

ANDREAS SATTLER

Informationelle Privatautonomie

Jus Privatum

264

Mohr Siebeck

JUS PRIVATUM
Beiträge zum Privatrecht

Band 264



Andreas Sattler

Informationelle Privatautonomie

Synchronisierung von
Datenschutz- und Vertragsrecht

Mohr Siebeck

Andreas Sattler, geboren 1982; Studium der Rechts- und Wirtschaftswissenschaften in Bayreuth und Nottingham (LL.M.); Promotionsstipendium der DFG und Mitgliedschaft im DFG-Graduiertenkolleg „Geistiges Eigentum und Gemeinfreiheit“, Universität Bayreuth; Dissertation (Emanzipation und Expansion des Markenrechts, Mohr Siebeck, 2015); Rechtsanwalt im Bereich IT-Recht bei CMS Hasche Sigle, Stuttgart; Akademischer Rat a.Z. am Lehrstuhl für Bürgerliches Recht, Recht des Geistigen Eigentums und Wettbewerbsrecht an der Ludwig-Maximilians-Universität München; Habilitation; Lehrbefähigung für die Fächer Bürgerliches Recht, Immaterialgüterrecht, deutsches und europäisches Wirtschaftsrecht und Datenrecht; Gründung und Co-Leitung des Center for Intellectual Property Law, Information and Technology (CIPLITEC); seit April 2022: Vertretung des Lehrstuhls für Zivil- und Wirtschaftsrecht, Medien- und Informationsrecht an der Albert-Ludwigs-Universität Freiburg.

Gedruckt und als Open Access Dokument zugänglich gemacht mit der freundlichen Unterstützung des *LMU Open Access Fonds*, des *LMU Post Doc Fonds*, der *Johanna und Fritz Buch Gedächtnisstiftung e.V.* und der Studienstiftung *ius vivum e.V.*

ISBN 978-3-16-161905-2 / eISBN 978-3-16-161906-9
DOI 10.1628/978-3-16-161906-9

ISSN 0940-9610 / eISSN 2568-8472 (Jus Privatum)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über <http://dnb.dnb.de> abrufbar.

© 2022 Mohr Siebeck Tübingen. www.mohrsiebeck.com

Dieses Werk ist lizenziert unter der Lizenz „Creative Commons Namensnennung – Keine Bearbeitungen 4.0 International“ (CC BY-ND 4.0). Eine vollständige Version des Lizenztextes findet sich unter: <https://creativecommons.org/licenses/by-nd/4.0/deed.de>

Das Buch wurde von Gulde Druck aus der Garamond gesetzt, in Tübingen auf alterungsbeständiges Werkdruckpapier gedruckt und von der Buchbinderei Spinner in Ottersweier gebunden.

Printed in Germany.

Vorwort

Daten werden seit einigen Jahren als „neues Gold“ oder „Öl des 21. Jahrhunderts“ bezeichnet. Diese Vergleiche hinken. Im Gegensatz zu Gold und Öl sind Daten immaterielle Güter. Infolgedessen ist ihre Nutzung weder ausschließlich noch rival. Ohne rechtliche Zuweisung beruht die Möglichkeit zur Datennutzung lediglich auf einem faktischen Zugang, allgemein zugängliche Daten kann jedermann nutzen (keine Ausschließbarkeit). Die Nutzung durch eine Person hindert nicht die zeitgleiche Nutzung dieser Daten durch weitere Personen (keine Rivalität). Kurzum: Aufgrund ihrer immateriellen Eigenschaften können Daten eine sehr vielseitig nutzbare Ressource sein.

