

Specht-Riemenschneider • Werry • Werry (Hrsg.)

Datenrecht in der Digitalisierung

Leseprobe, mehr zum Buch unter [ESV.info/978-3-503-18782-9](https://www.esv.info/978-3-503-18782-9)

Datenrecht in der Digitalisierung

Herausgegeben von

Prof. Dr. Louisa Specht-Riemenschneider

Inhaberin des Lehrstuhls für Bürgerliches Recht, Informations- und Datenrecht an der Rheinischen-Friedrich-Wilhelms-Universität Bonn sowie Direktorin des Instituts für Handelsrecht, Leiterin der Forschungsstelle für Rechtsfragen neuer Technologien sowie Datenrecht (ForTech),

Nikola Werry LL.M. (UK), Rechtsanwältin,
KPMG Law Rechtsanwaltsgesellschaft, Frankfurt a.M.

und

Susanne Werry LL.M. (UK), Rechtsanwältin,
Clifford Chance Deutschland LLP, Frankfurt a.M.

mit Beiträgen von

Dr. Simon Apel, Dr. jur. Malte Beyer-Katzenberger, Margarita Bidler, Linda Bienemann, Dr. Micha Brechtel, Prof. Dr. Lothar Determann, Dr. Tobias Dienlin, Prof. Dr. Martin Ebers, Jochen Eimer, Jörn Erbguth, Victoria Fast, Lava Gaff, Anne Britta Haas, Anton Haberl, Anka Hakert, Dr. Anke Hofmann, Michael Intveen, Prof. Dr. Wolfgang Kerber, Dr. Karsten Krupna, Prof. Dr. Franz Lehner, Dr. Dimitrios Linardatos, Sebastian Louven, Marina Lutz, Dr. Jan Henrik Pesek, Dipl.-Jur. Alisa Rank-Haedler, Charlotte Röttgen, Dr. Gunnar Sachs, Dr. Bernd Schmidt, Dr. Daniel Schnurr, Kay Schröder, Prof. Dr. Jan H. Schumann, Prof. Dr. Louisa Specht-Riemenschneider, Tobias Steudner, Lorenz Volbers, Nikola Werry, Susanne Werry, Prof. Dr. Thomas Widjaja, Dr. Michael Wohlfarth, Prof. Dr. Ling Yu

Leseprobe, mehr zum Buch unter [ESV.info/978-3-503-18782-9](https://www.esv.info/978-3-503-18782-9)

ERICH SCHMIDT VERLAG

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.

Weitere Informationen zu diesem Titel finden Sie im Internet unter

ESV.info/978-3-503-18782-9

Gedrucktes Werk: ISBN 978-3-503-18782-9

eBook: ISBN 978-3-503-18783-6

Alle Rechte vorbehalten

© Erich Schmidt Verlag GmbH & Co. KG, Berlin 2020

www.ESV.info

Dieses Papier erfüllt die Frankfurter Forderungen der Deutschen Nationalbibliothek und der Gesellschaft für das Buch bezüglich der Alterungsbeständigkeit und entspricht sowohl den strengen Bestimmungen der US Norm Ansi/Niso Z 39.48-1992 als auch der ISO Norm 9706.

Gesetzt aus der Stempel Garamond, 9/11 Punkt

Satz: multitext, Berlin

Druck und Bindung: Kösel, Altusried-Krugzell

Vorwort

Datenrecht – Ein Definitionsversuch

Der rechtliche Umgang mit Daten ist eine der zentralen Herausforderungen, vor der Wissenschaft und Praxis heute stehen. Daten sind dabei als unkörperliche Gegenstände nicht unmittelbar eigentumsfähig i.S.d. § 903 BGB, unterliegen aber zahlreichen anderen rechtlichen Regelungen. So können sie beispielsweise Gegenstand des Geheimnisschutzes sein oder auch deliktsrechtlichen und strafrechtlichen Schutz genießen. Das Datenschutzrecht unterstellt personenbezogene Daten dem Verbotsprinzip und gestattet ihre Verarbeitung allein bei Vorliegen einer Einwilligung oder eines anderen gesetzlichen Erlaubnistatbestands. Auch kartellrechtliche Fragen gewinnen nicht erst seit dem – gegenwärtig außer Vollzug gesetzten – Beschluss des Bundeskartellamtes¹, Facebook umfassende Beschränkungen bei der Verarbeitung von Nutzerdaten aufzuerlegen, an Bedeutung.

Das „Datenrecht“ kann insofern – ebenso wie das Internetrecht und das Medienrecht – als Querschnittsmaterie beschrieben werden, dessen einendes Element das Regelungsobjekt Daten ist. Erfasst sind dabei sowohl personenbezogene als auch nicht-personenbezogene Daten. Wie kein anderes Rechtsgebiet adressiert das Datenrecht aber nicht nur Regelungsaspekte *de lege lata*, sondern fragt vor allem nach den Regulierungsoptionen des Regulierungsobjektes Daten *de lege ferenda*. Es befindet sich damit in einer steten Entwicklung und versucht, mit den technischen und gesellschaftlichen Entwicklungen angemessen Schritt zu halten. Tatsächlich ist es aber häufig so, dass das Recht diesen Entwicklungen erst mit einem Abstand nachfolgt, was nicht selten mit einem erheblichen Maß an Rechtsunsicherheit einhergeht.

Daten zeichnen sich dabei dadurch aus, dass sie aufgrund ihrer Unkörperlichkeit ubiquitär verfügbar sind und eine Vervielfältigung und Weitergabe weltweit binnen Sekunden mit äußerst geringem Kostenaufwand möglich ist. Gleichzeitig kann ihre wirtschaftliche Bedeutung nicht hoch genug geschätzt werden. Dies wirft unter anderem die Frage auf, ob der derzeitige rechtliche Regelungsrahmen, der noch immer häufig an das körperliche Trägermedium anknüpft, noch angemessen ist, denn für ihre wirtschaftliche Relevanz, ihre Verwertung und Weitergabe ist dieses körperliche Trägermedium längst nicht mehr ausschlaggebend.

¹ Vgl. https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2019/07_02_2019_Facebook.html (24. 03. 2019).

Bei der Ausgestaltung eines Regelungsrahmens für den Umgang mit Daten sind aber nicht nur rechtliche Aspekte zu berücksichtigen. Die Ausgestaltung von Rechtspositionen an unkörperlichen Gütern bedarf stets der Rechtfertigung. Da hierfür auch und gerade ökonomische Erwägungen in Betracht kommen, ist zwingend auch eine Auseinandersetzung mit ökonomischen Gesichtspunkten gefordert. Dieses Handbuch greift daher auch ökonomische Erwägungen auf, wo sie sinnvoll und erforderlich sind.

Denkt man an die datenschutzrechtlichen Herausforderungen unserer Zeit, so sind diese im Umgang mit Daten auch und gerade durch das Phänomen der Informationsüberlastung des Betroffenen gekennzeichnet. Auch dieses Problem kann nicht allein aus juristischer Perspektive gelöst werden, sondern fordert eine interdisziplinäre Betrachtung: In diese müssen bildwissenschaftliche Erkenntnisse (Standardisierung von Informationen durch Symbole) ebenso einbezogen werden, wie Erwägungen aus Verhaltensforschung und Psychologie zur Erörterung des sogenannten Privacy Paradox. Dieses beschäftigt sich mit der Frage, ob eine Asymmetrie zwischen theoretischer Sorge um den sorgsamsten Umgang mit personenbezogenen Daten und tatsächlichem Verhalten existiert und wie dieser Asymmetrie ggf. begegnet werden kann.

All diese – z.T. interdisziplinär zu betrachtenden – Problembereiche haben wir mit den übrigen komplexen und – z.T. rechtsvergleichend zu betrachtenden – rechtlichen Fragestellungen im Umgang mit Daten zusammengeführt, um den Versuch einer ersten Grenzziehung des sich noch im Entstehen befindlichen „Datenrechts“ zu unternehmen. Dabei treten täglich neue Fragen auf und wohl kein Rechtsgebiet unterliegt einer solchen Aktualitätsanpassung, wie das Datenrecht. Es ist daher ein Akt der Unmöglichkeit, bei Drucklegung dieses Handbuchs tatsächlich sämtliche tagesaktuellen Fragen umfangreich aufgearbeitet zu haben, ohne dass die wissenschaftliche Tiefe dabei in Mitleidenschaft gezogen würde. Wir haben uns daher dafür entschieden, einige Fragen für eine zweite Auflage aufzusparen, so etwa den Umgang mit Daten im Prozess. Auch die explizite Adressierung von Zugangsansprüchen zu Daten außerhalb des Kartellrechts z. B. gegen den Staat oder im Sinne des Vorschlags eines „Daten-für-alle-Gesetzes“ bleibt einer Neuauflage vorbehalten.

Für die Erstauflage haben wir stattdessen die uns – v. a. in der privat- und datenschutzrechtlichen Diskussion – am relevantesten erscheinenden Bereiche des Datenrechts durch mit der Materie in Praxis und Wissenschaft betraute Kollegen und Kolleginnen aufarbeiten lassen und uns dabei den folgenden Bereichen gewidmet:

Dr. Malte Beyer-Katzenberger erläutert einleitend die politische Relevanz verschiedener Facetten des Datenrechts. Das Datenschutzrecht – und dabei insbesondere die Datenschutzgrundverordnung – spielt in seiner Anwendbarkeit eine erhebliche Rolle für das Datenrecht. *Dr. Karsten Krupna* und *Dr. Bernd Schmidt* skizzieren daher zunächst die Grundzüge des europäischen Datenschutzrechts und geben einen Überblick über die wichtigsten Aspekte (§ 2.1). Gefolgt wird der

Überblick von Beiträgen, die sich vertieft mit verschiedenen Bereichen des Datenschutzes auseinandersetzen. *Nikola* und *Susanne Werry* stellen die europäische Rechtslage betreffend den internationalen Datentransfer dar, gehen auf Herausforderungen verschiedener Instrumente ein und stellen Lösungsansätze vor (§ 2.2). Zwei in der aktuellen Wirtschaft sehr relevanten Bereichen für Datenschutzfragen widmen sich *Lava Gaff* mit dem Thema Datenschutz bei Virtual und Augmented Reality (§ 2.3) und *Marina Lutz* mit dem Thema Datenschutz im Online-Marketing (§ 2.4), in dem sowohl auf das Zusammenspiel zwischen Datenschutz und unlauterem Wettbewerb, wie auch die ePrivacy-Verordnung eingegangen wird. *Michael Intveen* greift das Thema ePrivacy-Verordnung auf und beleuchtet diese aus dem Blickwinkel ihrer Auswirkungen auf den für die Digitalisierung ebenfalls sehr relevanten Bereich der automatisierten Fahrzeugsysteme und des vernetzten Fahrens (§ 2.5).

In enger Verbindung mit dem Datenschutzrecht steht das Privacy Paradox, das als Phänomen allerdings der interdisziplinären Betrachtung bedarf. *Prof. Dr. Thomas Widjaja* und *Prof. Dr. Jan Schumann* widmen sich gemeinsam mit *Margarita Bidler* sowie *Tobias Steudner* daher zunächst aus wirtschaftswissenschaftlicher Perspektive den Kundenwahrnehmungen und dem Kundenverhalten beim Bezahlen von digitalen Dienstleistungen mit personenbezogenen Daten (§ 3.1), bevor *Dr. Tobias Dienlin* das Privacy Paradox aus psychologischer Perspektive erörtert (§ 3.2). Kann eine Asymmetrie zwischen theoretischer Sorge um den Umgang mit personenbezogenen Daten und dem tatsächlichen Verhalten der Betroffenen, in dem nicht selten eine massenhafte Hingabe von Daten zu beobachten ist, tatsächlich festgestellt werden, ließe sich dieser Asymmetrie möglicherweise jedenfalls in einem gewissen Umfang durch eine Verbesserung der Informationsvermittlung entgegenwirken. Wie eine solche Informationsvermittlung durch Visualisierung verbessert werden kann, untersuchen *Prof. Dr. Louisa Specht-Riemenschneider* und *Linda Bienemann* aus rechtlicher Sicht (§ 3.3) sowie *Kai Schröder*, der die Potentiale der Informationsvisualisierung im Datenschutz aus kommunikationswissenschaftlicher Perspektive diskutiert (§ 3.4).

Einen weiteren wesentlichen Bereich des Datenrechts stellen potentielle Vermögensrechte an Daten dar. *Prof. Dr. Wolfgang Kerber* erläutert hier einleitend Dateneigentum, Datenzugangsrechte und Datengovernance aus ökonomischer Perspektive (§ 4.1), bevor *Charlotte Röttgen* Rechtspositionen an Daten *de lege lata* und *de lege ferenda* im europäischen Rechtsraum diskutiert (§ 4.2). Auch andernorts wird die Frage von Rechten an Daten gestellt, am relevantesten sind dabei wohl die Erwägungen aus den USA und China. *Apl. Prof. Dr. Lothar Determann* (§ 4.3) und *Prof. Dr. Ling Yu* (§ 4.4) erläutern die Rechtslage in diesen Staaten.

Neben vermögensrechtlichen Rechtspositionen an Daten spielt auch der vertragsrechtliche Umgang mit Daten eine erhebliche Rolle und dies v. a. deshalb, weil Daten mittlerweile ein nicht unerheblicher ökonomischer Wert zugesprochen wird. Im Vorfeld der Erörterungen zur Typisierung von Verträgen, in denen Daten den Leistungsgegenstand darstellen (*Alisa Rank-Haedler*, § 5.2) sowie der Frage, ob Daten eine Gegenleistung im Vertrag darstellen können (*Dr. Dimitrios*

Linardatos, § 5.3), beschäftigt sich *Prof. Dr. Franz Lehner* daher mit der Preis- und Wertermittlung von Daten und Informationen (§ 5.1). *Dr. Simon Apel* und *Dr. Anke Hofmann* erörtern sodann Daten in der Unternehmenstransaktion (§ 5.4), bevor *Anne Britta Haas* den vertragsrechtlichen Teil des Handbuchs mit der Darstellung des Outsourcings und insbesondere der Herausforderungen des Cloud Computings schließt (§ 5.5).

§ 6 widmet sich dem Phänomen der Kryptowährungen. *Jörn Erbguth* diskutiert hier Bitcoin, E-Geld und virtuelle Währungen, bevor *Anka Hakert* die Besteuerung dieser Kryptowährungen in den Blick nimmt (§ 6.2).

Ein wesentliches Thema für den Bereich des Datenrechts ist auch die Ausübung von Marktmacht durch Daten, die in § 7 aus ökonomischer (*Dr. Daniel Schnurr*, *Viktoria Fast* und *Dr. Michael Wohlfahrt*, § 7.1) und juristischer Perspektive (*Sebastian Louven*, § 7.2) eruiert wird.

