Big Data and Law

Caldarola / Schrey

2020
ISBN 978-3-406-74393-1
C.H.BECK

Caldarola/Schrey

Big Data and Law

Big Data and Law

A Practitioner's Guide

by

Maria Cristina Caldarola
Joachim Schrey

2020

Published by
Verlag C.H.Beck oHG, Wilhelmstraße 9, 80801 München, Germany,
email: bestellung@beck.de

Co-published by
Hart Publishing, Kemp House, Chawley Park, Cumnor Hill, Oxford, OX2 9PH, United Kingdom,
online at: www.hartpub.co.uk

and

Nomos Verlagsgesellschaft mbH & Co. KG, Waldseestraße 3–5, 76530 Baden-Baden, Germany,
email: nomos@nomos.de

Published in North America by Hart Publishing
An Imprint of Bloomsbury Publishing 1385 Broadway, New York, NY 10018, USA
email: mail@hartpub.co.uk

Suggested citation:
Caldarola/Schrey, Big Data and Law, p. [#]

ISBN 978 3 406 74393 1 (C.H.BECK)
ISBN 978 1 5099 3193 4 (HART)
ISBN 978 3 8487 6212 5 (NOMOS)

Wilhelmstr. 9, 80801 München
Printed in Germany by
Friedrich Pustet GmbH & Co. KG
Gutenbergstraße 8, 93051 Regensburg
Typeset by
Reemers Publishing Services GmbH, Krefeld
Cover: Druckerei C.H.Beck Nördlingen

chbeck.de/nachhaltig

Preface

Data are often referred to as the "oil of the 21st century" and Big Data applications are seen as a new "oil platform" to extract this lucrative resource. However, like oil platforms, Big Data applications only yield their treasure to those who have not only the right infrastructure and technical expertise but also an understanding of the legal ramifications.

This book has been written to expose and close a gap in German and European legal commentaries when it comes to Big Data. It examines not only data protection and its legal ramifications but also the Big Data environment as affected by laws including the German Civil Code (BGB), intellectual property law and data protection law. Its German language version was published in December 2018 by the Munich-based publishing house C.H.Beck Verlag.

The book deals with personal and non-personal data (factual data or anonymous data), two types of data which are often combined for Big Data analyses. They often come from the different right holders, are subject to different national laws, trigger different legal requirements and/or are used for different analytical purposes.

In this guide, we offer practical and descriptive solutions for setting up a Big Data project by addressing interdependencies – among data types, right holders, applicable law, lawful ground/legal requirements, purposes – and relevant areas of legal practice. It combines these variable aspects for companies in various Big Data scenarios and offers legally reliable and controllable solutions.

With numerous guidelines and graphics, this book is a practical legal guide to gathering, storing and analyzing personal and other types of data in Big Data applications. It provides comprehensive, practice-oriented assistance and reliability for planning in everyday business in a Big Data environment. It is aimed in particular at lawyers, computer scientists, business economists, managing directors, managers, analysts, consultants, auditors, and internal and external data protection officers.

Stuttgart/Frankfurt am Main
November 2019

Dr. iur. Maria Cristina Caldarola, LL.M., MBA
Prof. Dr. iur. Joachim Schrey

Contents

Preface V
Abbreviations XIII
Legend XV
Bibliography XVII
List of Figures XXI

A. Introductory remarks 1
I. Why Big Data? 1
II. Why must a party not established in the EU comply with GDPR with respect to Big Data applications? 1
1. General principles 1
2. Companies established in the EU (Art. 3 (1) GDPR) 2
3. Companies not established in the EU (Art. 3 (2) GDPR) 2
4. Offering of goods or services to data subjects in the EU 2
5. Monitoring the behaviour of subjects in the EU 4
6. Data processing facilities in a place where Member State law applies (Art. 3 (3) GDPR) 4
7. Limits of the scope of application – opening clauses 4
8. Most relevant opening clauses in the GDPR 5
a) Data processing in employment contexts (Art. 88 GDPR) 5
b) Designation of a data protection officer in cases other than Art. 37 (1) GDPR 6
c) Processing carried out in the public interest or in compliance with a legal obligation 6
9. Summary 6
III. Which data are affected? 7
IV. What are the differences between the data types? 8
V. Which verification steps need to be considered for a Big Data application? 11

