicht** auf die neue Rechtslage **übertragen** werden. Kern des deutschen Datenschutzrechts ist nunmehr mit der DSGVO ein europäischer Rechtsakt, welcher direkt anwendbar ist. Diese Verordnung ist, wie bereits dargelegt,[59] vollkommen autonom von nationalen Gesetzen auszulegen.

46 Allenfalls im Einzelfall – insbesondere bei den Spezialgesetzen wie dem TMG und dem TKG – mögen Gerichtsentscheidungen weiterhin relevant sein. Das sollte dann aber jeweils gründlich geprüft werden. Insbesondere sind auch diese datenschutzrechtlichen Spezialgesetze nunmehr im Lichte der DSGVO auszulegen, so dass potenziell sogar unveränderte Normen anders zu werten sein können.

57 BVerwG, Urt. v. 27.3.2019 – 6 C 2.18, ECLI:DE:BVerwG:2019:270319U6C2.18.0.

58 BVerwG, Urt. v. 27.3.2019 – 6 C 2.18, ECLI:DE:BVerwG:2019:270319U6C2.18.0, Rn. 47.

59 Vgl. oben Rn. 23.

Kapitel 2

Grundlagen des Datenschutzrechts

Übersicht

Rn.

I. Datenschutz im Anwendungsbereich des EU-Rechts 1
II. Schutzgut des Datenschutzrechts . . . 3
1. Schutz der natürlichen Personen . 4
2. Schutz des freien Datenverkehrs . 7
III. Grundbegriffe des Datenschutzrechts 10
1. Personenbezug 10
2. Datenverarbeitung 14
3. Verantwortlicher 15
IV. Zusammenspiel mit anderen Rechtsmaterien 17
1. Wettbewerbsrecht 19
2. Kartellrecht 21
a) Missbräuchliche Nutzung von Kundendaten 22
b) Missbräuchliche Zugangsverweigerung zu Daten 25
c) AGB-Recht 26

Rn.

3. Besonderer Geheimnisschutz . . . 30
a) Berufsrechtliche Schweigepflichten 31
b) Strafrechtliche Schweigepflichten 32
c) Fernmeldegeheimnis 34
d) Schutz von Geschäftsgeheimnissen 36
4. Arbeits- und Mitbestimmungsrecht 39
a) Umfang von Datenerhebungen im Bewerbungsgespräch 40
b) Betriebsvereinbarungen als datenschutzrechtliche Erlaubnisvorschrift 43
c) Einsicht in Personalakten. . . . 44
d) Kündigungsschutz für Datenschutzbeauftragte 46

I. Datenschutz im Anwendungsbereich des EU-Rechts

Für die Unternehmenspraxis, an die sich dieses Buch maßgeblich richtet, ist vor allem derjenige Teil des Datenschutzrechts relevant, der die Verarbeitung von Daten eben durch private Wirtschaftsunternehmen betrifft. Dieser Bereich ist durch einen grundsätzlichen **Vorrang des Europarechts** – und mit ihm sowohl des Sekundärrechts (einschließlich der DSGVO) als auch der EU-Grundrechtsverbürgungen – vor dem nationalen Recht geprägt. Die relevanten Grundlagen des Datenschutzrechts – einschließlich der jeweiligen Grundrechtsverbürgungen – ergeben sich insoweit aus dem Unionsrecht. **1**

Praxishinweis

Deshalb gelten nur für Datenverarbeitungsvorgänge außerhalb des Anwendungsbereichs des primären und sekundären Unionsrechts weiter direkt etwaige nationale Grundrechtsverbürgungen, also z. B. auch das vom BVerfG

entwickelte „Recht auf informationelle Selbstbestimmung". Im Anwendungsbereich des EU-Rechts gilt hingegen ein grundsätzlicher Vorrang der EU-Datenschutzgrundrechte.

2 Eine Einschränkung von diesen Grundsätzen gilt dort, wo das Unionsrecht Umsetzungsspielräume eröffnet – im Falle der DSGVO also bei den Öffnungsklauseln, die den Mitgliedstaaten konkretisierende Regelungen gestatten. Bei nationalen Gesetzen, die von diesen Öffnungsklauseln Gebrauch machen, können auch die nationalen Grundrechtsverbürgungen beachtenswert sein.[1]

II. Schutzgut des Datenschutzrechts

3 Das EU-Datenschutzrecht verfolgt im Wesentliche zwei Ziele: Zum einen dient es dazu, die Menschen (also im juristischen Sprachgebrauch „natürliche Personen") bei der Verarbeitung der sie betreffenden Daten zu schützen. Zum anderen soll die das Datenschutzrecht mittlerweile sehr wesentlich prägende DSGVO aber auch den freien Datenverkehr innerhalb der EU sicherstellen.[2]

1. Schutz der natürlichen Personen

4 Im Kern des Datenschutzrechts steht der **Schutz der natürlichen Personen, auf die sich die Daten beziehen**. Anders als der Begriff „Datenschutz" es nahelegt, geht es primär also nicht um den Schutz der Daten an sich, sondern um die dahinterstehende Person. Teilweise besteht hier freilich eine Wechselwirkung: So umfasst das Datenschutzrecht z. B. auch Vorgaben für die Gewährleistung der Datensicherheit,[3] weil durch eine ungewollte Veröffentlichung von Daten nicht nur deren Integrität, sondern auch die Rechte der betroffenen Person beeinträchtigt werden können.

5 Das Schutzgut ist sogar grundrechtlich verankert: namentlich in dem **Grundrecht auf Schutz personenbezogener Daten** nach **Art. 8 der EU-Grundrechte-Charta (GrCh)**.[4] Danach hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Hierauf nehmen die ErwG 1 und 2 DSGVO

1 Zu Einzelheiten dieser „konkurrierenden Mehrfachbindung" und der einschlägigen Rechtsprechung des BVerfG ausführlich: BeckOK-DS/*Schneider*, Syst. B Rn. 11.

2 Vgl. Art. 1 Abs. 1 DSGVO.

3 Zur Datensicherheit siehe Kap. 13.

4 Quasi als Vorbilder für diese Grundrechtsverbürgung gelten im Wesentlichen die Europarats-Konvention Nr. 108 und auch Art. 8 EMRK; daneben gibt es teilweise vergleichbare Grundrechtsverbürgungen in den mitgliedstaatlichen Verfassungen; vgl. *Knecht*, in: Schwarze/Becker/Hatje/Schoo, EU-Kommentar, 4. Aufl. 2019, Art. 8 GrCh Rn. 1.

unmittelbar Bezug und legen es als das Hauptziel der DSGVO fest, das Grundrecht auf Schutz personenbezogener Daten ungeachtet der Staatsangehörigkeit und des Aufenthaltsortes der betroffenen Person zu wahren.

Der **grundrechtliche Kerngehalt** des „Rechts auf Datenschutz" besteht aus drei Säulen und ergibt sich aus Art. 8 Abs. 2 GrCh. Danach dürfen diese Daten nur (1) nach Treu und Glauben, (2) für festgelegte Zwecke und (3) mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Auch das Recht jeder Person, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken, ist grundrechtlich verankert. Schließlich ist grundrechtlich die Überwachung durch eine unabhängige Stelle vorgegeben. **6**

Praxishinweis

Der EuGH legt die DSGVO regelmäßig im Lichte der GRCh einschließlich des Art. 8 GrCh aus; so hat er zuletzt in seinem Urteil vom 16.7.2020 (Rs. C-311/18) in Sachen *Schrems II*[5] Art. 45 DSGVO im Lichte der in Art. 7, 8 und 47 verbrieften Garantien der GRCh ausgelegt und konstatiert, dass die verfahrensgegenständliche Übermittlung personenbezogener Daten in einen Drittstaat regelmäßig u. a. in das Recht auf Schutz personenbezogener Daten (Art. 8 Abs. 1 GRCh) eingreife.

2. Schutz des freien Datenverkehrs

Ein weiteres Schutzgut der DSGVO besteht in der Gewährleistung eines **freien Datenverkehrs** innerhalb der EU. Nach Art. 1 Abs. 3 DSGVO darf der freie Verkehr personenbezogener Daten in der Union aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden. **7**

Die DSGVO untersagt es also Mitgliedstaaten, eigenständig nationale Maßnahmen zum Schutz personenbezogener Daten zu ergreifen und diese Beschränkung der Grundfreiheiten mit dem Bestreben nach einem höheren Schutzniveau zu rechtfertigen.[6] Ebenso ist es den Mitgliedstaaten verwehrt, das Datenschutzniveau eines anderen Mitgliedstaats als nicht ausreichend zu qualifizieren; Datenverarbeitungen in einem anderen Mitgliedstaat müssen identisch zu solchen innerhalb des eigenen Mitgliedstaates behandelt werden.[7] **8**

5 Siehe Kap. 19 Rn. 96.
6 BeckOK-DS/*Schantz*, Art. 1 DSGVO Rn. 9.
7 Paal/Pauly/*Ernst*, Art. 1 DSGVO Rn. 14.

Beispiel

Aus diesem Grund sind z. B. mitgliedstaatliche Vorschriften untersagt, die aus Gründen eines besseren Datenschutzes eine Speicherung von Daten im Inland verlangen.

9 Zulässig bleiben jedoch solche Schutzmaßnahmen der Mitgliedstaaten, die anderen Zielsetzungen als einem höheren Datenschutzstandard folgen, auch wenn sie de facto zu einer Einschränkung des freien Datenverkehrs führen.[8] Die Abgrenzung kann in Einzelfall sehr schwierig sein.[9]

III. Grundbegriffe des Datenschutzrechts

1. Personenbezug

10 Das wichtigste Merkmal zur Definition des Anwendungsbereichs – und damit auch zur Abgrenzung von anderen Rechtsmaterien – ist der „Personenbezug" der Daten. Nur wenn Daten einen solchen Personenbezug aufweisen, unterfallen sie der DSGVO und den sonstigen Datenschutzvorschriften.

11 Der für das gesamte Datenschutzrecht zentrale Begriff des „**personenbezogenen Datums**" ist in Art. 4 Nr. 1 DSGVO definiert. Demnach ist Personenbezug dann gegeben, wenn sich die jeweilige Information auf eine natürliche Person und nicht ausschließlich auf Sachen bezieht. Die Person muss durch die Information identifiziert oder zumindest identifizierbar sein.

Beispiel

In Abgrenzung zu personenbezogenen Daten haben Sachdaten keinen Personenbezug; bspw. „Das Handy ist mit einer 16 Megapixel Kamera ausgestattet." Entsprechend kann auch keine Person identifiziert werden.[10]

12 Wenn die natürliche Person nicht unmittelbar aus den Informationen des Datums identifiziert werden kann, ist ein Bezug dennoch gegeben, wenn eine entsprechende Identifizierung mit Hilfe von Verknüpfungen mit weiteren Informationen hergestellt werden kann.[11]

---

8 Mitteilung der Europäischen Kommission, Building a European Data Economy, COM(2017) 9 final, S. 5; Ehmann/Selmayr/*Zerdick*, Art. 1 DSGVO Rn. 13.

9 BeckOK-DS/*Schantz*, Art. 1 DSGVO Rn. 9.

10 Taeger/Gabel/*Arning/Rothkegel*, Art. 4 DSGVO Rn. 9.

11 Taeger/Gabel/*Arning/Rothkegel*, Art. 4 DSGVO Rn. 30.

Das Gegenstück zu personenbezogenen Daten sind **anonyme Daten**. Wann ein ausreichender „Grad an Anonymität" gegeben ist, so dass die DSGVO unanwendbar ist, ist in der Praxis häufig nicht leicht festzustellen. Grundsätzlich gilt, dass Anonymität bei Informationen vorliegt, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder bei personenbezogenen Daten, die (nachträglich) in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Anonyme Daten sind gemäß Erwägungsgrund 26 Satz 5 und 6 nicht vom Anwendungsbereich der DSGVO umfasst.[12] **13**

Praxishinweis

Denkbare Vorgehensweisen zur Anonymisierung:[13]

- Löschung von identifizierenden Merkmalen (Name, Adresse, Bankverbindung),
- Aggregation von Daten,
- Bildung von Gruppen und/oder die kontrollierte Einbringung von Zufallsfehlern.

2. Datenverarbeitung

Ein weiteres bedeutsames Merkmal zur Bestimmung des Anwendungsbereichs ist die „Datenverarbeitung" gem. Art. 4 Nr. 2 DSGVO. Die DSGVO fasst unter dem Merkmal der Datenverarbeitung eine ganze Reihe von Nutzungsvorgängen zusammen:[14] Umfasst ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie **14**

- das Erheben;
- das Erfassen;
- die Organisation;
- das Ordnen;
- die Speicherung;
- die Anpassung oder die Veränderung;
- das Auslesen;
- das Abfragen;
- die Verwendung;
- die Offenlegung durch Übermittlung;

12 Taeger/Gabel/*Arning/Rothkegel*, Art. 4 DSGVO Rn. 47.
13 Kühling/Buchner/*Klar/Kühling*, Art. 4 DSGVO Rn. 34.
14 Paal/Pauly/*Ernst*, Art. 4 DSGVO Rn. 20.

- die Verbreitung oder eine andere Form der Bereitstellung;
- der Abgleich oder die Verknüpfung;
- die Einschränkung;
- das Löschen oder die Vernichtung.

Praxishinweis

Ein automatisiertes Verfahren liegt vor, wenn bestimmte Aufgaben mit Hilfe einer informationstechnischen Infrastruktur, wie z. B. Hardware, Software oder Übertragungsnetze, unter Einbeziehung personenbezogener Daten wahrgenommen werden (bspw. über PCs, Netzwerke mit Servern, Notebooks, Smartphones oder auch den Einsatz digitaler Kamerasysteme etc.).

Weiterhin sollte darauf geachtet werden, dass das „aufbau- und ablauforganisatorische Umfeld" in seiner Gesamtheit berücksichtigt wird. Dazu zählen Speichermedien, wie Disketten, USB-Sticks, externe Festplatten und CDs, aber auch Videokameras, Kopierer, Multifunktionsgeräte sind Datenverarbeitungsanlagen. Diese spielen bei der Beurteilung eine Rolle, da dort personenbezogene Daten zwischengespeichert oder gar langfristig gespeichert werden können.[15]

Ein nicht-automatisiertes Verfahren ist bei einer manuellen Verarbeitung gegeben. Trotz manueller Verarbeitung werden von der DSGVO dennoch sog. Dateisysteme gem. Art. 4 Nr. 6 DSGVO erfasst, also z. B. Karteien. Nicht umfasst bleiben allerdings unstrukturierte Akten, Aufzeichnungen oder Notizen, wie z. B. Papierakten, in denen die Daten selbst nicht strukturiert sind.[16]

3. Verantwortlicher

15 Der zentrale Begriff zur Bestimmung des persönlichen Anwendungsbereichs der DSGVO ist derjenige des Verantwortlichen. Der Verantwortliche ist der hauptsächliche Träger der Pflichten nach der DSGVO. Der Begriff des Verantwortlichen ist in Art. 4 Nr. 7 DSGVO definiert. Verantwortlicher ist danach derjenige, der alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.[17] Dies kann eine natürliche oder juristische Person, eine Behörde, Einrichtung oder andere Stelle sein. Eine solche Verantwortlichkeit kann sich für jeden, der Daten für *sich* verarbeitet, ergeben. Letzteres unterscheidet den Verantwortlichen auch vom Auftragsverar-

15 BeckOK-DS/*Schild*, Art. 4 DSGVO Rn. 34.
16 BeckOK-DS/*Schild*, Art. 4 DSGVO Rn. 33.
17 Paal/Pauly/*Ernst*, Art. 4 DSGVO Rn. 55.

beiter,[18] der Daten nicht für sich selbst, sondern lediglich „im Auftrag" und auf Weisung eines Verantwortlichen verarbeitet.

Der Begriff des Verantwortlichen ist auch nicht auf eine einzelne Stelle limitiert. Denkbar ist gem. Art. 26 Abs. 1 Nr. 1 DSGVO eine **gemeinsame Verantwortlichkeit**.[19] Eine solche ist dann gegeben, wenn zwei oder mehrere Stellen gemeinsam über die Zwecke und Mittel der Datenverarbeitung entscheiden. Dies ist gekennzeichnet durch eine gemeinsame Kontrolle über die Datenverarbeitungsprozesse, wobei die Verantwortlichen hierbei grundsätzlich auch einen gemeinsamen Zweck verfolgen müssen.[20] Für die gemeinsame Kontrolle bedarf es keiner gleichberechtigten oder gleichmäßigen Verantwortung, vielmehr können die Verantwortlichen unterschiedlich stark und in unterschiedlicher Weise in die Datenverarbeitung eingebunden sein.[21] **16**

IV. Zusammenspiel mit anderen Rechtsmaterien

Das Datenschutzrecht fokussiert – wie gezeigt – auf den Schutz natürlicher Personen bei der Verarbeitung der auf sie bezogenen Daten. Vor allem der vorstehend erläuterte „**Personenbezug**" grenzt das Datenschutzrecht von anderen rechtlichen Vorgaben im Umgang mit Informationen (ohne Personenbezug) im Unternehmen ab. Daneben grenzt der Begriff der „**Datenverarbeitung**" das Datenschutzrecht von anderen rechtlichen Vorgaben im Hinblick auf den Umgang mit den jeweiligen Personengruppen – also im Wesentlichen Kunden und Mitarbeiter (ohne Bezug zu einer **Datenverarbeitung**) – ab. **17**

In der Unternehmensrealität müssen die **verschiedenen rechtlichen Anforderungen** aber zumeist in Deckung gebracht werden und das Datenschutzrecht bildet nur eine Facette, die bei der Umsetzung einer konkreten Maßnahme zu beachten ist. Nachfolgend soll deshalb ein grober Überblick über typische „**Schnittmengen**" mit anderen Rechtsbereichen gegeben werden, um für das Zusammenspiel mit anderen Regelungsmaterien die notwendige Sensibilität zu erzeugen: **18**

1. Wettbewerbsrecht

Eine Schnittmenge des Datenschutzrechts zum Wettbewerbsrecht besteht insbesondere im Bereich der Werbung. In Deutschland gilt es im Hinblick auf belästi- **19**

18 Zur Auftragsverarbeitung siehe Kap. 7.
19 Zur gemeinsamen Verantwortlichkeit s. Kap. 8 Rn. 3 ff.
20 BeckOK-DS/*Spoerr*, Art. 26 DSGVO.
21 BeckOK-DS/*Spoerr*, Art. 26 DSGVO; EuGH, EuZW 2018, 534, 537 Rn. 43.

gende Werbung, die lauterkeitsrechtliche Regelung des § 7 UWG zu berücksichtigen. Dabei gilt, dass gem. § 7 UWG z. B. E-Mail-Werbung nur zulässig ist, soweit eine vorherige ausdrückliche Einwilligung i. S. v. § 7 Abs. 2 Nr. 3 UWG vorliegt oder die Voraussetzungen des § 7 Abs. 3 UWG erfüllt sind. Im Verhältnis zur DSGVO ergeben sich im Hinblick auf die Voraussetzungen der Einwilligung im Direktmarketing hierbei spezielle Anforderungen.[22]

Praxishinweis

Gerade bei Werbeaktionen, wie z. B. Gewinnspielen und Newslettern etc., muss den Anforderungen beider Rechtsbereiche entsprochen werden. Bei einer Zusendung von Werbung via E-Mail handelt es sich gemäß § 7 Abs. 1, Abs. 2 Nr. 3 UWG um eine unzulässige Belästigung, es sei denn, es liegt eine vorherige ausdrückliche Einwilligung des Adressaten hierzu vor. Selbiges gilt z. B. bei Werbung mit einem Telefonanruf gegenüber einem Verbraucher, § 7 Abs. 1, Abs. 2 Nr. 2 UWG.

20 Die datenschutzrechtliche Wertung folgt dabei grundsätzlich der wettbewerbsrechtlichen Bewertung: Soweit das UWG eine (z. B. postalische) Kontaktaufnahme ohne vorherige Einwilligung explizit gestattet, wird regelmäßig auch die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO zugunsten des Verantwortlichen ausgehen. Insoweit ist zu berücksichtigen, dass die Regelung in § 7 UWG großteils der Umsetzung des Art. 13 RL 2002/58/EG dient – es sich europarechtlich also um datenschutzrechtliche Regelungen handelt, auch wenn der deutsche Gesetzgeber sich für eine Umsetzung im UWG entschieden hat.

2. Kartellrecht

21 Auch das Kartellrecht weist Schnittmengen mit dem Datenschutzrecht auf. Vor allem steht hierbei die Fragestellung des Marktmissbrauchs durch unfaire Datenverarbeitungspraktiken oder durch Verweigerung des Zugangs zu bestimmten Daten im Vordergrund.[23]

a) Missbräuchliche Nutzung von Kundendaten

22 Dies verdeutlichte das Bundeskartellamt mit seiner Facebook-Entscheidung, in der es erstmals einen sog. Konditionenmissbrauch aus einer Datenschutzverletzung ableitete.[24] Die Behörde untersagte dem sozialen Netzwerk, Nutzungsbe-

22 Auer-Reinsdorff/Conrad/*Conrad/Treeger*, § 34 Rn. 503.
23 Taeger/*Louven*, DSRITB 2019, 703, 708 f.
24 BKartA, BeckRS 2019, 4895.

dingungen zu verwenden, die ohne Einwilligung der Nutzer eine Zusammenführung von Nutzerdaten über verschiedene Produkte und Drittangebote hinweg beinhalteten.

Nach Auffassung des Bundeskartellamts verstieß Facebook als marktbeherrschendes Unternehmen für soziale Netzwerke für private Nutzer in Deutschland dadurch gegen das kartellrechtliche Verbot des Missbrauchs einer marktbeherrschenden Stellung gem. § 19 Abs. 1 GWB, dass die Registrierung von einer Einwilligung in Nutzungskonditionen abhängig gemacht wurde, die mit datenschutzrechtlichen Anforderungen unvereinbar sei. Infolgedessen sei die Einwilligung nicht wirksam und entsprechende Datenverarbeitungen unzulässig. **23**

Die aufschiebende Wirkung der Verfügung ist zwar vom OLG Düsseldorf mit Entscheidung vom 26.8.2019 im Eilverfahren wieder hergestellt worden, so dass das Unternehmen bis zum Abschluss des Beschwerdeverfahrens die Untersagungsverfügung nicht umsetzen muss.[25] Dies begründete das OLG Düsseldorf damit, dass Facebook zwar womöglich marktbeherrschend sei, aber die Datenverarbeitung keinen relevanten Wettbewerbsschaden bewirke.[26] Weiterhin sei der erforderliche Kausalzusammenhang zwischen Nutzungsbedingungen und Marktstellung nicht hinreichend nachgewiesen worden.[27] Mit anderen Worten: Selbst wenn die beanstandete Datenverarbeitung gegen Datenschutzbestimmungen verstößt, liege darin nicht zugleich ein Verstoß gegen das Kartellrecht. Diese Entscheidung wird im Schrifttum kritisiert[28]; das letzte Wort ist hier also noch nicht gesprochen. **24**

b) Missbräuchliche Zugangsverweigerung zu Daten

Auch unter dem Aspekt der missbräuchlichen Verweigerung des Zugangs zu bestimmten (ggf. auch personenbezogenen) Daten besteht ein Berührungspunkt zum Kartellrecht. Hierzu gibt es jedoch erst wenige Entscheidungen; ein praxisrelevantes Beispiel bildet der Zugang unabhängiger Marktteilnehmer auf dem Kfz-Teilemarkt zu bestimmten bei Fahrzeugherstellern vorhandenen Daten einschließlich der Fahrzeugidentifikationsnummer.[29] **25**

25 OLG Düsseldorf, Beschl. v. 26.8.2019 – VI-Kart 1/19 (V), MMR 2019 Rn. 742.
26 OLG Düsseldorf, Beschl. v. 26.8.2019 – VI-Kart 1/19 (V), MMR 2019 Rn. 18.
27 OLG Düsseldorf, Beschl. v. 26.8.2019 – VI-Kart 1/19 (V), MMR 2019 Rn. 45.
28 Vgl. *Bunte*, EWiR 2019, 575.
29 OLG Frankfurt, GRUR-RR 2017, 231.