§ 8 beleuchtet sodann digitale Geschäftsmodelle – Datenbasierte Chancen und Risiken für Unternehmen (*Lorenz Volbers* und *Anton Haberl*), bevor in § 9 die Haftung für fehlerhafte Daten aufgearbeitet wird. Besonders relevant scheint dabei die Haftung für fehlerhafte Gesundheitsdaten (*Jochen Eimer* und *Dr. Jan Henrik Pesek*, § 9.1), die Haftung für fehlerhafte Daten beim autonomen Fahren (*Prof. Dr. Martin Ebers*, § 9.2) sowie die Haftung für fehlerhafte Daten in der Industrie 4.0 (*Dr. Gunnar Sachs*, § 9.3). Hier könnten weitere zahlreiche haftungsrelevante Bereiche erörtert werden, beispielsweise die Haftung für fehlerhafte Daten in Suchmaschinenergebnisseiten und Suchmaschinenergänzungsvorschlägen. Die erste Konturierung eines Datenrechts verlangt aber nach einer Schwerpunktsetzung auch im Verhältnis zu den übrigen Kapiteln. Den Abschluss des Werks bildet eine Erörterung von *Dr. Simon Apel* und *Dr. Micha Brechtel* zur Zwangsvollstreckung in Datenbestände (§ 10).

Wir bedanken uns herzlich bei den Autoren für die gute Zusammenarbeit. Ein besonderer Dank gilt auch Frau *Rebecca Rohmer* vom Lehrstuhl für Bürgerliches Recht, Informations- und Datenrecht der Rheinischen Friedrich-Wilhelms-Universität Bonn, die die teils mit erheblichem Aufwand verbundene redaktionelle Betreuung des Handbuchs vollständig übernommen hat und deren Genauigkeit, Fleiß und Einsatz nicht genug gelobt werden können.

Bonn/Frankfurt am Main, im April 2019

Louisa Specht-Riemenschneider
Nikola Werry
Susanne Werry

Inhaltsübersicht

Vorwort: Datenrecht – Ein Definitionsversuch <i>(Prof. Dr. Specht-Riemenschneider; Nikola Werry LL.M.; Susanne Werry LL.M.)</i>	5
Inhaltsverzeichnis	11
§ 1 Neuartige Rechtsfragen in Bezug auf Daten in Zeiten des Internets der Dinge, von Big Data und Künstlicher Intelligenz? – Anmerkungen aus rechtspolitischer Perspektive <i>(Dr. Malte Beyer-Katzenberger)</i>	37
§ 2 Datenschutzrecht	61
§ 2.1 Überblick zum europäischen Datenschutzrecht <i>(Dr. Karsten Krupna; Dr. Bernd Schmidt, LL.M.)</i>	63
§ 2.2 Internationaler Transfer personenbezogener Daten <i>(Nikola Werry LL.M.; Susanne Werry LL.M.)</i>	93
§ 2.3 Datenschutz bei Virtual und Augmented Reality <i>(Lava Gaff)</i>	153
§ 2.4 Datenschutz im Onlinemarketing <i>(Marina Lutz)</i>	203
§ 2.5 Auswirkungen der ePrivacy-Verordnung im Automobilsektor <i>(Michael Intveen)</i>	251
§ 3 Privacy Paradox	283
§ 3.1 Kundenwahrnehmungen und Kundenverhalten beim Bezahlen von digitalen Dienstleistungen mit personenbezogenen Daten <i>(Margarita Bidler, M.Sc.; Tobias Steudner, M.Sc.; Prof. Dr. Jan H. Schumann; Prof. Dr. Thomas Widjaja)</i>	285
§ 3.2 Das Privacy Paradox aus psychologischer Perspektive <i>(Dipl.-Psych. Dr. Tobias Dienlin)</i>	305
§ 3.3 Informationsvermittlung durch standardisierte Bildsymbole <i>(Prof. Dr. Specht-Riemenschneider; Linda Bienemann)</i>	324
§ 3.4 Potentiale der Informationsvisualisierung im Datenschutz – eine kommunikationswissenschaftliche Betrachtung <i>(Kay Schröder)</i>	345
§ 4 Vermögensrechte an Daten	361
§ 4.1 Dateneigentum, Datenzugangsrechte und Datengovernance aus ökonomischer Perspektive <i>(Prof. Dr. Wolfgang Kerber)</i>	363
§ 4.2 Rechtspositionen an Daten: Die Rechtslage im europäischen Rechtsraum <i>(Charlotte Röttgen)</i>	371

§ 4.3 Rechtspositionen an Daten: Die Rechtslage in den USA (Prof. Dr. Lothar Determann)	408
§ 4.4 Rechtspositionen an Daten: Die Rechtslage in China (Prof. Dr. Ling Yu).....	440
§ 5 Vertragsrechtliche Implikationen	469
§ 5.1 Preis- und Wertermittlung für Daten und Informationen (Prof. Dr. Franz Lehner)	471
§ 5.2 Daten als Leistungsgegenstand: Vertragsrechtliche Typisierung (Alisa Rank-Haedler).....	489
§ 5.3 Daten als Gegenleistung im Vertrag mit Blick auf die Richtlinie über digitale Inhalte (Dr. Dimitrios Linardatos)	506
§ 5.4 Datenbestände in der Unternehmens-Transaktion (M&A) (Dr. Simon Apel; Dr. Anke Hofmann)	560
§ 5.5 Daten-Outsourcing (Anne Britta Haas, LL. M.)	589
§ 6 Kryptowährungen	641
§ 6.1 Bitcoin/E-Geld/Virtuelle Währungen (Jörn Erbguth)	643
§ 6.2 Die Besteuerung von Kryptowährungen (Anka Hakert, LL.M.) ...	693
§ 7 Marktmacht durch Daten	743
§ 7.1 Marktmacht durch Daten: Eine Analyse aus ökonomischer Perspektive (Victoria Fast, M.Sc.; Dr. Daniel Schnurr; Dr. Michael Wohlfarth).....	745
§ 7.2 Marktmacht durch Daten: Eine Analyse aus rechtswissenschaftlicher Perspektive (Sebastian Lowven).....	779
§ 8 Digitale Geschäftsmodelle – Datenbasierte Chancen und Risiken für Unternehmen	
(Anton Haberl; Lorenz Volbers)	821
§ 9 Haftung für fehlerhafte Daten	843
§ 9.1 Haftung für fehlerhafte Gesundheitsdaten (Jochen Eimer, LL.M.; Dr. Jan Henrik Pesek).....	845
§ 9.2 Haftung für fehlerhafte Daten beim autonomen Fahren (Prof. Dr. Martin Ebers)	874
§ 9.3 Haftung für fehlerhafte Daten – Industrie 4.0 (Dr. Gunnar Sachs) .	915
§ 10 Datenbestände in Zwangsvollstreckung und Insolvenz	
(Dr. Simon Apel; Dr. Micha Brechtel)	941
Herausgeberinnen	983
Stichwortverzeichnis	985

Inhaltsverzeichnis

Vorwort: Datenrecht – Ein Definitionsversuch	5
Inhaltsübersicht	9
§ 1 Neuartige Rechtsfragen in Bezug auf Daten in Zeiten des Internets der Dinge, von Big Data und Künstlicher Intelligenz? – Anmerkungen aus rechtspolitischer Perspektive	37
A. Die Datenwirtschaft in Zeiten des Internets der Dinge, von Big Data und Künstlicher Intelligenz.....	40
B. Was ist der rechtliche Befund aus gemein-europäischer Sicht?	41
C. Rechtspolitischer Handlungsbedarf für IoT-Daten?	42
I. Welche Aspekte sind in der Diskussion zu berücksichtigen? Welche Daten und welche Aspekte genießen bereits Schutz?	42
II. Zwischenergebnis: Welche rechtspolitischen Ziele sollten verfolgt werden?.....	46
III. Welcher Wert wird bei der Datenerzeugung geschöpft?	47
IV. Ist der Handlungsbedarf sektorbezogen oder sektorübergreifend?	48
D. Rechtliche Antworten	49
E. Evidenzbasierte Politikgestaltung	51
F. Was folgt?	53
§ 2 Datenschutzrecht	61
§ 2.1 Überblick zum europäischen Datenschutzrecht	63
A. Begriff und Regelungsumfeld	66
B. Anwendungsbereich des europäischen und mitgliedstaatlichen Datenschutzrechts	68
I. Die Verarbeitung personenbezogener Daten (sachlicher Anwendungsbereich)	68
II. Ausnahmen vom Anwendungsbereich der DS-GVO.....	69
III. Der räumliche Anwendungsbereich	71
C. Grundsatz der Rechenschaftspflicht und Datenschutzorganisation	73
D. Rechtfertigungstatbestände	75
E. Recht auf Datenübertragbarkeit	78
F. Privacy by Design und Privacy by Default	81

I.	Die Sicherstellung der Einhaltung von Art. 25 DS-GVO durch den Verantwortlichen und Maßnahmen zur Risikominimierung gegenüber dem Hersteller	81
II.	Die Sicherstellung der Einhaltung von Art. 25 DS-GVO durch den Verantwortlichen und Maßnahmen zur Risikominimierung gegenüber dem Auftragsverarbeiter	84
G.	Meldung von Datenschutzverletzungen	84
I.	Meldung an die Aufsichtsbehörde	85
II.	Meldung innerhalb von 72 Stunden nach Kenntnis	85
III.	Maßnahmenplan bei Datenschutzverletzung	87
IV.	Verpflichtung der Beschäftigten	88
H.	Auftragsverarbeitung und internationaler Datentransfer	89
I.	Auftragsverarbeitung nach der DS-GVO	89
II.	Internationaler Datentransfer	91
§ 2.2	Internationaler Transfer personenbezogener Daten	93
A.	Einleitung	94
B.	Grundsätze des Datentransfers	95
I.	Innerhalb Deutschlands/EU/EWR.	95
II.	Außerhalb der EU/dem EWR.	96
C.	Internationaler Datentransfer (im Einzelnen)	97
I.	Artikel 45 DS-GVO – Datentransfer aufgrund eines Angemessenheitsbeschlusses	97
1.	Grundsätze	97
2.	Gegenwärtig bestehende Angemessenheitsbeschlüsse	99
3.	Folgen und Auswirkungen auf bestehende Angemessenheitsbeschlüsse	99
4.	Überprüfung von Angemessenheitsbeschlüssen.	100
5.	Privacy Shield (als Sonderfall des Angemessenheitsbeschlusses)	100
a)	Einleitung und Hintergrund.	100
b)	Entwicklung	101
aa)	Safe Harbor-Abkommen	101
bb)	Safe Harbor-Urteil.	101
cc)	Privacy Shield.	102
c)	Kritik.	103
d)	Alternativen und Ausblick.	105
II.	Artikel 46 DS-GVO.	105
1.	Einleitung und Hintergrund.	105
2.	Behördenvereinbarungen.	109
3.	Verbindliche interne Datenschutzvorschriften – Artikel 47 DS-GVO.	110
a)	Einleitung und Hintergrund.	110
b)	Adressatenkreis	114

c) Inhaltliche Anforderungen	116
aa) Interne rechtliche Verbindlichkeit	116
bb) Vermittlung durchsetzbarer Rechte	118
cc) Inhaltliche Mindestanforderungen	120
d) Verfahren zur Genehmigung	122
e) Fortgeltung bestehender BCR	125
4. Standarddatenschutzklauseln, die von der Kommission erlassen werden	126
a) Einleitung und Hintergrund	126
b) Existierende Standarddatenschutzklauseln	127
c) Standarddatenschutzklauseln zwischen Verantwortlichen.....	127
d) Standarddatenschutzklauseln für Auftragsverarbeiter .	129
5. Standarddatenschutzklauseln von einer Aufsichtsbehörde	130
6. Genehmigte Verhaltensregeln gemäß Artikel 40.....	131
a) Grundsätze	131
b) Entstehungsprozess	132
c) Genehmigte Verhaltensregeln	132
d) Für allgemein gültig erklärte Verhaltensregeln	132
e) Überwachungsstellen	133
f) Rechtswirkung	133
g) Ausblick.....	134
h) Praxiserfahrung.....	135
7. Genehmigter Zertifizierungsmechanismus.....	136
a) Einleitung.....	136
b) Verfahren	136
c) Vorgehen	136
d) Kleine und mittlere Unternehmen	137
e) Fazit	138
8. Artikel 46 Abs. 3 – Genehmigungsbedürftige Garantien..	139
III. Artikel 49	140
1. Artikel 49 Abs. 1 UAbs. 1 lit. a)	141
2. Artikel 49 Abs. 1 UAbs. 1 lit. b)	142
3. Artikel 49 Abs. 1 UAbs. 1 lit. c)	143
4. Artikel 49 Abs. 1 UAbs. 1 lit. d).....	144
5. Artikel 49 Abs. 1 UAbs. 1 lit. e)	144
6. Artikel 49 Abs. 1 UAbs. 1 lit. f)	146
7. Artikel 49 Abs. 1 UAbs. 1 lit. g)	146
8. Artikel 49 Abs. 1 UAbs. 2, Abs. 6	147
9. Artikel 49 Abs. 3	149
10. Artikel 49 Abs. 5.....	149
D. Brexit-Problematik: Welche Lösungen kann es geben?	150
E. Fazit	151

§ 2.3 Datenschutz bei Virtual und Augmented Reality	153
A. Einführung: AR und VR	155
I. Gang der Untersuchung	156
II. Technische Grundlagen und Funktionen.....	156
1. Technische Grundlagen	156
2. Datenschutzrechtlich relevante Funktionen	157
a) VR-Funktionen	157
b) AR-Funktionen	159
B. AR und VR aus datenschutzrechtlicher Perspektive	159
I. Vorrang der Verordnung über Privatsphäre und elektronische Kommunikation („ePrivacy-Verordnung (E)“)	159
II. Anwendbarkeit des Datenschutzrechts	160
1. Sachlich	160
2. Räumlich	161
III. Tracking des Nutzers	161
1. Körper-, Kopf- und Eye-Tracking für VR	162
a) „Interaktionsdaten“ des Nutzers als Gesundheitsdaten, Art. 9 Abs. 1 DS-GVO	162
b) Eye-Trackingdaten als biometrische Daten, Art. 9 Abs. 1 DS-GVO	165
c) Rechtmäßigkeit des Körper-, Kopf- und Eye-Trackings.....	166
aa) Anforderungen an die Einwilligung	166
bb) Anforderungen an die Einwilligung eines Kindes....	169
cc) Vereinbarkeit mit Datenschutzgrundsätzen	170
2. Tracking durch AR-Anwendungen	172
a) Verarbeitung von Standortdaten (Positions-Tracking)	172
b) Verarbeitung von Nutzerdaten für AR.....	173
c) Rechtmäßigkeit der Verarbeitung von Nutzerdaten für AR.....	173
3. Zusammenfassung.....	176
IV. Nutzung von Smartcams für AR und VR.....	176
1. Anwendungsvorrang des KUG	177
2. Rechtmäßigkeit der Umgebungserfassung durch Videostream für AR und VR?	180
a) Verarbeitung von Nutzerdaten und personenbezogenen Daten Dritter	180
b) Verarbeitung sensibler Daten, Art. 9 Abs. 1 DS-GVO	181
c) Nur bedingte Rechtmäßigkeit	182
3. Umgebungserfassung für AR als „Videoüberwachung öffentlich zugänglicher Räume“, § 4 BDSG?	185
4. Rechtmäßigkeit der dreidimensionalen Erfassung des physischen Raums für eine „AR-Cloud“	187
a) Verarbeitung personenbezogener Daten.....	188
b) Rechtmäßigkeit einer AR-Cloud?.....	189

