Data Warehouse

Caldarola

2024
ISBN 978-3-406-80649-0
C.H.BECK

schnell und portofrei erhältlich bei
beck-shop.de

Die Online-Fachbuchhandlung beck-shop.de steht für Kompetenz aus Tradition. Sie gründet auf über 250 Jahre juristische Fachbuch-Erfahrung durch die Verlage C.H.BECK und Franz Vahlen.
beck-shop.de hält Fachinformationen in allen gängigen Medienformaten bereit: über 12 Millionen Bücher, eBooks, Loseblattwerke, Zeitschriften, DVDs, Online-Datenbanken und Seminare. Besonders geschätzt wird beck-shop.de für sein umfassendes Spezialsortiment im Bereich Recht, Steuern und Wirtschaft mit rund 700.000 lieferbaren Fachbuchtiteln.

Caldarola

Data Warehouse

beck-shop.de
DIE FACHBUCHHANDLUNG

beck-shop.de
DIE FACHBUCHHANDLUNG

Data Warehouse

Einführung für die Praxis

Herausgegeben von

Dr. iur. Maria Cristina Caldarola, LL.M., MBA

Bearbeitet von der Herausgeberin und von

Victoria Copeland, LL.B., Dr. Till Jaeger, Thomas Kahl,
Dr. Grace Nacimiento, LL.M., Dr. Fabian Niemann,
Dr. Ioannis Revolidis, Prof. Dr. Joachim Schrey,
Dr. Angelica Maria Schwarz, Ole Sieverding,
Nina Spieler, LL.M., Martin Szugat

beck-shop.de
DIE FACHBUCHHANDLUNG

2024

C.H.BECK

Zitiervorschlag: Caldarola Data Warehouse/Bearbeiter S. …

beck-shop.de
DIE FACHBUCHHANDLUNG
www.beck.de

ISBN 978 3 406 80649 0

© 2024 Verlag C. H. Beck oHG
Wilhelmstraße 9, 80801 München
Druck und Bindung: Beltz Bad Langensalza GmbH
Am Fliegerhorst 8, 99947 Bad Langensalza

Satz: Fotosatz H. Buck
Zweikirchener Str. 7, 84036 Kumhausen
Umschlag: Ralph Zimmermann – Bureau Parapluie

myclimate
shape our future
chbeck.de/nachhaltig

Gedruckt auf säurefreiem, alterungsbeständigem Papier
(hergestellt aus chlorfrei gebleichtem Zellstoff)

Alle urheberrechtlichen Nutzungsrechte bleiben vorbehalten.
Der Verlag behält sich auch das Recht vor, Vervielfältigungen dieses Werkes
zum Zwecke des Text and Data Mining vorzunehmen.

Bearbeitungsverzeichnis

Dr. Maria Cristina Caldarola, LL.M., MBA *Justitiarin Robert Bosch GmbH*
Stuttgart / Deutschland
Sie ist eine erfahrene Unternehmensjuristin im IT- und IP-Bereich bei der Robert Bosch GmbH. Sie verfügt über ein breites Spektrum an Erfahrungen und Fähigkeiten in den Themen Lizenzen, Patente, Marken, Domains, Software, Cloud, Digitale Ökosysteme, Big Data, Kundendatenschutz und Industrie 4.0. Darüber hinaus ist sie Gründerin und Geschäftsführerin des Start-up Unternehmen CU3IC – www.cu3ic.com – das Innovationsberatung im cross-industriellen Bereichen sowie in BOP Märkten anbietet. Dr. Caldarola ist Lehrbeauftragte an diversen Universitäten wie St. Gallen (Schweiz), Keio (Japan). Sie ist Co-Autorin des Buches Big Data und Recht und sie schreibt regelmäßig eine Duett-Kolumne – www.duet-interviews.com – zum Thema Big Data anlässlich derer sie Koryphäen aus aller Welt zu den brennenden Fragen unserer Zeit interviewt.

beck-shop.de
DIE FACHBUCHHANDLUNG

Victoria Copeland, LL.B. Ehemals wissenschaftliche Mitarbeiterin *Noerr PartGmbB*
Frankfurt am Main / Deutschland
Sie ist Absolventin der EBS Law School in Wiesbaden. Sie war als wissenschaftliche Mitarbeiterin und Referendarin im Frankfurter Büro der Noerr PartGmbB tätig.

Dr. Till Jaeger *Rechtsanwalt und Partner JBB Rechtsanwälte Jaschinski Biere Brexl Partnerschaft mbB*
Berlin / Deutschland
Er ist Mitbegründer des Instituts für Rechtsfragen der Freien und Open Source Software (ifrOSS). Als Fachanwalt für Urheber- und Medienrecht liegt der Schwerpunkt seiner praktischen und wissenschaftlichen Arbeit auf freien Lizenzmodellen.

Thomas Kahl *Rechtsanwalt und Partner Taylor Wessing*
Frankfurt am Main / Deutschland
Als Fachanwalt für Informationstechnologierecht ist er Mitglied der Praxisgruppe TMT sowie der Industry Group Compliance der Sozietät. Er berät nationale wie internationale Unternehmen zu allen rechtlichen Fragestellungen der Informationstechnologien. Er begleitet seit vielen Jahren Unternehmen in Entwicklungs- und Digitalisierungsprojekten und der Implementierung innovativer Technologien.
Er ist Experte für die Umsetzung der Vorgaben der DS-GVO sowie bereichsspezifischer Vorgaben des Datenschutzrechts mit Fokus auf Automotive & Mobility und regulierte Industrien und verfügt über umfassende Erfahrung in der Beratung von Datenschutzvorfällen, Cyber-Attacken und aufsichtsbehördlichen wie gerichtlichen Verfahren.