B. Types of data 15
I. Personal data 16
1. Definition of "personal data" pursuant to Art. 4 (1) GDPR 16
2. Identifiability of personal data (Examples) 18
a) Dynamic IP addresses 18
b) Personnel or customer numbers 18
c) VIN/Vehicle registration numbers 19
d) Special categories of personal data 19
e) Location, traffic and usage data 20
f) Characteristics of specific data sources 21
aa) Social Media 21
bb) Open Data 23
cc) Data acquisition through Apps 23
II. Non-personal data 24
III. Databases and collections 25
1. Collections of works, data or other independent elements, § 4 German Copyright Act 26
2. Database protection rights 27
3. Protection of individual elements of a database or a collection 29
a) Database model 29
b) Data format 30
c) Interface 31
IV. Protection as business or trade secret 31
V. Householder's right with regard to the collection of factual data 32
VI. Virtual householder's right 33
VII. Factual data linked to IP addresses or other identifying characteristics 34
VIII. No data ownership 35

C. The controller ... 37
I. Processor ... 38
1. Controller-to-processor agreement (C2P) ... 39
2. Obligation to separate the databases ... 40
3. Other obligations of the processor ... 41
4. Securing instruments for compliance with data protection obligations of a controller of Big Data Applications with regard to the processor ... 41
a) Selection and prior checking ... 42
b) C2P agreement ... 42
II. Joint controllers, Art. 26 GDPR ... 43
1. Internal relationship between the joint controllers ... 44
2. Provision of the internal agreement ... 45
3. External Relationship Between the Joint Controllers and the Data Subject ... 45
III. Dynamic matrix structures ... 45
1. Participation in projects of multiple responsible entities ... 45
2. Employee secondment/supply of temporary staff ... 46
3. Joint controllers within the meaning of Art. 26 GDPR with regard to project participations ... 47
IV. Cloud computing ... 47
1. Storing in your own cloud ... 47
2. Use of third-Party cloud storage ... 48

D. Specific requirements and tasks of the data protection officer with regard to Big Data applications ... 49
I. Specialist knowledge ... 49
II. Organizational and operational involvement of the data protection officer ... 49
III. Communication with data subjects ... 50
IV. Information and monitoring obligations ... 50
V. Cooperation and control obligations ... 51
VI. Internal procedure in the event of a data protection violation ... 51

E. Lawful ground for data processing (collection, acquisition, transmission, evaluation and commercialization) ... 53
I. Statutory lawful grounds for personal data ... 54
1. Performance of a contract ... 57
2. Balance of interests ... 58
3. Works council agreements ... 59
4. Consent ... 60
a) Declaration of consent ... 62
b) Formal requirements ... 62
c) Free Will ... 63
d) Indication of the purpose of the collection and processing ... 64
e) Transmission to third parties, in particular to countries outside the EU ... 64
f) Right to withdraw consent ... 66
g) *Opt-in* and *opt-out* solutions ... 67
II. Processing of non-personal factual data ... 68
1. Processing of factual data ... 68
2. Obtaining data from data collections/databases ... 68
3. Obtaining data from Open Data projects ... 69
4. Data from publicly available sources ... 69

F. Data processing and data cycle (level of data purpose) ... 71
I. Data processing ... 71
II. Life cycle of data ... 71
III. Collection of personal data for purposes other than their use in Big Data applications – a change of purpose ... 73
1. The purpose of data collection and processing ... 73
2. The "purpose" of contracts for the supply and use of data ... 74
3. The problem of dynamic purpose changes in Big Data applications ... 74
a) The link between the original and new purpose ... 76

b) The context of data collection ... 76
c) The type of personal data ... 76
d) Possible consequences of the intended subsequent processing for the data subjects 76
e) The existence of appropriate guarantees ... 77