5. Zusammenfassung	191
V. Rechtmäßigkeit des AR-Einsatzes im Arbeitsumfeld	192
1. Verarbeitung von Beschäftigtendaten durch AR-Nutzung	193
2. Rechtmäßigkeit nach § 26 Abs. 1 BDSG	193
3. Einwilligung des Arbeitnehmers	194
4. Zusammenfassung	196
VI. Data Protection by Design und Data Protection by Default: Pflichten von AR- und VR-Anbietern, Art. 25 DS-GVO	196
1. Data Protection by Design	196
2. Data Protection by Default	199
VII. Erforderlichkeit einer Datenschutz-Folgenabschätzung für AR- und VR-Anwendungen, Art. 35 DS-GVO	199
C. Zusammenfassung und Ausblick	200
§ 2.4 Datenschutz im Onlinemarketing	203
A. Übersicht	204
I. Einführung	204
II. Arten und Werkzeuge des Onlinemarketings	206
1. Cookies, Digital Fingerprinting und Werbe-IDs	207
2. Targeting	208
a) Tracking	209
b) Profiling und Online-Behavioral-Advertising	209
c) Cross-Media-Marketing (Cross-Device-Tracking)	210
d) Re-Marketing	211
3. Social Media-Marketing	211
4. E-Mail-Werbung	212
B. Rechtsgrundlagen	212
I. DS-GVO	212
II. BDSG	214
III. TMG und TKG	215
IV. ePrivacy-Verordnung	216
1. Allgemeines	216
2. Verordnungsentwurf der Kommission	217
3. Wesentliche Inhalte des Entwurfs nach dem LIBE-Ausschuss	219
C. Einzelprobleme	220
I. Verbot mit Erlaubnisvorbehalt – die Erlaubnistatbestände der DS-GVO	220
1. Berechtigte Interessen, Art. 6 Abs. 1 S. 1 lit. f)	220
2. Vertragserfüllung	222
3. Einwilligung	222
a) Widerruflichkeit	223
b) Formerfordernisse	224
c) Abgabe in Kenntnis der Sachlage und für den konkreten Fall	224
d) Alteinwilligungen	227

e) Elektronische Form der Einwilligung	229
f) Freiwilligkeit und Koppelungsverbot	230
II. Gestattung einzelner Marketingmaßnahmen	232
1. Tracking mittels Cookies, Fingerprints, Werbe-IDs	232
a) Bisherige Rechtslage	232
b) Rechtslage nach der DS-GVO – Interimslösung	233
c) Ausblick ePrivacy-Verordnung	235
2. Analytics	237
3. Profiling	238
4. Cross-Media-Marketing (Cross-Device-Tracking)	240
5. Social Media-Marketing	241
a) Social Plugins	241
b) Verantwortlichkeit von Social Media-Seitenbetreibern	242
6. E-Mail-Werbung	244
a) UWG	245
b) Datenschutzrecht	247
III. Betroffenenrechte	249
1. Auskunft (Art. 15 DS-GVO)	249
2. Berichtigung (Art. 16 DS-GVO)	249
3. Löschung (Art. 17 DS-GVO)	249
4. Einschränkung der Verarbeitung (Art. 18, 19 DS-GVO) ..	250
5. Datenübertragbarkeit (Art. 20 DS-GVO)	250
6. Widerspruch (Art. 21 DS-GVO)	250
§ 2.5 Auswirkungen der ePrivacy-Verordnung	
im Automobilssektor	251
A. Einführung	251
B. Kernpunkte der neuen ePrivacy-Verordnung	253
I. Tragende Erwägungsgründe	253
II. Wesentliche Bestimmungen der neuen ePrivacy-Verordnung ..	263
III. Problempunkte in der neuen ePrivacy-Verordnung	268
C. Auswirkungen der neuen ePrivacy-Verordnung auf den	
Bereich vernetztes Fahren („Connected Cars“)	270
I. Automatisierte Fahrzeugsysteme und vernetztes Fahren ..	270
II. Technische Anwendungen im Bereich Connected Cars	273
III. Elektronische Kommunikation im Bereich Connected Cars	
und Verarbeitung der insoweit erhobenen Daten	276
D. Fazit	280
§ 3 Privacy Paradox	283
§ 3.1 Kundenwahrnehmungen und Kundenverhalten beim Bezahlen	
von digitalen Dienstleistungen mit personenbezogenen Daten ..	285
A. Einleitung	288
B. Privacy Calculus Theorie	290
I. Nutzenwahrnehmung	291

II. Risikowahrnehmung	291
C. Einflussfaktoren auf die Kundenwahrnehmung der Datenpreisgabe.	292
I. Individuelle Faktoren	292
1. Generelle Privatsphärebedenken	292
2. Sozio-demografische Faktoren	293
3. Persönlichkeitsmerkmale	293
4. Individuelle Neigungen	294
5. Individuelle Erfahrungen	295
6. Kulturelle Faktoren.....	295
II. Service- und unternehmensspezifische Faktoren	296
1. Sensibilität der Daten	296
2. Relevanz der Daten.....	297
3. Kontrolle	297
4. Vertrauen	298
III. Schutzmöglichkeiten	299
1. Individueller Selbstschutz	300
2. Stellvertreterkontrolle.....	301
D. Affektive Prozesse bei der Kundenwahrnehmung	302
E. Zusammenfassung und Handlungsempfehlungen	303
§ 3.2 Das Privacy Paradox aus psychologischer Perspektive	305
A. Einleitung	307
B. Was ist Privatheit?.	308
C. Wie lässt sich Verhalten erklären?	310
D. Wie lässt sich Verhalten im Internet verstehen?.	312
I. Personenbezogene Faktoren.....	312
II. Umweltbezogene Faktoren.....	313
E. Das Privacy Paradox	314
I. Historie	314
II. Analyse	316
F. Diskussion	319
I. Bewertung.....	319
II. Gesellschaftliche Implikationen	321
G. Fazit	323
§ 3.3 Informationsvermittlung durch standardisierte Bildsymbole	324
A. Einleitung	325
B. Gang der Untersuchung	328
C. Scheitern der textbasierten datenschutzrechtlichen Einwilligung	329
D. Konzepte effizienter Informationsvermittlung	331
E. Vorteile visueller Informationsvermittlung	334
F. Informationspflichten der Datenschutzerklärung	335

I.	Informationspflichten nach der DS-GVO	336
II.	Informationspflichten nach BDSG-neu und TMG	337
III.	Entfall von Informationspflichten	338
IV.	Zur Visualisierung geeignete Informationen	338
G.	Erforderlichkeit eines Schichtenmodells.	339
I.	Ausgestaltung	339
II.	Rechtliche Zulässigkeit des Schichtenmodells	341
H.	Vorteile der Verwendung des Schichtenmodells.	342
I.	Fazit.	343
§ 3.4	Potentiale der Informationsvisualisierung im Datenschutz – eine kommunikationswissenschaftliche Betrachtung	345
A.	Einleitung	345
B.	Vergleichbare Ansätze im Datenschutz	349
I.	Die Entwicklung einer Bildsprache für Datenverarbeitungsvorgänge	350
II.	Creative Commons-Ansatz im Datenschutz	351
C.	Informationsvisualisierung durch Icons	353
§ 4	Vermögensrechte an Daten	361
§ 4.1	Dateneigentum, Datenzugangsrechte und Datengovernance aus ökonomischer Perspektive	363
A.	Einleitung	363
B.	Zur Diskussion über ein Ausschließlichkeitsrecht an Daten. ..	364
C.	Zur Diskussion über Zugangsrechte an Daten und optimale Governance-Lösungen für Daten	367
§ 4.2	Rechtspositionen an Daten:	
	Die Rechtslage im europäischen Rechtsraum	371
A.	Einleitung.	373
B.	Rechtspositionen an Daten im Rechtsraum der Europäischen Union.	375
I.	Schutz von Daten über den Eigentumsschutz am Trägermedium	375
II.	Urheberrechtlicher Schutz von Datenbanken und Datenbankwerken	376
1.	Ausschließliches Recht an Daten bei Datenbankwerken ..	377
a)	Inhalt und Struktur des Datenbankwerks	377
b)	Unabhängige Zugänglichkeit	377
c)	Schutz von Daten in Form eines Datenbankwerks ..	378
2.	Sui generis-Leistungsschutzrecht von Datenbanken	378
3.	Fazit	380
III.	Schutz von Geschäftsgeheimnissen	380
1.	Geheimnisschutz = Schutz von Informationen	381

2. Daten als Geschäftsgeheimnisse	382
3. Möglichkeit einer Datenzuordnung	383
IV. Schutz von Daten über das Datenschutzrecht.....	383
1. Datenschutz und Schutz von Daten.....	384
2. Inhaltliche Ausgestaltung des Datenschutzrechts.....	384
a) Das Recht auf Datenübertragbarkeit nach der DS-GVO	385
b) Das Recht auf Datenübertragbarkeit nach französischem Beispiel	386
3. Fazit	386
V. Zusammenfassung	387
C. Wie werden Daten vertragsrechtlich behandelt?	388
I. Status Quo in der Praxis.....	388
II. Richtlinienvorschlag über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte.....	390
D. Wie werden Daten eines Unternehmens in der Insolvenz behandelt?	392
I. Daten des Insolvenzschuldners	393
1. Zuordnungsanforderungen für die Massebefangenheit ...	393
2. Sonderfall: Datenschutzrechtliche Position eines Dritten .	394
II. Insolvenz des Cloud-Anbieters und Daten Dritter.....	395
III. Vorreiterrolle Luxemburg.....	396
IV. Zusammenfassung	397
E. Entwicklungen/Bestrebungen der Europäischen Union/ auf Unionsebene	397
I. Mitteilung „Aufbau einer Europäischen Datenwirtschaft“ ..	398
1. Zugang zu Daten.....	398
2. Interoperabilität von Daten	399
3. Data Producer’s Right	400
II. Zusammenfassung	401
F. Ansätze der Wissenschaft, Daten zuzuordnen	401
I. Herleitung eines Dateneigentums aus § 303a StGB.....	402
II. Recht am eigenen Datenbestand	404
III. Zuordnung über das Datenschutzrecht	405
IV. Zusammenfassung	405
G. Zusammenfassung und Ausblick	406
§ 4.3 Rechtspositionen an Daten: Die Rechtslage in den USA	408
A. Einführung	410
B. Daten und Informationen	411
C. Eigentumsrechte an Informationen an sich und in Werken, Datenbanken, Gegenständen und Immobilien	413
I. Eigentum im amerikanischen Recht	413
II. Immobilieneigentum (Real Property)	417
III. Eigentum an beweglichen Sachen (Personal Property)	418

IV. Schutz von Geschäftsgeheimnissen (Trade Secret Law)	419
V. Patente	420
VI. Markenrecht (trademark law)	421
VII. Urheberrecht (copyright law)	422
VIII. State law on misappropriation – Schutz vor missbräuchlicher Verwendung.	425
IX. Data Privacy – Schutz der Privatsphäre	426
X. Zusammenfassung.	428
D. Rechte und Beschränkungen des Zugriffs auf Informationen	429
I. Beschränkungen zum Schutz der Privatsphäre (data privacy law)	429
II. Computer Interference Laws	429
III. Umwelt- und Wettbewerbsrecht.	429
IV. Verträge	430
V. Konkursrecht.	431
E. Interessen an Daten	431
I. Fahrzeugeigentümer	431
II. Fahrer und Passagiere	432
III. Andere Verkehrsteilnehmer	433
IV. Hersteller	433
V. Zusatzdienstanbieter.	435
VI. Autohändler und -lieferanten	435
VII. Versicherungsgesellschaften	436
VIII. Strafverfolgung und Regierungsbehörden.	436
F. Sollte ein neues Eigentumsrecht an Daten geschaffen werden?	437
I. Kreativität und technologischer Fortschritt	437
II. Kontraindikation zum Schutz der Privatsphäre	439
G. Zusammenfassung	439
§ 4.4 Rechtspositionen an Daten: Die Rechtslage in China	440
A. Einleitung.	442
B. Rechtspositionen an Daten in China	443
I. Schutz von Geschäftsgeheimnissen.	443
1. Definition des Geschäftsgeheimnisses	443
a) Nicht öffentlich	444
b) Geschäftlicher Wert	445
c) Geheimhaltung.	446
2. Tatbestand des § 9 cUWG	447
3. Rechtsfolgen	448
a) Zivilrechtliche Rechtsfolgen	448
b) Verwaltungsrechtliche Rechtsfolgen	449
c) Strafrechtliche Rechtsfolgen	450
II. Schutz von Datenbanken und Datenbankwerken	451
1. Urheberrechtlicher Schutz von Datenbankwerken	451
a) Schutzvoraussetzungen	451

b) Schutz von Daten in Form eines Datenbankwerks ...	452
c) Rechtsinhalte und Schrankenregelungen	453
2. Wettbewerbsrechtlicher Schutz von Datenbanken	453
III. Schutz von Daten über das Datenschutzrecht	454
1. Definition der „Personenbezogenen Information“	457
2. Inhaltliche Ausgestaltung	457
3. Rechtsfolgen	458
IV. Strafrechtlicher Schutz von personenbezogenen Daten	459
C. Wie werden Daten vertragsrechtlich behandelt?	461
D. Wie werden Daten eines Unternehmens in der Insolvenz behandelt?	463
E. Ansätze und Entwicklung	464
I. Dateneigentum	464
II. Data Controller: Recht am eigenen Datenbestand	465
III. Datenrecht sui generis	466
F. Zusammenfassung und Ausblick	467
§ 5 Vertragsrechtliche Implikationen	469
§ 5.1 Preis- und Wertermittlung für Daten und Informationen	471
A. Bedeutungszunahme von Daten und Notwendigkeit der Wertermittlung	472
B. Begriffsverständnis und Zusammenhang von Daten und Informationen	474
C. Wie kann man Daten messen?	476
D. Herausforderungen in Verbindung mit der monetären Bewertung von Daten	478
E. Der Preis von personenbezogenen Daten	481
F. Methoden zur Ermittlung des Datenwerts	483
G. Fazit	487
§ 5.2 Daten als Leistungsgegenstand: Vertragsrechtliche Typisierung ..	489
A. Abgrenzung Daten als Gegenleistung und Daten als Leistungsgegenstand	490
B. Vorfragen	491
I. Personenbezug der Daten	491
II. Rechtlicher Rahmen	492
1. Datenschutzrechtlicher Rahmen	492
2. Strafrechtlicher Rahmen	493
3. Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union sowie die geplante Richtlinie zu Verträgen über digitale Inhalte	494
III. Konsequenzen bei Verstößen gegen den rechtlichen Rahmen	494
1. Mögliche Nichtigkeit nach § 134 BGB	494