Dies erklärt, warum Daten zunehmend in den Fokus der Gesetzgeber im europäischen Mehrebenensystem geraten und warum die Gesetzgeber nach Wegen suchen, um die Nutzung von Daten zu fördern; stets in der Erwartung, dass dadurch die wirtschaftliche Effizienz, die technische Innovation und damit letztlich der volkswirtschaftliche Wohlstand gesteigert werden. Die Vorschläge für Ansprüche auf Datenzugang und Datenüberlassung (Data Act), aber auch das Konzept einer Datentreuhand (Data Governance Act) sind aktuelle Beispiele dafür, dass der unionale Gesetzgeber nach Mechanismen sucht, um den „Datenschatz“ zu heben. Dabei bezieht der Gesetzgeber zunehmend auch personenbezogene Daten ein. Er folgt damit der wirtschaftlichen Realität. Zahlreiche Dienstleistungen der Betreiber von mehrseitigen Plattformen, insbesondere von Suchmaschinen oder Kommunikationsnetzwerken, werden derzeit maßgeblich durch personalisierte Werbung finanziert. Diese basiert auf dem Einsatz von Tracking-Technologien und der Erstellung von Interessenprofilen anhand des Online-Verhaltens der Nutzer/innen. Weil diese omnipräsenten Geschäftsmodelle bei der Verabschiedung der DS-GVO jedoch weitgehend ausgeblendet wurden und zudem auch nicht berücksichtigt wurde, dass zahlreiche prominente Persönlichkeiten die vermögenswerten Bestandteile ihrer Persönlichkeitsrechte kommerziell verwerten, befindet sich die DS-GVO auf einem Kollisionskurs mit dem Schuldrecht und der ökonomischen Realität. Der Konflikt zwischen der staatlichen Pflicht zum Schutz der informationellen Selbstbestimmung einerseits und der gleichzeitigen Achtung der Privatautonomie der Datensubjekte und der datenverarbeitenden Unternehmen andererseits ist mittlerweile offenkundig. Dennoch besteht derzeit kein überzeugender rechtlicher Rahmen, der die grundrechtliche Pflicht zum Schutz der Datensubjekte und die

wirtschaftliche Realität zum Ausgleich bringt. Diese schwierige Aufgabe wird stattdessen an die Rechtsanwender und damit insbesondere an den EuGH überantwortet.

Die vorliegende Arbeit macht einen Vorschlag, wie dieses Spannungsverhältnis aus dem Schutz von Datensubjekten und der Anerkennung von personenbezogenen Daten als Objekt vertraglicher Austauschbeziehungen aufgelöst werden kann. Dabei bewahrt der Vorschlag den tradierten Rahmen des Rechts auf informationelle Selbstbestimmung, erweitert aber den Handlungsspielraum für Datensubjekte und solche datenverarbeitende Unternehmen, die keine dominanten Gatekeeper sind. Infolgedessen ermöglicht das nachfolgend vorgeschlagene Modell einer abgestützten informationellen Privatautonomie die Synchronisierung von Datenschutz- und Vertragsrecht.

Die Arbeit lag der Juristischen Fakultät der Ludwig-Maximilians-Universität München im Wintersemester 2021/22 als Habilitationsschrift vor. Sie hat entscheidend von einer Reihe von Personen profitiert. Mein Dank gilt in erster Hinsicht meinem akademischen Lehrer, Herrn Professor Ansgar Ohly, der sich früh für dieses Thema begeistern konnte und mir für diese Untersuchung ideale Bedingungen und größtmögliche Freiheiten am Lehrstuhl gewährt hat. Herrn Professor Hans Christoph Grigoleit danke ich herzlich für die sehr zügige Erstellung des Zweitgutachtens und wertvolle inhaltliche Hinweise und Anregungen. Herrn Professor Herbert Zech und Herrn Professor Matthias Leistner danke ich für zahlreiche anregende Gespräche und Diskussionen zum Thema. Herrn Professor Franz Hofmann und Herrn Professor Martin Stierle danke ich für die gute und freundschaftliche Zusammenarbeit an der LMU. Der Druck und die Zugänglichmachung als Open-Access-Publikation wurden großzügig durch den LMU Open Access Fonds, den LMU PostDoc Fonds, die Johanna und Fritz Buch Gedächtnis-Stiftung und die Studienstiftung *ius vivum* gefördert.

Besonders herzlich danke ich meiner Familie. Meine Frau und mein Sohn mussten mit mir durch die düsteren Täler schreiten, die eine Habilitationsschrift regelmäßig mit sich bringt. Ihnen ist diese Arbeit gewidmet.