G. Third country transfer/Applicable law (Level of applicable law) ... 79

H. Development of a Big Data application ... 83
I. Collection of data ... 84
II. Obtaining and acquiring data from data service providers ... 84
1. Legality of the collecting data provided by a data supplier ... 84
2. Legitimacy of data acquisition from third parties ... 85
3. Rectifying deficiencies ... 85
III. Combination of data ... 86
1. Lawfulness of combining different data categories at the level of data retrieval ... 88
2. Combining personal data from different data sources ... 88
3. Combining personal data with factual data or anonymous data ... 89
4. Combination of personal data from different countries of origin ... 90
5. Combining different personal data collected for different purposes ... 90
6. Rectifying deficiencies ... 93
IV. Extending the range: anonymization/pseudonymization of data stored in a Big Data database ... 95
1. Pseudonymization (Art. 4 No. 5 GDPR) ... 95
2. Anonymization ... 98
3. Encryption and secrecy ... 100
4. De-anonymization for large amounts of data that allow re-identification ... 101
5. Data Trustee ... 102
a) Requirements for a data trustee ... 103
b) Contractual penalty for breach of duties or for overcoming joint management controls ... 103
V. Transmission of data from several controllers to a central Big Data application ... 103
VI. Evaluation and analysis of data ... 104
1. Lawful grounds for the evaluation and analysis of personal data ... 104
2. Big Data applications for the analysis of data with reference to employees or applicants ... 105
a) Applicant analysis ... 105
aa) Collection and Processing of Employee Data in Developing Algorithms for People Analytics Applications ... 106
bb) Analysis of applicant data in people analytics applications ... 107
b) Employee analysis ... 108
aa) Analyses for the purpose of employee retention ... 108
bb) People analytics application with reference to data from social networks ... 108
cc) People analytics application with reference to other publicly accessible data ... 108
dd) Limit of people analytics applications ... 109
c) Stress and mood analyses ... 109
d) Databases for project analysis ... 109
e) Prohibition of completely automatically generated individual decisions ... 110
3. Collective agreements ... 110
4. Rights of the works council to participate (in Germany § 87 (1) No. 6 BetrVG) ... 111
5. Special cases ... 112
a) Scoring ... 112
b) User profile ... 113
VII. Continuation of personal reference even after evaluation and analysis of data ... 113
1. Analysis of personal data records insofar as personal references still exist or can be restored ... 113
2. Evaluation of pseudonymized data records ... 114
3. Evaluation of non-personal data, factual data or anonymized data ... 114
VIII. Use of personal data or person-related evaluation/analysis results ... 114

I. Erasure obligations ... 117
I. Development of an erasure concept ... 119
II. Implementation of a data erasure concept ... 120
III. Necessary elements of a data erasure concept? ... 121
1. Description of retention and erasure obligations ... 121
2. What is the relevant law for determining retention and erasure obligations? ... 121
3. Legal retention obligations ... 121
4. Erasure periods for archiving data on the basis of consent ... 122
5. Determining erasure periods from the purpose of use, the applicable statutory provisions and the business process reference of the processed data ... 122
6. Types of data for which the intended use provides the basis for determining the retention period ... 123
a) Determining a purpose and associated lawful ground for personal data ... 123
b) Purpose and retention of non-personal data ... 123
IV. Start times of retention and erasure obligations ... 123
V. Assignment of data types to erasure classes ... 124
VI. Resolution of conflicts when using one data type in different databases ... 124
VII. What does "erasure" of data mean in contrast to its "blocking", "masking", "pseudonymization" or "anonymization"? ... 125
VIII. Obligation to erase personal data regarding a data subject ... 127
1. Reasons ... 127
a) Personal data ... 127
b) Non-personal data ... 128
2. Date ... 128
3. Reasons for exclusion ... 129
4. Right *to be forgotten* ... 129
5. Right to limitation of processing ... 130
IX. Erasure obligations towards licensors, data suppliers etc. independent of the data content ... 130
X. Uniform erasure period for all documents and data ... 131
XI. Erasure obligations for cross-border data processing ... 132
XII. Storage locations and erasure obligations ... 133

J. Relevant rights of data subjects in Big Data applications according to the GDPR ... 135
I. Information obligations according to Art. 13, 14 GDPR ... 135
II. Rights of data subjects pursuant to Art. 15 *et seq.* GDPR ... 137
1. Right to access ... 137
2. Right to rectification ... 137
3. Right to erasure and *to be forgotten* ... 138
4. Right to restriction of processing ... 138
5. Right to data portability ... 138
6. Right to lodge a complaint ... 139
III. Records of processing activities according to Art. 30 GDPR ... 139
IV. Implementation of technical and organizational measures to protect personal data from unauthorized access ... 140
1. Access control ... 141
2. (Virtual) Access control ... 141
3. Admission control ... 142
4. Data medium control ... 142
5. Access and user control ... 142
6. Control of disclosure, transmission and transport ... 143
7. Input and storage control ... 143
8. Contract control ... 143
9. Availability control ... 144
10. Separation control ... 144
11. Recoverability ... 144
12. Reliability ... 145
13. Data integrity ... 145
14. Sanction for non-existent or inadequate technical and organizational measures ... 145