Praxishinweis

Beide Entscheidungen sind für die Praxis von höchster Relevanz: Die Entscheidungen des Bundeskartellamts und des OLG Düsseldorf offenbaren, wie kartellrechtliche Wertungen durch die DSGVO (insbesondere über die Auslegung von Erlaubnistatbeständen der DSGVO) beeinflusst werden können.

c) AGB-Recht

26 Auch das AGB-Recht hat starke Bezüge zum Datenschutzrecht. Dies ist dem Umstand geschuldet, dass die Verarbeitung personenbezogener Daten durch Unternehmen in vielen Fällen im Zusammenhang mit privatrechtlichen Vertragsverhältnissen erfolgt, z. B. mit Kunden oder Mitarbeitern. Besonders beachtenswert ist hierbei, dass vor allem „datenschutzrechtliche" Vereinbarungen, allen voran vorformulierte Einwilligungserklärungen, im Regelfall einer AGB-Kontrolle i. S. d. §§ 305 ff. BGB unterliegen.[30]

27 In der Praxis ist festzustellen, dass viele Unternehmen sich auch unnötig durch eine falsche Gestaltung eine vermeidbare AGB-Kontrolle einfangen; das gilt vor allem für **Datenschutzerklärungen** nach Art. 13 und 14 DSGVO. Dienen Datenschutzerklärungen ausschließlich der gesetzlich verlangten Informationserteilung, können sie einer AGB-Kontrolle nicht unterzogen werden.[31] Soweit eine Datenverarbeitung jedoch Entgeltcharakter aufweist oder eine Datenschutzerklärung zusätzliche Pflichten der betroffenen Person begründen soll, schließt dies einen rein informativen Inhalt der Datenschutzerklärung aus und sie kann als Vertragsbestimmung i. S. d. § 305 Abs. 1 S. 1 BGB qualifiziert werden, die wiederum in vollem Umfang einer AGB-Kontrolle unterliegt.[32] Schädlich kann in diesem Zusammenhang insbesondere eine zu starke Verzahnung der Datenschutzerklärung mit den Nutzungsbedingungen sein. In diesem Sinne hat das LG Berlin entschieden, dass eine „Privacy Policy" der AGB-Kontrolle unterliegt, wenn diese nach ihrem objektivem Wortlaut bei dem Empfänger den Eindruck hervorruft, mit ihr solle der Inhalt eines vertraglichen oder Rechtsverhältnisses bestimmt werden.[33]

30 So für Einwilligungserklärungen: Forgó/Helfrich/Schneider/*Ehmann*, Teil IX Kap. 1 Rn. 27 unter Verweis u. a. auf BGH, Urt. v. 1.2.2018, GRUR 2018, 545.

31 OLG Hamburg, GRUR-RR 2015, 361 Rn. 48 ff.

32 *Wendehorst/Graf von Westphalen*, NJW 2016, 3745, 3750.

33 LG Berlin, Urt. v. 16.1.2018, MMR 2018, 328, 330.

Praxishinweis

Es sollte deshalb dringend vermieden werden, von dem Nutzer zu verlangen, dass er sich „mit den Datenschutzhinweisen einverstanden erklärt".

Gegenstand der AGB-Kontrolle können auch vom Unternehmen vorformulierte Leistungsbeschreibungen sein, die eine Datenverarbeitung überhaupt erst zur Erfüllung des Vertrags erforderlich machen.[34] **28**

Praxishinweis

Ein in der Praxis ebenfalls sehr häufig anzutreffender Fehler besteht darin, den Nutzer auf der Grundlage eines allgemein vorformulierten Hinweises bestätigen zu lassen, dass er die **Datenschutzerklärung gelesen** oder zur Kenntnis genommen habe. Bereits eine solche Klausel ist i. S. d. § 309 Nr. 12b BGB als formularmäßig erteilte Tatsachenbestätigung unwirksam.[35]

Soweit eine Klausel der AGB-Kontrolle nicht standhält, können Unternehmen in vertragsrechtlicher Hinsicht nicht auf sie zurückgreifen. Dann könnte es passieren, dass Datenverarbeitungen ohne die notwendige Rechtsgrundlage stattfinden. Die Verwendung unwirksamer AGB kann zudem zu empfindlichen Folgen im Hinblick auf das UKlaG und UWG führen und eine Schadensersatzhaftung aus culpa in contrahendo nach sich ziehen.[36] **29**

3. Besonderer Geheimnisschutz

In manchen Fällen werden personenbezogene Daten nicht nur durch die DSGVO und die bereichsspezifischen Datenschutzgesetze geschützt, sondern zusätzlich durch besondere gesetzliche **Geheimhaltungs- und Verschwiegenheitspflichten**. **30**

a) Berufsrechtliche Schweigepflichten

So unterliegen z. B. Geheimnisse, die einem Arzt, Apotheker, Rechtsanwalt, Notar, Steuerberater oder Wirtschaftsprüfer in dessen jeweiliger Funktion anvertraut worden sind, einer gesetzlichen Schweigepflicht, die auch über den Tod der betroffenen Person hinaus gilt. Diese Pflicht bestimmter Berufsträger zur Verschwiegenheit ergibt sich primär aus den jeweils für sie geltenden berufsrechtlichen Vorschriften, also z. B. der Berufsordnung für Ärzte (vgl. § 9 MBO-Ä), **31**

34 LG Berlin, Urt. v. 16.1.2018, MMR 2018, 328, 330.
35 So ausdrücklich LG Berlin, Urt. v. 16.1.2018, MMR 2018, 328, 331.
36 *Wendehorst/Graf von Westphalen*, NJW 2016, 3745, 3750.

für Rechtsanwälte aus § 43a Abs. 2 BRAO und § 2 BORA, für Notare aus § 18 BNotO, für Steuerberater aus § 57 Abs. 1 StBerG und für Wirtschaftsprüfer aus § 43 Abs. 1 S. 1 WiPrO. Solche Geheimnisse werden oftmals auch personenbezogene Daten umfassen; also z. B. soweit sie sich auf eine natürliche Person als Patient oder Mandant beziehen.

b) Strafrechtliche Schweigepflichten

32 Daneben und grundsätzlich unabhängig von den berufsrechtlichen Pflichten folgt eine gesetzliche Schweigepflicht – wiederum für Angehörige bestimmter Berufe – auch aus dem Strafrecht, und zwar aus § 203 StGB. Neben den oben genannten Berufsgruppen unterfallen dieser Klausel zusätzlich z. B. auch Angehörige von privaten Unfall-, Kranken- und Lebensversicherungen sowie die jeweils für sie **berufsmäßig tätigen Gehilfen** (z. B. Sprechstundenhilfen, Referendare etc.).

Praxishinweis

Im hiesigen Kontext besonders wichtig ist auch die Erstreckung der Geheimhaltungspflicht auf die jeweils bei den Verpflichteten bestellten (betrieblichen) Datenschutzbeauftragten: Nach § 203 Abs. 4 S. 1 StGB macht sich der **Datenschutzbeauftragte** einer Stelle, die dem Geheimhaltungsregime unterfällt, selbst strafbar, wenn er ein ihm in seiner Eigenschaft bekannt gewordenes Geheimnis offenbart.

33 In der Praxis wirkt sich die Überschneidung von Datenschutzrecht und gesetzlichen Schweigepflichten oft aus, wenn nach beiden Rechtsmaterien geschützte Informationen einem Dritten bekannt gegeben werden sollen, ohne dass eine gesetzliche Vorschrift dies anordnen oder gestatten würde. Wird hier datenschutzrechtlich also auf das Instrument einer **Einwilligung** gesetzt, ist die Erklärung parallel als eine wirksame **Befreiung von der Schweigepflicht** auszugestalten.[37]

c) Fernmeldegeheimnis

34 Eine auch in der Unternehmenspraxis relevante Berührung gibt es ferner zum **Fernmeldegeheimnis** nach § 88 TKG. Nach § 88 Abs. 2 S. 1 TKG ist jeder Diensteanbieter zur Wahrung des Fernmeldegeheimnisses verpflichtet. Diensteanbieter ist nach § 3 Nr. 6 TKG jeder, „der ganz oder teilweise geschäftsmäßig a) Telekommunikationsdienste erbringt oder b) an der Erbringung solcher Dienste“

37 Siehe hierzu das Muster von *Arning*, in: Moos, Datenschutz- und Datennutzungsverträge, 2. Aufl. 2018, § 41.

mitwirkt. Telekommunikationsdienste sind nach § 3 Nr. 24 TKG „in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen".

Vor allem die Datenschutzaufsichtsbehörden sehen Arbeitnehmer als solche „Dritte" im Sinne dieser Regelung an, wenn ihnen vom Arbeitgeber die **Privatnutzung** dienstlicher Telekommunikationsdienste wie z. B. der beruflichen **E-Mail** beziehungsweise des **Internetzugang** erlaubt werde.[38] Die juristische Literatur beurteilt dies zwar wohl überwiegend anders[39] und auch die Rechtsprechung hat sich bisher gegen eine Geltung des Fernmeldegeheimnisses in diesen Konstellationen ausgesprochen;[40] es bleibt aber eine gewisse Rechtsunklarheit. **35**

d) Schutz von Geschäftsgeheimnissen

Schließlich können sich datenschutzrechtliche Vorgaben überschneiden mit den Regelungen zum Schutz von **Geschäftsgeheimnissen**. Insoweit ist zunächst zu beachten, dass am 26.4.2019 das neue Geschäftsgeheimnisgesetz (GeschGehG) in Kraft getreten ist, welches die EU-Geschäftsgeheimnisrichtlinie[41] (verspätet) umgesetzt hat. **36**

Geschäftsgeheimnisse sind Informationen, die nicht allgemein bekannt oder ohne Weiteres zugänglich, von wirtschaftlichem Wert und Gegenstand von angemessenen Geheimhaltungsmaßnahmen durch den Geheimnisinhaber sind (§ 2 Nr. 1 GeschGehG). Dabei kann es sich, muss es sich aber nicht um personenbezogene Informationen handeln. Geschäftsgeheimnisse können neben (zumeist anonymen) Geschäftsstrategien, Businessplänen oder Marktanalysen z. B. auch Sammlungen von Kunden- oder Lieferantendaten, Informationen über Personalangelegenheiten oder auch bestimmte Erfindungen sein. **37**

Besonders zu bedenken ist, dass nach dem GeschGehG Informationen nur geschützt sind, wenn sie geheim, von wirtschaftlichem Wert und zudem durch angemessene Maßnahmen geschützt sind. **38**

---

38 Siehe hierzu Kap. 15 Rn. 79.

39 *Wybitul*, NJW 2014, 3605, 3609; *Fülbier/Splittgerber*, NJW 2012, 1995, 1999; Plath/*Stamer/Kuhnke*, § 32 BDSG Rn. 98 ff.; Weth/Herberger/Wächter/*Baumgartner*, S. 363, 380; mit weiterführender Argumentation *Thüsing*, § 3 Rn. 75 ff.

40 LAG Niedersachsen, Urt. v. 31.5.2010 – 12 Sa 875/09, MMR 2010, 639; LAG Berlin-Brandenburg, Urt. v. 16.2.2011 – 4 Sa 2132/10, NZA-RR 2011, 342, 343 f.; VG Karlsruhe, Urt. v. 27.5.2013 – 2 K 3249/12, NVwZ-RR 2013, 797, 801.

41 Richtlinie (EU) 2016/943 vom 8.6.2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl. EG Nr. L 157 vom 15.6.2016, S. 1.

Praxishinweis

Bei letztgenannter Voraussetzung ergibt sich in der Praxis eine relevante Überlappung mit datenschutzrechtlichen Anforderungen: Die **angemessenen Maßnahmen zur Geheimhaltung**, die nach GeschGehG erforderlich sind, müssen im Fall von personenbezogenen Daten zugleich als angemessene **technische oder organisatorische Maßnahme** im Sinne von Art. 32 DSGVO qualifiziert werden können, damit die Schutzmaßnahmen auch den datenschutzrechtlichen Anforderungen genügen.

4. Arbeits- und Mitbestimmungsrecht

39 Zu dem Arbeits- und Mitbestimmungsrecht weist das Datenschutzrecht eine besondere Nähe auf. In der Praxis kommt es vor allem bei der Verarbeitung von Beschäftigtendaten sehr häufig vor, dass Anforderungen aus beiden Rechtsgebieten zu berücksichtigen sind. Die in der Praxis bedeutsamsten Schnittmengen werden nachfolgend kurz aufgezeigt.[42]

a) Umfang von Datenerhebungen im Bewerbungsgespräch

40 Datenschutzrechtlich gilt, dass personenbezogene Daten eines Bewerbers nur dann erhoben werden dürfen, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist (§ 26 Abs. 1 S. 1 Alt. 1). Zum Umfang der hierbei zugelassenen Datenerhebungen hat sich bereits vor der DSGVO und außerhalb des Regelungsbereichs des BDSG auf Basis zivilrechtlicher Vorschriften eine ausdifferenzierte Rechtsprechung zum sog. **Fragerecht des Arbeitsgebers** herausgebildet, die hier wertungsmäßig mit zu berücksichtigen ist.

41 Hiernach ist das Recht des Arbeitgebers, einem Bewerber Fragen zu stellen, auf Fragen beschränkt, an deren Beantwortung der Arbeitgeber ein berechtigtes, billigenswertes und schutzwürdiges Interesse hat, das so stark ist, dass das Interesse des Arbeitnehmers dahinter zurücktritt. Grundsätzlich sind hierbei nur solche Fragen zulässig, die in einem sachlichen Zusammenhang mit den Pflichten des Arbeitnehmers aus dem Arbeitsverhältnis stehen.[43]

42 Siehe hierzu im Detail Kap. 15.

43 Kühling/Buchner/*Maschmann*, § 26 BDSG Rn. 29 m. w. N.

Beispiel

Der Arbeitgeber darf keine Fragen stellen, bei denen es um Risiken geht, die die Rechtsordnung ausdrücklich ihm zuweist, beispielsweise die Frage nach der **Schwangerschaft** einer Bewerberin.[44]

Darf der Arbeitgeber nach diesen Grundsätzen eine bestimmte Frage nicht stellen, ist ihm datenschutzrechtlich auch die Erhebung der als Antwort mitgeteilten personenbezogenen Daten untersagt. **42**

b) Betriebsvereinbarungen als datenschutzrechtliche Erlaubnisvorschrift

Betriebsvereinbarungen können eine Doppelfunktion haben. Betriebsverfassungsrechtlich übt die Arbeitnehmervertretung darüber ihr Recht auf Mitbestimmung in betrieblichen Angelegenheiten aus. Daneben kann ihnen auch eine bedeutsame datenschutzrechtliche Funktion zukommen: Gemäß § 26 Abs. 1 S. 1 BDSG kann die Verarbeitung von Beschäftigtendaten u. a. auch gerechtfertigt sein, wenn sie zur Ausübung oder Erfüllung der sich aus einer Kollektivvereinbarung (d. h. einem Tarifvertrag oder einer Betriebs- oder Dienstvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. **43**

Praxishinweis

In der Praxis ist deshalb bei der Gestaltung und Verhandlung einer Betriebsvereinbarung darauf zu achten, ob und, wenn ja, welche datenschutzrechtliche Legitimationswirkung ihr zukommen soll. Macht eine Betriebsvereinbarung eine bestimmte Datenverarbeitung erforderlich, so wird sie über § 26 Abs. 1 S. 1 BDSG erlaubt. Es können in solche Betriebsvereinbarungen aber auch weitergehende, datenschutzrechtliche Erlaubnistatbestände integriert werden.[45]

c) Einsicht in Personalakten

Datenschutzrechtlich besitzen auch Beschäftigte nach Art. 15 DSGVO ein Recht auf Auskunft über die zu ihrer Person durch den Arbeitgeber gespeicherten personenbezogenen Daten. **44**

Parallel hat ein Arbeitnehmer nach § 83 Abs. 1 S. 1 BetrVG im bestehenden Arbeitsverhältnis das Recht, in die über ihn geführten Personalakten Einsicht zu **45**

44 Kühling/Buchner/*Maschmann*, § 26 BDSG Rn. 29.
45 BeckOK-DS/*Riesenhuber*, 34. Ed. 1.11.2020, § 26 BDSG Rn. 52.

nehmen. Dieser Anspruch ist sehr breit angelegt und überschneidet sich inhaltlich mit dem datenschutzrechtlichen Auskunftsanspruch. So wird unter „Personalakte" nach herrschender Meinung jede Sammlung von Unterlagen verstanden, die mit dem Arbeitnehmer in einem inneren Zusammenhang steht, und zwar unabhängig von Form, Material, Stelle und Ort, an dem sie geführt wird.[46]

Praxishinweis

Diese Parallelität ist wichtig zu beachten, weil dem Arbeitnehmer unter Umständen auf Basis einer etwa parallel zu einem Auskunftsanspruch geltend gemachten Personalakteneinsicht mehr Informationen herauszugeben sind. So ist das Recht auf Erhalt einer Kopie gemäß Art. 15 Abs. 4 DSGVO beschränkt durch die Rechte und Freiheiten anderer Personen[47]. Das Einsichtsrecht des Arbeitnehmers in seine Personalakte nach § 83 Abs. 1 S. 1 BetrVG ist gesetzlich hingegen nicht in gleicher Weise eingeschränkt. Das Einsichtsrecht des Arbeitnehmers besteht bezüglich aller Aufzeichnungen, die sich mit seiner Person und dem Inhalt der Entwicklung seines Arbeitsverhältnisses befassen und kann deshalb auch Informationen über andere Personen umfassen, soweit diese Daten in der Personalakte gespeichert sind, z. B. Hinweise anderer Mitarbeiter auf ein etwaiges Fehlverhalten des Arbeitnehmers.[48]

d) Kündigungsschutz für Datenschutzbeauftragte

46 Ein weiterer praxisrelevanter Anknüpfungspunkt zum Arbeitsrecht ergibt sich aus § 38 Abs. 2 BDSG i.V.m. § 6 Abs. 4 S. 2 und 3 BDSG. Danach gilt für den betrieblichen Datenschutzbeauftragten ein besonderer **Kündigungsschutz**: Die Kündigung des Arbeitsverhältnisses des Datenschutzbeauftragten ist hiernach unzulässig, es sei denn, dass Tatsachen vorliegen, welche eine Kündigung aus wichtigem Grund zulassen würden. Dieser Sonderkündigungsschutz besteht noch ein Jahr nach dem Ende der Tätigkeit als Datenschutzbeauftragter fort.

47 Diese Regelung ist auch europarechtlich wirksam; insbesondere bedarf es hierfür keiner Öffnungsklausel in der DSGVO, weil es sich im Kern nicht um eine datenschutzrechtliche, sondern eine arbeitsrechtliche Regelung handelt.[49]

46 BAG, Urt. v. 7.5.1980 – 4 AZR 214/78, BeckRS 1980, 30706869 Rn. 11.
47 Gola/*Franck*, Art. 15 DSGVO Rn. 33.
48 LAG Baden-Württemberg, Urt. v. 20.12.2018 – 17 Sa 11/18, NZA-RR 2019, 242, 249.
49 So LAG Nürnberg, Urt. v. 19.2.2020 – 2 Sa 274/19, NZA-RR 2020, 299, 301.

Kapitel 3

Anwendungsbereich des Datenschutzrechts

Übersicht

Rn.

I. Überblick über die einschlägigen Regelungen der DSGVO 2
II. Sachlicher Anwendungsbereich . . . 12
1. Verarbeitung personenbezogener Daten, Art. 2 Abs. 1 DSGVO . . . 12
2. Ausnahmetatbestände, Art. 2 Abs. 2 bis 4 DSGVO. 18
III. Räumlicher Anwendungsbereich, Art. 3 DSGVO 34
1. Niederlassungsprinzip, Art. 3 Abs. 1 DSGVO 36
a) Verarbeitung im Rahmen der Tätigkeiten der Niederlassung eines Verantwortlichen. 38
b) Verarbeitung im Rahmen der Tätigkeiten der Niederlassung eines Auftragsverarbeiters . . . 44

Rn.

2. Marktortprinzip, Art. 3 Abs. 2 DSGVO. 49
a) Anbieten von Waren oder Dienstleistungen, Art. 3 Abs. 2 lit. a DSGVO. 52
b) Verhaltensbeobachtung, Art. 3 Abs. 2 lit. b DSGVO . . 64
c) Betroffene Person in der EU 72
3. Räumlicher Anwendungsbereich bei mehreren Beteiligten 77
4. Räumliche Reichweite der Betroffenenrechte 81
5. Geltung der DSGVO im EWR . . 82
IV. Anwendungsbereich mitgliedstaatlicher Regelungen 83
V. Anwendungsbereich sonstiger ausfüllender Normen 100

Die Vorschriften der DSGVO sind nur dann zu beachten, wenn ihr Anwendungsbereich eröffnet ist. Von der Eröffnung des Anwendungsbereichs hängt zudem ab, ob die Aufsichtsbehörde für den Datenschutz sachlich nach Art. 55 Abs. 1, 51 Abs. 1 DSGVO zuständig ist.[1] **1**

I. Überblick über die einschlägigen Regelungen der DSGVO

Art. 99 bestimmt den zeitlichen Anwendungsbereich der DSGVO. Art. 2 und 3 DSGVO enthalten die zentralen Vorschriften, welche den sachlichen und den räumlichen Anwendungsbereich der Verordnung festlegen. **2**

Nach Art. 2 Abs. 1 DSGVO ist vom **sachlichen Anwendungsbereich** der Verordnung die ganz oder teilweise automatisierte Verarbeitung von personenbezogenen Daten, aber auch die nichtautomatisierte Verarbeitung von Daten erfasst, sofern letztere in einem Dateisystem gespeichert sind oder werden sollen. Art. 2 **3**

1 Vgl. hierzu Kap. 15 Rn. 5 ff.

Abs. 2 DSGVO enthält einige Ausnahmen, bei denen die Verordnung keine Anwendung findet.

4 Eine spezifische Regelung zum **persönlichen Anwendungsbereich** findet sich in der Verordnung nicht. Allerdings sieht die Regelung über den räumlichen Anwendungsbereich in Art. 3 DSGVO vor, dass die Verordnung nur für Verarbeitungen durch Verantwortliche oder durch Auftragsverarbeiter gilt, wofür im Übrigen auch natürliche Personen in Betracht kommen.

5 Nach Art. 3 Abs. 1 DSGVO ist der **räumliche Anwendungsbereich** für Datenverarbeitungen eröffnet, die im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgen.[2] Hat ein Verantwortlicher oder ein Auftragsverarbeiter keine Niederlassung in einem Mitgliedstaat, gilt die DSGVO gemäß Art. 3 Abs. 2, wenn dieser Daten von Personen verarbeitet, die sich in der Union befinden und die Datenverarbeitung im Zusammenhang mit dem Anbieten von Waren oder Dienstleistungen an solche Personen erfolgt oder das Verhalten solcher Personen in einem Mitgliedstaat beobachtet wird.