Stuttgart, im Mai 2022

Andreas Sattler

Inhaltsübersicht

Vorwort	V
Inhaltsverzeichnis	IX
Einführung	1
1. Kapitel: Grundrechtliche Gewährleistung von informationeller Privatautonomie	15
A. Dominanz der abwehrrechtlichen Dimension der Grundrechte	17
B. Asymmetrische Grundrechtssensibilität der DS-GVO	32
C. Gefährdung der informationellen Privatautonomie	57
D. Fazit: Privatrechtssensible Auslegung der DS-GVO	66
2. Kapitel: Subsidiarität der Interessenabwägung	73
A. Die Interessenabwägung als Generalklausel	75
B. Erleichterung der Datenverarbeitung durch eine Interessenabwägung	96
C. Herausforderungen einer Datenverarbeitung auf Grundlage der Interessenabwägung	99
D. Fazit: Funktion als Schrittmacher	139
3. Kapitel: Entlastungsfunktion der vertragsakzessorischen Datenverarbeitung	143
A. Komplexes Verhältnis zum nationalen Schuldrecht	145
B. Erleichterungen durch eine vertragsakzessorische Datenverarbeitung	148
C. Herausforderungen der vertragsakzessorischen Datenverarbeitung	152
D. Fazit: Entlastungsfunktion von Art. 6 Abs. 1 lit. b DS-GVO	202

4. Kapitel: Die Einwilligung als Nukleus des europäischen Datenschuldrechts	205
A. Vorrang der Einwilligung	206
B. Die Einwilligung zwischen Unter- und Übermaßverbot	230
C. Stufenleiter der Einwilligung	247
D. Fazit	273
5. Kapitel: Stufenmodell der Erlaubnistatbestände	277
A. Erste Stufe: Enge Auslegung der Interessenabwägung	278
B. Zweite Stufe: Enge Auslegung der Vertragsakzessorietät	287
C. Dritte Stufe: Flexibilisierung des Einwilligungstatbestands	297
D. Übersicht zum Stufenmodell	356
6. Kapitel: Erforderliche Abstützung der informationellen Privatautonomie	359
A. Standardisierte Kennzeichnung und Privacy Score	361
B. Kontroll-Cockpit für datenschutzrechtliche Erklärungen	381
Zusammenfassung	413
Literaturverzeichnis	425
Stichwortverzeichnis	461

Inhaltsverzeichnis

Vorwort	V
Inhaltsübersicht	VII
Einführung	1
I. Gegenstand und Zielsetzung	1
II. Forschungsstand	8
III. Gang der Untersuchung	11
1. Kapitel: Grundrechtliche Gewährleistung von informationeller Privatautonomie	15
<i>A. Dominanz der abwehrrechtlichen Dimension der Grundrechte</i>	<i>17</i>
I. Das RaiS als Grundlage des deutschen Datenschutzrechts	19
1. Industrialisierung und technischer Fortschritt	20
2. Prägender Einfluss der (Rechts-)Soziologie	21
3. Prägung durch Erfahrungen der nationalsozialistischen Diktatur	23
4. Extensive Auslegung der verfassungsgerichtlichen Urteile	24
II. Folgenlose Kritik am einheitlichen Schutzansatz	26
1. Kritik am rechtssoziologisch determinierten Zeitgeist	27
2. Kritik an der überschießenden Umsetzung des RaiS	28
3. Fazit: Fehlende privatrechtliche Unterfütterung des Datenschutzes	30
<i>B. Asymmetrische Grundrechtssensibilität der DS-GVO</i>	<i>32</i>
I. Wirkung europäischer Grundrechte im Privatrechtsverhältnis	34
II. Schutz- und Gewährleistung durch Art. 7 und Art. 8 GRCh	36
1. Keine Abgrenzung der Schutzbereiche durch den EuGH	37
2. Keine (klare) Schutzbereichsabgrenzung in der Literatur	39
3. Geringe Berücksichtigung der aktiven Entfaltungsfreiheit	41
a) Achtung des Privat- und Familienlebens, Art. 7 GRCh	41
b) Schutz personenbezogener Daten, Art. 8 GRCh (Art. 16 AEUV)	43
aa) Schutzbereich des Art. 8 GRCh	43
bb) Primärrechtlicher Vorrang der Einwilligung	46
III. Schutz der unternehmerischen Freiheit, Art. 16 GRCh	48