2. Datenschutzaufsicht, Verbandsklagerecht bzw. Sanktionen im Datenschutzrecht	495
C. Denkbare Vertragsinhalte	495
D. Bisherige Einordnung durch die Rechtsprechung	496
E. Vertragstypologische Einordnung	497
I. Kaufvertrag	498
1. Sachkauf (§§ 433 ff. BGB)	498
2. Rechtskauf bzw. Kauf eines sonstigen Gegenstandes (§ 453 BGB)	498
II. Werklieferungsvertrag § 650 BGB	500
III. Werkvertrag (§ 631 BGB)	501
IV. Mietvertrag (§ 535 BGB)	501
V. Pacht (§ 581 BGB)	502
VI. Dienstvertrag (§ 611 BGB)	503
F. „Steuerungsmöglichkeiten“ im Vertrag	504
§ 5.3 Daten als Gegenleistung im Vertrag mit Blick auf die Richtlinie über digitale Inhalte	506
A. Einführung	509
B. Vorschlag einer Richtlinie über digitale Inhalte (DIRL)	512
I. Hintergrund, Ziele und Entwicklung	512
II. Verhältnis der DIRL zu anderen Rechtsakten	513
1. Datenschutzrechtliche Regelungen	513
2. Vertragsrechtliche Regelungen	513
III. Partieller Vollharmonisierungsansatz der DIRL	514
C. Inhalt und Anwendungsbereich der DIRL	515
I. Personeller Anwendungsbereich	515
II. Sachlicher Anwendungsbereich	516
1. Verträge über die Bereitstellung von digitalen Inhalten ..	516
2. Ausgenommene Verträge	517
3. Daten als Gegenleistung	518
a) Gemäß Art. 3 Abs. 1 DIRL gegenleistungsfähige Daten	519
b) Einwilligung oder Daten als Leistungsgegenstand? ..	520
aa) Meinungsstand	520
bb) Stellungnahme und eigener Ansatz	522
(1) Grundsatz der informierten Einwilligung	523
(2) Unternehmenspraxis und ökonomische Erwägungen .	525
(3) Missachtung der Anbieterinteressen	525
(4) Autonome Erfüllung durch den Schuldner wird unmöglich	527
(5) Eigener Ansatz: Einwilligung als Wirksamkeitsvoraussetzung	528
cc) Auswirkungen des Art. 6 Abs. 1 lit. b) DS-GVO	529
dd) Freiwilligkeit und Wirksamkeit der Einwilligung	530

(1) Freiwillige Einwilligung und Koppelungsverbot	531
(2) Daten als Gegenleistung und Koppelungsverbot	531
(3) Folgen eines Verstoßes gegen das Koppelungsverbot. .	533
ee) Widerruflichkeit der Einwilligung	534
c) Synallagmatische Verknüpfung von Leistung und Gegenleistung?	539
aa) Auswirkungen.	541
bb) Daten zur Erfüllung vertraglicher und gesetzlicher Pflichten	542
(1) Personenbezogene Daten zur Erfüllung vertraglicher Pflichten	542
(2) Personenbezogene Daten zur Erfüllung rechtlicher Pflichten	544
(3) Sonstige Daten.	544
cc) Rechtsfolge bei unberechtigter Kommerzialisierung der von Art. 3 Abs. 1 UAbs. 2 DURL erfassten Daten	545
dd) Passive Datenpreisgabe	546
d) Entgeltcharakter der Daten als Gegenleistung	548
e) Einheiten von Kryptowährungen als Gegenleistung ..	550
4. Schuldrechtliches oder dingliches Rechtsgeschäft?	551
D. Leistungspflichten und Rechtsbehelfe bei Leistungsstörungen	554
I. Leistungszeit	554
II. Leistungsinhalt	555
III. Vertragsbeendigung	557
§ 5.4 Datenbestände in der Unternehmens-Transaktion (M&A)	560
A. Einführung	561
I. Grundlagen: Formen des Unternehmenskaufs.	563
1. Asset-Deal	563
2. Share-Deal	563
II. Strukturierung/Vorbereitung der Transaktion durch Due Diligence und Geheimhaltungsvereinbarung/NDA	564
III. Bedeutung der Rechtswahl.	565
1. Vertragsstatut	565
2. Territorialitätsprinzip	566
IV. Kategorisierung der datenrechtlichen Bezugsobjekte	567
1. Sondergesetzlich geschützte Daten	567
a) Urheberrecht und verwandte Schutzrechte.	567
b) Geschäfts- und Betriebsgeheimnisse, Know-how	567
c) Personenbezogene Daten.	570
2. Vertraglich geschützte Daten.	571
B. Daten im Asset-Deal	572
I. Sondergesetzlich geschützte Daten	572
1. Urheberrecht und verwandte Schutzrechte	572
2. Geschäfts- und Betriebsgeheimnisse, Know-how.	574
a) Konkretisierung des Know-hows.	575

b) Verkäuferpflichten im Zusammenhang mit der Überlassung des Know-hows.	576
c) Absicherungsklauseln	576
3. Personenbezogene Daten.	577
a) Offenlegung anonymisierter und pseudonymisierter Daten im Rahmen eines Asset-Deals	578
b) Insbesondere: Datenschutzrechtliche Beurteilung der Due Diligence	579
c) Übertragung von Mitarbeiterdaten	580
d) Erwerb von Kundendaten.	582
aa) Kundendaten aus bestehenden Vertragsverhältnissen .	582
bb) Isolierte Übertragung von Kundendaten	584
II. Vertraglich geschützte Daten.	586
C. Daten im Share-Deal	586
I. Sondergesetzlich geschützte Daten.	586
1. Urheberrecht und verwandte Schutzrechte	586
2. Geschäfts- und Betriebsgeheimnisse, Know-how	587
3. Personenbezogene Daten	587
II. Vertraglich geschützte Daten.	588
§ 5.5 Daten-Outsourcing	589
A. Outsourcing im Allgemeinen	590
I. Begriff des Outsourcings	590
II. Klassifizierung des Outsourcings als Auftragsverarbeitung oder sonstige Übermittlung.	591
III. Outsourcing im Konzern.	593
B. Cloud Computing	594
I. Definition des Cloud Computing und Virtualisierung	594
II. Beteiligte beim Cloud Computing	596
III. Cloud Modelle	597
IV. Cloud-Service Modelle.	598
V. Empfehlungen von Aufsichtsbehörden vor Inkrafttreten der DS-GVO	599
VI. Überblick über die datenschutzrechtlichen Herausforderungen beim Cloud Computing	600
VII. Anwendbares Recht	602
VIII. Übermittlung an einen Dritten oder Auftragsverarbeitung	604
IX. Ausgewählte cloud-spezifische Herausforderungen bei einer Auftragsverarbeitung	607
1. Dokumentation der Weisung und Weisungsgebundenheit	607
2. Offenlegung und schriftliche Fixierung der Subunternehmer	608
3. Unterstützungspflichten des Auftragsverarbeiters.	611
a) Anfragen von Betroffenen	611
b) Datenschutz-Folgenabschätzung und Meldepflichten.	613
c) Vergütung der Unterstützungsleistung	614

4. Datenlöschung	614
5. Prüf- und Auskunftsrechte des Verantwortlichen	615
6. Einschaltung von Auftragsverarbeitern oder Unterauftragsverarbeitern außerhalb der EU/EEA	616
7. Haftung des Auftragsverarbeiters	618
C. Daten- und IT-Sicherheit	618
I. Allgemeines	618
1. Beurteilung der technischen Situation und Entscheidung über die erforderlichen technischen und organisatorischen Maßnahmen	619
2. Konkrete Maßnahmen zur IT-Sicherheit	620
II. Herausforderungen der Datensicherheit im Bereich Cloud Computing	620
III. IT-Sicherheit und Zertifizierungen	623
1. Allgemeines	623
2. Genehmigte Verhaltensregeln und genehmigte Zertifizierungsverfahren unter der DS-GVO	625
a) Genehmigte Verhaltensregeln	625
b) Genehmigte Zertifizierungsverfahren	626
IV. Besonderheiten für „kritische Infrastrukturen“: Das BSIG	626
D. Verarbeitung besonderer Kategorien personenbezogener Daten	627
E. Herausgabeverlangen ausländischer Behörden und Gerichte	628
I. Extraterritoriale Zugriffsansprüche	629
II. Regelungen der DS-GVO zur Datenübermittlung und Offenlegung	630
III. Dilemma der in Anspruch genommenen Unternehmen	631
IV. Europäisches oder nationales Modell als Lösung?	631
F. Industrie- und sektorspezifische Herausforderungen bei der Weitergabe von Daten im Rahmen von Outsourcing und Cloud Computing	632
I. Strafbarkeit der Weitergabe von Daten durch Berufsgeheimnisträger	632
II. Outsourcing im Bank- und Finanzsektor	634
III. Outsourcing in der Healthcare-Industrie	638
§ 6 Kryptowährungen	641
§ 6.1 Bitcoin/E-Geld/Virtuelle Währungen	643
A. Daten als Zahlungsinstrumente mit ggf. weiteren Funktionen	644
I. Begriffsklärungen	644
II. Dimensionen	645
B. Funktionsweise	645
I. Autonomie des Systems	645
II. Forderungscharakter	646

III. Weitere Funktionalitäten	646
IV. Token-Design	647
C. Technische Realisierung	647
I. Technologische Grundlagen	647
1. Kryptographische Hashfunktionen	647
2. Kryptographische Signatur	648
II. Ablage auf einem Server	650
III. Ablage auf einer Blockchain	651
1. Bitcoin und die Bitcoin-Blockchain	651
a) Grundprinzipien	651
b) Bitcoin-Adressen	652
c) Bitcoin-Transaktionen	653
d) Bitcoin-Blöcke	654
e) Mining (Proof-of-Work)	655
f) Bitcoin-Wallets	656
g) Bitcoin-Exchanges	659
h) Privatheit der Transaktionen	659
2. Weiterentwicklungen	660
a) Payment Channels und Lightning Networks	660
b) Anonyme Transaktionen	662
c) Smart Contracts	664
d) Gerichteter azyklischer Graph (DAG)/Hashgraph ..	665
e) Andere Consens-Mechanismen	667
f) Consortium Blockchains	668
3. Probleme und Grenzen der Blockchains	669
a) Energieverbrauch des Proof-of-Work Mining	669
b) Skalierbarkeit und Transaktionsgebühren	670
c) Blockchain-Governance	671
IV. Ablage auf einem Speichermedium des Inhabers	673
1. Geldkarte	673
2. Payment Channels und nicht publizierte signierte Transaktionen	674
D. Juristische Einordnung	674
I. Bitcoins	674
1. Rechtsnatur im Zivilrecht	674
2. Token-Economy/Sachenrecht	675
3. Vertrags- und Leistungsstörung	676
4. Zwangsvollstreckung	676
5. Strafrechtliche Vermögensabschöpfung	677
a) Einziehbare Objekte	677
b) Grund der Einziehung	678
c) Non-conviction-based confiscation	678
d) Beschlagnahmung	679
6. Regulierung	679
a) Aktuelle Regulierung	679

b) Weitere Entwicklung der Regulierung	680
c) Internationale Regulierung	681
7. Datenschutz	682
a) Personenbezogene Daten	682
b) Haushaltsausnahme	683
c) Datenschutzrechtlich Verantwortlicher	683
d) Auftragsverarbeiter	684
e) Rechtfertigung	684
f) Weitere Anwendungen	685
8. Haftung für illegale Inhalte	686
II. E-Geld	687
1. Wann handelt es sich um E-Geld?	687
2. Erlaubnisvorbehalt	690
III. Verschieden Tokenarten – Klassifikation für Initial Coin Offerings (ICOs)	690
1. Kryptowährungen – Zahlungs-Token	690
2. Utility Token – Nutzungs-Token	690
3. Security/Asset Token – Anlage-Token	691
E. Ausblick	692
§ 6.2 Die Besteuerung von Kryptowährungen	693
A. Einleitung	693
B. Kryptowährungen im deutschen Steuerrecht	696
I. Ertragsteuer	696
1. Einordnung als immaterielles Wirtschaftsgut	696
2. Einkunftsart	698
a) Überblick	698
b) Abgrenzung der privaten von der gewerblichen Tätigkeit	699
3. Gewerbliche Einkünfte	703
a) Bilanzierende Unternehmen	703
aa) Bilanzierungsfähigkeit von Kryptowährungen	703
bb) Aktivierung und ertragsteuerliche Folgen	704
(1) An- und Verkauf von Kryptowährungen gegen Euro ..	704
(2) An- und Verkauf von Kryptowährungen im Tausch gegen andere Wirtschaftsgüter	704
(3) Selbst geschaffene Kryptowährungen	705
b) Sonstige Unternehmer, § 4 Abs. 3 EStG	707
c) Besteuerung von ICOs	707
4. Nicht gewerbliche Einkünfte	708
a) Einkünfte aus dem Verkauf und Tausch von Kryptowährungen	709
aa) Einkünfte aus Kapitalvermögen gem. § 20 EStG?	709
(1) Überblick	709
(2) Keine Einkünfte aus Kapitalvermögen durch Veräußerung von Kryptowährungen	710

bb) Einkünfte aus privaten Veräußerungsgeschäften gem. § 23 EStG.	711
(1) Anschaffung	711
(2) Veräußerung	712
(3) Haltefrist	712
(4) Fristberechnung	714
(5) Ermittlung des Veräußerungsgewinns	717
(6) Zeitpunkt der Besteuerung	722
b) Sonstige Einnahmen im Zusammenhang mit Kryptowährungen	723
aa) Hard Forks	723
bb) Airdrops	724
cc) Mining	726
II. Umsatzsteuer	728
1. Der Einsatz von Kryptowährungen als Entgelt	728
2. Mining von Kryptowährungen	732
C. Grenzüberschreitende Aktivitäten von Unternehmen mit Sitz in Deutschland	733
I. Einsatz von Kryptowährungen als Zahlungsmittel	733
II. Mining-Aktivitäten	734
D. Sonstige Kryptoassets und die Forderung nach einer Datensteuer	735
I. Sonstige Kryptoassets	736
1. Security und Equity Token	736
2. Utility Token	737
3. Forwards und Futures	740
4. Sonstige virtuelle Wirtschaftsgüter	740
II. Die Forderung nach einer Besteuerung von Daten (Digitalsteuer)	741
§ 7 Marktmacht durch Daten	743
§ 7.1 Marktmacht durch Daten:	
Eine Analyse aus ökonomischer Perspektive	745
A. Einführung	748
B. Wettbewerbsvorteile durch Daten	750
I. Datensammlung und Profilbildung mittels Trackingtechnologien	751
II. Datengetriebene Qualitätsverbesserung und Personalisierung	753
III. Zielgerichtete Werbung	756
IV. Preisdiskriminierung	760
C. Marktmacht durch Daten	762
I. Zugang zu Daten	762
II. Netzwerkeffekte und mehrseitige Märkte	764
III. Wechselkosten	766