Dr. Grace Nacimiento, LL.M. *Rechtsanwältin und Partnerin*
GvW Graf von Westphalen Rechtsanwälte Steuerberater Partnerschaft mbB
Düsseldorf / Deutschland
Sie ist Co-Leiterin des Fokusbereichs Digitalisierung und Technologie und Mitglied in der Praxisgruppe TMC/IP. Sie berät seit über 20 Jahren Unternehmen in den Kommunikations-, Medien- und Technologiebranchen in regulatorischen und rechtlichen Fragestellungen, u.a. im Bereich Markt-, Entgelt- und Zugangsregulierung, öffentliche Sicherheit, Datenschutz und Zugang zu knappen öffentlichen Gütern (Frequenzspektrum und Nummernressourcen). Sie berät Unternehmen im Bereich New Space zu weltraum- und satellitenrechtlichen Fragen. Im Automobilsektor unterstützt sie Unternehmen umfassend in Fragen zur Einführung digitaler Dienste und berät seit einigen Jahren verstärkt industrieübergreifend in Themen der Vernetzung (IoT) und M2M-Kommunikation.

Dr. Fabian Niemann *Rechtsanwalt und Partner Bird & Bird LLP*
Frankfurt am Main / Deutschland
Er ist Co-Leiter der internationalen Technology & Communications Gruppe von Bird & Bird und spezialisiert auf IT- und Datenschutzrecht, insbesondere Fragen Datenökonomie, Cloud und KI und zu neuen Geschäftsmodellen und Technologien. Er hat in Bonn, Honolulu, Köln und London studiert und promoviert.

beck-shop.de
DIE FACHBUCHHANDLUNG

Dr. Ioannis Revolidis *Juniorprofessor Universität Malta*
Malta
Er studierte Rechtswissenschaften an der Aristoteles Universität, Thessaloniki; 2010 juristische Staatsprüfung in Griechenland; 2011 Magister Juris an der Aristoteles Universität, Thessaloniki; zwischen 2013–2019 Wissenschaftlicher Mitarbeiter am Institut für Rechtsinformatik, Leibniz Universität Hannover; 2019 Promotion; seit September 2021 Inhaber der Juniorprofessur im Internetrecht und Recht der Blockchain (Tenure Track) an der Juristischen Fakultät der Universität von Malta.

Prof. Dr. Joachim Schrey *Rechtsanwalt und emeritierter Partner Noerr PartGmbB*
Frankfurt am Main / Deutschland
Bis 2022 Fachanwalt für Informationstechnologierecht.
Er ist seit über 30 Jahren im IT- und Datenschutzrecht tätig. Bis 2021 war er zudem Honorarprofessor an der Goethe-Universität Frankfurt am Main

Dr. Angelica Maria Schwarz *Rechtsanwältin, Eidgenössisch diplomierte Steuerexpertin, Voser Rechtsanwälte KIG*
Baden / Schweiz
Sie arbeitet als Rechtsanwältin in der Schweiz und ist vorwiegend im Bereich des nationalen und internationalen Steuerrechts für Privatpersonen und Gesellschaften tätig. Sie ist spezialisiert auf rechnungslegungsrechtliche und steuerrechtliche Fragen rund um das Thema Big Data und datengetriebene Geschäftsmodelle. Ihre Dissertation verfasste sie über die handels- und steuerrechtliche Behandlung von Daten unter besonderer Berücksichtigung von verrechnungspreislichen Aspekten.

beck-shop.de
DIE FACHBUCHHANDLUNG

Ole Sieverding *Geschäftsführer CyberDirekt GmbH*
Berlin / Deutschland
Das Berliner Insurtech hat sich dem Kampf gegen Cyber-Gefahren verschrieben, um die fortschreitende Digitalisierung zu ermöglichen. Neben digitalen Präventionsangeboten bietet das Start-Up kleinen und mittleren Unternehmen auf einer innovativen Technologieplattform die Absicherung von Cyber-Risiken über spezielle, maßgeschneiderte Versicherungslösungen an. Seine Erfahrungen aus der Praxis gibt Sieverding als Gastdozent an der Dualen Hochschule Baden-Württemberg in Heidenheim zum Thema „Digitalisierung in der Versicherungswirtschaft" an Studierende des Studiengangs „BWL-Versicherung" weiter. Sieverding selbst studierte an der University of Westminster in London und besitzt einen Abschluss in Corporate Finance von der International School of Management Dortmund. Nach Stationen unter anderem im Vertrieb in Hamburg sowie im Underwriting im Versicherungsmarktplatz Lloyds in London, war er sechs Jahre als Underwriting Manager Cyber bei dem Spezialversicherer Hiscox in München tätig. Im Rahmen seiner Tätigkeit als Produktverantwortlicher der Cyber-Versicherung für Deutschland und Österreich trieb er die Ausgestaltung der Cyber-Versicherungslösung für Geschäftskunden entscheidend voran. Zusätzlich war Sieverding beim Gesamtverband der Deutschen Versicherungswirtschaft (GDV) in der Arbeitsgruppe Cyber-Versicherung maßgeblich an der Entwicklung der ersten Cyber-Musterbedingungen beteiligt