IV. Schutz der allgemeinen Handlungsfreiheit von Datensubjekten	50
V. Informationelle Privatautonomie und gerichtliche Kooperation	53
<i>C. Gefährdung der informationellen Privatautonomie</i>	<i>57</i>
I. Begriffliche Bezeichnung als Zuspitzung	58
II. Konstitutionalisierung des sekundärrechtlichen Datenschutzes	58
1. Verarbeitungsverbot als Einhaltung des Untermaßverbots	59
2. Verstoß gegen das Übermaßverbot (Verhältnismäßigkeit)	60
3. Anerkennung der Kommerzialisierung (Daten als Gegenleistung)	64
<i>D. Fazit: Privatrechtssensible Auslegung der DS-GVO</i>	<i>66</i>
2. Kapitel: Subsidiarität der Interessenabwägung	73
<i>A. Die Interessenabwägung als Generalklausel</i>	<i>75</i>
I. Berechtigte Interessen des Verantwortlichen oder Dritter	76
1. Begrenzung des Drittinteresses zugunsten einer Datenverarbeitung	77
2. Irrelevanz von Drittinteressen zulasten einer Datenverarbeitung	79
II. Erforderlichkeit der Datenverarbeitung zur Interessenwahrung	80
III. Kein Überwiegen der Interessen des Datensubjekts	82
1. Dichotomie der Interessen	82
2. Formulierung zugunsten der Rechtmäßigkeit	83
3. Fehlen von Abwägungskriterien	84
a) Persönliche Eigenschaften von Datensubjekten	85
b) Erwartungshorizont der Datensubjekte	86
c) Öffentlich zugängliche personenbezogene Daten	87
IV. Option zur Herstellung der Entscheidungszuständigkeit	89
1. Einordnung des Widerspruchsrechts	90
a) Widerspruchsbegründung	91
b) Rechtsfolge: Qualifizierte Interessenabwägung	92
2. Kollision mit der Widerruflichkeit der Einwilligung	93
<i>B. Erleichterung der Datenverarbeitung durch eine Interessenabwägung</i>	<i>96</i>
I. Erleichterung: Flexible Reaktion auf die ubiquitäre Datenverarbeitung	97
II. Erleichterung: Reagibilität auf die Multi-Relationalität	98
<i>C. Herausforderungen einer Datenverarbeitung auf Grundlage der Interessenabwägung</i>	<i>99</i>
I. Herausforderung: Paradoxon aus Unsicherheit und geringer Flexibilität	99
1. Fehlende Konkretisierung der Interessenabwägung	100
a) Art. 6 Abs. 1 lit. f DS-GVO als missglückte Generalklausel	101
b) Nachteile einer Typisierung durch Richterrecht	103
c) Interimistische Maßnahmen zur Konkretisierung	105