V. General principles for the processing of personal data in Art. 5 GDPR ... 145
1. General principles for the processing of personal data ... 145
2. Principle of accountability (Art. 5 (2) GDPR) ... 146
3. Sanctioning a breach of these principles ... 146

K. Data protection impact assessment ... 147

L. System data protection when operating Big Data applications ... 149
I. System data protection for personal data ... 149
1. Fundamental right to informational self-determination ... 149
2. The fundamental right to ensure the integrity and confidentiality of information technology systems ... 150
3. Indirect effect of fundamental rights between private individuals; Interpretation of guidelines ... 150
4. Ensuring confidentiality through technical and organizational measures ... 151
II. System data protection for non-personal data only in a Big Data Application ... 153

M. Protection of Big Data applications ... 155
I. Technical and organizational measures ... 155
II. Protection of the algorithms underlying the Big Data application ... 155
III. Compliance management system ... 156
IV. Aspects of copyright contract law in the database management system ... 157

N. Legal consequences of non-compliance with the legal requirements set out in this guide 159
I. Sanctions in case of violation of data protection regulations ... 160
1. Administrative fines ... 160
2. Material and non-material damages supplemented by power to bring collective actions ... 162
3. Misdemeanours ... 162
4. Entry in central trade register (loss of entitlement to participate in public tenders) ... 162
5. Penalties according to the BDSG ... 162
6. Supervisory intervention rights of the data protection supervisory authorities ... 163
II. Legal consequences of infringement of copyrights in collective works or database protection rights ... 164
1. Injunctive relief ... 164
2. Damages claim ... 164
3. Enforcement of copyright claims ... 164
4. Destruction claim ... 165
5. Liability of the controller ... 165
6. Right to information ... 165
7. Criminal offences ... 165
III. Violation of virtual householder's rights ... 166
1. Injunctive relief ... 166
2. Damage claims ... 166
3. Subordinate claims ... 166
4. Relevance under criminal law ... 166
IV. Sanctions for infringing business or trade secrets pursuant to the German Trade Secrets Act ... 167
1. Criminal offences ... 167
2. Civil law Claims under the German Trade Secrets Act ... 167
V. Contractual claims ... 168