IV. Skalen-, Verbund- und Feedbackeffekte.....	768
V. Zugangsgewährung und Datenaustausch	770
VI. Diskriminierung, vertikale Integration und Marktmacht- übertragung.....	771
1. Diskriminierung von Drittanbietern in Plattformmärkten	772
2. Marktmachtübertragung.....	772
D. Maßnahmen zur Abschwächung von Datenmacht	774
I. Erhöhung der Transparenz.....	774
II. Recht auf Datenübertragbarkeit.....	775
III. Zugangsverpflichtung zu Datenpools	776
E. Schlussbemerkungen	777
§ 7.2 Marktmacht durch Daten:	
Eine Analyse aus rechtswissenschaftlicher Perspektive	779
A. Einleitung und kartellrechtliche Hintergründe	781
I. Verbot des Missbrauchs einer marktbeherrschenden Stellung	783
II. Fusionskontrolle	784
III. Verbot wettbewerbsbeschränkender Kooperationen.....	784
B. Daten und Marktmacht.....	786
I. Marktbestimmung bei datenbezogenen Geschäftsmodellen..	786
1. Defizite herkömmlicher Bestimmungsmöglichkeiten bei Plattformen	786
2. Kartellrechtliche Erfassung von Plattformen.....	788
3. Unentgeltliche Leistungen und „Bezahlung mit Daten“ ..	789
4. Unterschiedliche Kategorien von Daten	790
II. Datenmacht und Marktmacht	791
1. Marktanteilsbezogene Bewertung der Marktstellung....	791
2. Marktbeherrschung bei Plattformen.....	792
a) Netzwerkeffekte	792
b) Multi-Homing.....	793
c) Skalierung und Größenvorteile.....	795
d) Zugang zu Daten	796
e) Innovation	798
3. Relative oder überlegene Marktmacht	801
III. Marktmachtmissbrauch.....	803
1. Verhältnis des Missbrauchsverbots zu anderen objektiven Rechtsmaterien	803
2. Essential Facilities Doctrine und Geschäftsverweigerung .	804
3. Behinderungsmisbrauch und Lock-in.....	806
4. Diskriminierungsmisbrauch	807
5. Ausbeutungsmisbrauch.....	808
C. Zugangsbedingungen zu Daten	811
I. Informationsaustausch.....	812
1. Outsourcing und Lieferantenplattformen	813
2. Daten-Kooperationen.....	815

3. Blockchain.....	816
II. Standardisierung und Normierung.....	817
III. Schnittstelleninformationen.....	819
§ 8 Digitale Geschäftsmodelle – Datenbasierte Chancen und Risiken für Unternehmen.....	821
A. Der unternehmerische Zielkonflikt.....	823
B. „Data is the new oil“.....	829
I. Daten als Basis digitaler Geschäftsmodelle.....	830
II. Datengetriebene Geschäftsmodelle.....	830
1. Datenstrategie.....	833
2. Data Governance und Datenmanagement.....	834
C. DS-GVO – Der Schutz des Kunden.....	836
D. Herausforderungen digitaler Geschäftsmodelle im Spannungsfeld Innovation vs. Sicherheit.....	838
E. Fazit: Datengetriebene Vision und Verantwortung.....	840
§ 9 Haftung für fehlerhafte Daten.....	843
§ 9.1 Haftung für fehlerhafte Gesundheitsdaten.....	845
A. Digitalisierung im Gesundheitswesen.....	846
I. Hintergrund.....	846
II. Aktuelle Entwicklungen.....	847
1. Medizin 4.0.....	847
2. Telemedizin.....	847
3. Mobile Health.....	849
III. Rechtliche Einordnung digitaler Gesundheitsprodukte und -anwendungen.....	850
1. Hintergrund.....	850
2. Produktklassifizierung durch Zweckbestimmung und Wirkweise.....	851
3. Software als Medizinprodukt.....	851
4. Grenzen subjektiver Zweckbestimmung.....	852
5. Exkurs: Software als Arzneimittel.....	853
IV. Marktteilnehmer im Bereich digitaler Gesundheitsprodukte und -anwendungen.....	853
B. Fehlerhafte Gesundheitsdaten.....	854
I. Definition der Gesundheitsdaten.....	854
II. Ebenen der Fehlerhaftigkeit.....	854
C. Haftung für fehlerhafte Gesundheitsdaten.....	855
I. Haftung für Medizinprodukte.....	856
1. Haftung vor Marktreife.....	856
a) § 823 Abs. 2 BGB.....	856
b) ProdHaftG.....	857
aa) Anwendbarkeit des ProdHaftG.....	857

bb) Berücksichtigung des § 1 Abs. 2 Nr. 5 ProdHaftG	859
c) Ergebnis	859
d) Exkurs: Probandenversicherung	859
2. Haftung nach Marktreife	860
a) § 823 Abs. 1 BGB	860
aa) Umfang der Verkehrssicherungspflichten	860
(1) Konstruktions-, Fabrikations- und Instruktionspflichten	861
(2) Produktbeobachtungspflichten	861
(3) Reaktionspflichten	862
bb) Konkretisierung der Verkehrssicherungspflichten bei Medizinprodukten	862
(1) Produktbeobachtungspflichten nach § 3 MPSV	863
(2) Reaktionspflichten nach § 14 MPSV	863
b) § 823 Abs. 2 BGB	864
aa) Verletzung von Schutzgesetzen	864
bb) § 4 MPG als Schutzgesetz	865
cc) Exkurs: IT-Sicherheitsgesetze als Schutzgesetze	865
c) ProdHaftG	865
aa) Fehlerhafte Produkte	866
bb) Produkthersteller	866
cc) Software als Produkt	866
dd) Beweislastumkehr nach EuGH	867
d) Ergebnis	868
II. Haftung für sonstige Produkte	869
III. Exkurs: Haftungsbeschränkungen	870
1. Gesetzliche Haftungsbeschränkungen	870
2. Vertragliche Haftungsbeschränkungen	871
a) AGB	871
b) Einbeziehung gegenüber dem tatsächlichen Nutzer	871
c) Inhaltliche Grenzen von AGB	872
d) Ergebnis	872
D. Schluss/Ausblick	872
§ 9.2 Haftung für fehlerhafte Daten beim autonomen Fahren	874
A. Einleitung	877
I. Daten als „Antrieb“ autonomer Fahrzeuge	877
II. Präzisierung der Fragestellung	878
III. Gang der Darstellung	879
IV. Disclaimer	879
B. Autonomes Fahren: Rechtsbeziehungen im Internet der Dinge	880
I. Das digitale Ökosystem autonomer Fahrzeuge	880
1. In-Car-Technologien	881
2. Backend-Prozesse	882
3. V2V- und V2I-Kommunikation	883
II. Potentielle Fehlerquellen und Schädiger	884

C. Schadensersatzansprüche gegen den Nutzer des Fahrzeugs ..	885
I. Haftung für vermutetes Verschulden (§ 18 Abs. 1 S. 1 StVG)	885
II. Verschuldenshaftung (§ 823 Abs. 1 BGB)	886
D. Schadensersatzansprüche gegen den Fahrzeughalter	887
I. Gefährdungshaftung (§ 7 Abs. 1 StVG)	887
II. Abschaffung der Gefährdungshaftung de lege ferenda?	888
E. Schadensersatzansprüche gegen den Fahrzeugverkäufer	889
I. Sachmängelhaftung	889
II. Haftung für mangelhafte Backend-Daten	890
F. Schadensersatzansprüche gegen den Fahrzeughersteller	891
I. Haftungsszenarien	891
II. Haftungsgrundlagen	892
1. Überblick	892
2. Unterschiede zwischen der Produkt- und Produzentenhaftung	892
III. Produkt- und Produzentenhaftung für fehlerhafte Daten?	893
1. ProdHaftG	894
2. Deliktische Produzentenhaftung (§ 823 Abs. 1 BGB)	895
IV. Haftungssubjekte	896
1. Endhersteller	896
2. Zulieferer, insb. Software- und Datenlieferanten	896
3. Weitere Haftungssubjekte	897
V. Fabrikationsfehler	897
VI. Konstruktionsfehler	898
1. Fehlerhafte Software als Konstruktionsfehler	898
2. Technische Standards	898
3. Sicherheitserwartungen an die fahrzeugeigene Software.	899
4. Sicherheitserwartungen an selbstlernende Software	900
5. Grenzen der Herstellerhaftung: Stand von Wissenschaft und Technik	902
VII. Instruktionsfehler	903
VIII. Produktbeobachtungs- und Rückrufpflichten	904
1. Produktbeobachtungspflichten	904
2. Produktrückrufpflicht und Pflicht zum kostenlosen Software-Update	905
IX. Beweislastverteilung, insb. bei Konstruktionsfehlern	906
1. Beweisprobleme	906
2. Event Data Recorder	907
3. Zwischenergebnis	908
G. Schadensersatzansprüche gegen IT-Dienstleister, insb. Backend-Betreiber	908
I. Haftungsbegrenzungen nach dem TMG	909
1. Abgestufte Haftung nach dem TMG	909
2. Haftung von Backend-Betreibern	909
II. Vertragliche Gewährleistungshaftung	910

III. Deliktische Ansprüche aus § 823 Abs. 1 BGB.....	911
H. Ausblick	912
§ 9.3 Haftung für fehlerhafte Daten – Industrie 4.0	915
A. Industrie 4.0	916
I. Ziele	917
II. Wesentliche Herausforderungen	918
B. Haftungsrisiken	920
I. Vertragliche Gewährleistung.....	920
1. Schuldrechtliche Besonderheiten.....	921
2. Datenfehler.....	922
3. Verschuldensunabhängige Gewährleistungsrechte	922
4. Anspruch auf Schadenersatz oder Ersatz vergeblicher Aufwendungen	923
a) Vertretenmüssen	923
b) Haftungsfolgen	924
II. Außervertragliche Haftung.....	925
1. Verschuldensabhängige Deliktshaftung	925
a) Sach- oder Personenschäden	926
b) Schäden an Datenbeständen	927
aa) Eigentum an Daten.....	927
bb) Daten als „sonstiges Recht“ i. S. v. § 823 Abs. 1 BGB .	928
2. Produkthaftung	929
a) Anwendungsbereich.....	929
b) Herstellereigenschaft	930
c) Produktfehler	930
C. Haftungslücken in der Industrie 4.0	932
I. Unvermeidbare Fehler.....	933
II. Maschinenhaftung?	933
III. Mögliche Lösungsansätze	935
D. Maßnahmen zur Risikoreduzierung	936
I. Vertragliche Gestaltungsmöglichkeiten.....	936
II. Digital Governance	937
E. Fazit	939
§ 10 Datenbestände in Zwangsvollstreckung und Insolvenz.....	941
A. Einführung	944
I. Grundlagen zum Zwangsvollstreckungsrecht	946
1. Allgemeines	946
2. Problem: Offenbarung der Daten im Zwangsvollstreckungsverfahren.....	948
a) Aus Gläubigersperspektive	948
b) Aus Schuldnersperspektive	950

3.	Vollstreckung in einzelne Gegenstandskategorien	951
a)	Körperliche Gegenstände (Datenträger)	951
b)	Unkörperliche Gegenstände	952
aa)	Ausgangspunkt	952
bb)	Insbesondere: Vertragliche Nutzungsrechte	952
II.	Grundlagen zum Insolvenzrecht	953
1.	Übergang der Verwaltungs- und Verfügungsbefugnis	953
2.	Insolvenzmasse	954
3.	Verträge in der Insolvenz	955
III.	Rechtliche Kategorisierung der datenrechtlichen	
	Bezugsobjekte	956
1.	Sondergesetzlich geschützte Daten	957
a)	Urheberrecht und verwandte Schutzrechte	957
aa)	Datenbankwerk, §§ 2 Abs. 2, 4 Abs. 2 S. 1 UrhG	957
bb)	Datenbankherstellerrecht, §§ 87a UrhG	958
cc)	Weitere Anknüpfungspunkte im UrhG	959
b)	Geschäftsgeheimnisse, Know-how	959
c)	Personenbezogene Daten	961
d)	Allgemeines Persönlichkeitsrecht (Kommerzielle Elemente)	961
e)	Vertraglich geschützte Daten	962
f)	Sonstige Daten	963
2.	Datenträger	963
B.	Daten in der Zwangsvollstreckung	963
I.	Allgemeines	963
II.	Sondergesetzlich geschützte Daten	964
1.	Urheberrecht und verwandte Schutzrechte	964
2.	Geschäfts- und Betriebsgeheimnisse, Know-how	966
3.	Personenbezogene Daten	966
4.	Allgemeines Persönlichkeitsrecht (Kommerzielle Elemente)	968
5.	Vertraglich geschützte Daten	969
C.	Daten in der Insolvenz	970
I.	Massezugehörigkeit von Daten	970
II.	Aussonderung von Daten in der Insolvenz	971
1.	Urheberrecht, Leistungsschutzrechte und verwandte Schutzrechte	971
2.	Personenbezogene Daten	972
3.	Allgemeines Persönlichkeitsrecht (Kommerzielle Elemente)	972
4.	Vertraglich und insb. auftragsrechtlich geschützte Daten	972
III.	Vertragsgestaltung	973
1.	Anwendbares Recht und internationale Zuständigkeit	973
2.	Insolvenzrechtliche Schranken vertraglicher Gestaltung	974

3. Sicherung des Datenzugriffs	975
4. Sicherung von Nutzungsrechten	976
IV. Datenschutz in der Insolvenz.	978
1. Meinungsstand unter Geltung des BDSG a.F.	979
2. Rechtslage seit Geltung der DS-GVO	980
a) Datenschutzrechtliche Verantwortlichkeit des Insolvenzverwalters	980
b) Datenschutzrechtliche Verantwortlichkeit des vorläufigen Insolvenzverwalters	981
Herausgeberinnen	983
Stichwortverzeichnis	985

§ 10

Datenbestände in Zwangsvollstreckung und Insolvenz

Dr. Simon Apel^{}; Dr. Micha Brechtel^{**}*

* Dr. Simon Apel ist Rechtsanwalt bei SZA Schilling, Zutt & Anschütz und Lehrbeauftragter an der Universität Mannheim.

** Dr. Micha Brechtel ist Rechtsanwalt bei SZA Schilling, Zutt & Anschütz und Lehrbeauftragter an der Ruprecht-Karls-Universität Heidelberg.