beck-shop.de
DIE FACHBUCHHANDLUNG

Nina Spieler *Ehemalige Mitarbeiterin Bird & Bird LLP*
Frankfurt am Main / Deutschland
Sie hat vielseitige Erfahrungen im digitalen und internationalen Handels-, Wirtschafts-, Wettbewerbs- und Umweltrecht in der EU, der USA und dem Nahen Osten. Sie absolvierte ihr Jurastudium an der Sciences Po Paris, Columbia Law School und Harvard Law School, und arbeitet aktuell für eine internationale Kanzlei in Brüssel.

Martin Szugat *Geschäftsführer Datentreiber GmbH*
Weilheim / Deutschland
Als studierter Bioinformatiker hat er das Beratungsunternehmen Datentreiber gegründet und die Methode und Werkzeuge des Datenstrategie-Designs erfunden. Außerdem ist er Programmdirektor mehrerer internationaler Fachkonferenzen zur angewandten KI und Dozent an verschiedenen Hochschulen und Bildungseinrichtungen.

Vorwort

I. Warum ein Data Warehouse so wichtig wird?

Im digitalen Zeitalter und damit mit dem Aufkommen digitaler Geschäftsmodelle benötigen Unternehmen Daten. Diese müssen gemanaget werden und das am besten mit einem Data Warehouse!

Wir kennen Warenhäuser aus der Warenwirtschaft. Es sind Lagerhäuser, in denen Unternehmen Waren für den späteren Ge- und Verbrauch lagern, sei es für die Herstellung ihrer Produkte oder sei es für den späteren Verkauf an ihre Kunden. Die Lagerlogistik operierte in den letzten Jahrzehnten nach dem „Just-in-time" Prinzip, d.h. die richtige Menge sollte zur richtigen Zeit am richtigen Ort sein. Es ist eine moderne Strategie zur Optimierung der Materialbeschaffung und der Vernetzung der Unternehmen mit dem Ziel des Abbaus von Lagerkapazitäten und der Verkürzung von Wegen, um Zeit und Kosten bei der Produktion zu sparen. Dafür sind klare Strukturvorgaben in der eigenen Produktion und auch eine enge Zusammenarbeit mit Zulieferern nötig.

Auch Daten benötigen eine Lagerhaltung. Auch an deren Lagerhaltung besteht das Bedürfnis nach Effizienz, Effektivität, Skalierbarkeit und Vernetzung. Unternehmen benötigen Daten als „single point of reference" und auf einer „need to know basis". Für gute Ergebnisse der digitalen Geschäftsmodelle – welche auch immer es sein mögen – müssen Daten genau, konsistent, relevant, legal, aktuell, akkurat und auf einer „time to market basis" zur Verfügung stehen.

beck-shop.de
DIE FACHBUCHHANDLUNG

II. Das stellt Verantwortliche vor neue Fragen und Herausforderungen!

Natürlich sind die Anforderungen an die Lagerhaltung von Daten andere als die von Waren. Und natürlich ist die Lagerhaltung von Daten weniger materiell als vielmehr digital und immateriell (cloud-basiert).

Bei Daten sind Gesetze und vertragliche Vereinbarungen der Bezugsquellen zu beachten. Konkret heißt das Datenschutz, Informationssicherheit, Kartellrecht, IP-Recht, Haftung und möglicherweise auch die eingesetzte Blockchaintechnologie. Es kommen in einem Data Warehouse viele Aspekte zusammen, die ein Unternehmen beim Betrieb einer meist cloud-basierten Datenhaltung zu beachten hat, um Haftungsrisiken zu meiden, compliant zu sein und um die Chance des Daten-Sharings, der Datenökonomie, der Datenautomatisierung und der Datenmonetarisierung in vollem Umfang nutzen zu können. Und genau diese legalen Anforderungen sind bei der technischen Datenarchitektur mit zu berücksichtigen.

Das Ziel eines Data Warehouse ist einen umfassenden Überblick über die vorhandenen Daten im Unternehmen zu erhalten und zu geben und damit die Entscheidungen zur Unternehmensplanung zu unterstützen. Damit die Ziele eines Data Warehouse verwirklicht werden können, müssen neben den legalen Aspekten auch technische Punkte erfüllt sein wie z.B. die Erstellung einer zentralen Datenhaltung, die Trennung von Daten in einem operativen Umfeld und einem Testumfeld, die Datenintegration verschiedener Informationsquellen, die Historisierung der Daten…

Die Anforderungen an ein modernes Data Warehouse sind vielfältig und je nach Unternehmen, Geschäftsbedürfnissen und Stand des bestehenden Data Warehouse Systems

unterschiedlich ausgerichtet. Mit einem Data Warehouse können Unternehmen schneller Einblicke gewinnen, auf erweiterte Analysen zugreifen, die volle Kontrolle über ihre Daten behalten und ihre Reaktionsfähigkeit mit Echtzeitdaten verbessern. Möglich sind auch mit Hilfe von Business Intelligenz ergänzende Prognosen aus den Daten zu ziehen, um Unternehmen in die Lage zu versetzen, Daten in verwertbare Erkenntnisse zu verwandeln – ohne Einschränkungen hinsichtlich Größe, Leistung und Kosten.