O. Big Data Applications as a service ... 169

P. Recommended Actions ... 175

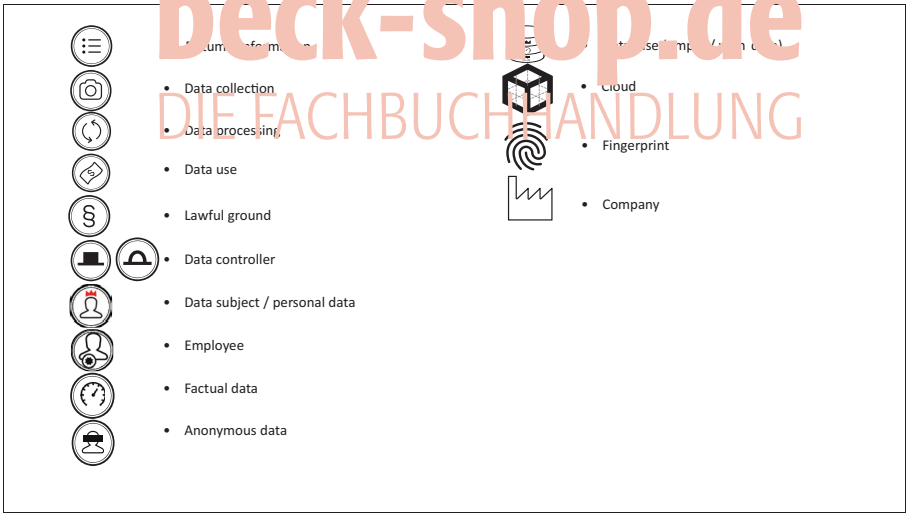
Index of keywords ... 177

Abbreviations

a. F.	*alte Fassung*; old version
AO	*Abgabeordnung*; Tax Code https://www.gesetze-im-internet.de/englisch_ao/index.html
Art.	Article
BDSG	*Bundesdatenschutzgesetz*; Federal Data Protection Act https://www.gesetze-im-internet.de/englisch_bdsg/index.html
BGB	*Bürgerliches Gesetzbuch*; Civil Code https://www.gesetze-im-internet.de/englisch_bgb/index.html
BGH	*Bundesgerichtshof*; Federal Court of Justice
BVerfG	*Bundesverfassungsgericht*; Federal Constitutional Court
C2P	Controller-to-processor
Data Protection Directive	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046
ed(s).	editor(s)
Fn.	Footnote
GDPR	General Data Protection Regulation https://gdpr-info.eu/
GeschGehG	*Geschäftsgeheimnisgesetz*; Trade Secrets Act
GG	*Grundgesetz*; Basic Law https://www.gesetze-im-internet.de/englisch_gg/index.html
GWB	*Gesetz gegen Wettbewerbsbeschränkungen*; Act against restraints of competition https://www.gesetze-im-internet.de/englisch_gwb/index.html
HGB	*Handelsgesetzbuch*; Commercial Code https://www.gesetze-im-internet.de/englisch_hgb/index.html
IoT	Internet of Things
i. V. m.	*in Verbingung mit*; in conjunction with
LG	*Landgericht*; Regional Court
M2M	Machine to Machine
mn.	Margin number
No.	Number
OLG	*Oberlandesgericht*; Higher Regional Court
OWiG	*Ordnungswidrigkeitengesetz*; Regulatory Offences Act https://www.gesetze-im-internet.de/englisch_owig/index.html
p.	Page
PatG	*Patentgesetz*; Patent Act https://www.gesetze-im-internet.de/englisch_patg/index.html
Rs.	*Rechtsprechung*; Case
StVG	*Straßenverkehrsgesetz*; Road Traffic Act https://www.gesetze-im-internet.de/englisch_stvg/index.html
TFEU	Treaty on the Functioning of the European Union https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT
TKG	*Telekommunikationsgesetz*; Telecommunications Act https://germanlawarchive.iuscomp.org/?p=692
TMG	*Telemediengesetz*; Telemedia Act
u. a.	*inter alia*; amongst others

UKlaG	*Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen;* Act on Actions for Injunctive Relief for Breaches of Consumer law and Other Laws
UrhG	*Urheberrechtsgesetz*; Copyright Act https://www.gesetze-im-internet.de/englisch_urhg/index.html
UWG	*Gesetz gegen den unlauteren Wettbewerb*; Act against Unfair Competition https://www.gesetze-im-internet.de/englisch_uwg/index.html
WP	Working Paper

Legend



Bibliography

Ahlberg, Hartwig/Götting, Horst-Peter (eds.) *Beck'scher Online-Kommentar Urheberrecht*, 17th edition, 1.4.2017

Artikel-29-Working Party *Working Paper 4/2007*, WP 136, "Personal Data"

Artikel-29-Working Party *Working Paper 5/2014 re Anonymization Techniques*, WP 216, from 10.4.2014

Artikel-29- Working Party *Working Paper 5/2012 re Cloud Computing*, WP 196, from 1.7.2012

Auer-Reinsdorff, Astrid/Conrad, Isabell (eds.) *Beck'sches Mandatshandbuch IT-Recht*, 2011

Auer-Reinsdorff, Astrid/Conrad, Isabell (eds.) *Handbuch IT- und Datenschutzrecht*, 2nd edition 2016

Bitkom Potenziale und Einsatz von Big Data, Ergebnisse einer repräsentativen Befragung von Unternehmen in Deutschland, 5.5.2014, https://www.bitkom.org/Publikationen/2014/Studien/Studie-Big-Data-in-deutschen-Unternehmen/Studienbericht-Big-Data-in-deutschen-Unternehmen.pdf (cited: https://www.bitkom.org/Publikationen/2014/Studien/Studie-Big-Data-in-deutschen-Unternehmen/Studienbericht-Big-Data-in-deutschen-Unternehmen.pdf)

Conrad, Isabell/Grützmacher, Malte (eds.) *Recht der Daten und Datenbanken in Unternehmen*, 2014

Conraths, Timo/Krüger, Stefan Das virtuelle Hausrecht des Online-Spiel-Betreibers, Wirksame Rechtsschutzmöglichkeiten für Online-Spiel-Anbieter abseits des Vertragsrechts, *MMR* 2016, 310 et seq.