Literatur: *Ahlberg/Götting* (Hrsg.), Beck'scher OnlineKommentar Urheberrecht, 24. Ed. 2019, München: C. H. Beck; *Ann/Loschelder/Grosch* (Hrsg.), Praxishandbuch Know-how-Schutz, 2010, Köln: Carl Heymanns Verlag; *Apel*, Anm. zu EuGH, Urt. v. 10.11.2016 – C-174/15 – Stichting Leenrecht, MR-Int 2016, 104–107; *ders.*, Rez. zu Sassenberg/Faber, Rechtshandbuch Industrie 4.0 und Internet of Things, InTeR 2017, 226–227; *ders.*, Überlegungen zu einer Reform des Lichtbildschutzrechts (§ 72 UrhG), in: Götz von Olenhusen/Gergen (Hrsg.), Kreativität und Charakter: Recht, Geschichte und Kultur in schöpferischen Prozessen, Festschrift für Martin Vogel zum siebzigsten Geburtstag, 2017, Hamburg: Dr. Kovač, S. 205–226; *ders./Walling*, Das neue Geschäftsgeheimnisgesetz: Überblick und erste Praxishinweise, DB 2019, 891–898; *Auer-Reinsdorff/Conrad* (Hrsg.), Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, München: C. H. Beck; *Bamberger/Roth/Hau/Poseck* (Hrsg.), Beck'scher OnlineKommentar BGB, 50. Ed. 2019, München: C. H. Beck; *Baumbach/Lauterbach/Albers/Hartmann* (Hrsg.), ZPO, 77. Aufl. 2019, München: C. H. Beck; *Bartenbach*, Patentlizenz- und Know-how-Vertrag, 7. Aufl. 2013, Köln: Verlag Dr. Otto Schmidt; *Becker*, Lauterkeitsrechtlicher Leistungsschutz für Daten, GRUR 2017, 346–355; *Becker-Eberhard*, Gerichtsvollzieher und Datenschutz unter der Datenschutzgrundverordnung der EU, DGVZ 2018, 129–136; *Benkard* (Begr.), PatG, 10. Aufl. 2006, München: C. H. Beck; *Berberich/Kanschik*, Daten in der Insolvenz, NZI 2017, 1–10; *Berger*, Property Rights to Personal Data? An Exploration of Commercial Data Law, ZGE 2017, 340–355; *ders.*, Immaterielle Wirtschaftsgüter in der Insolvenz, GRUR 2013, 321–335; *Beuthien*, Statt Genugtuung für das Opfer Frohlocken des Täters? Zur rechtswidrigen Verwertung der Kohl-Protokolle, GRUR 2018, 1021–1025; *Beyer/Beyer*, Verkauf von Kundendaten in der Insolvenz – Verstoß gegen datenschutzrechtliche Bestimmungen?, NZI 2016, 241–245; *Bisges* (Hrsg.), Handbuch Urheberrecht, 2016, Berlin: Erich Schmidt Verlag; *Bitter*, Rechtssträgerschaft für fremde Rechnung, 2006, Heidelberg: Mohr Siebeck; *ders.*, Die Nutzungsüberlassung in der Insolvenz nach dem MoMiG (§ 135 Abs. 3 InsO), ZIP 2010, 1–15; *ders.*, Das Verwertungsrecht des Insolvenzverwalters bei besitzlosen Rechten und bei einer (Doppel-)Treuhand am Sicherungsgut, ZIP 2015, 2249–2259; *Boehm/Pesch*, Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung, MMR 2014, 75–79; *Brammsen*, Reformbedürftig! – Der Regierungsentwurf des neuen Geschäftsgeheimnischutzgesetzes, BB 2018, 2446–2450; *Bull*, Wieviel sind „meine Daten“ wert?, CR 2018, 425–432; *Bultmann*, Aussonderung von Daten in der Insolvenz, ZInsO 2011, 992–996; *Cepl/Voß* (Hrsg.), Prozesskommentar zum Gewerblichen Rechtsschutz, 2. Aufl. 2018, München: C. H. Beck; *Christians/Liepin*, The Consequences of Digitalization for German Civil Law, ZGE 2017, 331–339; *Czarnetzki/Röder*, Daten und Herausgabeansprüche in der Insolvenz, in: Conrad/Grützmacher (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, 2014, Köln: Verlag Dr. Otto Schmidt, S. 332–346; *Dreier/Schulze* (Hrsg.), Urheberrechtsgesetz, 7. Aufl. 2019, München: C. H. Beck; *Emptying*, Immaterialgüterrechte in der Insolvenz, 2003, Frankfurt: Peter Lang; *Engelhardt/Klein*, Bitcoins – Geschäfte mit Geld, das keines ist, MMR 2014, 355–360; *Erman* (Begr.), BGB, Band 1, 15. Aufl. 2017, Köln: Verlag Dr. Otto Schmidt; *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten A zum 71. Deutschen Juristentag, 2016, München: C. H. Beck; *Freudenberg*, Zwangsvollstreckung in Persönlichkeitsrechte, 2006, Baden-Baden: Nomos; *Ganter*, Patentlizenzen in der Insolvenz des Patentgebers, NZI 2011, 833–843; *Gsell/Krüger/Lorenz/Reimann/Harke* (Hrsg.), Beck'scher OnlineGrosskommentar BGB, Stand: 01.04.2019, München: C. H. Beck; *Hammes*, Keine Eigenverwaltung ohne Berater, NZI 2017, 233–241; *Hartung*, Datenschutz und Insolvenzverwaltung, ZInsO 2011, 1225–1236; *Heermann/Schlingloff* (Hrsg.), Münchener Kommentar zum Lauterkeitsrecht, Band 2, 2. Aufl. 2014, München: C. H. Beck; *Heine*, Bitcoins und Botnetze – Strafbarkeit und Vermögensabschöpfung bei illegalem Bitcoin-Mining, NStZ 2016, 441–446; *Henn/Apel*, Der Drittauskunftsanspruch nach § 19 Abs. 2 MarkenG, MarkenR 2016, 345–352; *Hölder/Schmoll*, Patentlizenz- und Know-how-Ver-

träge in der Insolvenz – Teil II: Insolvenz des Lizenzgebers, GRUR 2004, 830–836; *Hoeren*, EU-Kommission: Entwurf einer VO über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der EU, ZD-Aktuell 2018, 05930; *Hümmerich/Lücke/Mauer* (Hrsg.), Arbeitsrecht, 8. Aufl. 2014, Baden-Baden: Nomos; *Jansen/Michaels* (Hrsg.), *Beyond the State: Rethinking Private Law*, 2008, Heidelberg: Mohr Siebeck; *Jülicher*, Die Aussonderung von (Cloud-)Daten nach § 47 InsO, ZIP 2015, 2063–2066; *Jungclaus*, Zu einem dogmatischen Grundfehler des § 108a InsO-E in der Fassung des Referentenentwurfs des BMJ v. 18.01.2012, ZInsO 2012, 724–726; *Kalbfus*, Die EU-Geschäftsgeheimnis-Richtlinie, GRUR 2016, 1009–1017; *Kiefer*, Das Geschäftsgeheimnis nach dem Referentenentwurf zum Geschäftsgeheimnisgesetz: Ein Immaterialgüterrecht, WRP 2018, 910–917; *Kirchhof/Stürner/Eidenmüller* (Hrsg.), Münchener Kommentar zur Insolvenzordnung, Band 1, 4. Aufl. 2019, München: C. H. Beck; *Kirchhof/Stürner/Eidenmüller* (Hrsg.), Münchener Kommentar zur Insolvenzordnung, Band 2, 3. Aufl. 2013, München: C. H. Beck; *Kilian/Heussen* (Hrsg.), Computerrechts-Handbuch, 34. EL 2018, München: C. H. Beck; *Köhler/Bornkamm/Fedderson* (Hrsg.), UWG, 37. Aufl. 2019, München: C. H. Beck; *Kleespies*, Die Domain als selbstständiger Vermögensgegenstand in der Einzelzwangsvollstreckung, GRUR 2002, 764–775; *Koós*, Die europäische Geschäftsgeheimnis-Richtlinie – ein gelungener Wurf?, MMR 2016, 224–228; *Krüger/Rauscher* (Hrsg.), Münchener Kommentar zur ZPO, Band 1, Band 2, 5. Aufl. 2016, München: C. H. Beck; *Kur/von Bombard/Albrecht* (Hrsg.), Beck'scher OnlineKommentar Markenrecht, 17. Ed. 2019, München: C. H. Beck; *Lejeune*, Das Geschäftsgeheimnisgesetz, ITRB 2018, 140–144; *Loewenheim* (Hrsg.), Handbuch des Urheberrechts, 2. Aufl. 2010, München: C. H. Beck; *McGuire*, 10 Fragen & Antworten zum neuen Geheimnisschutz, GRUR-Newsletter 1/2018, 4–8; *dies.*, Monismus – Ein Irrweg?, in: Dreier/Reto (Hrsg.), Vom Magenttonband bis Social Media, Festschrift 50 Jahre Urheberrecht, 2015, München: C. H. Beck, S. 289–304; *Moos/Schefzig/Arning* (Hrsg.), Die neue Datenschutz-Grundverordnung, 2018, Berlin: De Gruyter; *Musielak/Voit* (Hrsg.), ZPO, 16. Aufl. 2019, München: Vahlen; *Obergfell*, Big Data und Urheberrecht, in: Ahrens/Bornkamm/Fezer/Koch/McGuire/Würtenberger (Hrsg.), Festschrift für Wolfgang Büscher, 2017, Köln: Carl Heymanns, S. 223–332; *Ohly*, Das neue Geschäftsgeheimnisgesetz im Überblick, GRUR 2019, 441–451; *Paal/Pauly* (Hrsg.), DS-GVO BDSG, 2. Aufl. 2018, München: C. H. Beck; *Paulus/Matzke*, Digitalisierung und private Rechtsdurchsetzung, CR 2017, 769–778; *Peukert*, Persönlichkeitsbezogene Immaterialgüterrechte?, ZUM 2000, 710–721; *Rath*, Risiken und Nebenwirkungen beim Software Escrow, CR 2013, 78–81; *Rückert*, Vermögensabschöpfung und Sicherstellung bei Bitcoins, MMR 2016, 295–300; *Säcker/Rixecker/Oetker/Limpberg*, Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 1, 7. Aufl. 2015, München: C. H. Beck; *Säcker/Rixecker/Oetker/Limpberg*, Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 6, 7. Aufl. 2018, München: C. H. Beck; *Sassenberg/Faber* (Hrsg.), Rechtshandbuch Industrie 4.0 und Internet of Things, 2017, München: C. H. Beck; *Sattler*, Personenbezogene Daten als Leistungsgegenstand, JZ 2017, 1036–1046; *Schack*, Urheber- und Urhebervertragsrecht, 8. Aufl. 2017, Heidelberg: Mohr Siebeck; *Schmidt* (Hrsg.), InsO, 19. Aufl. 2016, München: C. H. Beck; *Schmidt-Kessel* (Hrsg.), Rechtsdurchsetzung ohne Staat, 2019 (im Erscheinen), Heidelberg: Mohr Siebeck; *Schricker/Loewenheim* (Hrsg.), Urheberrecht, 5. Aufl. 2017, München: C. H. Beck; *Schuster/Tobuschat*, Geschäftsgeheimnisse in der Insolvenz, GRUR-Prax 2019, 248–250; *Schwartzmann/Jaspers/Thüsing/Kugelmann* (Hrsg.), Heidelberger Kommentar DS-GVO/BDSG, 2018, Heidelberg: C. F. Müller; *Sosnitza*, Die Zwangsvollstreckung in Persönlichkeitsrechte, JZ 2004, 992–1002; *Specht/Zerbst*, Considering the relationship between the civil law treatment of data and data protection law in Germany, JIPITEC 2018, 504–512; *Spindler*, Verträge über digitale Inhalte – Anwendungsbereich und Ansätze, MMR 2016, 147–153; *ders.*, Verträge über digitale Inhalte – Haftung, Gewährleistung und Portabilität, MMR 2016, 219–224; *Stein/Jonas* (Hrsg.), ZPO, Band 8, 23. Aufl. 2017, Heidelberg: Mohr

Siebeck; *Steinrötter*, Vermeintliche Ausschließlichkeitsrechte an binären Codes, MMR 2017, 731–736; *Teubner*, Globale Zivilverfassungen: Alternativen zur staatszentrierten Verfassungstheorie, ZaöRV 2003, 1–28; *Thole*, Der (vorläufige) Insolvenzverwalter als Verantwortlicher i. S. d. Art. 4 Nr. 7 DS-GVO, ZIP 2018, 1001–1011; *Uhlenbruck/Hirte/Vallender* (Hrsg.), Insolvenzordnung, 15. Aufl. 2019, München: Vahlen; *Ulmer*, Urheber- und Verlagsrecht, 3. Aufl. 1980, Berlin: Springer; *Veil*, Die Datenschutz-Grundverordnung: des Kaisers neue Kleider, NVwZ 2018, 686–696; *Wandtke/Bullinger* (Hrsg.), Praxiskommentar zum Urheberrecht, 5. Aufl. 2019, München: C.H. Beck; *Weiß/Reisener*, Datensparsamkeit, Datenvermeidung und Pseudonymisierung: Problembewusstsein für Datenschutz in der Insolvenzverwaltung?!, ZInsO 2017, 416–420; *Weitbrecht*, Die Doppeltreuhand – Grundstruktur, Insolvenzfestigkeit, Verwertung, NZI 2017, 553–560; *Wieczorek/Schütze* (Begr.), ZPO, Band 10/1, 4. Aufl. 2015, Berlin: De Gruyter; *Wieczorek/Schütze* (Begr.), ZPO, Band 10/2, 4. Aufl. 2015, Berlin: De Gruyter; *Wimmer*, Neue Reformüberlegungen zur Insolvenzfestigkeit von Lizenzverträgen, ZIP 2012, 545–557; *Zech*, Information als Schutzgegenstand, 2012, Heidelberg: Mohr Siebeck; *ders.*, „Industrie 4.0“ – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151–1160; *Zimmermann*, Immaterialgüterrechte und ihre Zwangsvollstreckung, 1998, Remscheid: Gardez; *ders.*, Das Erfinderrecht in der Zwangsvollstreckung, GRUR 1999, 121–128; *Zöller* (Begr.), ZPO, 32. Aufl. 2018, Köln: Verlag Dr. Otto Schmidt.

A. Einführung

- 1 Jede Diskussion über Daten als vermögenswertes (Privat-)Rechtsgut ist bis zu einem gewissen Grade müßig, wenn Ansprüche in Zusammenhang mit diesem Rechtsgut nicht – grundsätzlich¹ – notfalls zwangsweise durchgesetzt werden können und es im Falle des Zahlungsausfalls des Inhabers nicht im Wege des Insolvenzverfahrens von dessen Gläubigern verwertet werden kann.² Durch die erste Möglichkeit erhält ein privatrechtlicher Anspruch auf Nutzung oder Übergabe der Daten erst seine „Zähne“ und seine Durchsetzbarkeit auch gegen den Willen des (sei es gesetzlich, sei es vertraglich) verpflichteten Schuldners.³ Die zweite Möglichkeit stellt sicher, dass sich der Inhaber gegenüber seinen Gläubigern nicht ohne weiteres seiner Zahlungsverpflichtung entziehen und das vermögenswerte Recht erhalten kann, wenn er zur Deckung seiner Verbindlichkeiten nicht mehr in der Lage ist.⁴ Sowohl dem zwangsvollstreckungsrechtlichen als auch dem insolvenzrechtlichen Gesichtspunkt ist gemeinsam, dass er im Wesentlichen staatlich determiniert ist. Die Parteien stoßen hier an (im Ausgangspunkt

¹ Freilich ggf. abhängig von weiteren Voraussetzungen und nicht unbeschränkt.

² Ähnl. *Faust*, in: Gutachten A zum 71. Deutschen Juristentag, 2016, S. A10 (zur Diskussion über ein „Sachenrecht an Daten“), *Steinrötter*, MMR 2017, 731, 735 und zum Vertragsrecht *Sattler*, JZ 2017, 1036, 1042 f.

³ Vgl. allgemein zum Zweck des Zwangsvollstreckungsverfahrens nur BVerfG, Beschl. v. 19.10.1982 – 1 BvL 34/80, 1 BvL 55/80, NJW 1983, 559; *Götz*, in: Krüger/Rauscher, MüKo ZPO, Bd. 2, 5. Aufl. 2016, § 704 Rn. 1; *Lackmann*, in: Musielak/Voit, ZPO, 16. Aufl. 2019, Vor §§ 704 ff. Rn. 1.