Kurz: Ein Datawarehouse dient – für welchen Zweck auch immer – der Datenbereitstellung. Und das per Virtualisierung!

III. Was können wir mit diesem Buch dazu beitragen?

Das Buch soll den Lesern einen Praxisleitfaden an die Hand geben, in dem einige wichtige rechtliche Aspekte näher beleuchtet werden – seien es Aspekte aus dem Datenschutz, der Informationssicherheit, dem Kartellrecht, dem IP-Recht, der Haftung und der Blockchaintechnologie. Diese müssen in einem automatisierten Data Warehouse technisch berücksichtigt und umgesetzt werden, damit Unternehmen Haftungsrisiken meiden und ihren „Datenschatz" heben können. Aufgrund der Leitsätze werden darüber hinaus zusammengefasste praxisorientierte Hilfestellungen und Ergebnisse gegeben. Graphische Illustrationen sollen komplexe Sachverhalte visuell veranschaulichen.

IV. Danksagung

beck-shop.de
DIE FACHBUCHHANDLUNG

Herzlichen Dank an alle Autoren, die keine Mühen und Einsatz gescheut haben, dieses Buch in anregender Zusammenarbeit zu realisieren. Für alle war es eine große Herausforderung die Vielseitigkeit der rechtlichen Fragestellungen an ein Data Warehouse strukturiert, komprimiert und übersichtlich darzustellen. Auch die mannigfaltigen Einsatzmöglichkeiten eines Data Warehouse wie auch die reichlich zu beachtenden unterschiedlichen Gesetze, spiegeln die Komplexität im Hinblick auf Planung und Betrieb eines Data Warehouse wider.

Herzlichen Dank auch an Karin Kampitsch von der Agentur Bransch und Partner, die verflochtene Aspekte dieses Themenkreises mit ihren Bildern professionell visualisiert, umgesetzt und uns auf dieser Reise begleitet hat.

Nun wünschen wir allen Lesern viel Vergnügen und neue Erkenntnisse mit diesem Buch.

Stuttgart, im Dezember 2023 Dr. iur. Maria Cristina Caldarola, LL.M., MBA

Inhaltsverzeichnis

Bearbeitungsverzeichnis V
Vorwort IX
Abkürzungsverzeichnis XXI
Abbildungsverzeichnis XXVII
Literaturverzeichnis XXIX
Weiterführende Materialien XLIII

A. Einführung 1

B. Das Data Warehouse 3
I. Der Datenbegriff 3
1. Einleitung 3
2. Technischer Datenbegriff 4
II. Entstehung von Daten 4
1. Datafication 4
2. Data Economy 5
III. Datenwertschöpfung & Datenverwaltung mit dem Data Warehouse 6
1. Datenbasierte Entscheidungen 6
2. Datenerschließung 7
3. Datenverfeinerung 8
4. Analytik-Reifegrad-Modell 9
5. Datenwürfel 11
6. Datenverwertung 12
7. Datengetriebene Organisationen 13
8. Datenarchitektur 14
9. Big Data 15
10. Datenmodelle 16
11. Spezialisierte Data Warehouse-Lösungen 17
12. Datenorganisation 17
13. Datenmanagement 18
IV. Nutzen eines Data Warehouse 19
1. Anwendungsbereiche von Big Data Analytics im Rahmen der ökonomischen Wertschöpfung 19
a) Scoring-Profile 20
b) Wartungsprognosen (Predictive Maintenance) 21
c) Bekämpfung von Finanzkriminalität 22
d) Kundenerlebnis 22
2. Unternehmensdatenkapital 23
3. Ausblick 24
V. Fazit und Würdigung 24

C. Inhaber/Betreiber eines Data Warehouse 25
I. Inhaber und Betreiber – Rollenbeschreibung und Unterschiede 25
1. Inhaber eines Data Warehouse 26
2. Eigentum an Daten als absolutes Recht 26
3. Urheberrecht an Datenbanken 27

beck-shop.de
DIE FACHBUCHHANDLUNG

4. Datenbankschutzrecht als Leistungsschutzrecht 28
5. Data Act – geänderte Vorschriften über den rechtlichen Schutz von Datenbanken 31
6. Relative Rechte an Datenbeständen 33
7. Recht der betroffenen Person an sie betreffenden personenbezogenen Daten 33
8. Rolle als Verantwortlicher im datenschutzrechtlichen Sinne 35
9. Datenbesitz kraft Skripturakt 36
10. Digitales Hausrecht 37
II. Rechte an Datenbankinhalten 39
1. Urheberrechtsfähige Datenbankinhalte 39
2. Wettbewerbsrecht 40
III. Betreiber von Datenbanken 41
1. Rechtliche Stellung des Betreibers in Abgrenzung zum Inhaber 42
2. Rechtliche Einordnung der Betreiberstellung 42
a) Auftragsverarbeiter im datenschutzrechtlichen Sinne 43
b) Beauftragter im Sinne der 662 ff. BGB 44
c) Dienstverpflichteter im Sinne der §§ 611 ff. BGB 45
d) Kommissionär im Sinne der 383 ff. HGB 46
3. Zwitterstellung: Der Datentreuhänder 47
a) Einfache Datentreuhand 48
b) Hinterlegungsstelle (Escrow Agent) für Daten 51
IV. Sonderkonstellation Open Data 52
V. Personenmehrheit als Inhaber von Daten 53
1. Verein 54
2. Genossenschaft 55
3. Gesamthandsgemeinschaften und Bruchteilsgemeinschaft 56
4. Gemeinsame Verantwortlichkeit im datenschutzrechtlichen Sinne . . 58
VI. Gesamtergebnis und Empfehlung 59