6 Eine Rechtswahl im Rahmen eines Vertrages, mit der die Anwendung der DSGVO abbedungen werden soll, dürfte unwirksam sein, da es sich bei datenschutzrechtlichen Vorschriften um Eingriffsnormen i. S. v. Art. 9 Abs. 1 Rom I-VO handelt, bei denen eine Rechtswahl unzulässig ist.[3]

Praxishinweis

Zu beachten ist, dass der Anwendungsbereich jeweils für einen bestimmten Datenverarbeitungsvorgang, durchgeführt durch eine bestimmte datenverarbeitende Stelle, eröffnet ist.[4] Es ist daher denkbar, dass dieselbe Stelle dieselben personenbezogenen Daten sowohl innerhalb als auch außerhalb des Anwendungsbereichs der Verordnung verarbeitet.[5]

7 Die Verordnung eröffnet den Mitgliedstaaten an vielen Stellen die Möglichkeit, die Vorschriften der Verordnung durch eigene datenschutzrechtliche Vorschriften zu präzisieren oder einzuschränken.

---

2 Das Gebiet der Union bestimmt sich nach Art. 52 EUV und Art. 355 AEUV.

3 Simitis/Hornung/Spiecker gen. Döhmann/*Hornung*, Art. 3 DSGVO Rn. 70; Kühling/Buchner/*Klar*, Art. 3 DSGVO Rn. 105.

4 Vgl. in Bezug auf den räumlichen Anwendungsbereich auch BeckOK-DS/*Hanloser*, Art. 3 DSGVO Rn. 10; Gola/*Piltz*, Art. 3 DSGVO Rn. 18. Art. 2 Abs. 1 „gilt für die … Verarbeitung"; Art. 3 Abs. 2 „… findet Anwendung auf die Verarbeitung … durch einen Verantwortlichen …".

5 Gola/*Piltz*, Art. 3 DSGVO Rn. 18.

Soweit sich eine Datenverarbeitung im Rahmen dieser Öffnungsklauseln bewegt, ist daher noch zu prüfen, welches mitgliedstaatliche Recht zur Ausfüllung zur Anwendung kommt. Die Verordnung selber macht hierzu keine Vorgaben.[6] Es bleibt daher den Mitgliedstaaten überlassen, den Anwendungsbereich der nationalen Regelung zu bestimmen. **8**

[Rn. 9–11 entfallen]

II. Sachlicher Anwendungsbereich

1. Verarbeitung personenbezogener Daten, Art. 2 Abs. 1 DSGVO

Nicht jede Verarbeitung personenbezogener Daten eröffnet den sachlichen Anwendungsbereich der Verordnung. So ist zum Beispiel die Verarbeitung personenbezogener Daten durch die betroffene Person selbst schon nicht vom Schutzzweck der DSGVO umfasst.[7] **12**

Zudem muss es sich laut Art. 2 Abs. 1 DSGVO entweder um eine ganz oder teilweise automatisierte Verarbeitung handeln oder um eine nichtautomatisierte Verarbeitung, bei der die Daten in einem Dateisystem gespeichert werden oder werden sollen. **13**

Der Begriff „automatisiert" wird in der DSGVO nicht näher definiert. Erwägungsgrund 15 DSGVO stellt dem Begriff der automatisierten Verarbeitung den Begriff der „manuellen" Verarbeitung gegenüber und verdeutlicht damit zugleich, dass „manuell" gleichbedeutend ist mit „nichtautomatisiert". **14**

Letztlich gibt es bei dem Begriff „**automatisiert**" in der Praxis keine Schwierigkeiten in der Handhabung. Sofern es sich um elektronische Datenverarbeitung handelt, handelt es sich grundsätzlich auch um automatisierte Datenverarbeitung. Dem Wortlaut des Art. 2 Abs. 1 DSGVO ist wohl auch zu entnehmen, dass das Vorliegen einer nur **teilweise automatisierten Verarbeitung** dazu führt, dass das Datenschutzrecht auch auf die nichtautomatisierten Bestandteile dieser Verarbeitung Anwendung finden kann. Unter Heranziehung der Legaldefinition des Verarbeitungsbegriffs in Art. 4 Nr. 2 DSGVO bedeutet dies, dass sowohl die automatisierten als auch die nichtautomatisierten Bestandteile eines **Vorgangs** beziehungsweise einer **Vorgangsreihe** in ihrer Gesamtheit im sachlichen Anwendungsbereich des Datenschutzrechts liegen können.[8] Und zwar selbst dann, wenn der manuelle Bestandteil des Vorgangs für sich genommen nicht die Vo- **15**

6 Lediglich in Erwägungsgrund 153 S. 6 gibt der Unionsgesetzgeber eine Art kollisionsrechtliche Empfehlung.

7 Simitis/Hornung/Spiecker gen. Döhmann/*Roßnagel*, Art. 2 DSGVO Rn. 18.

8 Vgl. Gola/*Gola*, Art. 2 DSGVO Rn. 5.

raussetzungen für die Eröffnung des sachlichen Anwendungsbereichs für nichtautomatisierte Verarbeitungen erfüllen würde.

Beispiel

Die manuelle Erhebung von Daten im Rahmen einer Kundenbefragung oder Umfrage ist als Bestandteil einer teilweise automatisierten Verarbeitung vom sachlichen Anwendungsbereich umfasst, wenn die Daten anschließend elektronisch weiterverarbeitet werden, da die Erhebung zur gleichen Vorgangsreihe zu zählen ist.

16 Im Gegensatz zur automatisierten Verarbeitung liegt die **nichtautomatisierte** bzw. **manuelle** Verarbeitung personenbezogener Daten nur dann im sachlichen Anwendungsbereich der Verordnung, wenn die Daten in einem **Dateisystem** gespeichert werden bzw. gespeichert werden sollen. Das Ziel der Speicherung in einem Dateisystem muss dabei hinreichend konkret sein (Englisch: „intended"). Die bloße Möglichkeit oder Wahrscheinlichkeit einer solchen Speicherung reicht nicht.[9]

17 Der Begriff des „Dateisystems" ist in Art. 4 Nr. 6 DSGVO legaldefiniert als *„jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob die Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird*".[10] Die konkreten Ordnungskriterien sind unerheblich. Es reicht, dass die Daten so strukturiert sind, dass sie in der Praxis zur späteren, dem Erhebungszweck entsprechenden Verwendung leicht wiederauffindbar sind.[11] In Erwägungsgrund 15 wird demgegenüber erwähnt, dass **Akten, Aktensammlungen und ihre Deckblätter**, die nicht nach bestimmten Kriterien geordnet sind, nicht in den Anwendungsbereich der Verordnung fallen.

Beispiel

Auch personenbezogene Daten auf **Papier** können somit im sachlichen Anwendungsbereich der Verordnung liegen, sofern sie entweder Bestandteil

9 Plath/*Plath*, Art. 2 DSGVO Rn. 15; aA Paal/Pauly/*Ernst*, Art. 2 Rn. 10; Simitis/Hornung/Spiecker gen. Döhmann/*Roßnagel*, Art. 2 Rn. 16.

10 Der Begriff des „Dateisystems" ist augenscheinlich die einzige Neuerung im Vergleich zu der ansonsten wortgleichen Vorgängerregelung in Art. 3 Abs. 1 DSRL, in der der Begriff „Datei" verwendet wurde. Dieser Änderung ist jedoch keine weitere Bedeutung beizumessen. Dies zeigt ein Vergleich z. B. mit den englischen Sprachfassungen der Richtlinie und der Verordnung, in denen jeweils der Begriff „filing system" verwendet wird.

11 EuGH, Urt. v. 10.7.2018 – C-25/17, ZD 2018, 469, 471, Rn. 60–62.

einer teilweise automatisierten Datenverarbeitung sind oder wenn sie Bestandteil einer strukturierten Sammlung von Daten in Papierform sind (z. B. in **Personal- und Krankenakten** oder **Kundenlisten)**. Der Umgang mit einem einzelnen Ausdruck eines **Datenbankauszugs oder handschriftlichen Notizen aus einer Datenbank** wird dagegen häufig außerhalb des sachlichen Anwendungsbereichs liegen, da diese in der Regel weder Bestandteil des Datenverarbeitungsvorgangs sind, zu dem die Datenbank gehört, noch Bestandteil einer strukturierten Sammlung von Daten in Papierform. Es gibt insofern keine über den Datenverarbeitungsvorgang hinausgehende Fortwirkung der Anwendbarkeit des Datenschutzrechts.[12] Werden mehrere solcher Ausdrucke oder Notizen zusammen strukturiert abgelegt, kann jedoch eine strukturierte Sammlung und damit ein Dateisystem entstehen, welches dann wieder in den sachlichen Anwendungsbereich der Verordnung fiele.

2. Ausnahmetatbestände, Art. 2 Abs. 2 bis 4 DSGVO

Gemäß Art. 2 Abs. 3 DSGVO gilt die Verordnung nicht für die Verarbeitung personenbezogener Daten durch die **Organe, Einrichtungen, Ämter und Agenturen der Union**. Stattdessen gilt gemäß Art. 2 Abs. 3 DSGVO die Verordnung (EG) Nr. 45/2001. Zudem lässt die Verordnung gemäß Art. 2 Abs. 4 DSGVO die Anwendung der sog. **E-Commerce-Richtlinie** 2000/31/EG unberührt. Da Art. 1 Abs. 5 lit. b E-Commerce-Richtlinie in Bezug auf Fragen des Datenschutzes auf die DSRL verweist, was gemäß Art. 94 Abs. 2 DSGVO als Verweis auf die DSGVO zu lesen ist, sind die E-Commerce-Richtlinie und die DSGVO für Dienste der Informationsgesellschaft nebeneinander anwendbar.[13] Dieses Nebeneinander kann in der Praxis insbesondere dann zu Wertungswidersprüchen führen, wenn sich bezüglich eines Datenverarbeitungsvorgangs die datenschutzrechtlichen Pflichten und die Haftungsprivilegierungen aus Art. 12 ff. E-Commerce-Richtlinie überlagern. Ob die Haftungsprivilegierungen auch für datenschutzrechtliche Pflichten gelten, ist umstritten.[14] **18**

12 Plath/*Plath*, Art. 2 DSGVO Rn. 11. Es existiert in der DSGVO keine dem § 27 Abs. 2 BDSG a. F. entsprechende Regelung, welche den Anwendungsbereich des Datenschutzrechts noch auf personenbezogene Daten erstreckte, die offensichtlich aus einer automatisierten Verarbeitung entnommen worden sind.

13 BeckOK-DS/*Bäcker*, Art. DSGVO 2 Rn. 33; Ehmann/Selmayr/*Zerdick*, Art. 3 DSGVO Rn. 17; anders Plath/*Plath*, Art. 2 DSGVO Rn. 31, der von einer Ausnahme von der Anwendbarkeit der Verordnung auszugehen scheint.

14 Vgl. BeckOK-DS/*Bäcker* Art. 2 DSGVO Rn. 33; Ehmann/Selmayr/*Zerdick*, Art. 3 DSGVO Rn. 17; Plath/*Plath*, Art. 2 DSGVO Rn. 31; Sydow/*Ennöckl*, Art. 2 DSGVO Rn. 17.

19 Die ePrivacy-Richtlinie 2002/58/EG hat als lex specialis gemäß Art. 95 DSGVO Vorrang gegenüber der DSGVO, soweit in der Richtlinie Pflichten festgelegt sind, die dasselbe Ziel verfolgen.

20 Zudem findet die Verordnung trotz Eröffnung des sachlichen Anwendungsbereichs keine Anwendung, wenn einer der Ausnahmetatbestände aus Art. 2 Abs. 2 DSGVO vorliegt.

21 So findet die Verordnung keine Anwendung, wenn die Verarbeitung im Rahmen einer Tätigkeit erfolgt, die nicht in den Anwendungsbereich des Unionsrechts fällt (Art. 2 Abs. 2 lit. a DSGVO) – also außerhalb der **Zuständigkeiten der EU** liegt, welche in Art. 3, 4 und 6 des Vertrags von Lissabon (AEUV) festgelegt sind. Dazu gehört unter anderem die nationale Sicherheit.[15]

22 Die Anwendung ist auch dann ausgeschlossen, wenn die Verarbeitung durch die Mitgliedstaaten im Rahmen der gemeinsamen **Außen- und Sicherheitspolitik** im Anwendungsbereich von Titel V Kapitel 2 des Vertrags über die EU (EUV) erfolgt (Art. 2 Abs. 2 lit. b DSGVO).

23 Ebenso findet die DSGVO keine Anwendung auf Datenverarbeitung durch zuständige Behörden, zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung (Art. 2 Abs. 2 lit. d DSGVO).

24 Der relevanteste der Ausnahmetatbestände ist jedoch Art. 2 Abs. 2 lit. c DSGVO für Datenverarbeitung durch natürliche Personen zur Ausübung **ausschließlich persönlicher oder familiärer Tätigkeiten**. Dieser Ausnahmetatbestand wird entsprechend der Begrifflichkeit in vielen anderen Sprachfassungen („household activity", „activité domestique", „hushållsverksamhet") auch als „**Haushaltsausnahme**" bezeichnet. Sie dient dazu, die private Grundrechtsausübung vor einer übermäßigen Regulierung zu schützen.[16]

25 In Erwägungsgrund 18 DSGVO wird klargestellt, dass eine Datenverarbeitung mit Bezug zu **beruflichen und wirtschaftlichen Tätigkeiten** nicht von der Ausnahme umfasst ist, so dass etwa die Verarbeitung von Daten in einem Familienbetrieb nicht von dem Ausnahmetatbestand erfasst wäre.

26 Ausnahmetatbestände sind als solche grundsätzlich **restriktiv** auszulegen.[17] Was eine persönliche oder familiäre Tätigkeit ist, wird sich letztlich nach der **Verkehrsanschauung** richten.[18] Persönliche Tätigkeiten im Sinne der Ausnahme sind solche, die der Selbstentfaltung und Freiheitsausübung in der Freizeit

---

15 Vgl. Erwägungsgrund 16.

16 BeckOK-DS/*Bäcker* Art. 2 DSGVO Rn. 12; Simitis/Hornung/Spiecker gen. Döhmann/*Roßnagel*, Art. 2 DSGVO Rn. 23; Gola/*Gola*, Art. 2 DSGVO Rn. 33.

17 Vgl. Paal/Pauly/*Ernst*, Art. 2 DSGVO Rn. 21.

18 Paal/Pauly/*Ernst*, Art. 2 DSGVO Rn. 18.

oder im privaten Raum dienen.[19] Zu dem typisch persönlichen bzw. familiären Bereich gehören **Freizeit**, **Urlaub** und **privater Konsum**.[20] Eine Gewinnerzielungsabsicht schließt die Anwendbarkeit der Ausnahme nicht zwangsläufig aus, so dass die Datenverarbeitung im Rahmen eines privaten Verkaufs von der Ausnahme umfasst sein kann.[21] Beispielhaft nennt Erwägungsgrund 18 DSGVO das Führen eines **Schriftverkehrs** oder eines **Anschriftenverzeichnisses**. Das Führen eines digitalen Adressbuchs in einer Internetanwendung kann somit ebenso von der Ausnahme erfasst sein wie die Nutzung von elektronischen Kommunikationsdiensten wie E-Mail oder Instant Messaging zu privaten Zwecken oder das Abspeichern von Urlaubsfotos, die andere Personen abbilden.[22] Das Betreiben von digitalen Kameras (z. B. Überwachungskameras, sog. Dash-Cams und Drohnenkameras), die Bereiche außerhalb der privaten Sphäre des Betreibers erfassen, ist von der Ausnahme hingegen nicht gedeckt und fällt zumindest bei Speicherung der Bilddaten in den sachlichen Anwendungsbereich der DSGVO.[23]

Ausdrücklich nennt Erwägungsgrund 18 auch die Nutzung **sozialer Netzwerke** **27**
und sonstige Online-Tätigkeiten als weitere Beispiele, die von dieser Ausnahme umfasst sein können. Unklar ist, ob damit von der **Lindqvist-Rechtsprechung** des EuGH zur Vorgängervorschrift in Art. 3 Abs. 2 DSRL abgewichen werden soll.[24] Der EuGH ging davon aus, dass die Veröffentlichung von personenbezogenen Daten im Internet, so dass diese einer unbegrenzten Zahl von Personen zugänglich gemacht werden, offensichtlich nicht zum **Privat- oder Familienleben einer Person** gehöre und dies von der Haushaltsausnahme daher nicht umfasst sei.[25] Ob diese Einschätzung im Rahmen der Verordnung fortgilt, erscheint zumindest fraglich.

Die Richtlinie datiert aus dem Jahr 1995 und die Lindqvist-Entscheidung aus **28**
dem Jahre 2003. Das heute bekannteste soziale Netzwerk Facebook wurde erst danach im Jahr 2004 gegründet.[26] Der Dienst Twitter existiert erst seit 2006. Bereits im Jahr 2012 gaben 71 % von 1008 befragten privaten Internetnutzern an, dass sie private Daten online abspeichern, um diese mit vielen Menschen auf einer Plattform zu teilen.[27] In Erwägungsgrund 6 DSGVO erkennt der Unionsge-

19 Simitis/Hornung/Spiecker gen. Döhmann/*Roßnagel*, Art. 2 DSGVO Rn. 24; BeckOK-DS/*Bäcker* Art. 2 DSGVO Rn. 12.
20 Gola/*Gola*, Art. 2 DSGVO Rn. 15.
21 Vgl. Simitis/Hornung/Spiecker gen. Döhmann/*Roßnagel*, Art. 2 DSGVO Rn. 7; Kühling/Buchner/*Kühling/Raab*, Art. 2 DSGVO Rn. 8.
22 Vgl. Plath/*Plath*, Art. 2 DSGVO Rn. 22.
23 Paal/Pauly/*Ernst*, Art. 2 DSGVO Rn. 5; vgl. EuGH, Urt. v. 11.12.2014 – C-212/13, Rn. 22, 33.
24 Ausführlich hierzu BeckOK-DS/*Bäcker*, Art. 2 DSGVO Rn. 17 ff.
25 EuGH, Urt. v. 6.11.2003 – C-101/01, Rn. 47.
26 Siehe http://about.fb.com/company-info/, zuletzt abgerufen am 10.2.2021.
27 *Bitkom*, Vertrauen und Sicherheit im Netz, S. 10.

setzgeber zudem an, dass zunehmend natürliche Personen personenbezogene Daten im Internet weltweit zugänglich machen. Trotz dieser Feststellung hat sich der Gesetzgeber jedoch nicht dazu durchringen können, die Anwendbarkeit der Haushaltsausnahme für Veröffentlichungen im Internet klarzustellen.[28]

29 Zwar spricht einiges dafür, dass sich die Verkehrsanschauung so entwickelt hat, dass die (unbegrenzte) Veröffentlichung von Daten Dritter in einem sozialen Netzwerk und in anderen Onlinediensten von der Haushaltsausnahme umfasst sein kann. Einer Entscheidung des EuGH vom 14.2.2019 lässt sich jedoch entnehmen, dass dieser an seiner Lindqvist-Entscheidung festhält.[29] Und auch die überwiegende Meinung in der Literatur geht davon aus, dass die Haushaltsausnahme in der Verordnung wie schon im Rahmen der Richtlinie „**öffentlichkeitsfeindlich**" ist.[30] Im Rahmen der Nutzung sozialer Netzwerke wird daraus die Konsequenz gezogen, dass diese Ausnahme nur greift, wenn der **Kreis der Empfänger der Daten** auf einen engen Familien- und Freundeskreis beschränkt wird.[31]

30 Eine Datenverarbeitung unterfällt auch nur dann der Haushaltsausnahme, wenn sie zur Ausübung einer Tätigkeit erfolgt, die **ausschließlich** persönlich oder familiär ist. Sobald eine Tätigkeit neben dem persönlich-familiären Bezug auch nur teilweise einen Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit hat, bleibt der sachliche Anwendungsbereich für die im Rahmen dieser Tätigkeit vorgenommene Datenverarbeitung eröffnet.[32]

Praxishinweis

Ebenso wie die Eröffnung des Anwendungsbereichs sind auch die Ausnahmen vom Anwendungsbereich auf eine bestimmte Verarbeitung (bzw. Tätigkeit) und nicht auf das Datum als solches bezogen.[33] Der für die initiale Erhebung eines Datums geltende Rechtsrahmen bestimmt nicht zwangsläufig den Rechtsrahmen für jegliche zukünftige Verarbeitung dieses Datums. Ein im beruflichen Kontext erhobenes Datum kann daher von einer natürlichen Person zur Ausübung ausschließlich persönlicher Tätigkeiten außerhalb des

28 Im Gesetzgebungsverfahren wollte das Europäische Parlament zwar noch aufnehmen lassen, dass die Haushaltsausnahme für Veröffentlichungen gelten soll, bei denen davon auszugehen ist, dass der Kreis der Empfänger begrenzt ist. Dieser Vorschlag hat jedoch keinen Eingang in den Text gefunden. Vgl. Simitis/Hornung/Spiecker gen. Döhmann/*Roßnagel*, Art. 2 DSGVO Rn. 7.

29 EuGH, Urt. v. 14.2.2019 – C-345/17, Rn. 43.

30 Paal/Pauly/*Ernst*, Art. 2 DSGVO Rn. 21; *Schantz*, NJW 2016, 1841, 1843; Gola/*Gola*, Art. 2 DSGVO Rn. 21.

31 Gola/*Gola*, Art. 2 DSGVO Rn. 21.

32 Paal/Pauly/*Ernst*, Art. 2 DSGVO Rn. 19; *Härting*, Rn. 313.

33 Vgl. Rn. 6 oben.

Anwendungsbereichs der DSGVO verarbeitet werden. Umgekehrt gilt das gleiche. Entgegen einer weit verbreiteten Ansicht erscheinen sogar parallele Verarbeitungen eines Datums innerhalb und außerhalb des Anwendungsbereichs bzw. einer Ausnahme denkbar (z. B. Verwendung von ansonsten beruflich verwendeten Kontaktdaten für eine rein private Verabredung).[34]

Soweit eine natürliche Person die personenbezogenen Daten Dritter im Rahmen der Haushaltsausnahme verarbeitet, stellt sich die Frage, wie die Verarbeitung dieser Daten durch andere Beteiligte zu bewerten ist. Zunächst stellt Erwägungsgrund 18 DSGVO klar, dass die Verordnung für Verantwortliche oder Auftragnehmer gilt, die die **Instrumente für persönliche oder familiäre Tätigkeiten** bereitstellen. Diese Klarstellung kann jedoch die Prüfung der Voraussetzungen der Eröffnung des Anwendungsbereiches der Verordnung auf die Verarbeitung durch diese Anbieter nicht ersetzen. **31**

Im Hinblick auf die personenbezogenen Daten, die die Nutzung eines solchen Instrumentes (z. B. eines Online-Speicherplatzes) betreffen, ergeben sich dabei keine Besonderheiten. Im Hinblick auf die **Daten Dritter**, die ein Nutzer im Rahmen der Haushaltsausnahme mit einem solchen Instrument verarbeitet (z. B. Speicherung von Familienfotos im Online-Speicherplatz eines Anbieters), wird die Prüfung der Eröffnung des sachlichen Anwendungsbereichs jedoch zunehmend verschachtelt. Der sachliche Anwendungsbereich wird zwar für den Anbieter des jeweiligen Instrumentes regelmäßig nach Art. 2 Abs. 1 DSGVO eröffnet sein. Im Rahmen der Prüfung der Eröffnung des **persönlichen Anwendungsbereichs** werden jedoch verschiedene Fragen aufgeworfen. So entscheiden zum Beispiel Anbieter von E-Mail-Diensten oder von Online-Speicherplatz in der Regel nicht über den Zweck, zu dem die personenbezogenen Daten in diesem Dienst durch den Nutzer verarbeitet werden.[35] Vielmehr werden die Zwecke der Verarbeitung der Daten, die von einem Nutzer in einem Dienst im Rahmen einer persönlichen oder familiären Tätigkeit verarbeitet werden, in der Regel von eben diesem Nutzer allein festgelegt. Der Anbieter des für die „Haushaltsverarbeitung" verwendeten Instrumentes ist somit kein Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO, so dass der persönliche Anwendungsbereich der Verordnung für ihn insoweit zumindest nicht als Verantwortlichen **32**

34 A. A. wohl Gola/*Gola*, Art. 2 DSGVO Rn. 22; a. A. auch Paal/Pauly/*Ernst*, Art. 2 DSGVO Rn. 19; Simitis/Hornung/Spiecker gen. Döhmann/*Roßnagel*, Art. 2 DSGVO Rn. 28.