⁴ Vgl. § 1 S. 1 InsO; *Stürmer*, in: Kirchof/Stürmer/Eidenmüller, MüKo InsO, Bd. 1, 4. Aufl. 2019, Einl. Rn. 1.

durch das Gewaltmonopol des Staates gesetzte) Grenzen, ihre jeweiligen gegenseitigen Rechte durch vertragliche Absprachen oder eigene Maßnahmen zu sichern, zu verteidigen oder durchzusetzen.⁵

Wer sich mit dem „Datenrecht“, wie es in diesem Handbuch verstanden wird,⁶ beschäftigt, stößt in diesem Zusammenhang auf eine gute und eine schlechte 2 Nachricht. Die gute Nachricht ist, dass es für einen Teil des Datenrechts bereits gesetzliche Anknüpfungspunkte gibt.⁷ Neben den allgemeinen verfahrensrechtlichen Regelungen vor allem in ZPO und InsO, die grundsätzlich auch einen für das „Datenrecht“ nutzbaren Rahmen bieten,⁸ sind zumindest für Daten, die eine immaterialgüterrechtlich schutzfähige Gestalt erhalten haben, gesetzliche Sondervorschriften zu Zwangsvollstreckung vorhanden.⁹

Die schlechte Nachricht ist, dass jenseits dieses Rahmens für die Praxis noch zahl- 3 reiche Leerstellen bestehen, die bislang weder durch den Gesetzgeber noch durch die Gerichte abschließend geklärt wurden.¹⁰ Dies betrifft insbesondere den Umgang mit personenbezogenen Daten (nicht nur des Schuldners, sondern vor allem auch Dritter), mit Betriebs- und Geschäftsgeheimnissen sowie mit überhaupt nicht in immaterialgüterrechtlich geschützter Weise niedergelegten Daten (etwa Maschinendaten, die kein Betriebs- und Geschäftsgeheimnis darstellen): So enthalten weder die DS-GVO (für personenbezogene Daten) noch die Richtlinie

⁵ Bei Zwangsvollstreckung und Insolvenz stoßen Konzepte, die ein „Privatrecht ohne Staat“ diskutieren (vgl. etwa die Beiträge in *Jansen/Michaels*, *Beyond the State: Rethinking Private Law*, 2008), an gewisse Grenzen; gleichwohl werden auch hierzu Modelle praktiziert oder zumindest diskutiert, s. nur zur zwangsweisen Durchsetzung bei Domain-Streitigkeiten durch private Schiedsgerichte der ICANN bereits *Teubner*, *ZaöRV* 2003, 1, 19, 21 und zur jüngeren Diskussion u. a. um (sich selbst vollstreckende?) „Smart Contracts“ *Paulus/Matzke*, CR 2017, 769, 772 ff. sowie die Beiträge in *Schmidt-Kessel*, *Rechtsdurchsetzung ohne Staat*, im Erscheinen.

⁶ Siehe oben Vorwort.

⁷ Vgl. auch allgemein *Bull*, CR 2018, 425 Rn. 18.

⁸ *Christians/Liepin*, ZGE 2017, 331, 335 f. halten diese allgemeinen Regelungen sogar für gänzlich ausreichend; vgl. entsprechend auch die optimistische Einschätzung der Justizministerinnen und Justizminister der Länder Baden-Württemberg, Bayern, Berlin, Hamburg, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt und Schleswig-Holstein hierzu s. *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15.05.2017, insb. S. 60 ff., 84 ff.; mit Recht differenzierend zu diesem Bericht jedoch *Steinrötter*, MMR 2017, 731, 735 f.

⁹ Siehe nur §§ 112 ff. UrhG.

¹⁰ Grundlegend in der Literatur zum hier behandelten Themenkreis jedoch bereits *Hauck*, in: *Ann/Loschelders/Grosch*, *Praxishandbuch Know-how-Schutz*, 2010, Kap. 8 (Know-how); *Müller*, in: *Conrad/Grützmaker*, *Recht der Daten und Datenbanken im Unternehmen*, 2014, § 24 Rn. 31 ff. und *Czarnetzki/Röder*, in: *Conrad/Grützmaker*, *Recht der Daten und Datenbanken im Unternehmen*, 2014, § 25 (jeweils zu Daten); zu Fragen der Insolvenz auch *Berberich/Kanschik*, *NZI* 2017, 1; zu Lizenzen in der Zwangsvollstreckung s. ferner *Bartenbach*, *Patentlizenz- und Know-how-Vertrag*, 7. Aufl. 2013, Rn. 624 ff.

zum Schutz von Geschäftsgeheimnissen¹¹ Regelungen zum Zwangsvollstreckungs- und Insolvenzverfahren. Dies gilt erst recht für (noch nicht verabschiedete) Unionsrechtsakte, die schon gar nicht beanspruchen, zuordnungsbezogene Aspekte des Datenrechts vollständig oder weitgehend zu regeln.¹² Beide hier behandelten Verfahren halten zudem das Damoklesschwert des Bekanntwerdens der betroffenen Daten im Verfahren bereit, was in vielen Fällen zur Zerstörung des rechtlichen Schutzes bzw. des wirtschaftlichen Wertes führen würde.¹³

- 4 Für die Praxis ist es angesichts der stetig steigenden wirtschaftlichen Bedeutung von Datensätzen gleichwohl entscheidend, dass ungeachtet der bestehenden Regelungsdefizite Lösungen für einen effektiven Umgang mit Datensätzen in Zwangsvollstreckung und Insolvenz gefunden werden. Nachfolgend sollen daher jeweils nach Darstellung der Grundlagen für das Zwangsvollstreckungs- und Insolvenzrecht Handreichungen hierfür entwickelt und geboten werden.

I. Grundlagen zum Zwangsvollstreckungsrecht

1. Allgemeines

- 5 Die Durchsetzung von Ansprüchen im Wege der Zwangsvollstreckung erfolgt mit Blick auf das Gewaltmonopol des Staates bei Vorliegen der Voraussetzungen (Titel, Klausel, Zustellung) durch Maßnahmen und Entscheidungen staatlicher Institutionen, namentlich durch Gerichtsvollzieher (insb. bei Vollstreckung in körperliche Sachen, vgl. §§ 808 ff., 883 ZPO), durch Vollstreckungsgerichte (insb. bei Vollstreckung in Forderungen und Rechte, vgl. §§ 828 ff. ZPO, und Erzwingung vertretbarer und unvertretbarer Handlungen, vgl. §§ 887 f. ZPO) sowie – im hiesigen Kontext wohl nicht relevant – durch Grundbuchämter (bei Zwangsvoll-

¹¹ RL 2016/943/EU des Europäischen Parlamentes und des Rates v. 08.06.2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl. EU v. 15.06.2016, L 157, S. 1; der Regierungsentwurf für ein dieses umsetzende Gesetz zum Schutz von Geschäftsgeheimnissen (GehSchG) greift immerhin das Zwangsvollstreckungsverfahren auf, siehe § 19 Abs. 3 RegE-GeschGehG, s. dazu näher unten Rn. 39.

¹² Etwa der Entwurf einer Verordnung über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der EU, COM (2017) 495 final, der sich jeder Aussage über die Rechtsinhaberschaft an den betroffenen Daten enthält; allgemein zu diesem bislang wenig diskutierten Entwurf knapp *Hoeren*, ZD-Aktuell 2018, 05930; *Schmitz*, in: *Moos/Schefzig/Arning*, Die neue Datenschutz-Grundverordnung, 2018, Kap. 2 Rn. 42. Auch der Vorschlag der Kommission für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, COM (2015) 634 final spricht zwar personenbezogene oder andere Daten als potentiell „Zahlungsmittel“ für digitale Inhalte an (Art. 3 Abs. 1), verhält sich aber ebenfalls nicht zu Fragen der Zwangsvollstreckung oder Insolvenz hinsichtlich solcher Daten; allgemein zu diesem Vorschlag s. nur *Faust*, in: *Gutachten A zum 71. Deutschen Juristentag*, 2016, S. A13 ff.; *Spindler*, MMR 2016, 147, 219.

¹³ *Hauck*, in: *Ann/Loschelder/Grosch*, Praxishandbuch Know-how-Schutz, 2010, Kap. 8 Rn. 1 a. E.

streckung in das unbewegliche Vermögen, vgl. §§ 864 ff. ZPO und ZVG). Im hier behandelten Komplex des Datenrechts dürfte dabei die Vollstreckung in körperliche Sachen (namentlich Datenträger jedweder Art)¹⁴ und Rechte (insbesondere gewerbliche Schutzrechte, Rechte aus Lizenzverträgen, aber möglicherweise auch sonstige vermögenswerte Rechte, § 857 ZPO)¹⁵ im Vordergrund stehen. Dies auch deshalb, weil eine Behandlung der Datenbestände „an sich“ ohne Rücksicht auf ihre Verkörperung auf einem Datenträger als Sache im Sinne des deutschen Zivilrechts zumindest *de lege lata* nicht möglich ist.¹⁶ Dass Datenbestände bzw. die an ihnen bestehenden Rechte in verschiedener Hinsicht mittelbar oder unmittelbar Gegenstand der Zwangsvollstreckung sein können, ist nicht mehr zweifelhaft: Den dafür erforderlichen wirtschaftlichen Wert (auch wenn dieser ggf. schwer zu beziffern ist)¹⁷ werden sie in aller Regel aufweisen.¹⁸

Bei Datenbeständen ist die Frage des Vorgehens bei der Zwangsvollstreckung aus Gläubigersicht jedoch häufig mehrdimensional:¹⁹ Es genügt oft nicht, nur in den 6
Gegenstand zu vollstrecken, der das Datum enthält;²⁰ es muss auch sichergestellt sein, dass die wirtschaftliche Verwertung der enthaltenen Daten als solche (tatsächlich und rechtlich) möglich ist und dass der tatsächliche Zugriff auf diese gewährleistet ist.²¹ Daher ist vor Einleitung von Zwangsvollstreckungsmaßnahmen stets genau zu prüfen, welche im Einzelfall erforderlich sind, um die benötigte Verwertungsmöglichkeit zu erhalten.²²

¹⁴ S. nur BGH, Urt. v. 15. 11. 2006 – XII ZR 120/04, NJW 2006, 2394 Rn. 16; *Fritzsche*, in: Bamberger/Roth/Hau/Poseck, BeckOK BGB, 50. Ed. 2019, § 90 Rn. 24 (jeweils zu Software und m. w. Nachw. zur Gegenauffassung).

¹⁵ Für Bitcoins, wenn auch skeptisch, *Boehm/Pesch*, MMR 2014, 75, 78; *Engelhardt/Klein*, MMR 2014, 355, 359; zur Anwendbarkeit strafrechtlicher Einziehungs- und Vermögensverfallsregelungen auf Bitcoins, BGH, Beschl. v. 27. 07. 2017 – 1 StR 412/16, NStZ 2018, 411; *Heine*, NStZ 2016, 441, 444 f.; *Rückert*, MMR 2016, 295; dieser mit dem hier behandelten Komplex durchaus verwandten Thematik kann hier allerdings schon aus Raumgründen nicht näher nachgegangen werden.

¹⁶ S. nur OLG Hamburg, Beschl. v. 24. 03. 2015 – 10 U 5/11, MMR 2015, 740, 741 (zu „Audiodateien“); *Fritzsche*, in: Bamberger/Roth/Hau/Poseck, BeckOK BGB, 50. Ed. 2019, § 90 Rn. 24; anders offenbar *Müller*, in: Conrad/Grützmaker, Recht der Daten und Datenbanken im Unternehmen, 2014, § 24 Rn. 33; eingehend hierzu oben § 4 Rn. 1.

¹⁷ S. hierzu oben § 4.2 Rn. 40.

¹⁸ Ausführlich *Hauck*, in: Ann/Loschelder/Grosch, Praxishandbuch Know-how-Schutz, 2010, Kap. 8 Rn. 2 ff. (zum Know-how).

¹⁹ Vgl. auch *Müller*, in: Conrad/Grützmaker, Recht der Daten und Datenbanken im Unternehmen, 2014, § 24 Rn. 44.

²⁰ *Paulus/Matzke*, CR 2017, 769, 775 f., 778.

²¹ Zu der Frage, ob der Gläubiger auch den Anspruch auf Herstellung einer Kopie des entsprechenden Datensatzes haben kann.

²² *Hauck*, in: Ann/Loschelder/Grosch, Praxishandbuch Know-how-Schutz, 2010, Kap. 8 Rn. 18 weist zudem darauf hin, dass das Vorgehen sich auch danach unterscheiden kann, ob man gegen den Inhaber der Datenbestände oder gegen einen vertraglich Nutzungsberechtigten vollstrecken möchte.

7 **Praxishinweis:** Abhängig vom Gegenstand der Zwangsvollstreckung wird vielfach auch eine Kombination mehrerer Vollstreckungsmaßnahmen erforderlich sein, um einerseits den tatsächlichen Zugriff auf die Daten zu erlangen und andererseits das Recht zu ihrer Verwendung zu erwerben.

8 Die Zwangsvollstreckung stößt zudem an ihre Grenzen, wo Vermögen vom Gesetzgeber unpfändbar gestellt wird (vgl. insb. § 811 Abs. 1 Nr. 5 ZPO betreffend den Schutz persönlicher Arbeitsleistung und dort Nr. 11 betreffend Geschäftsbücher u. a.) oder besonderen, außerhalb des Zwangsvollstreckungsrechts liegenden Grenzen unterliegt, wie dies beispielsweise mit Blick auf das Datenschutz- und allgemeine Persönlichkeitsrecht der Fall sein kann.

Zuständig für die Zwangsvollstreckung in das bewegliche Vermögen durch Pfändung (etwa: Datenträger als Sachen) ist der Gerichtsvollzieher (§§ 803, 808 ff. ZPO).

Für die Vollstreckung in Forderungen und andere vermögenswerte Rechte (etwa: Nutzungsrechte, Immaterialgüterrechte) ist das Amtsgericht als Vollstreckungsgericht zuständig (§§ 857, 828 Abs. 1, 764, 802 ZPO).²³

2. Problem: Offenbarung der Daten im Zwangsvollstreckungsverfahren

9 Sowohl für den Gläubiger als auch für den Schuldner bietet die oftmals gewünschte Vertraulichkeit der Daten Probleme im Kontext der Zwangsvollstreckung.

a) Aus Gläubigerperspektive

10 Für den Gläubiger beginnt dies schon beim Antrag: In prozessualer Hinsicht ist entscheidend, dass er sowohl zulässig ist als auch im Falle der Stattgabe einen hinreichend bestimmten Titel²⁴ für das Zwangsvollstreckungsverfahren nach sich zieht (vgl. zum Klageantrag § 253 Abs. 2 Nr. 2 ZPO).²⁵ Ähnlich wie bei Unterlassungs- und Auskunftsklagen kann auch die Formulierung eines Antrags, der auf Überlassung eines Rechts an Daten oder Herausgabe eines Datenbestandes gerichtet ist, eine besondere Herausforderung sein.²⁶ Eine möglichst genaue Beschreibung des betroffenen Datenbestands im jeweiligen Titel ist daher unumgänglich, da auch im Prozess um Daten und Know-how die erfassten Gegen-

²³ Hauck, in: Ann/Loschelder/Grosch, Praxishandbuch Know-how-Schutz, 2010, Kap. 8 Rn. 19.