Däubler, Wolfgang Gläserne Belegschaften, *Das Handbuch zum Beschäftigtendatenschutz*, 7th edition 2017

Dierks Bohle Rechtsanwälte *Rechtsgutachten zur elektronischen Datentreuhänderschaft im Auftrag der Telematikplattform für Medizinische Forschungsnetze*, 2008 (cited: Dierks, in: Telematikplattform für Medizinische Forschungsnetze, Rechtsgutachten zur elektronischen Datentreuhänderschaft)

Dzida, Boris *Big Data und Arbeitsrecht*, NZA 2017, 541 et seq.

Ehmann, Eugen/Selmayr, Martin (eds.) *Datenschutz-Grundverordnung Kommentar*, 2nd edition 2018

Engels, Thomas Datenschutz in der Cloud-Ist hierbei immer eine Auftragsdatenverarbeitung anzunehmen?, *K&R* 2011, 548 et seq.

Ernst, Stefan Die Einwilligung nach der Datenschutzgrundverordnung, Anmerkungen zur Definition nach Art. 4 Nr. 11 GDPR, *ZD* 2017, 110 et seq.

Forst, Gerrit Bewerberauswahl über soziale Netzwerke im Internet?, *NZA* 2010, 427 et seq.

Geppert, Martin/Schütz, Raimund (eds.) *Beck'scher TKG-Kommentar*, 4th edition, 2013

Gersdorf, Hubertus/Paal, Boris P. (eds.) *Beck'scher Online-Kommentar Informations- und Medienrecht*, 17th edition, 1.8.2018

Gola, Peter/Pötters, Stephan/Wronka, Georg *Handbuch Arbeitnehmerdatenschutz unter Berücksichtigung der Datenschutz-Grundverordnung*, 7th edition, 2016

Gola, Peter/Schomerus, Rudolf (eds.) *Bundesdatenschutzgesetz Kommentar*, 12th edition, 2015

Grünwald, Andreas/Nüßing, Christoph Machine To Machine (M2M)-Kommunikation, Regulatorische Fragen bei der Kommunikation im Internet der Dinge, *MMR* 2015, 378 et seq.

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (eds.) *Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschäftsverkehrs*, 46th update, January 2018

Hofmann, Johanna M., Anforderungen aus GDPR und NIS-RL an das Cloud Computing, *ZD-Aktuell* 2017, 05488

Höinghaus, Christoph Daten: Das Öl des 21. Jahrhunderts, Big Data wirtschaftlich sinnvoll einsetzen, CIO, 28.8.2015, https://www.cio.de/a/big-data-wirtschaftlich-sinnvoll-einsetzen,3246278 (cited: https://www.cio.de/a/big-data-wirtschaftlich-sinnvoll-einsetzen,3246278)

IDC/DELL EMC Studie "Das digitale Universum", Bericht für 2014, http://germany.emc.com/leadership/digital-universe/index.htm (cited: http://germany.emc.com/leadership/digital-universe/index.htm)

Katko, Peter/Babaei-Beigi, Ayda Accountability statt Einwilligung? Führt Big Data zum Paradigmenwechsel im Datenschutz?, *MMR* 2014, 360 et seq.

Kilian, Wolfgang/Heussen, Benno (eds.) *Computerrechts-Handbuch, Informationstechnologie in der Rechts- und Wirtschaftspraxis*, 33rd update, February 2017

Kinast, Karsten/Kühnl, Christina Telematik und Bordelektronik-Erhebung und Nutzung von Daten zum Fahrverhalten, *NJW* 2014, 3057 et seq.

Klug, Christoph Der Datenschutzbeauftragte in der EU, Maßgaben der Datenschutzgrundverordnung, *ZD* 2016, 315 et seq.