2. Restriktive Anwendung für personalisierte Direktwerbung	107
a) Technische Grundlagen automatisierter personalisierter Werbung	108
b) Restriktive Auslegung von Art. 6 Abs. 1 lit. f für Direktwerbung	111
aa) Ausgangspunkt: Personalisierte Werbung als anerkanntes Interesse	112
bb) Korrektur: Keine Direktwerbung durch Werbenetzwerke	115
3. Erweiterung des Anwendungsbereichs der Interessenabwägung	118
a) Verarbeitung besonders sensibler personenbezogener Daten . .	119
b) Verarbeitung von besonders sensiblen Daten im Kontext des IoT	123
c) Besonders sensible Daten als Trainingsdaten für ML	127
aa) Maschinelles Lernen: Trainieren statt Programmieren . .	128
bb) Trainieren von ML auf Grundlage einer Interessenabwägung	130
II. Herausforderung: Gefahr eines Unterlaufens der Einwilligung . . .	134
III. Herausforderung: Geringere faktische Kontrolldichte	136
<i>D. Fazit: Funktion als Schrittmacher</i>	139
3. Kapitel: Entlastungsfunktion der vertragsakzessorischen Datenverarbeitung	143
<i>A. Komplexes Verhältnis zum nationalen Schuldrecht</i>	145
<i>B. Erleichterungen durch eine vertragsakzessorische Datenverarbeitung</i>	148
I. Nationales Schuldrecht als Entdeckungsverfahren	148
II. Nationales Vertragsrecht als Differenzierungsfeld	150
<i>C. Herausforderungen der vertragsakzessorischen Datenverarbeitung . .</i>	152
I. Herausforderung: Überfordernde Angemessenheitskontrolle	153
1. Eingeschränkte Kontrolle des vertraglichen Synallagmas	155
a) Gründe für die Reduktion der gerichtlichen Kontrolldichte . .	156
b) Marktversagen als Grenze der reduzierten Kontrolldichte . . .	158
2. Personenbezogene Daten und Marktversagen	161
a) Mangelnde Aufmerksamkeit für den Hauptgegenstand	161
b) Personenbezogene Daten als Leistung – ein Zitronenmarkt . .	164
c) Geringe Kompensation durch eine aufmerksame Minderheit . .	166
d) Keine abschließende Regelung durch die Klausel-RL	168
e) Fehlender Maßstab für eine gerichtliche Angemessenheitskontrolle	170
3. Verdrängung der Klausel-RL durch die DS-GVO	174
a) Verhältnis von Klausel-RL und DS-GVO	174
b) Höhere Flexibilität der DS-GVO gegenüber der Klausel-RL . .	177

II. Herausforderung: Gefährdung des einheitlichen Datenschutzrechts	180
1. Geringe Regelungsdichte des Art. 6 Abs. 1 lit. b DS-GVO	180
2. Gefahr einer Umgehung der Anforderungen an die Einwilligung	182
3. Keine Überwindung der Defizite der Einwilligung	184
4. Komplexität und Fehleranfälligkeit der Rechtsfindung	185
5. Art. 6 Abs. 1 lit. b als Gefährdung der Regelungsziele der DS-GVO	187
6. Notwendigkeit umfassender Angleichung des Datenschuldrechts	191
III. Herausforderung: Keine Synchronisierung von DS-GVO	
und DID-RL	193
1. Keine Synchronisierung durch den europäischen Gesetzgeber . .	193
2. Mehrdeutige Stellungnahme des EDSA	196
3. Art. 6 Abs. 1 lit. b als potenzieller Fluchtweg aus der DID-RL . .	198
<i>D. Fazit: Entlastungsfunktion von Art. 6 Abs. 1 lit. b DS-GVO</i>	<i>202</i>
4. Kapitel: Die Einwilligung als Nukleus	
des europäischen Datenschuldrechts	205
<i>A. Vorrang der Einwilligung</i>	<i>206</i>
I. Gründe für einen Vorrang der Einwilligung	206
1. Datenschutz als Individualschutz	206
2. Systematik der DS-GVO	208
3. Einheitlichkeit der Rechtsanwendung	210
4. Unionsautonomie	212
II. Voraussetzungen der Einwilligung	214
1. Einwilligungsfähigkeit als Spezifikation der Freiwilligkeit	214
2. Bestimmtheit und Zweckbindung	216
3. Informiertheit	219
4. Freiwilligkeit der Einwilligungserteilung	221
5. Widerruflichkeit der Einwilligung	224
<i>B. Die Einwilligung zwischen Unter- und Übermaßverbot</i>	<i>230</i>
I. Grenzen des Übermaßverbots für Art. 7 Abs. 4 DS-GVO	231
1. Strenges Kopplungsverbot als Marktzutrittsbarriere	235
2. Kommerzialisierung durch Datensubjekte als Unternehmer	236
II. Grenzen des Übermaßverbots für die sog. freie Widerruflichkeit . .	237
1. Die freie Widerruflichkeit als Marktzutrittsbarriere	239
2. Kommerzialisierung durch Datensubjekte als Unternehmer	241
III. Fazit	245
<i>C. Stufenleiter der Einwilligung</i>	<i>247</i>
I. Die Grenzen der schlichten, einseitigen Einwilligung	247