35 Zudem wird der Anbieter häufig weder von der Existenz solcher Daten noch von deren Inhalt Kenntnis haben, so dass er im Hinblick auf solche Daten schon nicht in der Lage ist, einen Zweck festzulegen. Viele Pflichten des Verantwortlichen setzen zumindest eine Kenntnis der Existenz personenbezogener Daten voraus, so zum Beispiel die Informationspflichten in Art. 14 DSGVO.

eröffnet ist.[36] Hält man den Nutzer trotz der Unanwendbarkeit der DSGVO auf die von ihm vorgenommene Verarbeitung für einen Verantwortlichen i. S. d. DSGVO, kann der Anbieter begrifflich ein Auftragsverarbeiter des Nutzers i. S. v. Art. 4 Nr. 8 DSGVO sein, so dass der persönliche Anwendungsbereich für den Anbieter als Auftragsverarbeiter zumindest begrifflich eröffnet wäre.

33 Geht man von der Eröffnung des Anwendungsbereichs für den Anbieter des Instruments zur „Haushaltsverarbeitung" aus, ergeben sich weitere Schwierigkeiten. Gelangt man zum Beispiel zu dem Ergebnis, die Stelle, die ein Instrument zur „Haushaltsverarbeitung" bereitstellt, ist ein Verantwortlicher, ergeben sich Fragen, wie dieser Verantwortliche seine Pflichten gegenüber den durch die Haushaltsdatenverarbeitung betroffenen Personen erfüllen kann, ohne inhaltlich von deren Daten Kenntnis zu nehmen und dadurch mit dem Nutzer, der diese Daten verarbeitet, in Konflikt zu geraten. Gelangt man zu dem Ergebnis, der Anbieter, der ein solches Instrument zur Haushaltsverarbeitung bereitstellt, ist ein Auftragsverarbeiter des Nutzers, ergibt sich zum Beispiel die Frage, ob es eines Auftragsverarbeitungsvertrags nach Art. 28 Abs. 3 bedarf oder ob ein von der DSGVO eigentlich nicht vorgesehener „halber Auftragsverarbeiter" vorliegt.

Zumindest bei der Situation der Auftragsverarbeitung erscheint es jedoch angebracht, dass die Tätigkeit des Auftragsverarbeiters, der die Daten auf Weisung des Nutzers verarbeitet, ebenfalls von der Haushaltsausnahme umfasst ist, solange er sich nicht zum Verantwortlichen aufschwingt.[37]

Praxishinweis

Natürliche Personen verarbeiten Informationen über sich selbst und über andere in einem immer größer werdenden Umfang und sie nutzen dafür oft Instrumente, die von Unternehmen online bereitgestellt werden. Die Verarbeitung durch die natürlichen Personen liegt dabei häufig schon außerhalb des Schutzbereichs der DSGVO oder sie ist von der Haushaltsausnahme abgedeckt. In diesen Fällen sollte nicht vorschnell davon ausgegangen werden, dass die Beteiligung der Unternehmen an der Verarbeitung im Anwendungsbereich der Verordnung liegt. Dies ist vielmehr im Einzelfall genau zu prüfen.

36 In Erwägungsgrund 47 DSRL wurde dies für den Anbieter eines Telekommunikationsdienstes, der eine Nachricht mit personenbezogenen Daten übermittelt, ebenfalls so festgestellt. An den dahinter liegenden Überlegungen dürfte sich nichts geändert haben.

37 Spindler/Schuster/*Spindler/Dalby*, Art. 2 DSGVO Rn. 6; Auernhammer/*v. Lewinsky*, Art. 2 DSGVO Rn. 25; a. A. BeckOK-DS/*Bäcker* Art. 2 DSGVO Rn. 23.

III. Räumlicher Anwendungsbereich, Art. 3 DSGVO

Art. 3 DSGVO bestimmt, wann Verarbeitungsvorgänge vom räumlichen Anwendungsbereich der Verordnung erfasst sind. **34**

Abgesehen von Art. 3 Abs. 3 DSGVO ist der **Ort der Datenverarbeitung** als solcher für die Eröffnung des räumlichen Anwendungsbereichs nicht relevant.[38] Somit kann jeder Datenverarbeitungsvorgang weltweit im räumlichen Anwendungsbereich der Verordnung liegen. **35**

Praxishinweis

Wie im Folgenden aufgezeigt wird, ist der räumliche Anwendungsbereich der Verordnung sehr weit. Selbst eine Verarbeitung von Daten, die außerhalb der EU vorgenommen wird und Personen betrifft, die keinem Mitgliedstaat der EU angehören, kann dem europäischen Datenschutzrecht unterliegen. Ist der Verantwortliche in der EU niedergelassen, gilt dies unter Umständen sogar dann, wenn sich die betroffenen Personen dauerhaft außerhalb der EU befinden.

1. Niederlassungsprinzip, Art. 3 Abs. 1 DSGVO

Nach Art. 3 Abs. 1 DSGVO findet die Verordnung räumlich Anwendung auf die Verarbeitung personenbezogener Daten, „*soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftraggebers in der Union erfolgt, unabhängig davon, ob die Verarbeitung tatsächlich in der Union stattfindet*“ (**Niederlassungsprinzip**). **36**

Das europäische Datenschutzrecht hat einen eigenen **Begriff der Niederlassung**, der sich z. B. von den in Art. 49 AEUV, § 13 HBG oder § 4 Abs. 3 GewO verwendeten Begriffen unterscheidet. Nach Erwägungsgrund 22 DSGVO setzt eine Niederlassung die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist nach diesem Erwägungsgrund nicht ausschlaggebend. **37**

38 Art. 3 Abs. 3 DSGVO regelt in erster Linie die Datenverarbeitung am Ort von diplomatischen oder konsularischen Vertretungen der EU-Mitgliedstaaten außerhalb der EU, für die aufgrund des Völkerrechts das Recht des jeweiligen Mitgliedstaates gilt (vgl. Erwägungsgrund 25).

a) Verarbeitung im Rahmen der Tätigkeiten der Niederlassung eines Verantwortlichen

38 In Bezug auf die **Niederlassung eines Verantwortlichen** weisen der Wortlaut des Art. 3 Abs. 1 DSGVO und der Wortlaut der Vorgängerregelung in Art. 4 Abs. 1 lit. a DSRL ebenso wie die entsprechenden Erwägungsgründe große Ähnlichkeiten auf.

39 Angesichts dieser Parallelen dürfte die Rechtsprechung des EuGH zum Begriff der Niederlassung in der Richtlinie auch für die DSGVO weiterhin Bedeutung haben.[39] Zuletzt hat der EuGH im Fall „**Weltimmo**" die Grenzen dieses Begriffs ausgedehnt und eine sehr niedrige Schwelle für das Eingreifen des Niederlassungsprinzips angelegt. Nach dieser Entscheidung kann schon das Betreiben einer Webseite in der Sprache eines Mitgliedstaates mit auf den Mitgliedstaat bezogenen Angeboten als „effektive und tatsächliche Ausübung einer Tätigkeit" eines Unternehmens in dem Mitgliedstaat angesehen werden. Und ein einziger Vertreter des Unternehmens in diesem Mitgliedstaat, der im Zusammenhang mit der Website tätig wird, kann eine „feste Einrichtung" des Unternehmens sein.[40] Lediglich vorübergehend verortete Einrichtungen, wie z. B. Messestände, reichen hingegen nicht aus. Auch die Beauftragung eines Auftragsverarbeiters in der Union lässt keine Niederlassung des Verantwortlichen entstehen.[41]

Praxishinweis

Es reichen bereits sehr geringe Aktivitäten in einem Mitgliedstaat der EU, um eine Niederlassung des Verantwortlichen im Sinne der Verordnung entstehen zu lassen. Der Umstand, dass keine Tochtergesellschaften oder Zweigniederlassungen in der EU existieren, schließt die Anwendbarkeit der Verordnung nicht aus.

40 Liegt eine Niederlassung in der EU vor, ist weiterhin zu prüfen, ob die jeweilige Verarbeitung **im Rahmen der Tätigkeiten** dieser Niederlassung erfolgt.

41 Dies ist in der Regel unschwer zu bejahen, wenn die in Betracht gezogene Niederlassung in der EU zugleich der **satzungsmäßige Sitz** des Verantwortlichen ist (bzw. bei einer Einzelperson der **Geschäfts-** oder **Wohnsitz**). Denn mit Ausnahme von reinen Briefkastenfirmen ist der Sitz des Verantwortlichen in der

39 Plath/*Plath*, Art. 3 DSGVO Rn. 8; Gola/*Piltz*, Art. 3 DSGVO Rn. 7.

40 EuGH, Urt. v. 1.10.2015 – C-230/14, Rn. 24 ff.

41 Taeger/Gabel/*Schmidt*, Art. 3 DSGVO Rn. 9; Kühling/Buchner/*Klar*, Art. 3 DSGVO Rn. 38; Simitis/Hornung/Spiecker gen. Döhmann/*Hornung*, Art. 3 DSGVO Rn. 33; Spindler/Schuster/*Spindler/Dalby*, Art. 3 DSGVO Rn. 4; *Europäischer Datenschutzausschuss*, Guidelines 3/2018 on the territorial scope of the GDPR, S. 9.

Regel eine Niederlassung, an der sich eine Tätigkeit festmachen lässt, im Rahmen derer die Datenverarbeitung durch den Verantwortlichen erfolgt.

Die Datenverarbeitung erfolgt auch stets dann im Rahmen der Tätigkeit einer Niederlassung, wenn die Niederlassung **an der betrachteten Datenverarbeitung direkt beteiligt** ist. **42**

Schwieriger ist die Prüfung dieses Merkmals in Fällen, in denen der Sitz des Verantwortlichen in einem Drittstaat liegt und keine Niederlassung in der EU an der Datenverarbeitung direkt beteiligt ist. Diese Konstellation liegt in der Praxis insbesondere bei über das Internet aus einem Drittland angebotenen Dienstleistungen vor. Solche Fälle waren während der Geltungsdauer der Richtlinie lange umstritten. Der EuGH hatte in der Entscheidung „**Google-Spain**" jedoch klargestellt, dass eine Verarbeitung durch die Niederlassung selbst nicht erforderlich ist und es schon ausreicht, wenn die Niederlassung mit ihrer Tätigkeit in einem Mitgliedstaat zur Rentabilität der betrachteten Datenverarbeitung beiträgt.[42] Dies begründet nach Ansicht des EuGH eine „untrennbare Verbindung" zwischen der Tätigkeit der Niederlassung und der betrachteten Datenverarbeitung, was dazu führt, dass die Datenverarbeitung im Rahmen dieser Tätigkeit erfolgt.[43] Seit dieser Entscheidung fielen eine Vielzahl zuvor strittiger Szenarien klar in den räumlichen Anwendungsbereich der Richtlinie. Aufgrund der Parallelen zur Richtlinie kann auch im Rahmen der Verordnung auf diese Rechtsprechung des EuGH zurückgegriffen werden. Dagegen ließe sich zwar einwenden, dass mit der Einführung des Marktortprinzips durch Art. 3 Abs. 2 ein wesentlicher Grund für die extensive und flexible Auslegung der Vorgängerregelung durch den EuGH weggefallen ist. An dem Ansatz des EuGH, zur Gewährleistung eines wirksamen und umfassenden Schutzes des Rechts auf Privatleben eine weite Auslegung der Vorschriften zur Anwendbarkeit vorzunehmen, hat dies jedoch nichts geändert.[44] **43**

b) Verarbeitung im Rahmen der Tätigkeiten der Niederlassung eines Auftragsverarbeiters

Die Bezugnahme auf den Auftragsverarbeiter zur Eröffnung des Anwendungsbereichs des Datenschutzrechts ist neu. Es ist fraglich, inwieweit sich das oben beschriebene Verständnis des Begriffs der „Verarbeitung im Rahmen der Tätigkeiten einer Niederlassung des Verantwortlichen" auf den Auftragsverarbeiter übertragen lässt. **44**

Dieses Begriffsverständnis, welches sich während der Geltungsdauer der Richtlinie unter anderem durch die Rechtsprechung des EuGH herausgebildet hat, ist **45**

42 EuGH, Urt. v. 13.5.2014 – C-131/12, Rn. 52 ff.
43 EuGH, Urt. v. 13.5.2014 – C-131/12, Rn. 56, 57.
44 Zuletzt EuGH, Urt. v. 24.9.2019 – C-507/17, Rn. 50.

dadurch geprägt, dass sich der Begriff „im Rahmen der Tätigkeiten einer Niederlassung“ in der Richtlinie ausschließlich auf die Verarbeitung durch einen Verantwortlichen bezog.

46 Der Verantwortliche legt die Zwecke und Mittel der Verarbeitung fest und die Tätigkeiten seiner Niederlassungen haben potenziell eine sehr große Bandbreite. Der Auftragsverarbeiter hingegen verarbeitet die Daten nach Weisung und im Auftrag des Verantwortlichen. Gegenstand, Dauer, Umfang, Art und Zweck der Verarbeitung werden im Auftragsverarbeitungsvertrag festgelegt.[45]

47 Die Verarbeitung der Daten durch einen Auftragsverarbeiter ist somit ebenso wie der Rahmen seiner Tätigkeit in Bezug auf die Daten wesentlich durch seine vertraglich definierte Rolle bestimmt und begrenzt. Eine etwaige Datenverarbeitung außerhalb dieses Rahmens lässt den Auftragsverarbeiter, in der Regel zur Verantwortlichen Stelle werden.[46] Prüft man die Voraussetzungen des Art. 3 Abs. 1 DSGVO spezifisch für einen Auftragsverarbeiter, erscheint es daher geboten, dabei den Fokus auf den durch den jeweiligen **Auftragsverarbeitungsvertrag** vorgegebenen Tätigkeitsrahmen zu legen.

48 Im Unterschied zum Verantwortlichen spricht somit einiges dafür, dass für eine (Auftrags-)Verarbeitung im Rahmen der Tätigkeiten einer Niederlassung eines Auftragsverarbeiters in der Regel nur solche Niederlassungen relevant sind, die tatsächlich an der Auftragsverarbeitung mitwirken. Denn nur solche Niederlassungen nehmen Tätigkeiten vor, in deren Rahmen die relevante (Auftrags-)Verarbeitung liegen soll bzw. darf. Der Rahmen der Tätigkeiten einer Niederlassung ist somit bei einem Auftragsverarbeiter deutlich enger gefasst als bei einem Verantwortlichen.

2. Marktortprinzip, Art. 3 Abs. 2 DSGVO

49 Ist ein Verantwortlicher oder ein Auftragsverarbeiter **nicht in der EU niedergelassen**, kann sich die räumliche Anwendbarkeit der Verordnung aus Art. 3 Abs. 2 DSGVO ergeben.[47] Danach findet die Verordnung *Anwendung auf die*

45 Art. 28 Abs. 3 DSGVO; vgl. Kap. 7 Rn. 38.

46 Art. 28 Abs. 10 DSGVO; vgl. Kap. 7 Rn. 10.

47 Aufgrund der eindeutigen Formulierung „nicht in der Union niedergelassenen“ in Art. 3 Abs. 2 DSGVO entsteht zwischen Art. 3 Abs. 1 und Abs. 2 DSGVO eine Lücke für solche Stellen, die zwar Niederlassungen in der EU haben, deren Tätigkeiten aber einen Rahmen haben, in dem die fragliche Datenverarbeitung nicht stattfindet. Insbesondere bei Mischkonzernen ist eine solche Konstellation durchaus denkbar. In der Richtlinie existierte zwar eine vergleichbare Lücke, diese wurde jedoch durch die mitgliedstaatlichen Umsetzungsgesetze (z. B. auch im BDSG (bis 2018)) teilweise geschlossen. Ob und wie sich diese neue Lücke in der Praxis auswirkt, bleibt abzuwarten. Teilweise wird vorgeschlagen, die Lücke im Wege einer teleologischen Auslegung zu schließen.

Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht

1. *betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;*
2. *das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.*

Dieses sog. **Marktortprinzip** ist eine **wesentliche und vielleicht sogar die wichtigste Neuerung** der DSGVO im Vergleich zur Richtlinie, welche dem **Territorialitätsprinzip** folgend auf die Belegenheit von Verarbeitungsmitteln in einem Mitgliedstaat abstellte.[48] Die physischen Betriebs- und Organisationsstrukturen der verarbeitenden Stelle einschließlich des Standorts von Datenverarbeitungsanlagen ist für die Anwendbarkeit der Verordnung nach Art. 3 Abs. 2 nunmehr irrelevant. Dies ist angesichts der fortschreitenden Virtualisierung der Datenverarbeitung, bei der Datenverarbeitungskapazitäten ohne Bindung an einen bestimmten Ort zur Verfügung gestellt werden können, nur konsequent. Es führt jedoch gleichzeitig zu einer erheblichen Ausweitung des Anwendungsbereichs des europäischen Datenschutzrechts. **50**

Ein gewisser räumlicher **Bezug der Datenverarbeitung zum Territorium EU** ist jedoch auch im Rahmen des Marktortprinzips erforderlich. Dieser Bezug wird durch die betroffene Person vermittelt, welche sich gemäß Art. 3 Abs. 2 DSGVO in der EU befinden muss. Art. 3 Abs. 2 lit. a DSGVO setzt zudem voraus, dass Waren oder Dienstleistungen an betroffene Personen in der EU angeboten werden. Wohingegen Art. 3 Abs. 2 lit. b DSGVO voraussetzt, dass das beobachtete Verhalten einer Person in der EU erfolgt. **51**

a) Anbieten von Waren oder Dienstleistungen, Art. 3 Abs. 2 lit. a DSGVO

Eine „**Ware**" im Sinne des Europarechts ist jeder körperliche Gegenstand, der einen Geldwert hat und Gegenstand eines Handelsgeschäfts sein kann.[49] Eine „**Dienstleistung**" im Sinne des Europarechts ist eine vom Begriff der „Ware" abgegrenzte, in der Regel gegen Entgelt erbrachte Leistung.[50] Mit einem Zusatz in Art. 3 Abs. 2 lit. a DSGVO hat der Unionsgesetzgeber allerdings klargestellt, dass auch solche Angebote erfasst sein sollen, bei denen keine Zahlung zu leis- **52**

48 Art. 4 Abs. 1 lit. c DSRL. Nach § 1 Abs. 5 S. 2 BDSG (bis 2018) war erforderlich, dass personenbezogene Daten „im Inland" erhoben, verarbeitet oder genutzt werden.

49 EuGH, Urt. v. 10.12.1968 – C-7/68, Slg. 1968, 633, Rn. 2; EuGH, Urt. v. 14.7.1977 – C-1/77, Slg. 1977, 1473, Rn. 4.

50 Art. 57 AEUV.

ten ist. Dadurch sollen offenbar insbesondere Online-Dienste erfasst werden, bei denen die Entgeltlosigkeit die Regel ist. Um willkürlich erscheinende Schutzlücken zu vermeiden, ist davon auszugehen, dass die Begriffe „Ware" und „Dienstleistung" nicht formalistisch zu betrachten sind, sondern auch unkörperliche Gegenstände wie Software oder Grenzfälle wie ein Gewinnspiel erfassen.[51]

53 Laut Erwägungsgrund 23 DSGVO ist für die Frage, ob ein Verantwortlicher oder Auftragsverarbeiter betroffenen Personen, die sich in der Union befinden, Waren oder Dienstleistungen anbietet, festzustellen, dass es dessen **offensichtliche Absicht** ist, ein solches Angebot betroffenen Personen in mindestens einem Mitgliedstaat zu machen.

54 Die Verwendung des Begriffs „Absicht" legt zwar nahe, dass es auf die tatsächliche innere Absicht der verarbeitenden Stelle ankommt. Die geforderte Offensichtlichkeit der Absicht und ein Vergleich mit anderen Sprachfassungen der Verordnung machen jedoch deutlich, dass es auf den **Empfängerhorizont** ankommt und eine etwaige abweichende innere Absicht daher unbeachtlich sein dürfte.[52] Entscheidend ist die inhaltliche Gestaltung des Angebots.[53]

55 Gemäß Erwägungsgrund 23 DSGVO reicht die bloße Möglichkeit, aus der EU heraus mit dem Verantwortlichen, dem Auftragsverarbeiter oder einem Vermittler über eine Webseite, eine E-Mail-Adresse oder auf anderem Wege in Kontakt zu treten, nicht aus, um eine solche Absicht anzunehmen.

56 Erwägungsgrund 23 DSGVO beschreibt jedoch auch Faktoren, die Anhaltspunkte für eine solche Absicht sein können. Dazu gehört die Verwendung einer **Sprache**, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, in dieser Sprache zu bestellen. Dabei muss es sich jedoch um eine andere Sprache handeln als die, die in dem Drittland gebräuchlich ist, in dem der Verantwortliche niedergelassen ist. Auch die Verwendung der englischen Sprache dürfte aufgrund ihrer weltweiten Gebräuchlichkeit keinen starken Anhaltspunkt bieten. Als weitere Anhaltspunkte werden in dem Erwägungsgrund die Verwendung der **Währung eines Mitgliedstaates** und die **Erwähnung von Kunden oder Nutzern**, die sich in der EU befinden, genannt.

57 Die Aufzählung der Kriterien in Erwägungsgrund 23 DSGVO ist nicht abschließend. Weitere Kriterien lassen sich aus der Rechtsprechung zu europäischen

51 Vgl. Taeger/Gabel/*Schmidt*, Art. 3 DSGVO Rn. 20: Plath/*Plath* Art. 3 DSGVO Rn. 18; Simitis/Hornung/Spiecker gen. Döhmann/*Hornung*, Art. 3 DSGVO Rn. 48.

52 Laut der englischen Sprachfassung des Erwägungsgrundes 23 DSGVO ist zu prüfen, „whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union."

53 Paal/Pauly/*Ernst*, Art. 2 DSGVO Rn. 16.

Vorschriften entnehmen, die schon länger auf das Marktortprinzip abstellen.[54] Insbesondere die Pammer- und Alpenhof-Entscheidung des EuGH zu Art. 15 Abs. 1 lit. c. der Brüssel-I-Verordnung ist hierfür relevant und wird in diesem Zusammenhang auch vom Europäischen Datenschutzausschuss herangezogen.[55] Dazu gehören zum Beispiel der Betrieb einer nationalen **Telefonnummer** in einem Mitgliedstaat oder die Verwendung einer länderspezifischen **Top-Level-Domain** mit Bezug zu einem Mitgliedstaat (z. B. „.de" für Deutschland oder „.fr" für Frankreich). Die Kriterien sind in einer **Gesamtbetrachtung** zu würdigen.