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder "Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018" from 26.4.2018

Kühling, Jürgen/Buchner, Benedikt (eds.) *Datenschutz-Grundverordnung Kommentar*, 2nd edition 2018

Leistner, Matthias Die Landkarte als Datenbank, Überlegungen zum Datenbankschutz für topografische Karten und geografische Daten, *GRUR* 2014, 528 et seq.

Leistner, Matthias Was lange währt …: EuGH entscheidet zur Schutzfähigkeit geografischer Karten als Datenbanken, *GRUR* 2016, 42 et seq.

Lindell, Yehuda/Pinkas, Benny Secure Multiparty Computation for Privacy-Preserving Data Mining, *Journal of Privacy and Confidentiality* 2009, 59 et seq. (cited: *Lindell/Pinkas*, in: The Journal of Privacy and Confidentiality, 2009, 59 et seq.)

Mantz, Reto/Spittka, Jan Anmerkung zu EuGH from19.10.2016-C-582/14, *NJW* 2016, 3582

Metschke, Rainer/Wellbrock, Rita Berliner Beauftragter für Datenschutz und Informationsfreiheit, Hessischer Datenschutzbeauftragter, *Datenschutz in Wirtschaft und Forschung*

Paal, Boris P./Pauly, Daniel A. (eds.) *Datenschutz-Grundverordnung*, Beck'sche Kompakt-Kommentare, 2nd edition 2018

Plath, Kai-Uwe (ed.) *Kommentar zum BDSG und zur DSGVO* [sowie] *den Datenschutzbestimmungen von TMG und TKG*, 3rd edition, 2018 (cited: editor, in: Plath, BDSG/DSGVO, 3rd edition 2018)

Rebmann/Säcker (eds.), *Münchener Kommentar zum BGB*, 7th edition 2017, to § 1004 BGB (cited: author, in: Rebmann/Säcker, MüKo, …).

Roßnagel, Alexander Fahrzeugdaten – wer darf über sie entscheiden?, *SVR* 2014, 281 et seq. (cited.: Roßnagel, 52. Verkehrsgerichtstag 2014, p. 282.)

Roßnagel, Alexander/Scholz, Philip Datenschutz durch Anonymität und Pseudonymität, Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, *MMR* 2000, 721 et seq.

Säcker, Franz Jürgen/Rixecker, Roland/Oetker, Hartmut/Limpberg, Bettina (eds.) *Münchener Kommentar zum BGB*, 7th edition, 2017

Schaffland, Hans-Jürgen/Wiltfang, Noeme (eds.) *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz Kommentar*, update 4/17, Februar 2017 (cited: eauthor, in: Schaffland/Wiltfang, GDPR/BDSG)

Schild, Hans-Hermann (eds.) *Praxis der Kommunalverwaltung*, November 2015 (cited.: Schild/Ronellenfitsch/Arlt/Dembowski/Müller/Piendl/Rydzy/Schriever-Steinberg/Topp/Wehrmann/Wellbrock, in: Praxis der Kommunalverwaltung, Amendment November 2015)

Simitis, Spiros (ed.) *Bundesdatenschutzgesetz Kommentar*, 8th edition, 2014

Spindler, Gerald Text und Data Mining – urheber- und datenschutzrechtliche Fragen, *GRUR* 2016, 1112 et seq.

Thalhofer, Thomas Recht an Daten in der Smart Factory, *GRUR-Prax* 2017, 225 et seq.

Weisser, Ralf/Färber, Claus Rechtliche Rahmenbedingungen bei Connected Car, Überblick über die Rechtsprobleme der automobilen Zukunft, MMR 2015, 506 et seq.

Werkmeister, Christoph/Brandt, Ella Datenschutzrechtliche Herausforderungen für Big Data, *CR* 2016, 233 et seq.

Wójtowicz, Monika/Cebulla, Manuel Anonymisierung nach der DSGVO, *PinG* 2017, 186 et seq.

Wolff, Heinrich Amadeus/Brink, Stefan (eds.) *Beck'scher Online-Kommentar Datenschutzrecht*, 25th edition, 1.8.2018

Wybitul, Tim/Rauer, Nils EU-Datenschutz-Grundverordnung und Beschäftigtendatenschutz, Was bedeuten die Regelungen für Unternehmen und Arbeitgeber in Deutschland?, *ZD* 2012, 160 et seq.