D. Datenschutz im Data Warehouse 61
I. Warum spielt der Datenschutz eine Rolle im Data Warehouse? 61
II. Worum geht es im Datenschutzrecht? 61
III. Welche Daten sind in einem Data Warehouse zu finden? 62
IV. Welche datenschutzrechtliche Rolle hat der Data Warehouse Betreiber? . 63
V. Mit welchen Daten-Eigenschaften muss das Data Warehouse umgehen? 63
VI. Welche datenschutzrechtlichen Variablen müssen gemanaget werden? . . 64
1. Bezugsquelle bzw. Rechtsinhaber 64
2. Datenarten 65
3. Verarbeitungszweck 65
4. Die Ermächtigungsgrundlage 66
5. Anwendbares Recht 66
VII. Welche Rechte bestehen an Daten? 67
VIII. Welche datenschutzrechtlichen Pflichten hat der Data Warehouse Betreiber? 68
1. Technische und organisatorische Maßnahmen 68
2. Transparenz 69
3. Löschung – Datensparsamkeit 70
4. Einwilligungs- und Widerrufsmanagement 72
5. Dokumentation – Führung eines Verfahrensverzeichnisses 72
6. Eingangs- und Ausgangskontrolle 73
7. Risikomanagement (insbes. Datenschutz-Folgenabschätzung) 74
8. Portabilität 75

beck-shop.de
DIE FACHBUCHHANDLUNG

IX. Was passiert bei Missachtung der datenschutzrechtlichen Pflichten? 75
X. Welche Möglichkeiten existieren zur Vermeidung datenschutzrechtlicher Pflichten? 76
XI. Unter welchem Regime können Daten im Data Warehouse genutzt werden? 77
XII. Was passiert bei Kombination und Vermengung von Daten im Data Warehouse? 78
1. Verarbeitungszweck und Ermächtigungsgrundlage 78
2. Zweckänderung 79
3. Kombination von personenbezogenen und nicht-personenbezogenen Daten 81
4. Kombination von rechtmäßig erhobenen und verarbeiteten Daten mit unrechtmäßig erhobenen und verarbeiteten Daten 81
XIII. Können Daten/Datenderivate aus dem Data Warehouse Bezugsquelle für Dritte sein? 81
1. Weitergabe 81
2. Zugangs- und Zugriffsrechte Dritter 82
XIV. Welche technischen Umsetzungen bieten sich für eine Data Warehouse Architektur an? 83
1. Data Warehouse Architektur 83
2. Datentagging 83
3. Blockchain Technologie 84
XV. Handlungsempfehlungen 84

E. Daten und Kartellrecht 87
I. Vorbemerkung 87
II. Daten im Kartellrecht 88
1. Kartellrechtliche Missbrauchsaufsicht: Datenbezogene Regelungen . 91
a) Wettbewerbsrelevante Daten 91
aa) Kartellrechtlicher Datenbegriff? 91
bb) Wettbewerbsrelevante Daten im Data Warehouse 92
b) Bewertung der Marktstellung von Unternehmen mit datenbasierten Geschäftsmodellen 94
aa) Feststellung einer Marktbeherrschung 94
(1) Grundsätze 94
(2) Zugang zu wettbewerbsrelevanten Daten 96
(3) Intermediationsmacht 98
bb) Überragende marktübergreifende Bedeutung für den Wettbewerb 99
cc) Relative/überlegene Marktmacht 101
c) Missbräuchliches Verhalten und Rechtfertigung in der Digitalwirtschaft 103
aa) Datenbezogener Missbrauch absoluter Marktmacht, § 19 Abs. 2 Nr. 4 GWB 104
(1) Zugangsverweigerung 104
(2) Rechtfertigung 106
(3) Konsequenzen für den Betreiber eines Data Warehouse . . 107
(4) Sonstige Missbrauchstatbestände 109
bb) Datenbezogener Missbrauch relativer/überlegener Marktmacht, § 20 Abs. 1a GWB 111
(1) Verbotenes Verhalten 111
(2) Rechtfertigung 111
(3) Konsequenzen für den Betreiber eines Data Warehouse . . 112

beck-shop.de
DIE FACHBUCHHANDLUNG

cc) Spezialfall: Datenbezogener Missbrauch bei überragender marktübergreifender Bedeutung für den Wettbewerb, § 19a Abs. 2 Satz 1 Nr. 4 GWB . . . 112
(1) Verbotenes Verhalten . . . 112
(2) Rechtfertigung . . . 114
d) Fazit . . . 115
2. Konsequenzen eines missbräuchlichen Verhaltens . . . 116
a) Verfügungen und einstweilige Maßnahmen des Bundeskartellamts, Vorteilsabschöpfung . . . 116
b) Bußgeldverfahren . . . 117
c) Rechtsschutz gegen Maßnahmen des Bundeskartellamts . . . 117
d) Zivilrechtliche Folgen . . . 118
III. Ausblick . . . 118