II.	Die Einwilligung in der Stufenleiter der Gestattungen	249
1.	Schlichte Einwilligung und schuldrechtliche Gestattung	250
2.	Die schuldrechtliche Gestattung als Stabilisierung von Beziehungen	257
III.	Das Verhältnis zwischen Einwilligung und Vertrag	261
1.	Die Argumente für eine Trennung der Einwilligung vom Vertrag	261
a)	Trennung zwischen Einwilligung und Vertrag in der DS-GVO	262
b)	Trennung zwischen Einwilligung und Vertrag in der DID-RL	263
2.	Die Einwilligung als Bestandteil vertraglicher Vereinbarungen	268
a)	Der deutsche Streit über die Rechtsnatur der Einwilligung	268
b)	Die Einwilligung als Instrument der Synchronisierung	269
c)	Konsequenzen der Ausdifferenzierung des Einwilligungsbegriffs	271
<i>D.</i>	<i>Fazit</i>	273
5.	Kapitel: Stufenmodell der Erlaubnistatbestände	277
<i>A.</i>	<i>Erste Stufe: Enge Auslegung der Interessenabwägung</i>	278
I.	Art. 6 Abs. 1 lit. f DS-GVO als Schrittmacher	279
II.	Wesentliche Herausforderungen für die Interessenabwägung	281
1.	Keine personalisierte Werbung durch Werbenetzwerke	282
2.	Begrenzung der Informationspflicht aus Art. 21 Abs. 4 DS-GVO	284
3.	Sensible personenbezogene Daten und Interessenabwägung	286
<i>B.</i>	<i>Zweite Stufe: Enge Auslegung der Vertragsakzessorietät</i>	287
I.	Grundsatz: Beschränkung auf unterstützende Verarbeitungen	288
II.	Erste Herausforderung: Personalisierung digitaler Produkte	290
1.	Kern der Abgrenzungsschwierigkeit	291
2.	Keine Lösungsvorschläge durch den Gesetzgeber	292
III.	Zweite Herausforderung: Einbeziehung von Dienstleistern	295
<i>C.</i>	<i>Dritte Stufe: Flexibilisierung des Einwilligungstatbestands</i>	297
I.	Gründe für eine Flexibilisierung	297
II.	Flexibilisierung der Freiwilligkeit der Einwilligung	298
1.	Kriterium: Marktmacht des Verantwortlichen	300
a)	Strenges anbieterbezogenes Kopplungsverbot	301
b)	Marktbezogenes Kopplungsverbot	302
c)	Art. 7 Abs. 4 als generalklauselartiges Berücksichtigungsgebot	303
aa)	Keine Angemessenheitskontrolle der Leistungsbeziehung	303
bb)	Freiwilligkeit als Ursache kompetenzieller Konflikte	306
cc)	Kartellrechtsakzessorische und asymmetrische Anwendung	311
2.	Kriterium: Eigenschaften des Datensubjekts	316
a)	Einwilligung durch Kinder	316