Wybitul, Tim/Ströbel, Lukas/Ruess, Marian Übermittlung personenbezogener Daten in Drittländer, Überblick und Checkliste für die Prüfung nach der GDPR, *ZD* 2017, 503 et seq.

Zieger, Christoph/Smirra, Nikolas Fallstricke bei Big Data-Anwendungen, Rechtliche Gesichtspunkte bei der Analyse fremder Datenbestände, *MMR* 2013, 418 et seq.

Zoebisch, Michael Stimmungsanalyse durch Call-Center, Datenschutzrechtliche Zulässigkeit der Analyse der emotionalen Verfassung anhand der Stimme, *DuD* 2011, 394 et seq.

List of Figures

Figure 1: How does data "originate"? 7
Figure 2: Data types 7
Figure 3: Data types and definitions 8
Figure 4: Right holders 8
Figure 5: Objective of protection 9
Figure 6: Lawful grounds 9
Figure 7: Prohibition rights 10
Figure 8: Legal consequences 10
Figure 9: Variable dependencies 11
Figure 10: Information 12
Figure 11: Documentation 12
Figure 12: Personal or factual data 17
Figure 13: Examples of personal data 18
Figure 14: Personal or factual data 24
Figure 15: Responsibilities of a data controller 38
Figure 16: Controller-to-processor agreement (C2P) 39
Figure 17: Client separation for Hosting/SaaS 41
Figure 18: Checks when receiving, processing and transferring data 42
Figure 19: Examination order when processing data 53
Figure 20: Prohibition subject to permission 54
Figure 21: Prohibition subject to lawful ground 54
Figure 22: Lawful grounds required per processor in a "sample processing chain" 55
Figure 23: Lawful grounds in a sample processing chain 55
Figure 24: Lawful grounds 56
Figure 25: Examination order when processing personal data 56
Figure 26: Collective agreement 59
Figure 27: Radius of collective agreement 60
Figure 28: Content of a consent 61
Figure 29: Consent in a sample processing chain 62
Figure 30: Requirement of transparency in a sample processing chain 65
Figure 31: Consent and withdrawal in a sample processing chain 67
Figure 32: Examination order when processing factual data 68
Figure 33: Examination order when processing databases 69
Figure 34: Data process/purpose 71
Figure 35: Principle of data economy 72
Figure 36: Life cycle of data 73
Figure 37: Principle of applicable law 79
Figure 38: Countries with adequate levels of data protection 80
Figure 39: Change of applicable law in a sample processing chain 80

Figure 40: Combination of lawful and unlawful data 86
Figure 41: Combination of data and applicable laws 86
Figure 42: Exemplary personal and factual data 87
Figure 43: Combination of personal and factual data 87
Figure 44: Application of data protection law to factual data 88
Figure 45: Combination of personal and anonymous data 89
Figure 46: Combination of data of different jurisdictions 90
Figure 47: Combination of data with different purposes and lawful grounds 91
Figure 48: Separation according to data type and purpose 91
Figure 49: Combination of same categories of data but from different legal entities 92
Figure 50: Combination of same categories of data but from different legal entities 92
Figure 51: Combination of same categories of data but from different legal entities 93
Figure 52: Combination of lawful and unlawful data 94
Figure 53: Example database with personal and factual data 95
Figure 54: Pseudonymization 96
Figure 55: Anonymization 99
Figure 56: Encryption/confidentiality 101
Figure 57: The *nature* of factual data 101
Figure 58: Example: Fulfilment of purpose 117
Figure 59: Principle of data minimization 119
Figure 60: Reasons for data erasure 127
Figure 61: Information obligations 135
Figure 62: Record of processing activities 139
Figure 63: Technical and organizational measures in a sample chain 152
Figure 64: Technical and organizational measures 152
Figure 65: Prohibition rights 159
Figure 66: Legal consequences 159
Figure 67: Responsibilities of a hosting provider 169
Figure 68: Responsibilities of a hosting user 170
Figure 69: Separation of clients in a hosting/SaaS environment 170
Figure 70: Authorization of a hosting/SaaS provider 171
Figure 71: Further authorization with additional legitimization 171
Figure 72: Multi-Cloud-approach 172
Figure 73: Checks when receiving, processing and transferring data 172
Figure 74: Data protection with different Big Data providers 173