F. Open Data im Data Warehouse . . . 121
I. Definitionen . . . 122
1. Open Data . . . 122
2. Open Government Data . . . 123
3. Verhältnis zu Open Access, Open Source und Open Content . . . 124
4. Public Domain . . . 125
II. Entwicklung des Open Data Konzepts . . . 126
III. Gesetzliche Rahmenbedingungen . . . 127
1. Open Data Gesetze . . . 128
a) Richtlinie 2019/1024/EU über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (Open-Data- und PSI-RL) . . . 130
b) Verordnung (EU) 2018/1807 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten (Datenverkehrs-VO) . . . 131
c) Gesetz zur Förderung der elektronischen Verwaltung (EGovG) . . . 132
d) Verordnung zur Festlegung der Nutzungsbestimmungen für die Bereitstellung von Geodaten des Bundes (GeoNutzV) . . . 133
e) Gesetz für die Nutzung von Daten des öffentlichen Sektors (DNG) . . . 134
2. Schutzrechte des geistigen Eigentums . . . 135
IV. Open Data und das Datenbankherstellerrecht . . . 136
1. Voraussetzungen für ein Datenbankherstellerrecht . . . 136
2. Gesetzliche Veröffentlichungspflichten und Datenbankherstellerrechte . . . 138
3. Datenbankherstellerrecht im internationalen Kontext . . . 140
V. Open Data Lizenzierung . . . 141
1. Verhältnis zu Schutzrechten des geistigen Eigentums . . . 141
2. Open Data Lizenzierung bei personenbezogenen Daten? . . . 142
3. Lizenzkategorien . . . 143
4. Open Data Lizenzen und Public Domain Erklärungen . . . 144
a) Datenlizenz Deutschland – Namensnennung – Version 2.0 (dl-de/by-2-0) . . . 144
b) Datenlizenz Deutschland – Zero – Version 2.0 (dl-de/zero-2-0) . . . 145
c) Open Data Commons Attribution License v1.0 (ODC-By-1.0) . . . 145
d) Open Data Commons Open Database License v1.0 (ODbL-1.0) . . . 146
e) Creative Commons Attribution 4.0 International Public License, Version 4.0 (CC-BY-4.0) . . . 148
f) Creative Commons Attribution-ShareAlike 4.0 International Public License, Version 4.0 (CC-BY-SA-4.0) . . . 149

beck-shop.de
DIE FACHBUCHHANDLUNG

g) CC0 1.0 Universal Public Domain Dedication (CC0-1.0) 149
h) Open Data Commons Public Domain Dedication and License (PDDL) 150
i) Kompatibilität von Open Data Lizenzen 150
VI. Zusammenfassung 152

G. Informationssicherheit, insb. Verschlüsselung, Anonymisierung und Pseudonymisierung 155
I. Rechtliche Ausgangssituation 155
1. Datenschutz 156
a) DS-GVO 156
aa) Informationssicherheit als Grundprinzip der DS-GVO 156
bb) Sicherheit der Verarbeitung/TOMs 157
cc) Anonymisierung als Gegenstück zu personenbezogenen Daten und Pseudonymisierung 158
dd) Prinzip des risikobasierten Ansatzes 159
ee) Risikoanalyse 161
b) E-Privacy Richtlinie 162
c) Deutsche Datenschutzgesetze 162
aa) Bundesdatenschutzgesetz (BDSG) 163
bb) Telekommunikations- und Telemediendatenschutzgesetz (TTDSG) 166
cc) Telekommunikationsgesetz (TKG) 166
dd) Landesdatenschutzgesetze und bereichsspezifische Datenschutzregelungen 167
2. IT-Sicherheitsgesetze 168
a) Europäischer Rahmen 168
b) Nationale Gesetzgebung 170
aa) BSIG 171
bb) Einordnung von Data Warehouses nach dem BSIG 171
(1) Data Warehouse als Kritische Infrastruktur 172
(2) Data Warehouse als digitaler Dienst 173
(3) Ergebnis und NIS-2-RL-Ausblick 173
cc) IT-Sicherheitspflichten nach dem BSIG 173
(1) Data Warehouse als Kritische Infrastruktur 174
(2) Data Warehouse als digitaler Dienst 175
dd) TTDSG 176
ee) TKG 176
3. Sonstiges 177
a) Allgemeine gesetzliche Complianceverpflichtungen 177
b) Vertragliche Verantwortlichkeit 178
4. Schlussfolgerungen: Wesentliche Verpflichtungen in Bezug auf die Informationssicherheit 178
II. Technische Umsetzung der Informationssicherheitsmaßnahmen 179
1. Authentifizierung und Zutritts- und Zugangskontrolle 179
a) Passwörter 180
b) Weitere Authentifizierungsmaßnahmen 180
2. Autorisierung und Zugriffs-, Nutzungs- und Weitergabekontrolle, Berechtigungsmanagement 181
3. Kryptografie und Verschlüsselung 182
a) Übersicht und Begrifflichkeiten 182
b) Anwendungen von Verschlüsselung 183
c) Arten von Kryptografie und Verschlüsselung 183