b) Unternehmerisch handelnde Datensubjekte	319
3. Kriterium: Situationsadäquates Verhalten des Verantwortlichen	321
4. Fazit	324
III. Flexibilisierung der Widerruflichkeit der Einwilligung	328
1. Teleologische Reduktion von Art. 7 Abs. 3 S. 1 DS-GVO	331
2. Kriterien für eine teleologische Reduktion	332
a) Marktmacht des Verantwortlichen	332
b) Unternehmerisch handelnde Datensubjekte	334
c) Als Verbraucher handelnde Datensubjekte	336
aa) Freie Widerruflichkeit als Anreiz für die sofortige Verwertung	337
bb) Zeitweise bindende Einwilligung und Datenaltruismus	340
3. Abstützungen einer Disposition über Art. 7 Abs. 3 S. 1 DS-GVO	341
a) Keine Disposition gegenüber marktmächtigen Verantwortlichen	342
b) Befristung der Unwiderruflichkeit im B2C-Verhältnis	343
c) Keine stillschweigende Verlängerung des Widerrufs Ausschlusses	345
d) Jederzeitiger Widerruf aus wichtigem Grund	347
aa) Widerrufsgründe aus der Sphäre des Verantwortlichen	348
bb) Widerrufsgründe aus der Sphäre des Datensubjekts	348
4. Fazit: Abgestützte Abdingbarkeit der sog. freien Widerruflichkeit	351
<i>D. Übersicht zum Stufenmodell</i>	<i>356</i>
6. Kapitel: Erforderliche Abstützungen der informationellen Privatautonomie	359
<i>A. Standardisierte Kennzeichnung und Privacy Score</i>	<i>361</i>
I. Fehlende Voraussetzungen für das Informationsmodell	361
II. Unionweit einheitliche Kennzeichnung	363
1. Rechtsgrundlage für eine unionsweite Standardisierung	363
2. Reichweite der Rechtsgrundlage für eine Standardisierung	365
3. Notwendigkeit einer mehrstufigen Darstellung von Information	366
a) Tatsächliche Verständlichkeit und verfügbare Vollständigkeit	367
b) Stufenweise Verbindlichkeit der Kennzeichnungskombination	369
c) Erste Informationsstufe: Kennzeichen-Kombination	370
4. Die Verarbeitungsgrundlage als zentrales Kriterium	373
III. Klassifikation als Anwendungsbereich für ML	377
IV. Fazit	379
<i>B. Kontroll-Cockpit für datenschutzrechtliche Erklärungen</i>	<i>381</i>
I. Kontroll-Cockpit als Ausgangspunkt für PIMS	383
II. Gesetzliche Anknüpfungspunkte in der DS-GVO	385

1. Einwilligung und Einwilligungswiderruf	386
a) Einwilligungserteilung	386
aa) Informiertheit der Einwilligung	386
bb) Differenziertheit der Einwilligung	389
cc) Ausdrücklichkeit der Einwilligung	391
b) Einwilligungswiderruf	393
aa) Einfachheit des Einwilligungswiderrufs	393
bb) Differenziertheit des Einwilligungswiderrufs	395
cc) Informationspflichten nach Einwilligungswiderruf	397
2. Widerspruch gegen die Datenverarbeitung, Art. 21 DS-GVO	398
a) Widerspruchserklärung	399
b) Begründung des Widerspruchs	403
c) Informationspflichten	405
d) Fazit	405
3. Datenschutz durch Technikgestaltung, Art. 25 Abs. 1 DS-GVO	406
a) Pflicht und Anreiz für die Implementierung eines Kontroll-Cockpits	406
b) Mindestanforderungen an ein Kontroll-Cockpit	408
III. Übersicht der Mindestanforderungen an ein Kontroll-Cockpit	409
 Zusammenfassung	 413
I. Hauptthese	413
II. Hauptthese	414
III. Hauptthese	416
IV. Hauptthese	417
V. Hauptthese	418
VI. Hauptthese	421
 Literaturverzeichnis	 425
Stichwortverzeichnis	461

Einführung

I. Gegenstand und Zielsetzung

Der rechtliche Schutz vor einer Verarbeitung von personenbezogenen Daten (verkürzt: Datenschutzrecht) ist ein sehr konfliktreiches Rechtsgebiet. Untersucht man das Datenschutzrecht aus privatrechtlicher Perspektive, so sind zwei große Konflikte besonders augenfällig.

Erstens befinden sich das Datenschutzrecht und die besonders erfolgreichen Geschäftsmodelle mehrseitiger Plattformen auf einem Kollisionskurs. Die amerikanischen Unternehmen *Google (Alphabet)*, *Amazon*, *Facebook (Meta Platforms)*, *Apple* und *Microsoft* (zusammengefasst: GAFAM) und ihre chinesischen Wettbewerber *Baidu*, *Alibaba* und *Tencent* (zusammengefasst: BAT) stehen stellvertretend für Geschäftsmodelle, die in einem großen Ausmaß auf der Verarbeitung von personenbezogenen Daten ihrer Endnutzer (und Dritter) für ein Profiling beruhen. Dieses Profiling, das durch den Einsatz von Techniken der sog. Künstlichen Intelligenz stetig verbessert wird, liefert die Grundlage dafür, Werbekunden gegen Geld eine personalisierte oder zumindest stratifizierte Werbung gegenüber den Endnutzern anbieten zu können.