Die Feststellung derartiger Kriterien ist in Bezug auf den Verantwortlichen unproblematisch möglich. Der **Auftragsverarbeiter** hat jedoch auf diese Kriterien in der Regel keinen Einfluss. Sie sind daher nicht geeignet, um auf eine entsprechende Absicht des Auftragsverarbeiters zu schließen. Zudem richtet sich das Angebot eines Auftragsverarbeiters an den Verantwortlichen und besteht darin, die Daten für den Verantwortlichen zu verarbeiten. Es richtet sich daher schon begrifflich nicht an die betroffenen Personen, so dass damit auch keine Absicht im Sinne des Erwägungsgrundes 23 verbunden ist.[56] Dementsprechend dürfte der räumliche Anwendungsbereich der Verordnung über Art. 3 Abs. 2 lit. a DSGVO in der Praxis für Auftragsverarbeiter fast nie eröffnet sein.[57] **58**

Liegt ein Angebot im Sinne des Art. 3 Abs. 2 lit. a DSGVO vor, ist zu prüfen, ob die in Betracht gezogene Verarbeitung personenbezogener Daten **im Zusammenhang** mit diesem Angebot steht. Detaillierte Anhaltspunkte in der Verordnung dafür, wann ein solcher Zusammenhang anzunehmen ist, fehlen.[58] **59**

---

54 Spindler/Schuster/*Spindler/Dalby*, Art. 3 DSGVO Rn. 10. Art. 6 Abs. 1 lit. b Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates vom 17.6.2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht („Rom I"); Art. 6 Verordnung (EG) Nr. 864/2007 des Europäischen Parlaments und des Rates vom 11.7.2007 über das auf außervertragliche Schuldverhältnisse anzuwendende Recht („Rom II"); Art. 15 Abs. 1 lit. c Verordnung (EG) Nr. 44/2001 des Rates vom 22.12.2000 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen („Brüssel I").

55 EuGH Urt. v. 7.12.2010 – C-585/08 und C-144/09 Rn. 83; *Europäischer Datenschutzausschuss*, Guidelines 3/2018 on the territorial scope of the GDPR, S. 17.

56 Im Ergebnis ebenso BeckOK-DS/*Hanloser*, Art. 3 DSGVO Rn. 34; Kühling/Buchner/*Klar*, Art. 3 DSGVO Rn. 89. Würde der Auftragsverarbeiter den betroffenen Personen Waren oder Dienstleistungen anbieten, wäre er im Hinblick auf die damit im Zusammenhang stehende Verarbeitung personenbezogener Daten in der Regel selbst Verantwortlicher.

57 A. A. wohl Simitis/Hornung/Spiecker gen. Döhmann/*Hornung*, Art. 3 DSGVO Rn. 54, zumindest dann, wenn der Auftragsverarbeiter die Infrastruktur betreibt, die sich an betroffene Personen in der Union richtet.

58 Nach der deutschen Sprachfassung des Erwägungsgrundes 23 soll die Datenverarbeitung der Verordnung unterliegen, wenn sie dem Anbieten von Waren oder Dienstleis-

60 Sofern die betroffene Personen in der EU, bezüglich derer personenbezogene Daten verarbeitet werden, und die Person in der EU, an die sich das Angebot richtet, identisch sind, dürfte ein solcher Zusammenhang stets gegeben sein.

61 Fraglich ist, ob ein relevanter Zusammenhang ebenfalls bestehen kann, wenn betroffene Person und Adressat des Angebots nicht identisch sind. Diese Frage wird zum Beispiel aufgeworfen, wenn eine Person in der EU bewusst ein Angebot in Anspruch nimmt, welches sich an Personen außerhalb der EU richtet, obwohl es vom selben Anbieter auch ein Angebot für die EU gibt.[59]

62 Richtet die verarbeitende Stelle einen Teil ihres Angebotes erkennbar an Personen außerhalb der EU, erscheint es unbillig zu fordern, dass sie Daten von Personen in der EU, die diesen Teil des Angebots in Anspruch nehmen, dennoch der Verordnung gemäß verarbeitet. Der jeweiligen Person, die sich bewusst gegen ein europäisches und für ein außereuropäisches Angebot entscheidet, wird der Schutz der Verordnung nicht im Sinne des Erwägungsgrundes 23 „vorenthalten". Zudem scheint der Wortlaut des Art. 3 Abs. 2 lit. a DSGVO eine **Identität von betroffener Person und Angebotsempfänger** vorauszusetzen, wenn dort von einer Zahlung von „diesen Personen" die Rede ist. Dieser Formulierung liegt das Verständnis zugrunde, dass die Personen, an die sich ein Angebot richtet, und die Personen, die das Angebot in Anspruch nehmen und gegebenenfalls bezahlen, identisch sind. In Erwägungsgrund 23 findet sich eine ähnliche Formulierung („diesen betroffenen Personen").

63 Somit spricht vieles dafür, dass ein ausreichender Zusammenhang zwischen Datenverarbeitung und Angebot nur dann bestehen kann, wenn betroffene Person und Angebotsempfänger identisch sind. Gleichzeitig ist bei einer derartigen **Personenidentität** in der Regel der erforderliche Zusammenhang zwischen dem Angebot und der Datenverarbeitung gegeben. Durch diesen Ansatz wird das ansonsten sehr unscharfe Merkmal des „Zusammenhangs" deutlich handhabbarer.

Praxishinweis

Soweit ein Unternehmen beabsichtigt, bestimmte Waren oder Dienstleistungen oder Teile davon nur Personen außerhalb der EU anzubieten, sollte darauf geachtet werden, dass dabei keine Anhaltspunkte erzeugt werden, die für ein Angebot an Personen in der EU sprechen. So wird vermieden, dass der räumliche Anwendungsbereich der Verordnung versehentlich für ein Produkt eröffnet wird, welches hierfür nicht geeignet ist. Ein aktives Aus-

---

tungen „dient". Allerdings zeigt ein Vergleich mit anderen Sprachfassungen, dass ein andersartiger Zusammenhang ebenfalls ausreichend sein dürfte. So reicht laut der englischen Sprachfassung ein „related to offering goods or services".

59 Dies ist bei Online-Diensten durchaus üblich. Europäische Nutzer verwenden außereuropäische Dienste häufig aufgrund ihrer Muttersprache.

sperren oder Umleiten europäischer Kunden weg von solchen Angeboten erscheint zwar nicht erforderlich, kann aber, ebenso wie ein entsprechender Disclaimer, als zusätzliche Vorsichtsmaßnahme sinnvoll sein.

b) Verhaltensbeobachtung, Art. 3 Abs. 2 lit. b DSGVO

Der räumliche Anwendungsbereich kann auch durch das Beobachten von Verhalten betroffener Personen in der EU gemäß Art. 3 Abs. 2 lit. b DSGVO eröffnet sein. **64**

Der Begriff der Verhaltensbeobachtung ist in Anbetracht von Erwägungsgrund 24 anscheinend auf das **Verhalten einer Person im Internet** beschränkt. Zumindest wird in Erwägungsgrund 24 deutlich, dass der Unionsgesetzgeber den Online-Bereich im Fokus hatte.[60] **65**

Die schlichte Erfassung der Daten über die Internetaktivität z. B. in einem gewöhnlichen **Serverlog** reicht für die Annahme einer Verhaltensbeobachtung allerdings nicht aus. „Beobachtung" geht schon begrifflich über die reine Erfassung von Daten hinaus.[61] Es muss sich vielmehr um ein zielgerichtetes Sammeln von Erkenntnissen handeln.[62] Dementsprechend ist gemäß Erwägungsgrund 24 DSGVO für ein Beobachten erforderlich, dass Internetaktivitäten der betroffenen Person tatsächlich nachvollzogen werden. Laut Erwägungsgrund 24 DSGVO liegt ein solches Nachvollziehen unter anderem dann vor, wenn durch die Beobachtung die Erstellung eines **Profils der Person ermöglicht wird**, welches Grundlage für die Person betreffende Entscheidungen bildet oder anhand dessen ihre persönlichen **Vorlieben, Verhaltensweisen oder Gepflogenheiten** analysiert oder vorausgesagt werden sollen. Dies legt nahe, dass der Begriff der Beobachtung eine gewisse Dauer und Intensität voraussetzt.[63] **66**

Offensichtlich sollen damit im Internet eingesetzte Technologien in den räumlichen Anwendungsbereich der Verordnung gebracht werden, die die Internetaktivitätsdaten von Nutzern erfassen (z. B. durch entsprechende Cookies oder sonstige Nutzerkennungen), sofern die erfassten Daten in eine Entscheidung in Bezug auf die betroffene Person münden oder die Daten zur Personalisierung von **67**

60 Die Beobachtung von Offline-Verhalten, welches in der EU erfolgt, wird ohnehin häufig eine Tätigkeit einer Niederlassung im Sinne des Art. 3 Abs. 1 DSGVO sein.

61 Die englische Sprachfassung des Art. 3 Abs. 2 lit. b DSGVO verwendet den Begriff „monitoring". In der schwedischen Sprachfassung ist von „övervakning", also „Überwachung" die Rede.

62 Taeger/Gabel/*Schmidt*, Art. 3 DSGVO Rn. 25.

63 Vgl. Spindler/Schuster/*Spindler/Dalby*, Art. 3 DSGVO Rn. 12; Ehmann/Selmayr/*Zerdick*, Art. 3 DSGVO Rn. 20; Kühling/Buchner/*Klar*, Art. 3 DSGVO Rn. 94; a. A. Taeger/Gabel/*Schmidt*, Art. 3 DSGVO Rn. 25.

Funktionalitäten oder Inhalten (z. B. **personalisierte Werbung**, personalisierte Vorschlagsfunktionen oder personalisierte Suchergebnisse) anhand eines Profils der Person eingesetzt werden.

68 Die Analyse von Internetaktivitätsdaten von Besuchern eines Webangebotes dürfte jedoch keine solche Verhaltensbeobachtung darstellen, sofern die Analyse **aggregiert** erfolgt und nicht den einzelnen Besucher im Fokus hat. **Web-Analyse-Verfahren**, die allein dazu dienen, eine Webseite insgesamt bedarfsgerecht zu gestalten oder bestimmte Kennzahlen im Hinblick auf die Funktionsfähigkeit der Webseite zu messen, dürften daher von Art 3 Abs. 2 lit. b DSGVO nicht erfasst sein.[64]

69 Art. 3 Abs. 2 lit. b DSGVO setzt zudem denklogisch voraus, dass die Person, deren Daten verarbeitet werden, und die Person, deren Verhalten mittels dieser Verarbeitung beobachtet wird, **identisch** sein müssen, wodurch auch stets der erforderliche Zusammenhang zwischen Verarbeitung und Verhaltensbeobachtung besteht.

70 Schließlich muss das beobachtete **Verhalten in der EU** erfolgen. Der Umstand, dass Art. 2 Abs. 3 lit. b DSGVO erfordert, dass sich zum einen die Person in der EU befindet und zum anderen ihr beobachtetes Verhalten in der EU erfolgt, legt nahe, dass es der Gesetzgeber für möglich hält, dass sich eine in der EU befindliche Person außerhalb der EU verhalten kann. Gerade bei den von Art. 3 Abs. 2 lit. a DSGVO erfassten Internetaktivitäten erscheint dies durchaus denkbar. So ist zum Beispiel die Frage, wo eine Tat bzw. Handlung mittels einer Webseite begangen wird, im Rahmen des Strafrechts oder des Zivilprozessrechts hoch umstritten. Daher scheint es vertretbar anzunehmen, dass das Verhalten einer in der EU befindlichen Person außerhalb der EU erfolgt, wenn diese Person einen Internetdienst verwendet, der auf Servern außerhalb der EU läuft.

71 Dadurch, dass das in der Vorgängerregelung des Art. 4 Abs. 1 lit. c DSRL verankerte Territorialitätsprinzip nicht in die Verordnung übernommen wurde, wird jedoch zum Ausdruck gebracht, dass der Standort von Datenverarbeitungsanlagen keine Bedeutung für die Eröffnung des räumlichen Anwendungsbereichs haben soll. Zudem wird Art. 3 Abs. 2 lit. b DSGVO in der Regel erst dann relevant werden, wenn die verarbeitende Stelle keine Niederlassung in der EU hat. Insgesamt ist somit der Wille des Unionsgesetzgebers deutlich erkennbar, die in der Union befindlichen betroffenen Personen möglichst umfassend zu schützen. Dementsprechend dürfte sich die Ansicht durchsetzen, dass das Verhalten von in der EU befindlichen Personen aus der Perspektive des europäischen Daten-

64 Sofern im Rahmen der Web-Analyse personenbezogene Daten verarbeitet werden, kann diese Verarbeitung jedoch sehr wohl im räumlichen Anwendungsbereich der Verordnung liegen, wenn das analysierte Webangebot ein Angebot an Personen in der EU im Sinne des Art 3 Abs. 2 lit. a DSGVO darstellt.

schutzrechts auch stets in der EU erfolgt, selbst wenn sie Internetdienste nutzen, die auf Servern außerhalb der EU angeboten werden.[65]

Praxishinweis

Art. 3 Abs. 2 lit. b DSGVO dehnt den räumlichen Anwendungsbereich der Verordnung unter Umständen sehr weit aus. Dies hat zum Beispiel die unbillig erscheinende Folge, dass Unternehmen, die keine Niederlassung in der EU haben und ihren Internetdienst ausschließlich an Personen außerhalb der EU richten und diesen zudem auf Servern außerhalb der EU betreiben, dennoch in den räumlichen Anwendungsbereich der Verordnung fallen können, wenn Nutzer aus der EU auf diesen Dienst zugreifen und der Dienst auf Verhaltensprofilen basierte Personalisierungsfunktionen anbietet.

c) Betroffene Person in der EU

Für die Eröffnung des räumlichen Anwendungsbereichs nach Art. 3 Abs. 2 lit. a oder lit. b DSGVO ist es zudem erforderlich, dass sich die betroffene Person, deren Daten verarbeitet werden, in der EU befindet. Die **Staatsangehörigkeit** der Person ist irrelevant. Das Gleiche gilt für ihren **Wohnsitz**. Zwar wurde in der Entwurfsphase der Verordnung noch darauf abgestellt, wo die Person **ansässig** ist. Dies wurde jedoch für die Endfassung nicht übernommen. Entscheidend ist vielmehr der tatsächliche **Aufenthaltsort** der betroffenen Person.[66] **72**

Ob sich eine betroffene Person in der EU aufhält oder nicht, ist eine Frage der Tatsachen. Damit ist diese Voraussetzung des Art. 3 Abs. 2 DSGVO zunächst rein deskriptiver Natur. Allerdings werden die **Zeiträume** des Aufenthalts einer Person in der EU und der Zeitraum der Verarbeitung der Daten dieser Person in vielen Fällen auseinanderfallen, so dass fraglich ist, wie mit einem solchen Auseinanderfallen umzugehen ist. **73**

Unter anderem wird hierzu vertreten, dass der jeweilige **Zeitpunkt der Verarbeitung** auch der relevante Zeitpunkt für die Bestimmung des Aufenthaltsortes und damit des räumlichen Anwendungsbereichs sei.[67] Dies führt zu willkürlichen Ergebnissen. Einerseits erscheint es im Interesse des effektiven Schutzes der Person nicht angemessen, dass bei der Datenverarbeitung zum Beispiel für die Dauer eines Aufenthaltes in einem Drittland nicht mehr die Vorschriften der Verordnung zu beachten sind.[68] Andererseits erscheint es im Interesse der Vorhersehbarkeit der Anwendbarkeit der Verordnung nicht angemessen, dass umge- **74**

65 So auch Simitis/Hornung/Spiecker gen. Döhmann/*Hornung*, Art. 3 Rn. 59.
66 So auch Plath/*Plath*, Art. 3 DSGVO Rn. 13.
67 *Albrecht*, CR 2016, 88, 90.
68 Vgl. Plath/*Plath*, Art. 3 DSGVO Rn. 14.

kehrt die Verarbeitung der Daten einer Person aus dem außereuropäischen Ausland für die Dauer eines kurzen Aufenthaltes in einem EU-Mitgliedstaat der Verordnung unterliegt.

75 Auch ein Abstellen auf den **Zeitpunkt der Erhebung** der Daten während des Aufenthalts in der EU führt zu derart willkürlichen Szenarien.[69] Das gleiche gilt für den Vorschlag des Europäischen Datenschutzausschusses, auf den Zeitpunkt der Unterbreitung des Angebots bzw. der Beobachtung abzustellen.[70]

76 Bei wechselnden Aufenthaltsorten der betroffenen Person innerhalb und außerhalb der EU erscheint vielmehr eine **wertende Betrachtung** angebracht, die frühestens beginnend mit dem erstmaligen Aufenthalt der Person in der EU so lange von einer Anwendbarkeit der Verordnung ausgeht, wie der **Schwerpunkt des Aufenthalts** der Person in der EU liegt.

3. Räumlicher Anwendungsbereich bei mehreren Beteiligten

77 Die Eröffnung des räumlichen Anwendungsbereichs ist für den Verantwortlichen und seinen Auftragsverarbeiter separat zu prüfen. Dies kann dazu führen, dass derselbe Verarbeitungsvorgang vom Verantwortlichen innerhalb des räumlichen Anwendungsbereichs vorgenommen wird, während der Auftragsverarbeiter diese Verarbeitung außerhalb des räumlichen Anwendungsbereichs durchführt, und umgekehrt.[71] Ein solches Auseinanderfallen ist ebenfalls denkbar, wenn es sich bei den Beteiligten um gemeinsam Verantwortliche i. S. d. Art. 26 DSGVO handelt.

Praxishinweis

Der Feststellung des Auseinanderfallens des räumlichen Anwendungsbereichs der DSGVO bei mehreren Stellen, die an derselben Datenverarbeitung beteiligt sind, sollte eine sorgfältige Prüfung vorausgehen. Auch wenn ein Beteiligter nicht in der EU niedergelassen ist, vermag seine Kooperation mit in der EU niedergelassenen Stellen einen territorialen Bezug zur EU zu begründen, der unter Art. 3 Abs. 2 DSGVO fällt.

---

69 So aber wohl Plath/*Plath*, Art. 3 DSGVO Rn. 14.

70 *Europäischer Datenschutzausschuss*, Guidelines 3/2018 on the territorial scope of the GDPR, S. 13.

71 Vgl. Taeger/Gabel/*Schmidt*, Art. 3 DSGVO Rn. 13; Simitis/Hornung/Spiecker gen. Döhmann/*Hornung*, Art. 3 DSGVO Rn. 32, 62; *Europäischer Datenschutzausschuss*, Guidelines 3/2018 on the territorial scope of the GDPR, S. 9 und 11; a. A. BeckOK-DS/*Hanloser*, Art. 3 DSGVO Rn. 12, für den Fall, dass der Verantwortliche einen in der Union niedergelassenen Verarbeiter beauftragt.

Fällt der räumliche Anwendungsbereich bei mehreren Beteiligten auseinander, stellen sich einige Fragen im Hinblick auf die datenschutzrechtlichen Pflichten, die die einzelnen Beteiligten treffen.[72] **78**

Ist der räumliche Anwendungsbereich für den Verantwortlichen eröffnet, für seinen Auftragsverarbeiter jedoch nicht, sind die Abweichungen im Verhältnis zu der Situation, in der die DSGVO für beide anwendbar ist, dadurch abgemildert, dass der Verantwortliche jeden Auftragsverarbeiter gemäß Art 28 Abs. 3 DSGVO vertraglich umfangreich datenschutzrechtlich verpflichten muss. Zudem ist es in solchen Fällen wahrscheinlich, dass auch die Vorschriften zum internationalen Datenverkehr aus Kapitel V der DSGVO zur Anwendung kommen.[73] **79**

Ist die Situation umgekehrt, ist also der Auftragsverarbeiter im und der Verantwortliche außerhalb des Anwendungsbereichs, ergeben sich erhebliche Abweichungen. Zwar dürfte die Pflicht zum Abschluss eines Vertrages nach Art. 28 DSGVO den Auftragsverarbeiter grundsätzlich treffen. Dieser Vertrag muss aber nicht diejenigen Pflichten enthalten, die offensichtlich von der Anwendbarkeit der DSGVO auf den Verantwortlichen abhängen, wie z. B. die Pflicht zur Unterstützung der Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nach Art. 28 Abs. 3 lit. e DSGVO, da Betroffenenrechte gegenüber dem Verantwortlichen in einem solchen Fall nicht existieren. Letztlich ist in einem solchen Fall jede Pflicht, die den Auftragsverarbeiter trifft, dahingehend zu prüfen, ob sie von der Anwendbarkeit der DSGVO auf den Verantwortlichen abhängig ist oder in sonstiger Weise geprägt wird. Damit ist eine erhebliche Rechtsunsicherheit für den Auftragsverarbeiter verbunden. Besonders prägnant ist diese Unsicherheit im Hinblick auf die Pflichten aus Kapitel V der DSGVO. Stellt die weisungsgemäße Übermittlung personenbezogener Daten an den im Drittland ansässigen Verantwortlichen für den in der EU niedergelassenen Auftragsverarbeiter eine Drittlandübermittlung im Sinne des Kapitel V dar? Dies erscheint kaum interessengerecht, wird aber vertreten.[74] **80**

---

72 Vgl. hierzu insgesamt *Europäischer Datenschutzausschuss*, Guidelines 3/2018 on the territorial scope of the GDPR, S. 9 ff.

73 Vgl. *Europäischer Datenschutzausschuss*, Guidelines 3/2018 on the territorial scope of the GDPR, S. 9 und 10; Simitis/Hornung/Spiecker gen. Döhmann/*Hornung*, Art. 3 DSGVO Rn. 32.

74 Gegen eine Anwendbarkeit der Regeln aus Kapitel V: Kühling/Buchner/*Klar*, Art. 3 DSGVO Rn. 38. Dafür: Simitis/Hornung/Spiecker gen. Döhmann/*Hornung*, Art. 3 DSGVO Rn. 34; *Europäischer Datenschutzausschuss*, Guidelines 3/2018 on the territorial scope of the GDPR, S. 11.

4. Räumliche Reichweite der Betroffenenrechte

81 Vom räumlichen Anwendungsbereich der DSGVO ist die räumliche Reichweite der Betroffenenrechte zu unterscheiden. Zumindest für das Recht auf Vergessenwerden nach Art. 17 DGSVO im Verhältnis zum Betreiber einer Suchmaschine hat der EuGH – unter anderem gestützt auf die Erwägungsgründe 10, 11 und 13 – festgestellt, dass der Unionsgesetzgeber diesem Recht keine Reichweite verliehen hat, die über das Gebiet der Union hinausgeht.[75]

Praxishinweis

Die Auswirkungen dieser Rechtsprechung des EuGH in der Praxis sind nur schwer greifbar. Sie erscheinen zumindest in Fällen erwägenswert, in denen die grundsätzlich denkbare exterritoriale Wirkung der DSGVO augenscheinlich dem völkerrechtlichen Prinzip der Nichteinmischung zuwiderläuft.