beck-shop.de
DIE FACHBUCHHANDLUNG

aa) Technischer Überblick über verschiedene Arten von Verschlüsselung . . . 183
bb) No-key – „Unverschlüsselte Verschlüsselung“ . . . 184
cc) Hash-Funktionen . . . 184
(1) Übersicht . . . 184
(2) Typen von Hash-Funktionen . . . 186
(2.1) SHA-1, SHA-2, SHA-3 . . . 186
(2.2) BLAKE . . . 187
dd) One Key – Symmetrische Verschlüsselung . . . 187
ee) Two Key – Asymmetrische Verschlüsselung . . . 188
ff) Andere Arten der Verschlüsselung . . . 189
d) Gängige Implementierungen von Verschlüsselungsmethoden . . . 189
aa) Symmetrisch . . . 189
bb) Asymmetrisch . . . 189
cc) Hybride Schemata und Kombinationen . . . 190
e) Die Stärke der Verschlüsselung und derzeit empfohlene Schlüssellängen . . . 191
4. Digitale Signatur . . . 192
a) Ziele und Methoden . . . 192
b) Signatur-Technologien (one-way) . . . 192
5. Sicherheits- und Abwehrmaßnahmen gegen Viren, Malware und ähnliche Attacken . . . 194
a) Arten von Malware und Attacken . . . 194
b) Sicherheits- und Abwehrmechanismen . . . 196
aa) Technische Maßnahmen . . . 196
(1) Einsatz von Firewalls . . . 196
(2) Minimierung und Absicherung von Netzübergängen (Schnittstellenkontrollen) . . . 197
(3) Abwehr von Schadprogrammen . . . 197
(4) Updates . . . 197
(5) Sichere Authentisierung (Zwei-Faktor-Authentifizierung) 198
bb) Organisatorische Maßnahmen . . . 198
(1) Zuweisung der Verantwortlichkeiten für Informationssicherheit . . . 198
(2) Erstellung eines Incident Response Plan . . . 198
(3) Durchführung nutzerorientierter Maßnahmen . . . 198
(4) Audits . . . 199
6. Sicherheit gegen höhere Gewalt und Verlust; Backups und Recovery 199
a) Arten von Backups . . . 199
b) Anforderungen an Backups und Recovery . . . 200
c) Planungs- und Testphase . . . 201
d) Die Sicherheit von Backups und Recovery . . . 201
aa) Verschlüsselung . . . 202
bb) Berechtigungskonzepte und Authentifizierung . . . 202
7. Depersonalisierung . . . 203
a) Grundsätzliche Voraussetzungen und Unterscheidung . . . 203
b) Methoden der Anonymisierung . . . 204
aa) Datenminimierung und -löschung . . . 204
bb) Datenmaskierung . . . 205
c) Methoden der Pseudonymisierung . . . 206
aa) Ansätze der Pseudonymisierung . . . 206
bb) Methoden zur Pseudonymisierung . . . 207

beck-shop.de
DIE FACHBUCHHANDLUNG

d) Re-Identifikation, Messung und Kontrolle von Anonymität und Pseudonymität . . . 208
III. Besondere Herausforderungen des Quantencomputings . . . 210
1. Überblick über das Problem der Quantencomputer . . . 210
2. Auswirkungen auf bestehende Technologien . . . 211
3. Auswirkungen der Quantencomputer auf Risikobasierten Ansatz und Stand der Technik . . . 212
a) DS-GVO . . . 214
b) NIS-Richtlinie . . . 215
4. Mögliche Anpassungen der vorhandenen Technologien . . . 216
a) No key: Hash-Funktionen . . . 216
b) One key: Symmetrische Verschlüsselung . . . 216
aa) Two-way symmetrische Verschlüsselung . . . 216
bb) One-way digitale Signaturen . . . 217
c) Two keys: Asymmetrische Verschlüsselung . . . 217
aa) Two-way Verschlüsselung . . . 217
bb) One-way Digitale Signaturen . . . 217
d) Neue quantensichere Technologien für Zwei-Schlüssel-Verschlüsselung und Signaturen . . . 218
aa) Two-keys Asymmetrische Verschlüsselung . . . 218
bb) Two-keys Digitale Signaturen . . . 218
5. Akteure und ihre Empfehlungen . . . 221
a) USA . . . 221
b) Europa . . . 222
c) Deutschland . . . 222
d) Übersicht . . . 222
e) Aktuelle Empfehlungen und Timeline . . . 223
IV. Dokumentation-, Melde- und Überprüfungspflichten . . . 224
1. Dokumentations- und Nachweispflichten . . . 225
a) DS-GVO . . . 225
b) BSIG . . . 225
c) Praktische Ausgestaltung . . . 226
2. Meldepflichten . . . 227
a) DS-GVO . . . 227
b) BSIG . . . 228
c) TKG . . . 229
d) Zusammenfassung . . . 229
3. Auditpflichten und Überprüfung der Wirksamkeit . . . 229
a) Auditpflichten . . . 230
b) Wirksamkeitsüberprüfung . . . 231