²⁴ Zu den möglichen Titeln s. §§ 704, 794 ZPO.

²⁵ Vgl. nur Müller, in: Conrad/Grützmaker, Recht der Daten und Datenbanken im Unternehmen, 2014, § 24 Rn. 35, 56; Becker-Eberhardt, in: Krüger/Rauscher, MüKo ZPO, Bd. 1, 5. Aufl. 2016, § 253 Rn. 88; Foerste, in: Musielak/Voit, ZPO, 6. Aufl. 2019, § 253 Rn. 29.

²⁶ Hauck, in: Ann/Loschelder/Grosch, Praxishandbuch Know-how-Schutz, 2010, Kap. 8 Rn. 21 zum Know-how.

stände nicht erst im Zwangsvollstreckungsverfahren ermittelt werden dürfen.²⁷ Um den augenfällig bestehenden Konflikt zur Geheimhaltung der betroffenen Datensätze zu vermitteln, wird in Zusammenhang mit der Zwangsvollstreckung in Know-how vorgeschlagen, die zur Zwangsvollstreckung in Patente²⁸ entwickelten Grundsätze entsprechend anzuwenden und eine Umschreibung des betroffenen Know-hows zuzulassen, die dem Vollstreckungsorgan einen gewissen Beurteilungsspielraum lässt.²⁹ Dieser Vorschlag ist *de lege lata* durchaus plausibel und für die Praxis auch für andere geheimhaltungsbedürftige Datenbestände ein potenzieller „Workaround“. Allerdings bleibt selbst dann, wenn sich die Rechtsprechung diese Auffassung zu eigen macht, der Grat zwischen unzulässigem bzw. angreifbarem Antrag und zulässiger Umschreibung schmal und schwer abzuschätzen. Für eine zufriedenstellende Lösung bedürfte es hier eines Tätigwerdens des Gesetzgebers.

Weitergehend schlägt *Hauck* (zum Know-how und erneut in Anlehnung an das Patentrecht) vor, dem Gläubiger in Analogie zu § 836 Abs. 3 S. 1 ZPO einen Auskunftsanspruch gegen den Schuldner zuzugestehen, mit dem der Gläubiger die zur Konkretisierung des Vollstreckungsgegenstands erforderlichen Informationen erlangen kann; diese Informationen sollen allerdings im Wege des Herausgabeanspruchs nicht dem Gläubiger, sondern dem Vollstreckungsgericht gegenüber offenbart werden. Der Auskunftsanspruch selbst soll wiederum nach §§ 836 Abs. 3 S. 2, 899 *cf.*, 888 ZPO durchsetzbar sein.³⁰ Dieser Vorschlag ist aus Gläubigersicht attraktiv. Ob allerdings der Verweis auf die nach *Hauck* vergleichbare Regelung in § 20 InsO (Auskunfts- und Mitwirkungspflicht des Schuldners im Eröffnungsverfahren gegenüber dem Insolvenzgericht) trägt, ist zu hinterfragen: Die Regelung aus § 20 InsO statuiert einen *öffentlich-rechtlichen* Auskunftsanspruch des Insolvenzgerichts gegen den Schuldner,³¹ während § 836 Abs. 3 S. 1 ZPO einen *privatrechtlichen* Anspruch postuliert.³² Ersterer dient – der Natur des Insolvenzverfahrens entsprechend – zur Wahrung der Interessen aller Gläubiger des Schuldners, während letzterer nur *inter partes* wirkt. Folglich erscheint es zweifelhaft, die Wertung des § 20 InsO auf § 836 Abs. 3 S. 1 ZPO zu übertragen. Da zudem bei Daten – anders als bei Forderungen – der Zugriff auf die Information

²⁷ Vgl. BAG, Urt. v. 15. 12. 1987 – 3 AZR 474/86, AP § 611 BGB Betriebsgeheimnis Nr. 5; eingehend hierzu *Bartenbach*, Patentlizenz- und Know-how-Vertrag, 7. Aufl. 2013, Rn. 2885 ff.

²⁸ BGH, Urt. v. 13. 12. 2007 – I ZR 71/05, GRUR 2008, 727 Rn. 9 – Schweißmodulgengenerator.

²⁹ *Bartenbach*, Patentlizenz- und Know-how-Vertrag, 7. Aufl. 2013, Rn. 2893 ff.; *Hauck*, in: Ann/Loschelder/Grosch, Praxishandbuch Know-how-Schutz, 2010, Kap. 8 Rn. 21.

³⁰ *Hauck*, in: Ann/Loschelder/Grosch, Praxishandbuch Know-how-Schutz, 2010, Kap. 8 Rn. 22 ff., ggf. in Verbindung mit der Sachpfändung von den die Informationen enthaltenden (physischen) Unterlagen, §§ 808 ff. ZPO; a. A. insoweit wohl *Smid*, in: Krüger/Rauscher, MüKo ZPO, Bd. 2, 5. Aufl. 2016, § 836 Rn. 11.

³¹ *Schmahl/Vuia*, in: Kirchhof/Stürner/Eidenmüller, MüKo InsO, Bd. 1, 4. Aufl. 2019, § 20 Rn. 3; *Windau*, in: Fridgen/Geiwitz/Göpfert, BeckOK InsO, 11. Ed. 2018, § 20 Rn. 1.

³² *Smid*, in: Krüger/Rauscher, MüKo ZPO, Bd. 2, 5. Aufl. 2016, § 836 Rn. 11.

bereits gleichbedeutend mit der Erlangung des Wertes ist, ist zudem die für eine Analogie erforderliche vergleichbare Interessenlage wohl nicht mehr gegeben.

b) Aus Schuldnerperspektive

- 12 Der Schuldner hingegen sieht sich dem Problem ausgesetzt, dass der Gläubiger im Erfolgsfall bereits einen erstinstanzlichen Titel regelmäßig zumindest vorläufig vollstrecken kann. In aller Regel³³ wird dem klagenden Gläubiger die vorläufige Vollstreckbarkeit gegen Sicherheitsleistung zugesprochen, die es ihm ermöglicht, bereits vor Rechtskraft des jeweiligen Titels aus diesem vorzugehen (§ 709 S. 1 ZPO). Ähnlich wie bei den immaterialgüterrechtlichen Auskunftsklagen (etwa aus § 19 MarkenG, § 101 UrhG, § 140b PatG) besteht hier jedoch das Problem, dass der Gläubiger bereits durch die *vorläufige* Vollstreckung des Titels *endgültige* Kenntnis von dem Gegenstand der Auskunft (hier: dem Datenbestand) erhält.³⁴ Auch wenn dies defensiv wirkt und daher aus taktischen Gründen oft eher zurückhaltend gehandhabt wird, sollte er daher bereits in der ersten Instanz³⁵ für den Fall des Unterliegens einen Vollstreckungsschutzantrag stellen (§ 712 ZPO).³⁶ Voraussetzung für diesen ist ein nicht zu ersetzender Vollstreckungsnachteil des beklagten Schuldners. Da dieser bei Auskunftsansprüchen gerade nicht schon in der endgültigen Offenbarung der begehrten Informationen gegenüber dem klagenden Gläubiger gesehen wird,³⁷ – Argument: Urteile über Auskunftsansprüche sind nicht in § 708 ZPO genannt und die regelmäßig für die vorläufige Vollstreckung erforderliche Sicherheitsleistung sowie der Schadensersatzanspruch des § 717 ZPO sichern den beklagten Schuldner hinreichend ab³⁸ – ist es erforderlich, dem Gericht darzulegen, dass im spezifischen Einzelfall die über die bloße Offenbarung hinausgehenden Folgen der Offenbarung für den Schuldner so gravie-

³³ Zu den Ausnahmefällen §§ 708, 710 ZPO sowie – im Ergebnis – § 720a ZPO (Sicherstellungsvollstreckung ohne Sicherheitsleistung).

³⁴ Vgl. nur *Eckhardt*, in: *Kur/von Bomhard/Albrecht, BeckOK MarkenR*, 17. Ed. 2019, § 19 MarkenG Rn. 41; *Henn/Apel*, *MarkenR* 2016, 345 m. Fn. 3.

³⁵ Ggf. auch im Berufungsverfahren, vgl. nur BGH, *Beschl. v. 19.01.206 – VI ZR 675/15*, *BeckRS* 2016, 02270 Rn. 4.

³⁶ Soweit dies nicht erfolgt ist, sollte versucht werden, nach § 707 ZPO eine einstweilige Einstellung der Zwangsvollstreckung zu erreichen.

³⁷ *Götz*, in: *Krüger/Rauscher, MüKo ZPO*, Bd. 2, 5. Aufl. 2016, § 707 Rn. 13 nennt den Auskunftsanspruch (zu pauschal) sogar als generelles Beispiel für den Fall, dass die Nachteile der Vollstreckung für den Schuldner „ohnehin gering“ seien und daher „kaum Anlass für eine Einstellung der Zwangsvollstreckung“ bestehe (ähnlich zu unterhaltsrechtlichen Auskunftsansprüchen OLG Schleswig, *Beschl. v. 15.09.1982 – 8 WF 157/82*, *SchlHA* 1982, 196 und zu patentrechtlichen Auskunftsansprüchen); tendenziell ebenso *Lunze*, in: *Cepl/Voß, Prozesskommentar zum Gewerblichen Rechtsschutz*, 2. Aufl. 2018, § 707 ZPO Rn. 30; zumindest im hiesigen Kontext wird man demgegenüber vielmehr sagen müssen: In der Regel sind die Folgen der Erfüllung eines Auskunftsanspruchs für den Schuldner gravierend, da er endgültig die Kontrolle über die offenbaren Informationen verliert.

³⁸ Vgl. nur BGH, *Beschl. v. 09.11.1995 – I ZR 220/95*, *GRUR* 1996, 78 f. – Umgehungsprogramm; OLG Hamburg, *Beschl. v. 21.12.2012 – 3 U 96/12*, *BeckRS* 2013, 06273 Rn. 16 ff. – *Ann Christin*; *Lunze*, in: *Cepl/Voß, Prozesskommentar zum Gewerblichen Rechtsschutz*, 2. Aufl. 2018, § 707 ZPO Rn. 28 ff.

rend sind, dass die Interessen des Gläubigers an der vorläufigen Vollstreckung ausnahmsweise weichen müssen. Dies kann etwa – im Bereich des Datenrechts naheliegend – dann der Fall sein, wenn die Offenbarung (man wird einschränken müssen: gewichtige) Betriebs- und Geschäftsgeheimnisse des Schuldners betrifft.³⁹ Folgt das Gericht erster Instanz diesem Argument nicht, kann vor dem Berufungsgericht⁴⁰ ein Antrag auf einstweilige Einstellung der Zwangsvollstreckung nach § 719 ZPO zu stellen sein.⁴¹ Im Übrigen sollte der Schuldner versuchen, gegenüber dem Gericht darauf hinzuwirken, dass die Sicherheitsleistung für die vorläufige Vollstreckbarkeit in angemessener Höhe festgesetzt wird; da nach – kritikwürdiger – Rechtsprechung für die zu leistende Sicherheit nicht (auch) der Wert der betroffenen Information für den Kläger, sondern (nur) der Aufwand für deren Zusammenstellung beim Schuldner maßgeblich sein soll,⁴² ist dies freilich nicht einfach. Bei Auskunftsansprüchen ist hierbei in der Praxis dann auch oft eine bedauerliche und hinsichtlich des (potenziellen) wirtschaftlichen Wertes der erlangten Erkenntnis für den Kläger nicht angebrachte Zurückhaltung der Gerichte zu beobachten.⁴³

Praxishinweis: Da auch die nur vorläufige Vollstreckung eines auf Überlassung eines Datenbestands oder Auskunft über den Inhalt eines Datenbestands gerichteten Titels, dem Kläger den Datenbestand endgültig offenbart, sollte der Beklagte ab der ersten Instanz die zur Verfügung stehenden Vollstreckungsschutzmöglichkeiten konsequent nutzen und auch darauf hinwirken, dass eine vorläufige Vollstreckbarkeit, wenn dann nur gegen eine angemessene Sicherheitsleistung gestattet wird.

13

3. Vollstreckung in einzelne Gegenstandskategorien

a) Körperliche Gegenstände (Datenträger)

Die Zwangsvollstreckung in (bewegliche) körperliche Gegenstände wegen einer Geldforderung richtet sich nach §§ 808 ff. ZPO. In diesen Fällen führt eine Zwangsvollstreckung in den Datenträger nicht zur Erlangung des Datenträgers durch den Gläubiger, sondern zu dessen Verwertung nach den vorgenannten Vorschriften. An den Gläubiger wird ein bei der Verwertung erzielter Geldbetrag in der Höhe der vollstreckten Forderung herausgegeben.

14

Geht es hingegen um die Zwangsvollstreckung in einen körperlichen Gegenstand wegen der Herausgabe dieses Gegenstandes an den Gläubiger, sind die §§ 883–886 ZPO maßgeblich.

³⁹ S. schon BGH, Beschl. v. 23. 01. 1956 – II ZR 20/56, LM § 719 ZPO Nr. 12.

⁴⁰ Bzw. in dritter Instanz dem BGH, § 719 Abs. 2 ZPO.

⁴¹ Vgl. nur BGH, Urt. v. 07. 09. 1990 – I ZR 220/90, GRUR 1991, 159, 160 – Zwangsvollstreckungseinstellung.

⁴² BGH, Beschl. v. 24. 11. 1994 – GSZ 1/94, GRUR 1995, 701, 702 – Rechtsmittelbeschwerde gegen Auskunftsverurteilung m. w. Nachw.; OLG Hamburg, Beschl. v. 21. 12. 2012 – 3 U 96/12, BeckRS 2013, 06273 Rn. 17 – Ann Christin; vgl. auch OLG Schleswig, Beschl. v. 15. 09. 1982 – 8 WF 157/82, SchlHA 2982, 196.

⁴³ *Henn/Apel*, MarkenR 2016, 345 m. Fn. 3 zum Markenrecht.

▼ Rechte an Daten werden in der Digitalisierung zunehmend relevant. Dabei geht es aber nicht nur um spezifische Fragen des Datenschutzrechts für neue Medien, sondern auch und gerade um Vermögensrechte an Daten, vertragsrechtliche Vorgaben für die Weitergabe und Nutzung von Daten, kartellrechtliche Fragen sowie die Zwangsvollstreckung in Datenbestände.

Das Handbuch gibt eine erste Definition des neuen Rechtsgebietes „Datenrecht“ und adressiert die hier auftretenden Fragestellungen. Dabei wagt es einen Blick über den juristischen Tellerrand hinaus auch in andere Disziplinen.

Leseprobe, mehr zum Buch unter ESV.info/978-3-503-18782-9



www.ESV.info