5. Geltung der DSGVO im EWR

82 Mit Beschluss des EWR-Ausschusses wurde die DSGVO in das EWR-Abkommen aufgenommen und die DSRL gelöscht. Die DSGVO wirkt seit Inkrafttreten des Beschlusses am 20.7.2018 gemäß Art. 7 EWR-Abkommen in Island, Liechtenstein und Norwegen verbindlich als innerstaatliches Recht wie in den Mitgliedstaaten der EU. Der Beschluss nimmt eine Reihe notwendiger Anpassungen und Klarstellungen der DSGVO für die EFTA-Staaten vor. Unter anderem sieht er vor, dass die Aufsichtsbehörden der EFTA-Staaten zwar an den Tätigkeiten des Europäischen Datenschutzausschusses teilnehmen, sie haben jedoch kein Stimmrecht und sind nicht für den Vorsitz wählbar. Es wird zudem klargestellt, dass die Ausdrücke „Mitgliedstaat" und „Aufsichtsbehörde" neben ihrer Bedeutung in der DSGVO auch die EFTA-Staaten beziehungsweise ihre Aufsichtsbehörden umfassen.[76]

IV. Anwendungsbereich mitgliedstaatlicher Regelungen

83 Mit der Feststellung, dass die Verordnung anwendbar ist, ist die Prüfung des anwendbaren Datenschutzrechts in der Regel noch nicht abgeschlossen.

---

75 EuGH, Urt. v. 24.9.2019 – C-507/17, Rn. 54, 62.

76 Beschluss des gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6.7.2018 zur Änderung des Anhangs XI (Elektronische Kommunikation, audiovisuelle Dienste und Informationsgesellschaft) und des Protokolls 37 (mit der Liste gemäß Artikel 101) des EWR-Abkommens [2018/1022].

Denn das mit der Verordnung verfolgte **rechtspolitische Ziel** der Errichtung eines einheitlichen Datenschutzregimes in der EU ist nur teilweise erreicht worden. Die Verordnung beinhaltet an vielen Stellen **Öffnungsklauseln**, welche die Mitgliedstaaten dazu verpflichten bzw. ihnen gestatten, eigene nationale Regelungen zu treffen. Soweit sich eine Datenverarbeitung im Rahmen dieser Öffnungsklauseln bewegt, ist daher auch zu prüfen, welches mitgliedstaatliche Recht neben der Verordnung zur Anwendung kommt.[77] **84**

Eine allgemeine **Kollisionsnorm** wie in Art. 4 DSRL sucht man in der Verordnung vergebens. Es bleibt daher den Mitgliedstaaten überlassen, festzulegen, wann eine nationale Regelung gilt. **85**

Nationale Regelungen in Deutschland

Für öffentliche Stellen des Bundes und der Länder ergibt sich der sachliche Anwendungsbereich aus § 1 Abs. 1 S. 1, Abs. 8 BDSG bzw. aus den Landesdatenschutzgesetzen und der räumliche Anwendungsbereich aus § 1 Abs. 4 S. 1 BDSG. Für öffentliche Stellen ist der Anwendungsbereich gegenüber der DSGVO deutlich erweitert. Die Regelung in § 1 Abs. 8 BDSG dient daher dazu, die DSGVO für öffentliche Stellen insoweit für entsprechend anwendbar zu erklären. **86**

§ 1 Abs. 5 BDSG bestimmt deklaratorisch, dass das BDSG keine Anwendung findet, soweit EU-Recht und insbesondere die DSGVO unmittelbar gelten. **87**

Soweit dies nicht der Fall ist, ist das BDSG auf die Verarbeitung durch nichtöffentliche Stellen sachlich gemäß § 1 Abs. 1 S. 2 BDSG und persönlich und räumlich gemäß § 1 Abs. 4 S. 2 BDSG anwendbar. **88**

Zur Bestimmung des sachlichen Anwendungsbereichs für die Verarbeitung durch nichtöffentliche Stellen wiederholt § 1 Abs. 1 S. 2 BDSG den Wortlaut des Art. 2 Abs. 1 und kombiniert ihn mit dem Wortlaut der Haushaltsausnahme aus Art. 2 Abs. 2 lit. c). Zur Auslegung und Anwendung dieser Vorschrift kann daher auf die entsprechenden Ausführungen zu Art. 2 DSGVO verwiesen werden.[78] Zu beachten ist allerdings, dass das BDSG gemäß § 1 Abs. 2 S. 1 BDSG im Verhältnis zu anderen Rechtsvorschriften des Bundes (mit Ausnahme des VwVfG des Bundes, § 1 Abs. 3) subsidiär ist. **89**

Die Regelung zum persönlichen und räumlichen Anwendungsbereich des BDSG für nichtöffentliche Stellen in § 1 Abs. 4 BDSG darf als verunglückt bezeichnet werden und sieht sich teilweise dem Vorwurf ausgesetzt, europarechtswidrig zu sein.[79] **90**

77 Siehe zu den Öffnungsklauseln Kap. 1 Rn. 8.

78 Siehe oben Rn. 12 ff. und 24 ff.

79 Vgl. Simitis/Hornung/Spiecker gen. Döhmann/*Hornung*, Art. 3 DSGVO Rn. 10 ff. und 64.

91 § 1 Abs. 4 S. 2 Nr. 1 erklärt das BDSG unter Wiedereinführung des Territorialitätsprinzips für nichtöffentliche Stellen für anwendbar, wenn der Verantwortliche oder der Auftragsverarbeiter personenbezogene Daten im Inland verarbeitet, obwohl die DSGVO in Art. 3 und Erwägungsgrund 22 vom Kriterium des Ortes der Datenverarbeitung bewusst Abstand genommen hat.[80] Das Merkmal der „Verarbeitung im Inland" ist aus § 1 Abs. 5 S. 2 BDSG a. F. bekannt und wurde im Geltungszeitraum der Richtlinie richtlinienkonform dahingehend ausgelegt, dass die Belegenheit der Verarbeitungsmittel entscheidend ist. Da die richtlinienkonforme Auslegung entfällt, seit die Richtlinie nicht mehr gilt, ist unklar, ob der deutsche Gesetzgeber das Merkmal der „Verarbeitung im Inland" auch in Zukunft als „Belegenheit der Verarbeitungsmittel" verstanden wissen will. Die Gesetzesbegründung bietet hierüber keinen Aufschluss, da sie schon aufgrund offensichtlich fehlerhafter Bezugnahmen kaum verständlich ist und auch inhaltlich falsch zu sein scheint.[81]

92 § 1 Abs. 4 S. 2 Nr. 1 kann dazu führen, dass die DSGVO für nichtöffentliche Stellen zur Anwendung kommt, wo die Verordnung nicht anwendbar ist (z. B. aufgrund der Verwendung eines in Deutschland belegenen Servers für eine Datenverarbeitung ohne sonstigen Bezug zur EU). Insoweit wäre es ein eigenständiges mitgliedstaatliches Gesetz. Als solches könnte es unanwendbar sein, wenn der Unionsgesetzgeber mit Art. 3 DSGVO die räumliche Reichweite des Datenschutzrechts im Hinblick auf die Regelungsbereiche der Verordnung abschließend regeln wollte. Denn das Datenschutzrecht ist Gegenstand der geteilten Zuständigkeit zwischen der Union und den Mitgliedstaaten und es gilt gemäß Art. 2 Abs. 2 S. 2 AEUV, dass die Mitgliedstaaten nur gesetzgeberisch tätig werden können, sofern und soweit die Union ihre Zuständigkeit nicht ausgeübt hat.[82] Die Prüfung, ob ein solcher Fall gegeben ist, bedarf einer vertieften europarechtlichen Analyse und kann hier nicht vorgenommen werden.

93 Geht man in einem konkreten Fall davon aus, dass das BDSG aufgrund von § 1 Abs. 4 S. 2 Nr. 1 auf die Datenverarbeitung durch nichtöffentliche Stellen als eigenständiges mitgliedstaatliches Gesetz anwendbar ist, ergibt sich zudem das Problem, dass zur Rechtsfindung auf die Vorschriften der Verordnung nicht zurückgegriffen werden kann (§ 1 Abs. 8 BDSG gilt in diesem Fall nicht) und das BDSG damit lückenhaft und unverständlich bleibt. Ob das BDSG insoweit noch den aus dem Rechtsstaatsprinzip folgenden Geboten der Normenklarheit und Bestimmtheit entspricht, darf bezweifelt werden.

---

80 BeckOK-DS/*Gusy/Eichenhofer*, § 1 BDSG Rn. 101a.

81 In der Begründung steht zum Beispiel, dass § 1 Abs. 4 S. 1 (sic) Nr. 3 BDSG (2018) dem § 1 Abs. 5 S. 2 BDSG (bis 2018) entspricht, BT-Drs. 18/11325 S. 80. Selbst wenn man dies als eine Bezugnahme auf § 1 Abs. 4 S. 2 Nr. 3 BDSG (2018) umdeutet, ist diese Aussage inhaltlich offensichtlich falsch.

82 Vgl. Calliess/Ruffert/*Calliess*, Art. 2 AEUV Rn. 13 ff.

Nach § 1 Abs. 4 S. 2 Nr. 2 ist das BDSG für nicht-öffentliche Stellen räumlich anwendbar, sofern die Verarbeitung der Daten im Rahmen der Tätigkeiten einer inländischen Niederlassung des Verantwortlichen oder Auftragnehmers erfolgt. Dies entspricht im Wesentlichen der Regelung des Art. 3 Abs. 1 DSGVO unter Beschränkung auf Niederlassungen in Deutschland. Zur Auslegung und Anwendung dieser Vorschrift kann daher auf die entsprechenden Ausführungen zu Art. 3 Abs. 1 DSGVO verwiesen werden.[83] **94**

Nach § 1 Abs. 4 S. 2 Nr. 3 ist das BDSG für nicht-öffentliche Stellen, die nicht in der Union und nicht im Europäischen Wirtschaftsraum niedergelassen sind, anwendbar, sofern sie in den Anwendungsbereich der Verordnung fallen. **95**

Auch wenn es an einer ausdrücklichen Bezugnahme fehlt, ist dies im Ergebnis ein Rechtsgrundverweis auf Art. 3 Abs. 2 und Abs. 3 DSGVO. Zur Auslegung und Anwendung dieser Vorschrift kann daher auf die entsprechenden Ausführungen zu Art. 3 Abs. 2 DSGVO verwiesen werden.[84] In der Praxis ist in erster Linie die Bezugnahme auf das in Art. 3 Abs. 2 Nr. 1 und 2 DSGVO beschriebene Marktortprinzip von Bedeutung.[85] **96**

Im Gegensatz zu § 1 Abs. 4 S. 2 Nr. 1 und 2 BDSG hat der Gesetzgeber bei § 1 Abs. 4 S. 2 Nr. 3 BDSG keine Einschränkung auf das Inland und somit keine Beschränkung auf Deutschland als Marktort vorgenommen. Weder muss sich die betroffene Person in Deutschland befinden, noch muss sich das Angebot von Waren und Dienstleistungen an Personen in Deutschland richten. Auch beobachtetes Verhalten muss nicht in Deutschland erfolgen. Solange die territorialen Anknüpfungspunkte in Art. 3 Abs. 2 DSGVO für irgendeinen Mitgliedstaat der Union gegeben sind, soll das BDSG gemäß § 1 Abs. 4 S. 2 Nr. 3 gelten. Dies führt zu offensichtlich unangemessenen Ergebnissen.[86] Eine Kollision mit den Datenschutzgesetzen anderer Mitgliedstaaten ist vorprogrammiert. So hat eine konsequente Anwendung von § 1 Abs. 4 S. 2 Nr. 3 BDSG i.V.m. Art. 3 Abs. 2 lit. a DSGVO zum Beispiel zur Folge, dass für die Datenverarbeitung durch ein in Argentinien niedergelassenes Unternehmen im Zusammenhang mit einem Angebot, welches sich ausschließlich an Perso- **97**

83 Siehe oben Rn. 34 ff.

84 Siehe oben Rn. 49 ff.

85 Eine Anwendbarkeit der Verordnung auf nicht-öffentliche Stellen nach Art. 3 Abs. 3 DSGVO wird in der Praxis nur vorkommen, wenn eine nicht-öffentliche Stelle Daten am Ort einer diplomatischen oder konsularischen Vertretung eines EU-Mitgliedstaates außerhalb der EU verarbeitet (vgl. Erwägungsgrund 25). Kurioserweise würde bei unkritischer Anwendung des § 1 Abs. 4 S. 2 Nr. 3 BDSG (2018) i.V.m. Art. 3 Abs. 3 DSGVO z. B. für die Datenverarbeitung eines peruanischen Unternehmens in der französischen Botschaft in Lima das BDSG (2018) gelten.

86 So auch Simitis/Hornung/Spiecker gen. Döhmann/*Hornung*, Art. 3 DSGVO Rn. 15.

nen in Spanien richtet, das BDSG zu beachten wäre. Das spanische Datenschutzrecht wird in diesem Fall jedoch ebenfalls gelten.

98 Die geschilderten Anwendungsprobleme im Zusammenhang mit § 1 Abs. 4 S. 2 Nr. 1 und Nr. 3 BDSG können vorliegend nicht abschließend begutachtet werden. Der Praktiker, der hiervon betroffen ist, sollte die Bewertung dieser Probleme durch Literatur, Rechtsprechung und Verwaltungspraxis im Auge behalten.

99 Ein kursorischer Blick auf die Umsetzungs- und Ergänzungsgesetze anderer Mitgliedstaaten reicht, um festzustellen, dass für verarbeitende Stellen hinter den Vorschriften der Verordnung wie bereits im Geltungszeitraum der Richtlinie ein Dickicht von mitgliedstaatlichen Datenschutzgesetzen liegt deren Anwendbarkeit im Einzelfall zu prüfen ist.

V. Anwendungsbereich sonstiger ausfüllender Normen

100 Neben mitgliedstaatlichen Datenschutzgesetzen können andere mitgliedstaatliche Normen für die datenschutzrechtliche Beurteilung relevant werden.

101 So stellt zum Beispiel Art. 6 Abs. 1 lit. c DSGVO im Sinne einer **Rechtsgrundverweisung** auf die Erfüllung einer rechtlichen Verpflichtung ab, „der der Verantwortliche unterliegt".[87]

102 Auch für die Wirksamkeit einer datenschutzrechtlichen **Einwilligung** wird in Sondersituationen auf mitgliedstaatliches Recht verwiesen. Dies ist bei der Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft nach Art. 8 Abs. 1 S. 3 DSGVO und bei der Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 2 lit. a DSGVO der Fall.

103 Diese ergänzenden Normen folgen ihren eigenen Anwendbarkeitsregeln, die im Einzelfall zu prüfen sind.

87 Siehe auch Art. 14 Abs. 5 lit. c und 28 Abs. 3 lit. a DSGVO, die ähnliche Verweise enthalten.

Kapitel 4

Datenschutzrechtliche Grundsätze

Übersicht

	Rn.
I. Bedeutung und Funktion der Datenschutzgrundsätze	1
II. Die Grundsätze im Einzelnen	4
1. Rechtmäßigkeit und Verarbeitung nach Treu und Glauben	4
2. Transparenz	7
3. Zweckbindung	10
4. Datenminimierung	15
5. Datenrichtigkeit	16
6. Speicherbegrenzung	20
7. Integrität und Vertraulichkeit	23
III. Die Rechenschaftspflicht	27

I. Bedeutung und Funktion der Datenschutzgrundsätze

Das Datenschutzrecht ist geprägt von mehreren fundamentalen Grundsätzen, die sozusagen das **Leitbild des Gesetzgebers** bildeten für die Ausgestaltung der datenschutzrechtlichen Pflichten. Diese Grundsätze liegen deshalb sämtlichen einzelnen in der DSGVO (und auch den Begleitgesetzen und den bereichsspezifischen Sondervorschriften) enthaltenen Pflichten zugrunde. **1**

Der EU-Gesetzgeber hat diesen Grundsätzen mit Art. 5 DSGVO eine eigenständige Vorschrift gewidmet und sie dadurch quasi „vor die Klammer" gezogen.[1] Für diejenigen, die sich erstmals mit dem Datenschutzrecht beschäftigen, bietet Art. 5 DSGVO deshalb eine gute Einstiegslektüre – beschreibt er doch in Kurzform den Pflichtenkanon nach der DSGVO. **2**

Beispiel

In Art. 5 Abs. 1 lit. a DSGVO ist der **Grundsatz der „Rechtmäßigkeit"** festgeschrieben – dieser bildet die Grundlage für die spezifischen Vorschriften, die Details dazu regeln, wann eine Verarbeitung personenbezogener Daten erlaubt ist, also insbesondere Art. 6 DSGVO, der konkrete Bedingungen für die Zulässigkeit einer Datenverarbeitung normiert.

Diese Verarbeitungsgrundsätze haben gleichwohl eine Praxisrelevanz: So messen die Gerichte diesen Grundsätzen bei ihren Entscheidungen durchaus Bedeutung zu. In einer Entscheidung des LG Bonn[2] sind sie für das Gericht sogar **3**

1 Vgl. *Strassemeyer*, K&R 2020, 176, 177.

Hauptprüfungsmaßstab für die Frage der Zulässigkeit der streitgegenständlichen Datenerhebungen. Dies ist Beleg dafür, dass einigen dieser Grundsätze unter der DSGVO ein stärkeres Gewicht zukommt als nach dem BDSG a. F. – namentlich z. B. dem Grundsatz der Datenminimierung (auch wenn das Gericht hier noch den „alten" Begriff der Datensparsamkeit nach § 3a BDSG a. F. verwendet), der nach altem Recht als reiner Programmsatz kaum rechtliche Konsequenzen nach sich gezogen hätte.

II. Die Grundsätze im Einzelnen

1. Rechtmäßigkeit und Verarbeitung nach Treu und Glauben

4 Die Prinzipien der Rechtmäßigkeit gemäß Art. 5 Abs. 1 lit. a Var. 1 DSGVO und der Verarbeitung nach Treu und Glauben gemäß Art. 5 Abs. 1 lit. a Var. 2 DSGVO prägen die **Struktur der DSGVO** in besonderem Maße. Wegen des Grundsatzes der Rechtmäßigkeit bedarf jede Datenverarbeitung einer **Rechtsgrundlage** i. S. d. Art. 6 Abs. 1 S. 1 DSGVO.[3] Dieser Rechtsgedanke wird „**Verbot mit Erlaubnisvorbehalt**" genannt – grundsätzlich ist deshalb jede Verarbeitung verboten, soweit nach Art. 6 Abs. 1 DSGVO (oder einer anderen Rechtsvorschrift) keine Erlaubnis existiert.

5 Zu den häufigsten Rechtfertigungsgründen gehören die **Einwilligung** gemäß Art. 6 Abs. 1 lit. a DSGVO, die Erfüllung des **Vertragszwecks** nach Art. 6 Abs. 1 lit. b DSGVO sowie die Verarbeitung aus Gründen **berechtigter Interessen** gemäß Art. 6 Abs. 1 lit. f DSGVO.[4] In Sonderkonstellationen müssen dabei zusätzliche Rechtmäßigkeitsanforderungen eingehalten werden, etwa die Voraussetzungen an die Rechtmäßigkeit einer (wirksamen) Einwilligung (Art. 4 Nr. 11, Art. 7 DSGVO), die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) und/oder die Übermittlung in Drittländer (Art. 44 ff. DSGVO).[5]

6 Eine genauere Definition des Bedeutungsgehalts der Verarbeitung nach **Treu und Glauben** gemäß Art. 5 Abs. 1 lit. a Var. 2 DSGVO existiert nicht.[6] Allerdings lassen sich aus dem inhärenten Fairnessgebot verschiedene für die Praxis relevante **Fallgruppen potenzieller Verstöße** bilden, die eine Annäherung er-

2 LG Bonn, Beschl. v. 29.5.2018 – 10 O 171/18, ZD 2018, 588.

3 Taeger/Gabel/*Voigt*, Art. 5 DSGVO Rn. 10.

4 Zu den Rechtfertigungsgründen siehe Kap. 5.

5 Taeger/Gabel/*Voigt*, Art. 5 DSGVO Rn. 10; siehe im Einzelnen zur Einwilligung auch Kap. 5 Rn. 243 und Kap. 19 Rn. 81; zu besonderen Kategorien personenbezogener Daten auch Kap. 5 Rn. 303; und zur Drittstaatenübermittlung auch Kap. 9 Rn. 123 und Kap. 19 Rn. 107.

6 Kühling/Buchner/*Herbst*, Art. 5 DSGVO Rn. 13; Taeger/*Piltz/Quiel*, DSRITB 2021, S. 1, 7.

möglichen: Grundsätzlich ist eine „faire" Datenverarbeitung gegeben, wenn durch den Verantwortlichen oder Auftragsverarbeiter keine unzulässige Rechtsausübung zu einem beachtlichen Nachteil des Betroffenen stattfindet.[7]

Beispiel

Verstöße gegen das **Fairnessgebot** liegen beispielsweise vor, soweit

- der Umfang der Verarbeitung personenbezogener Daten die durch den Verantwortlichen geweckten Erwartungen des Betroffenen massiv übersteigt – etwa bei heimlichen Verarbeitungen;[8]
- Wertungen der Europäischen Grundrechtecharta unterminiert werden;
- die vernünftigen Erwartungen der betroffenen Personen i. S. v. Art. 6 Abs. 1 lit. f DSGVO unberücksichtigt bleiben;
- das (allgemeine) Kopplungsverbot nach Art. 7 Abs. 4 DSGVO missachtet wird[9] und/oder
- die Abhängigkeit im Beschäftigungsverhältnis unberücksichtigt bleibt.[10]

Denkbare Anwendungsfälle können sich aus dem Einsatz bzw. der Verknüpfung verschiedener (innovativer) Technologien oder auch aus unvorhersehbaren Zweckänderungen ergeben. Ein aktuelles Beispiel kann etwa die überraschende Nutzung sog. Corona-Listen für polizeiliche Ermittlungszwecke, entgegen dem Wortlaut von Sperrklauseln in einigen Bundesländern sein.[11]

Insgesamt stellt der Grundsatz von Treu und Glauben eher einen **Auffangtatbestand** dar, der Konstellationen erfasst, in denen der Betroffene durch eine Verarbeitung seiner personenbezogenen Daten einen erheblichen Nachteil erfährt, der in einem massiven Widerspruch zum Kräftegleichgewicht des Verantwortlichen steht – (auch) unabhängig von einem Verstoß gegen ein gesetzliches Verbot.[12] Dementsprechend wird die Prüfung dieses Grundsatzes in der Praxis eher einen Ausnahmefall bilden.

---

7 Taeger/Gabel/*Voigt*, Art. 5 DSGVO Rn. 14.

8 Kühling/Buchner/*Herbst*, Art. 5 DSGVO Rn. 15; dahingehend auch *EDSA*, Guidelines 8/2020 Rn. 9 ff.

9 Anzumerken sei jedoch, dass die DSGVO kein absolutes Kopplungsverbot vorsieht, vgl. *Moos/Strassemeyer*, DSB 2020, 207, 208; siehe auch Kap. 17 Rn. 84.

10 Taeger/Gabel/*Voigt*, Art. 5 DSGVO Rn. 14 f.

11 Siehe dazu Pressemitteilung des Datenschutzbeauftragten von Rheinland-Pfalz, http://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/polizei-sollte-auf-corona-gaestelisten-nur-mit-richterlichem-beschluss-zugreifen-kugelmann-es-muss/, zuletzt abgerufen am 6.2.2021; Pressemitteilung Redaktion beck-aktuell, Regierung hält Gesetz für Polizei-Zugriff auf Corona-Gästelisten nicht für erforderlich, becklink 2017097.

12 Paal/Pauly/*Frenzel*, Art. 5 DSGVO Rn. 20; Auernhammer/*Kramer*, Art. 5 DSGVO Rn. 8–10; Kühling/Buchner/*Herbst*, Art. 5 DSGVO Rn. 17.