H. Nutzung einer Blockchain im Data Warehouse . . . 233
I. Einführung . . . 233
II. Die Blockchain-Definition . . . 235
1. Technologische Bestandteile . . . 235
a) Eine dezentralisierte Architektur . . . 236
b) Identitätsauthentifizierung . . . 238
c) Die drei grundlegende Erscheinungsformen von Blockchains . . . 239
aa) Öffentliche und erlaubnisfreie Blockchains . . . 239
bb) Private und genehmigte Blockchains . . . 241
cc) Konsortiale Blockchains . . . 242
2. Kontrolle und Governance der Blockchain . . . 242
3. Identität der Blockchain-Teilnehmer . . . 244

beck-shop.de
DIE FACHBUCHHANDLUNG

III. Drei wesentliche datenschutzrechtliche Probleme 245
1. Ist die DS-GVO innerhalb von Blockchains anwendbar? 245
a) Metadaten als personenbezogene Daten 246
b) Transaktionsdaten als personenbezogene Daten 248
2. Wer unterliegt als Verantwortlicher und Auftragsverarbeiter rechtlichen Verpflichtungen? 248
a) Private/erlaubnispflichtige Blockchain-Plattformen: Grundbuchamt 250
b) Konsortiale Blockchain-Plattform: Austausch von Kundendaten zwischen Banken 251
c) Öffentliche/erlaubnisfreie Blockchain Plattform: Kryptowährung 253
d) Schlussfolgerungen zu Verantwortlichen und Auftragsverarbeitern 254
3. Können Blockchain-Verantwortliche das Datenschutzrecht einhalten? 255
a) Rechtmäßige Gründe für die Verarbeitung 255
b) Pflichten des Verantwortlichen und des Auftragsverarbeiters . . . 256
c) Betroffenenrechte 257
IV. Fazit 258

I. Haftung und Versicherung 261
I. Einleitung: Haftungsrisiken – Was kann passieren? 261
1. Vorbemerkungen 261
2. Beispielshafte Szenarien 262
a) Äußere Einflüsse 262
b) Compliance Verstöße 264
II. Haftung für Rechtsverletzungen 265
1. Vorbemerkung 265
2. Datenschutzverletzungen 266
a) Haftung gegenüber Dritten 266
aa) Haftung des Unternehmens gegenüber Betroffenen 266
bb) Haftung des Unternehmens gegenüber sonstigen Dritten . . . 270
(1) Vertragliche Haftung 270
(2) Deliktische Haftung 272
cc) Haftung des Managements 272
(1) Innenhaftung 272
(2) Außenhaftung 273
b) Ordnungswidrigkeiten-, Straf- und sonstiges Sanktionsrecht . . . 274
aa) Haftung des Unternehmens 274
bb) Haftung des Managements 276
c) Anwendung auf die einschlägigen Szenarien 277
aa) Szenario 1: Revil-Fall 278
bb) Szenario 2: Datenschutzverletzungen 278
3. Sonstige Verletzung von Rechten Dritter 278
a) Urheber- und Leistungsschutzrecht 278
aa) Zivilrechtliche Haftung 278
(1) Haftung des Unternehmens 278
(2) Haftung des Managements 280
bb) Ordnungswidrigkeiten-, Straf- und sonstiges Sanktionsrecht . 281
b) Betriebs- und Geschäftsgeheimnisse 281
aa) Zivilrechtliche Haftung 281
(1) Haftung des Unternehmens 281
(2) Haftung des Managements 282

beck-shop.de
DIE FACHBUCHHANDLUNG

bb) Öffentlich-rechtliche Sanktionen – Ordnungswidrigkeiten, Straf- und sonstiges Sanktionsrecht 283
c) Anwendung auf die einschlägigen Szenarien 283
4. Sonstige regulatorische Vorgaben 284
a) Vorbemerkung 284
b) Gesetz über das Bundesamt in der Informationstechnik (BSIG) . 284
aa) Rechtsrahmen 284
bb) Öffentlich-rechtliche Sanktionen 285
cc) Zivilrechtliche Haftung 285
c) Weitere sektorspezifische Vorgaben 286
aa) Telekommunikation und Telemedien 286
bb) Banken und Versicherungen 287
cc) Gesundheit 288
d) Kartellrecht 288
e) Außenwirtschaftsrecht 290
f) EU Datenregulierung 291
g) Anwendung auf die einschlägigen Szenarien 293
III. Risikomanagement im Unternehmen 294
1. Vorbemerkung 294
2. Compliance Management System 294
a) Rechtliche Pflichten 294
b) Elemente 295
c) Implementierung 295
3. Praxisrelevante Problemfelder 296
a) Aufbau eines integrierten CMS und Data Governance 296
b) Haftungsvermeidende Strategien 298
c) Rechtsfeldbeobachtung 299
d) Versicherungsschutz 299
IV. Versicherung 300
1. Vorbemerkung 300
2. Cyberversicherung 302
a) Typischer Leistungsumfang 302
b) Kontextualisierung mit Szenarienbezug 303
3. Vermögensschadenhaftpflichtversicherung 305
a) Typischer Leistungsumfang 305
b) Kontextualisierung mit Szenarienbezug 305
4. Rechtsschutzversicherung 306
a) Typischer Leistungsumfang 306
b) Kontextualisierung mit Szenarienbezug 307
5. D&O Versicherung 307
a) Typischer Leistungsumfang 307
b) Kontextualisierung mit Szenarienbezug 308
V. Fazit 309

Stichwortverzeichnis 311

beck-shop.de
DIE FACHBUCHHANDLUNG