2. Transparenz

7 Das Transparenzgebot ist in Art. 5 Abs. 1 lit. a Var. 3 DSGVO statuiert.[13] Es legt fest, dass personenbezogene Daten in einer **für den Betroffenen nachvollziehbaren Art und Weise** verarbeitet werden müssen.[14]

8 Der Betroffene muss die Möglichkeit haben, sich auf Grundlage der zur Verfügung gestellten Informationen eigenständig für oder gegen die Verarbeitung und den jeweiligen Inhalt entscheiden zu können.[15] Eine Konkretisierung erfährt der Grundsatz insbesondere durch Erwägungsgrund 39 zur DSGVO, der bestimmt, dass Informationen und Mitteilungen zur Verarbeitung personenbezogener Daten in folgender Weise zur Verfügung gestellt werden müssen:

- leicht zugänglich,
- verständlich,
- in klarer und einfacher Sprache.[16]

9 Als Ausfluss des Transparenzgebots normieren vor allem die **Informations- und Auskunftspflichten** in den Art. 12–22 DSGVO, insbesondere Art. 13, 14 und 15 DSGVO konkretere Pflichten für den Verantwortlichen.[17]

3. Zweckbindung

10 Der Zweckbindungsgrundsatz gemäß Art. 5 Abs. 1 lit. b DSGVO ist ebenfalls von besonders hervorgehobener Bedeutung:[18] Danach dürfen personenbezogene Daten ausschließlich für die bei der Erhebung **festgelegten**, **eindeutigen** und **legitimen** Zwecke verarbeitet werden. Im Kern bedeutet dies, dass eine Datenerhebung quasi „auf Vorrat" unzulässig ist, weil hier ein Zweck bei der Erhebung noch nicht feststeht sondern erst nachträglich bestimmt werden soll.

11 Der Verantwortliche muss die Zwecke ausdrücklich festlegen, was einem Akt der Selbstbindung gleichkommt.[19] Dies muss bereits **vor dem Verarbeitungs-**

---

13 Dies wurde zuvor unter der DSRL ausschließlich unter Heranziehung des Grundsatzes von Treu und Glauben abgeleitet.

14 Paal/Pauly/*Frenzel*, Art. 5 DSGVO Rn. 21.

15 BeckOK-DS/*Wolff*, Syst. A. Rn. 69.

16 Taeger/Gabel/*Voigt*, Art. 5 DSGVO Rn. 17; siehe für eine umfassende Einordnung dieser Vorgaben auch *Strassemeyer*, K&R 2020, 176, 177 ff.

17 Taeger/Gabel/*Voigt*, Art. 5 DSGVO Rn. 18; zu den Betroffenenrechten siehe Kap. 6.

18 Der Zweckbindungsgrundsatz ist größtenteils kein Novum. Er ist ein Ausdruck des sog. Volkszählungsurteils des Bundesverfassungsgerichts (vgl. BVerfGE 65, 146) und fand sich bereits fast wortgleich in Art. 6 Abs. 1 lit. b S. 1 DSRL und in ähnlicher Form auch in Art. 8 Abs. 2 S. 1 GRCh, siehe dazu Kühling/Buchner/*Herbst*, Art. 5 DSGVO Rn. 20 f.

19 Paal/Pauly/*Frenzel*, Art. 5 DSGVO Rn. 27; siehe auch BeckOK-DS/*Wolff*, Syst. A. Rn. 24 f., der auch eine konkludente Festlegung für ausreichend erachtet.

vorgang geschehen und erfordert deshalb einige Vorüberlegungen.[20] Unbestimmte oder unzulässige Zwecke genügen mithin den Anforderungen an eine Festlegung nicht.[21]

Aus der Eindeutigkeit folgt die Notwendigkeit der **Konkretisierung** der jeweiligen Zwecke, indem sie ausdrücklich bezeichnet und inhaltlich hinreichend bestimmt werden.[22] Zwar ist keine bestimmte Form festgelegt, es empfiehlt sich aber eine schriftliche Dokumentation, die eine Nachweisfunktion erfüllen kann.[23] Der Begriff „eindeutig" bedeutet jedoch nicht, dass jeweils nur ein einziger Verarbeitungszweck festgelegt werden darf.[24] Es ist deshalb zulässig, von vornherein auch eine Mehrzahl von Zwecken festzulegen, soweit diese sämtlich hinreichend bestimmt sind.[25] **12**

Der Verarbeitungszweck ist **legitim**, soweit für ihn eine geeignete Rechtsgrundlage existiert und er nicht im Widerspruch zu einer geltenden Rechtsnorm steht.[26] **13**

Schließlich gilt für Verarbeitungen, die nicht 1:1 den ursprünglichen Erhebungszwecken entsprechen, dass sie nicht von vornherein unzulässig sind – sie müssen aber zumindest mit ihnen kompatibel sein.[27] Die **Kompatibilität** der Zwecke ist u. a. an den Kriterien aus Art. 6 Abs. 4 DSGVO zu messen,[28] die Aufschluss darüber geben, ob die (Weiter-)Verarbeitung zu einem anderen Zweck mit dem ursprünglichen Erhebungszweck vereinbar ist.[29] Soweit der Kompatibilitätstest negativ ausfällt, ist eine Weiterverarbeitung ohne Einwilligung ausgeschlossen.[30] **14**

Grundsätzlich möglich ist es aber, dass der Verantwortliche von der ursprünglichen Zwecksetzung abweicht, allerdings nur, wenn der neue Weiterverarbeitungszweck mit dem anfänglich festgelegten Zweck gemäß Art. 6 Abs. 4 DSGVO **kompatibel** ist, eine Rechtsvorschrift die **Zweckänderung** ausdrücklich zulässt oder eine dahingehende Einwilligung des Betroffenen vorliegt. **15**

---

20 ErwG 39 S. 6 DSGVO; Schantz/Wolff//*Wolff*, Rn. 401.
21 Schantz/Wolff//*Wolff*, Rn. 401.
22 Kühling/Buchner/*Herbst*, Art. 5 DSGVO Rn. 32.
23 Kühling/Buchner/*Herbst*, Art. 5 DSGVO Rn. 35.
24 Kühling/Buchner/*Herbst*, Art. 5 DSGVO Rn. 35.
25 Kühling/Buchner/*Herbst*, Art. 5 DSGVO Rn. 36.
26 Siehe bereits für die DSRL *Art.-29-Datenschutzgruppe*, WP 203, S. 19 f.; Kühling/Buchner/*Herbst*, Art. 5 DSGVO Rn. 37.
27 Schantz/Wolff/*Wolff*, Rn. 401.
28 Taeger/Gabel/*Voigt*, Art. 5 DSGVO Rn. 26; ausführlich zur Weiterverarbeitung siehe Kap. 5 Rn. 137.
29 Taeger/Gabel/*Voigt*, Art. 5 DSGVO Rn. 26; ausführlich zur Weiterverarbeitung siehe Kap. 5 Rn. 137.
30 ErwG 50 S. 1 DSGVO.

4. Datenminimierung

16 Der Datenminimierungsgrundsatz ist in Art. 5 Abs. 1 lit. c DSGVO niedergelegt. Er verlangt, dass der Umfang der verarbeiteten personenbezogenen Daten für den jeweiligen Zweck **angemessen**, **erheblich** und auf **das notwendige Maß** beschränkt ist. Die Anzahl der Verarbeitungsvorgänge ist hiernach aber nicht notwendigerweise zu beschränken.

Praxishinweis

Für die Überprüfung, ob die Verarbeitung dem Grundsatz der Datenminimierung gerecht wird, bietet sich eine vierstufige Prüfung an:[31]

- Ist die Verwendung anonymisierter Daten möglich?
- Sind die Daten dem Zweck angemessen?
- Sind die Daten für den Zweck erheblich?
- Sind die Daten auf ein notwendiges Maß beschränkt worden?

Die Datenmenge sollte auf das Maß beschränkt werden, das für die Zweckerreichung notwendig ist. Zudem sollte darauf geachtet werden, dass die Begrenzung auf ein notwendiges Maß auch die Genauigkeit personenbezogener Daten umfasst. Soweit also der Zweck der Verarbeitung durch aggregierte Daten erreicht werden kann, sollte dies auch geschehen.

5. Datenrichtigkeit

17 Das Gebot der Datenrichtigkeit ist in Art. 5 Abs. 1 lit. d DSGVO verankert. Danach muss der Verantwortliche darauf achten, dass personenbezogene Daten **sachlich richtig** und erforderlichenfalls **auf dem neuesten Stand** sind, damit sie die Realität repräsentieren.[32] Die personenbezogenen Daten sollen so den Betroffenen und dessen Verhältnisse korrekt widerspiegeln.[33]

18 Aus dem Grundsatz folgen unterschiedliche Gebote, abhängig von der einzelnen Verarbeitungsphase (erstmalige Erhebung und Speicherung oder die spätere Kontrolle):[34] Bereits bei der erstmaligen Speicherung muss der Verantwortliche die personenbezogenen Daten aktiv[35] auf Richtigkeit überprüfen.[36] Dies beinhal-

31 Vgl. Kühling/Buchner/*Herbst*, Art. 5 DSGVO Rn. 57.
32 BeckOK-DS/*Wolff*, Syst. A. Rn. 70; Paal/Pauly/*Frenzel*, Art. 5 DSGVO Rn. 39.
33 *Albrecht/Jotzo*, Teil 2 Rn. 10.
34 BeckOK-DS/*Wolff*, Syst. A. Rn. 71.
35 Gola/*Pötters*, DSGVO Art. 5 Rn. 24.
36 BeckOK-DS/*Wolff*, Syst. A. Rn. 71.

tet eine der üblichen Sorgfalt entsprechende Prüfung, ob Gesichtspunkte gegen die Richtigkeit sprechen.[37]

19 Wird zu einem späteren Zeitpunkt die Unrichtigkeit ersichtlich, muss der Verantwortliche die betroffenen Daten löschen oder korrigieren.[38] Art. 5 Abs. 1 lit. d DSGVO verlangt den Einsatz angemessener Überprüfungsmittel.[39] Im Falle einer längerfristigen Verarbeitung nehmen die Anforderungen an die Prüfung der sachlichen Richtigkeit zu, da das Risiko für eine Änderung des tatsächlichen Zustands steigt.[40]

20 Auch aus der eigenen Perspektive des Verantwortlichen ist die Richtigkeit der Daten in zweierlei Hinsicht bedeutsam: Einerseits können oft nur korrekte Daten den gewünschten wirtschaftlichen Erfolg und die pflichtgemäße Aufgabenerfüllung herbeiführen.[41] Anderseits steigern unrichtige Daten die Gefahr, dass Betroffene ihren Anspruch auf Berichtigung und Vervollständigung gemäß Art. 16 DSGVO geltend machen.[42] Zudem kann der Betroffene die Richtigkeit der Daten gemäß Art. 18 Abs. 1 lit. a DSGVO bestreiten und die Einschränkung der Datenverarbeitung i. S. d. Art. 4 Nr. 3 DSGVO verlangen, bis dieser die Richtigkeit der Daten nachweist.[43]

Praxishinweis

Soweit Daten sich auf einen bestimmten Zeitpunkt beziehen, werden sie nicht zwangsläufig dadurch falsch, dass sich die Verhältnisse des Betroffenen geändert haben.[44] Es sollte im Hinblick auf den Verarbeitungszweck differenziert werden:[45] Dies wird im Zusammenhang etwa mit Gesundheitsdaten, die bei einer Untersuchung gespeichert werden, deutlich. Dort ist es denkbar, dass es der Verarbeitungszweck gebietet, diese Daten trotz Veränderung des Gesundheitszustands nicht zu korrigieren. Umgekehrt kann der Verarbeitungszweck die Aktualität der Daten aber auch wesensnotwendig voraussetzen, wie etwa bei der Speicherung von Zutrittsberechtigungen oder finanziellen Verhältnissen in Hinblick auf eine Kreditgewährung.

37 BeckOK-DS/*Wolff*, Syst. A. Rn. 71.
38 *Albrecht/Jotzo*, Teil 2 Rn. 11.
39 BeckOK-DS/*Wolff*, Syst. A. Rn. 71.
40 Paal/Pauly/*Frenzel*, Art. 5 DSGVO Rn. 39.
41 Simitis/Hornung/Spiecker gen. Döhmann/*Roßnagel*, Art. 5 DSGVO Rn. 137; *Hoeren*, ZD 2016, 459.
42 Siehe hierzu auch Kap. 6 Rn. 343 ff.
43 *Albrecht/Jotzo*, Teil 2 Rn. 11.
44 *Albrecht/Jotzo*, Teil 2 Rn. 11.
45 Taeger/Gabel/*Voigt*, Art. 5 DSGVO Rn. 31.

6. Speicherbegrenzung

21 Der Grundsatz der Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. e DSGVO statuiert, dass personenbezogene Daten „*in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist*". Die DSGVO schreibt somit ein **zeitliches Limit für die Speicherung personenbezogener Daten** bis zur Zweckerreichung vor.[46] Die Speicherbegrenzung und der Grundsatz der Zweckbindung nach Art. 5 Abs. 1 lit. b DSGVO greifen ineinander. Der bereits angelegte Zweck bekommt eine Art „Haltbarkeitsdatum".[47] Jedenfalls bereits anonymisierte Daten sind – schon denklogisch aufgrund des Anwendungsbereichs in Art. 2 Abs. 1 DSGVO – von der Speicherbegrenzung ausgenommen. Eine Identifizierung Betroffener ist hierdurch ohnehin ausgeschlossen.[48]

Praxishinweis

Verantwortliche sollten deshalb für alle personenbezogenen Daten oder Datenkategorien eine Speicherfrist festlegen. Differenziert werden sollte zwischen einerseits der Zweckerreichung und andererseits den gesetzlich statuierten Aufbewahrungsfristen. Im Falle einer Aufbewahrung ausschließlich aus Gründen von Aufbewahrungsfristen empfiehlt es sich, technische und organisatorische Maßnahmen zu ergreifen, die eine anderweitige Verarbeitung verhindern.[49] Zudem sollte der Verantwortliche Fristen oder iterative Zeiträume für eine Überprüfung der Daten implementieren.[50] In der Regel erfolgt dies im Rahmen eines übergreifenden **Löschkonzepts**.[51]

22 Die Speicherbegrenzung bedingt u. a. die folgenden weiteren Pflichten des Verantwortlichen: die Pflicht zur (aktiven) Aufklärung des Betroffenen über die jeweilige Verarbeitungsdauer gemäß Art. 13 Abs. 2 lit. a bzw. 14 Abs. 2 lit. a DSGVO, die Pflicht auf Antrag zur erneuten, ggf. konkretisierten Benennung der Verarbeitungsdauer gemäß Art. 15 Abs. 1 lit. d DSGVO, die Pflicht zur Löschung gemäß Art. 17 Abs. 1 lit. a DSGVO oder Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 DSGVO nach entsprechendem Verlangen des Betroffenen.

---

46 Kühling/Buchner/*Herbst*, Art. 5 DSGVO Rn. 64.

47 Kühling/Buchner/*Herbst*, Art. 5 DSGVO Rn. 65.

48 Ausführlich zum Personenbezug siehe Kap. 2 Rn. 10 und Kap. 19 Rn. 21; siehe auch Simitis/Hornung/Spiecker gen. Döhmann/*Roßnagel*, Art. 5 DSGVO Rn. 155, der sogar Pseudonymisierungsmaßnahmen ausreichen lässt.

49 Simitis/Hornung/Spiecker gen. Döhmann/*Roßnagel*, Art. 5 DSGVO Rn. 159.

50 Simitis/Hornung/Spiecker gen. Döhmann/*Roßnagel*, Art. 5 DSGVO Rn. 159; Erwägungsgrund 39 S. 9 DSGVO.

51 Siehe dazu Kap. 12 Rn. 36.

Ausnahmen vom Grundsatz normiert Art. 5 Abs. 1 lit. e Hs. 2 DSGVO, der Verarbeitungen für im öffentlichen Interesse liegende **Archivzwecke**, für Zwecke der **wissenschaftlichen** und **historischen Forschung** und **statistische Zwecke** privilegiert. Bei einem entsprechenden Zweck ist weder dem Speicherbegrenzungs- noch dem Zweckbindungsgrundsatz Rechnung zu tragen. **23**

7. Integrität und Vertraulichkeit

Nach dem Grundsatz der Integrität und Vertraulichkeit gemäß Art. 5 Abs. 1 lit. f DSGVO müssen personenbezogene Daten zur Abwendung bestimmter Risiken in einer Weise verarbeitet werden, die eine **angemessene Sicherheit** der personenbezogenen Daten gewährleistet. Der Grundsatz hängt deshalb eng mit Art. 24 und Art. 32 DSGVO zusammen und verlangt vom Verantwortlichen entsprechende technische und organisatorische Maßnahmen.[52] **24**

Die Maßnahmen sollen insbesondere folgende zwei Kategorien von Risiken verhindern:[53] Zum einen soll eine **unbefugte** oder **unrechtmäßige Verarbeitung** verhindert werden. Eine unbefugte Verarbeitung liegt insbesondere dann vor, wenn die Verarbeitung durch unbefugte Dritte gemäß Art. 4 Nr. 10 DSGVO erfolgt; eine unrechtmäßige Verarbeitung ist etwa im Falle eines Verstoßes gegen den Rechtmäßigkeits- und Zweckbindungsgrundsatz gegeben. Zum anderen soll ein **unbeabsichtigter Verlust**, die **unbeabsichtigte Zerstörung** und **Schädigung** verhindert werden. Ein Verlust, die Zerstörung oder Schädigung ist gegeben, wenn personenbezogene Daten „[…] *abhandenkommen oder derart geändert werden, dass sie nicht mehr oder nur noch eingeschränkt für den vorgesehenen Zweck verarbeitet werden können*“.[54] **25**

Weiterhin soll der Grundsatz für **Datensicherheit** und eine lückenlos funktionierende IT-Infrastruktur sorgen. Primär verlangt Art. 5 Abs. 1 lit. f DSGVO deshalb vom Verantwortlichen, stets den Risiken und dem Stand der Technik entsprechende geeignete technische und organisatorische Maßnahmen zur Datensicherheit zu ergreifen.[55] Vor allem fortschreitende technische Entwicklungen verlangen deshalb bei zeitlich umfassenden Verarbeitungshandlungen iterative Überprüfungen der Risiken für Betroffene durch die zu verarbeitenden Daten im Verhältnis zu den eingesetzten Gegenmaßnahmen. **26**

---

52 Siehe hierzu im Einzelnen Kap. 13.

53 Kühling/Buchner/*Herbst*, Art. 5 DSGVO Rn. 73 ff.; es wird darauf hingewiesen, dass die genannten Risiken jedoch nicht abschließend sind. Dies verdeutlicht der Wortlaut „einschließlich“ in Art. 5 Abs. 1 lit. f DSGVO.

54 Kühling/Buchner/*Herbst*, Art. 5 DSGVO Rn. 75.

55 Ausführlich zu technischen und organisatorischen Maßnahmen siehe Kap. 13.

27 Welche Anforderungen im Detail an technische und organisatorische Schutzmaßnahmen zu stellen sind, wird insbesondere durch Erwägungsgrund 39 S. 12 DSGVO,[56] Art. 32 DSGVO[57] und Art. 25 DSGVO[58] konkretisiert.

III. Die Rechenschaftspflicht

28 Die Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO bedeutet, dass der Verantwortliche die Einhaltung der Grundsätze aus Art. 5 Abs. 1 DSGVO auch **nachweisen** kann.[59]

29 Aus dem Grundsatz folgt i.R.v. Art. 5 Abs. 2 Hs. 1 DSGVO zunächst, dass der Verantwortliche dafür Sorge zu tragen hat, dass die **Grundsätze aus Art. 5 Abs. 1 DSGVO eingehalten** werden. Dabei muss der Verantwortliche insbesondere die Anforderungen aus Art. 24 DSGVO umsetzen:[60] Art. 24 Abs. 1 DSGVO bestimmt dabei, dass Art und Umfang der bereitzustellenden Maßnahmen anhand einer **Risikoanalyse** festzumachen sind und diese Maßnahmen überprüft und aktualisiert werden müssen. Zusätzlich wird in Art. 24 Abs. 2 DSGVO auf den Anspruch an ein **umfassendes Datenschutzmanagement**[61] hingewiesen.

30 Die **Nachweispflicht** fordert eine Dokumentation der Verarbeitung und derjenigen Maßnahmen, durch die die Grundsätze jeweils eingehalten werden. Besonders im Zusammenhang mit **aufsichtsbehördlichen Überprüfungen** erlangt die Pflicht Bedeutung: Gemäß Art. 58 Abs. 1 lit. a DSGVO können Aufsichtsbehörden den Verantwortlichen zur Bereitstellung von entsprechenden Informationen anweisen.[62] Soweit der Verantwortliche die Einhaltung der Grundsätze aus Art. 5 Abs. 1 lit. a–f DSGVO nicht nachweisen kann, stellt dies eine Verletzung der Nachweispflicht aus Art. 5 Abs. 2 Hs. 2 DSGVO dar.[63]

---

56 Erwägungsgrund 39 S. 12 statuiert die Verhinderung des Zugangs Unbefugter.
57 Ausführlich zu technischen Maßnahmen siehe Kap. 13 Rn. 13 ff.
58 Ausführlich zu technischen Maßnahmen siehe Kap. 13 Rn. 13 ff.
59 Taeger/Gabel/*Voigt*, DSGVO Art. 5 Rn. 40.
60 Ausführlich zur Datenschutzorganisation siehe Kap. 11; Kühling/Buchner/*Herbst*, DSGVO Art. 5 Rn. 78.
61 Siehe hierzu Kap. 10.
62 Kühling/Buchner/*Herbst*, Art. 5 DSGVO Rn. 79.
63 Kühling/Buchner/*Herbst*, Art. 5 DSGVO Rn. 79.

Praxishinweis

Es empfiehlt sich eine genaue Überprüfung, ob hinreichende Maßnahmen zur Einhaltung der Verpflichtung ergriffen wurden. Ein Verstoß gegen die Nachweispflicht ist gemäß Art. 83 Abs. 5 lit. a DSGVO mit einem Bußgeld von bis zu 20.000.000 € oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes bewährt.

Die genaue **Form des Nachweises** der Einhaltung der Rechenschaftspflicht gibt Art. 5 Abs. 2 DSGVO nicht vor. Folgende beispielhafte Maßnahmen sind grundsätzlich als Nachweise geeignet:

- Einträge im Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO;
- eine Datenschutz-Folgeabschätzung gemäß Art. 35 Abs. 7 DSGVO;
- im Falle einer Verarbeitung auf Basis einer Einwilligung nach Art. 7 Abs. 1 DSGVO ein Eintrag in einer Datenbank oder eine unterschriebene Fassung der Erklärung;
- im Falle einer Verarbeitung auf Basis berechtigter Interessen eine schriftlich dokumentierte Interessenabwägung;
- interne Anweisungen (der Mitarbeiter) oder Richtlinien in Bezug auf konkrete Verarbeitungen;
- Kopien von Auftragsverarbeitungsverträgen;
- Dokumentationen von Datenschutzprüfungen/Audits, z. B. ausgefüllte Fragebögen, abgehakte Checklisten.

Die Rechenschaftspflicht führt im Rahmen eines **zivilrechtlichen Schadensersatzverfahrens** nach Art. 82 DSGVO jedoch nicht zu einer **Beweislastumkehr**.[64] Vielmehr gelten die allgemeinen Beweislastregeln und Darlegungsgrundsätze nach nationalem Recht, was ebenfalls für potenzielle sekundäre Darlegungslasten gilt – d. h. in Deutschland muss der Anspruchsteller (Betroffener) grundsätzlich alle schadensersatzbegründende Merkmale darlegen bzw. beweisen.[65] **31**

64 Siehe auch OLG Innsbruck, Urt. v. 13.2.2020 – 1 R 182/19b Ziff. II.4.
65 Taeger/*Moos*, DSRITB 2020, 451, 452.

Kapitel 5

Zulässigkeit der Verarbeitung personenbezogener Daten

Übersicht

Rn.

I. Überblick über die einschlägigen Regelungen der DSGVO *(Arning)* . . 1

II. Gesetzliche Erlaubnisvorschriften *(Arning)* 11

1. Verarbeitung personenbezogener Daten zu Zwecken der Vertragserfüllung oder zur Durchführung vorvertraglicher Maßnahmen . . . 12

a) Verarbeitung personenbezogener Daten zu Zwecken der Vertragserfüllung 18

b) Verarbeitung personenbezogener Daten zu Zwecken der Durchführung vorvertraglicher Maßnahmen 33

c) Erforderlichkeit der Datenverarbeitung für die genannten Zwecke 37

2. Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung . 56

3. Verarbeitung personenbezogener Daten auf Basis einer Interessenabwägung 63

a) Berechtigte Interessen des Verantwortlichen oder eines Dritten 70

b) Erforderlichkeit einer Datenverarbeitung zur Wahrung der berechtigten Interessen 75

c) Keine überwiegenden Interessen/Rechte der betroffenen Person am Ausschluss der Datenverarbeitung 76

4. Verarbeitung personenbezogener Daten zu Zwecken der Werbung 89

Rn.

5. Verhältnis der Alternativen des Art. 6 Abs. 1 DSGVO zueinander 105

6. Verhältnis zwischen besonders praxisrelevanten nationalen Vorschriften und der DSGVO. . 110

a) Videoüberwachung öffentlich zugänglicher Räume gem. § 4 BDSG 113

b) Scoring und Bonitätsauskünfte gem. § 31 BDSG. . . . 118

c) Verhältnis zwischen dem Kunsturhebergesetz und der DSGVO 130

7. Zweckänderung – Verarbeitung personenbezogener Daten zu einem anderen Zweck. 137

a) Zweckänderung auf Basis einer Rechtsvorschrift 139

b) Zweckänderung auf Basis einer Einwilligung 151

c) Zweckänderung auf Basis des Kompatibilitätstests gem. Art. 6 Abs. 4 DSGVO . 152

d) Weitere datenschutzrechtliche Pflichten im Fall der Zweckänderung 158

8. Verarbeitung besonderer Kategorien personenbezogener Daten 159

a) Besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO) 160

b) Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten . . 169

Rn.

c) Voraussetzungen für die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 2 DSGVO). 174
9. Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten – Art. 10 DSGVO . . 209
10. Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist – Art. 11 DSGVO. 215
a) Keine Pflicht zur Verarbeitung von identifizierenden Merkmalen 216
b) Pflichten und Privilegierung des Verantwortlichen gem. Art. 11 Abs. 2 DSGVO 219
11. Besondere Verarbeitungssituationen 236
12. Zulässigkeit der Verarbeitung personenbezogener Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden 241
13. Sanktionierung 242

Rn.

III. Einwilligung der Betroffenen *(Rohwedder)* 243
1. Überblick über die einschlägigen Regelungen. 244
2. Allgemeine Voraussetzungen der Einwilligung 247
a) Form der Willensbekundung 248
b) Freiwilligkeit 257
c) Erteilung für den bestimmten Fall 270
d) Transparenzgebot 271
e) Einwilligungen als Gegenstand von AGB. 277
f) Widerruflichkeit. 287
g) Nachweisbarkeit 291
h) Gültigkeitsdauer. 295
3. Einwilligung von Kindern 296
a) Voraussetzungen bei direkten Angeboten von Fernabsatzdiensten 297
b) Vergewisserungspflicht des Verantwortlichen 300
4. Einwilligung bei sensiblen Datenkategorien 303
5. Wirksamkeit von Alt-Einwilligungen 305

I. Überblick über die einschlägigen Regelungen der DSGVO

1 Dem Grundsatz des **Verarbeitungsverbots mit Erlaubnisvorbehalt** folgend, dürfen personenbezogene Daten nur mit Einwilligung der betroffenen Person oder auf Basis einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden, die sich entweder aus der DSGVO selbst, dem sonstigen Unionsrecht oder dem Recht der Mitgliedstaaten ergeben kann.[1]

2 In diesem Kapitel werden daher die in der DSGVO sowie die im BDSG **normierten Anforderungen an die Zulässigkeit der Verarbeitung personenbezogener Daten erläutert**, insbesondere die Voraussetzungen, unter denen die Verarbeitung personenbezogener Daten direkt auf die DSGVO oder das BDSG gestützt werden kann,[2] sowie die Anforderungen an eine wirksame Einwilligung der betroffenen Person.[3]

---

1 Art. 6 Abs. 1 DSGVO und Erwägungsgrund 40; siehe hierzu auch Kap. 4 Rn. 4 ff.
2 Siehe Rn. 11 ff.
3 Siehe Rn. 243 ff.

Die einschlägigen Regelungen zur Zulässigkeit der Verarbeitung personenbezogener Daten befinden sich vor allem in den **Art. 6–11 DSGVO**. **3**

Die **zentrale Vorschrift** in der DSGVO im Hinblick auf die Zulässigkeit der Verarbeitung von personenbezogenen Daten ist **Art. 6 DSGVO nebst den korrespondierenden Erwägungsgründen 40, 41 und 44–50**. So muss nach Art. 6 Abs. 1 DSGVO mindestens **eine der dort aufgeführten Bedingungen erfüllt sein**, damit der jeweils Verantwortliche personenbezogene Daten verarbeiten darf. Zu diesen Bedingungen zählen z. B. die Einwilligung (lit. a), die Verarbeitung zu Zwecken der Erfüllung eines Vertrages (lit. b) und die Verarbeitung zu Zwecken der Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (lit. f).[4] Einige dieser Bedingungen werden in den nachfolgenden Art. 7–11 DSGVO dann noch weiter spezifiziert, so z. B. die Voraussetzungen an eine wirksame Einwilligung in den Art. 7 und 8 DSGVO. **4**

Des Weiteren enthält Art. 6 DSGVO auch die Vorgaben für die **Zweckänderung**. Möchte also ein Verantwortlicher für einen bestimmten Zweck erhobene personenbezogene Daten für einen anderen (neuen) Zweck verarbeiten, muss er die Anforderungen des Art. 6 Abs. 4 DSGVO einhalten. **5**

Wie schon die Datenschutzrichtlinie 95/46/EG und das BDSG a. F. unterscheidet die DSGVO zwischen „normalen" personenbezogenen Daten und Daten, die aufgrund ihrer Sensibilität und des ihnen innewohnenden Diskriminierungspotenzials **besonders strikten Verarbeitungsvoraussetzungen** unterliegen.[5] Diese sind im Grundsatz in Art. 9 DSGVO sowie in den korrespondierenden Erwägungsgründen 51–56 geregelt.[6] Sie sind weitaus strikter als die in Art. 6 Abs. 1 DSGVO statuierten Voraussetzungen für die Verarbeitung „normaler" personenbezogener Daten.[7] So kann die Verarbeitung **besonderer Kategorien personenbezogener Daten** – die in Art. 9 Abs. 1 DSGVO spezifiziert werden – z. B. nicht wie die Verarbeitung „normaler" personenbezogener Daten auf Grundlage einer Interessenabwägung erfolgen.[8] **6**

Art. 10 DSGVO, zu dem es keinen korrespondierenden Erwägungsgrund gibt, enthält **Sonderregelungen** für die Verarbeitung personenbezogener Daten über **strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln**, die die generellen Vorgaben des Art. 6 Abs. 1 DSGVO ergänzen.[9] **7**

---

4 Siehe ausführlich Rn. 11 ff.

5 Siehe Art. 8 der Datenschutzrichtlinie 95/46/EG und § 3 Abs. 9 BDSG a. F.

6 Weit überwiegend wird vertreten, dass für die Verarbeitung besonderer Kategorien personenbezogener Daten neben den Anforderungen des Art. 9 DSGVO auch die Anforderungen des Art. 6 Abs. 1 DSGVO zu erfüllen sind, siehe ausführlich Rn. 170 ff.

7 Siehe ausführlich Rn. 11 ff.

8 Siehe ausführlich Rn. 159 ff.

9 Siehe ausführlich Rn. 209 ff.

8 Art. 11 DSGVO und der korrespondierende Erwägungsgrund 57 DSGVO beinhalten schließlich noch ergänzende Regelungen für den Fall, dass ein Verantwortlicher personenbezogene Daten verarbeitet, die betroffene Person (selbst) aber **nicht identifizieren** kann bzw. nicht (mehr) muss, um den mit der Datenverarbeitung verfolgten Zweck zu erreichen.[10]

9 Art. 85–91 DSGVO enthalten zudem noch spezielle Vorschriften für **besondere Verarbeitungssituationen**, wobei die Vorschriften zur Datenverarbeitung im **Beschäftigungskontext** (Art. 88 DSGVO), zur Datenverarbeitung zu **journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken** (Art. 85 DSGVO) sowie die Vorgaben zu Garantien und Ausnahmen in Bezug auf die Datenverarbeitung zu **im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken** (Art. 89 DSGVO) am praxisrelevantesten sein dürften.

10 Teilweise enthalten die genannten Vorschriften der DSGVO auch **Öffnungsklauseln**, die es dem jeweiligen EU-Mitgliedstaat und/oder der EU unter den dort genannten Voraussetzungen erlauben, Regelungen zu erlassen, die die DSGVO insoweit ergänzen.[11] In Deutschland hat der Gesetzgeber von vielen dieser Öffnungsklauseln Gebrauch gemacht. Die wichtigsten nationalen Regelungen zur Zulässigkeit der Datenverarbeitung befinden sich in Deutschland im BDSG und dort in den **§§ 22–31 BDSG**. Allerdings enthalten auch noch eine Vielzahl anderer Gesetze (einzelne) Vorschriften hierzu, z. B. die Sozialgesetzbücher, die Landesdatenschutzgesetze, das Gesundheitsdiagnostikgesetz etc. Diese regeln größtenteils aber (nur) spezielle Situationen, in denen personenbezogene Daten verarbeitet werden oder die Datenverarbeitung durch bestimmte Verantwortliche erfolgt. Da die für die Unternehmenspraxis wichtigsten Fälle (abschließend) in der DSGVO und ggf. ergänzend im BDSG geregelt werden, konzentriert sich dieses Kapitel im Folgenden auf diese Regelungen.

II. Gesetzliche Erlaubnisvorschriften

11 Im Folgenden sollen nun **die in der Datenverarbeitungspraxis von Unternehmen wichtigsten Rechtsgrundlagen**, die in der DSGVO oder im BDSG enthalten sind und auf deren Grundlage sich die Verarbeitung personenbezogener Daten stützen lässt, näher erläutert werden.

---

10 Siehe ausführlich Rn. 215 ff.

11 Siehe ausführlich zur Regelungssystematik im Datenschutzrecht und zur Funktionsweise der Öffnungsklauseln in der DSGVO Kap. 1 Rn. 7 ff.

1. Verarbeitung personenbezogener Daten zu Zwecken der Vertragserfüllung oder zur Durchführung vorvertraglicher Maßnahmen

Einer der wichtigsten Zwecke, für den in der Praxis personenbezogene Daten verarbeitet werden, ist **die Begründung, Durchführung und Beendigung von Verträgen** – und dies nicht nur, wenn die Verarbeitung von personenbezogenen Daten der wesentliche Gegenstand der Leistungserbringung ist. So ist es in den meisten Fällen allein schon erforderlich zu wissen, wer die Vertragsparteien sind; personenbezogene Daten können erforderlich sein, um die Vertragsparameter bestimmen zu können (so z. B. bei Versicherungsverträgen) etc. **12**

Vor diesem Hintergrund enthält die DSGVO – wie auch schon die Datenschutzrichtlinie 95/46/EG – eine **Erlaubnisvorschrift**, die die Verarbeitung personenbezogener Daten im Rahmen einer Vertragsbeziehung zu rechtfertigen vermag. So besagt **Art. 6 Abs. 1 lit. b DSGVO**, dass die Verarbeitung personenbezogener Daten rechtmäßig ist, wenn die „*Verarbeitung* […] *für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich* [ist]*, die auf Anfrage der betroffenen Person erfolgen*". **13**

Mithin enthält diese Vorschrift **zwei voneinander zu unterscheidende Erlaubnistatbestände**, die alternativ nebeneinander stehen: **14**

1. Die Verarbeitung ist für die **Erfüllung eines Vertrags** erforderlich, dessen Vertragspartei die betroffene Person ist.
2. Die Verarbeitung ist zur **Durchführung vorvertraglicher Maßnahmen** erforderlich, die auf Anfrage der betroffenen Person erfolgen.

> **Leitlinien des Europäischen Datenschutzausschusses**
>
> Der Europäische Datenschutzausschuss[12] hat Leitlinien für die **Verarbeitung personenbezogener Daten auf Grundlage von Art. 6 Abs. 1 lit. b DSGVO** im Zusammenhang mit der Erbringung von Onlinediensten gegenüber betroffenen Personen veröffentlicht.[13] Zwar beziehen sich diese Leitlinien insbesondere auf Onlinedienste. Doch lassen sich gerade die allgemeinen Ausführungen zu Art. 6 Abs. 1 lit. b DSGVO auch auf die „Offline-Welt" übertragen. **15**

12 Siehe zur Funktion und Organisation sowie den Aufgaben des Europäischen Datenschutzausschusses ausführlich Kap. 16 Rn. 14 f.

13 *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen, Version 2.0, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_de.pdf.

16 Unternehmen, die personenbezogene Daten auf Grundlage von Art. 6 Abs. 1 lit. b DSGVO verarbeiten wollen, ist zu **empfehlen**, die Leitlinien des Europäischen Datenschutzausschusses aufmerksam durchzuarbeiten und – wenn möglich – **diese auch zu befolgen**. Zwar besitzt der Europäische Datenschutzausschuss keine Kompetenz, die DSGVO rechtsverbindlich auszulegen, so dass durchaus auch eine Abweichung von diesen Leitlinien datenschutzrechtlich zulässig oder gar geboten sein kann, zumal die Datenschutzaufsichtsbehörden insbesondere nach dem Inkrafttreten der DSGVO relativ strenge Positionen vertreten. Die Kompetenz, die DSGVO rechtsverbindlich auszulegen, verbleibt bei den Gerichten, insbesondere dem EuGH, die nicht an die Leitlinien des Europäischen Datenschutzausschusses gebunden sind. Doch ist mit großer Sicherheit davon auszugehen, dass die deutschen Datenschutzaufsichtsbehörden – ebenso wie die Behörden in den anderen EU-Mitgliedstaaten – die DSGVO grundsätzlich so auslegen und anwenden werden, wie es der Europäische Datenschutzausschuss in den jeweiligen Leitlinien ausgeführt hat, zumal diese eine gewisse Bindungswirkung gegenüber den nationalen Datenschutzaufsichtsbehörden entfalten.[14] Somit besteht eine beträchtliche Rechtssicherheit, dass zumindest die Datenschutzaufsichtsbehörden eine Datenverarbeitung nicht beanstanden werden, soweit sich das verantwortliche Unternehmen dabei an die Leitlinien und anderen Vorgaben des Europäischen Datenschutzausschusses gehalten hat.

17 Möchte ein Unternehmen hingegen von den Leitlinien des Europäischen Datenschutzausschusses abweichen, sollte dies datenschutzrechtlich zuvor **geprüft** und die tatsächlichen Gründe sowie die rechtlichen Argumente hierfür **dokumentiert** werden.

a) Verarbeitung personenbezogener Daten zu Zwecken der Vertragserfüllung

18 Der Begriff der Vertragserfüllung ist **weit zu verstehen** und nicht mit dem zivilrechtlichen Begriff der Vertragserfüllung gleichzusetzen. Vielmehr umfasst der Begriff der Vertragserfüllung i. S. d. Art. 6 Abs. 1 lit. b DSGVO bereits den **Vertragsabschluss** selbst, der der eigentlichen Vertragserfüllung zeitlich vorgelagert ist.[15] Auch wenn dies in der Literatur teilweise vertreten wird, gehören die Anbahnung und die Verhandlung eines Vertrages nicht zur Vertragserfüllung i. S. d. Art. 6 Abs. 1 lit. b DSGVO.[16] So unterscheidet die DSGVO in Art. 6 Abs. 1 lit. b DSGVO zwischen der Durchführung vorvertraglicher Maßnahmen einerseits und der Vertragserfüllung andererseits und legt hierfür unterschiedliche Verarbeitungsvoraussetzungen fest. Vor diesem Hintergrund müssen die fraglichen Datenverarbeitungsaktivitäten nach hier vertretener Ansicht zumin-

14 Siehe z. B. Kühling/Buchner/*Dix*, Art. 70 DSGVO Rn. 10.
15 So z. B. auch Laue/Kremer/*Kremer*, § 2 Rn. 30; Plath/*Plath*, Art. 6 DSGVO Rn. 11.
16 So für die Anbahnung Plath/*Plath*, Art. 6 DSGVO Rn. 11.

dest unmittelbar mit dem Vertragsabschluss im Zusammenhang stehen, damit sie auf Art. 6 Abs. 1 lit. b Alt. 1 DSGVO gestützt werden können – dies ist bei der Anbahnung und der Verhandlung eines Vertrages aber eben nicht der Fall.[17]

Weiterhin umfasst der Begriff der Vertragserfüllung die **Herbeiführung des vertraglich geschuldeten Leistungserfolgs**,[18] die Vertragsänderung, die Abwicklung des Vertrages, also auch die Anfechtung, Beendigung bzw. Kündigung und die sonstige Ausübung eines Gestaltungsrechts, sowie die **Erfüllung von Nebenpflichten und sekundären Pflichten**, allen voran von Mängelgewährleistungsansprüchen.[19] **19**

Leitlinien des Europäischen Datenschutzausschusses

Nach Auffassung des Europäischen Datenschutzausschusses („EDSA") vermag Art. 6 Abs. 1 lit. b DSGVO grundsätzlich **keine Datenverarbeitung nach vollständiger Beendigung des Vertrages** zu rechtfertigen, z. B. zu Zwecken der Erfüllung von Aufbewahrungspflichten.[20] Hierfür sei regelmäßig eine andere Rechtsgrundlage erforderlich. Die Speicherung zur **Erfüllung von Aufbewahrungspflichten** muss nach Ansicht des EDSA demzufolge z. B. i. d. R. auf Art. 6 Abs. 1 lit. c DSGVO („Erfüllung einer rechtlichen Verpflichtung") i. V. m. mit der nationalen Rechtsvorschrift gestützt werden, die die jeweilige Aufbewahrungspflicht begründet (z. B. § 257 HGB und § 147 AO). Die Verarbeitung personenbezogener Daten im Zusammenhang **20**

17 So auch Laue/Kremer/*Kremer*, § 2 Rn. 30.

18 Kühling/Buchner/*Buchner/Petri*, Art. 6 DSGVO Rn. 33; *Taeger* weist zu Recht darauf hin, dass hiervon – der deutschen Besonderheit des Abstraktionsprinzips folgend – sowohl das Erfüllungs- als auch das Verpflichtungsgeschäft umfasst ist, Taeger/Gabel/*Taeger*, Art. 6 DSGVO Rn. 59.

19 Siehe z. B. Plath/*Plath*, Art. 6 DSGVO Rn. 11; Taeger/Gabel/*Taeger*, Art. 6 DSGVO Rn. 59; Gola/*Schulz*, Art. 6 DSGVO Rn. 28; a. A. im Hinblick auf die Beendigung des Vertrages: Simitis/Hornung/Spiecker gen. Döhmann/*Roßnagel*, Art. 6 DSGVO Rn. 30; siehe hierzu auch die Ausführungen des Europäischen Datenschutzausschusses, der die Auffassung vertritt, dass nur Datenverarbeitungen, die zur Erfüllung des Vertrages erforderlich sind, auf diese Rechtsgrundlage gestützt werden können. Auf sonstige Maßnahmen, die durch eine Nichterfüllung ausgelöst werden, oder auf andere Vorkommnisse bei der Erfüllung eines Vertrages sei sie jedoch nicht automatisch anwendbar, siehe *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen, Version 2.0, S. 13. Die Verarbeitung personenbezogener Daten zu Zwecken der Erfüllung von Gewährleistungsansprüchen oder einer Garantie kann aber wohl auch nach Auffassung des EDSA ggf. auf Art. 6 Abs. 1 lit. b DSGVO gestützt werden, *Europäischer Datenschutzausschuss*, a. a. O., S. 13.

20 *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen, Version 2.0, S. 13 f.

mit dem durch die Kündigung ausgelösten Verwaltungsaufwand, wie z. B. der Rücksendung von Waren oder Rückzahlungen, könne hingegen auf Art. 6 Abs. 1 lit. b DSGVO gestützt werden.[21]

21 Außerdem sei es nach Auffassung des EDSA **generell unzulässig**, zu einer neuen Rechtsgrundlage „zu wechseln", wenn die Datenverarbeitung nicht mehr auf Art. 6 Abs. 1 lit. b DSGVO gestützt werden kann, weil die betroffene Person ihre Daten ggf. nur deshalb zur Verfügung gestellt habe, weil sie davon ausgegangen sei, dass deren Verarbeitung ein notwendiger Teil der Vertragsbeziehung sei.[22] Ausnahmsweise sei es allerdings zulässig, Daten für bestimmte spezifische Zwecke auch nach Vertragsbeendigung weiterzuverarbeiten, so z. B. zur Erfüllung von Aufbewahrungspflichten oder Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. In diesem Fall müssten Verantwortliche hierfür eine (gesonderte) Rechtsgrundlage bestimmen und die betroffenen Personen vor Beginn der Datenverarbeitung über diese Datenverarbeitung und die Dauer der weiteren Aufbewahrung im Einklang mit den Transparenzanforderungen der DSGVO (insb. aus Art. 13 bzw. 14 DSGVO) informieren.[23]

22 Unklar bleibt, ob es sich bei dieser Information nach Auffassung des EDSA um ein **konstitutives Zulässigkeitserfordernis** handelt, also die Weiterverarbeitung nach Beendigung des Vertrages nur dann zulässig ist, wenn der Verantwortliche die betroffene Person hierüber vor Beginn der Verarbeitung informiert hat. Eine solche Auslegung wäre nach hier vertretener Meinung allerdings nicht mit Art. 6 DSGVO vereinbar, zumal die Erfüllung der Informationspflichten gem. Art. 13 bzw. Art. 14 DSGVO nach hier vertretener Ansicht keine Rechtmäßigkeitsvoraussetzung für die Datenverarbeitung ist.[24]

23 Aber auch gegen die restriktive Auffassung des EDSA an sich, dass eine Datenverarbeitung nach Beendigung eines Vertrages nur ausnahmsweise auf eine andere Rechtsgrundlage gestützt werden könne, wenn Art. 6 Abs. 1 lit. b DSGVO diese nicht mehr zu rechtfertigen vermag, bestehen nach hier vertretener Auffassung zumindest **ernsthafte Zweifel**, da die einzelnen Erlaubnis-

---

21 *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen, Version 2.0, S. 14.

22 *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen, Version 2.0, S. 14.

23 *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen, Version 2.0, S. 14.

24 Siehe Kap. 6 Rn. 109 ff.