Die Kollision zwischen dem Datenschutzrecht und den Geschäftsmodellen mehrseitiger Plattformen ist nicht neu. Solange Plattformbetreiber bei Verstößen gegen das Datenschutzrecht jedoch kaum ökonomische Konsequenzen zu befürchten hatten, genügte es aus ihrer Sicht, den Schutz personenbezogener Daten am Horizont zu beobachten. Das Datenschutzrecht zwang die großen Plattformbetreiber zu keinen oder allenfalls sehr geringen Anpassungen ihrer Geschäftsmodelle.

Am 25.05.2018 hat sich dieses Bild verändert. Obwohl das Potenzial für *tatbestandliche* Konflikte seit der Anwendbarkeit der DS-GVO¹ kaum zugenommen hat – die DS-GVO behält wesentliche Regelungsinhalte der Datenschutz-RL von 1995² bei – ist für die datenschutzrechtlich Verantwortlichen das Risiko, also die Kombination aus der Entdeckungswahrscheinlichkeit von Rechtsver-

¹ Verordnung (EU) 2016/679 v. 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119, v. 04.05.2016, S. 1 ff.

² Richtlinie 95/46/EG v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281, v. 23.11.1995, S. 31 ff.

stößen und der Höhe des potenziellen Bußgelds, mit der DS-GVO grundlegend gestiegen. Indem das potenzielle Bußgeld proportional mit dem ökonomischen Erfolg des Verantwortlichen steigt, bewahrt das Datenschutzrecht seine Relevanz auch mit zunehmender Größe des datenschutzrechtlich Verantwortlichen.

Unabhängig davon, ob die Auslegung und Anwendung der DS-GVO in der Praxis ein ausreichendes Mindestmaß an Rechtssicherheit bietet,³ ob die Kriterien und Details für die Bestimmung eines angemessenen und abschreckenden Bußgelds im Einzelfall überzeugen und ob es sinnvoll und ökonomisch tragfähig ist, den gleichen Regelungsansatz auf andere Rechtsverstöße auszudehnen.⁴ Es bestehen keine Zweifel: Die potenzielle Höhe eines Bußgelds gemäß Art. 83 DS-GVO hat die alte Erkenntnis bestätigt, dass die Steuerungsfunktion des Rechts maßgeblich von effektiven Mechanismen zu dessen Durchsetzung abhängt.⁵ Um Kollisionen mit der DS-GVO und potentiell hohe Bußgeldbescheide zu vermeiden,⁶ sind die Plattformbetreiber zunehmend gezwungen, ihre Geschäftsmodelle, jedenfalls aber die rechtliche Beziehung zu ihren Endnutzern anzupassen.

³ Erst im Jahr 2021 erreichten den EuGH erste Auslegungsfragen von fundamentaler Bedeutung: *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V) = NZKart 2021, 306ff.; *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems [III]*.

⁴ Vgl. Art. 26 (Geldbußen) des Vorschlags der EU-Kommission für eine Verordnung über bestreitere und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte) vom 15.12.2020, COM(2020) 842 final (englisch: Digital Markets Act oder kurz: DMA-Vorschlag); sowie Art. 42 (Sanktionen) des Vorschlags der EU-Kommission für eine Verordnung über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG vom 15.12.2020, COM(2020) 825 final (englisch: Digital Service Act oder kurz: DSA-Vorschlag).

⁵ Die Frage, wer neben den Datensubjekten und im Auftrag der betroffenen Datensubjekte (Art. 80 Abs. 1 DS-GVO) zusätzlich gemäß Art. 80 Abs. 2 und Art. 84 Abs. 1 DS-GVO zur Durchsetzung von Ansprüchen aus UWG und UKlaG aktivlegitimiert sein sollte, hat der BGH dem EuGH vorgelegt: *BGH*, Beschl. v. 28.05.2020, I ZR 186/17 = GRUR 2020, 896 (Rn. 35ff.) – *App-Zentrum*; Für eine Begrenzung auf qualifizierte Verbände: *Köhler*, WRP 2018, 1269 (1272); *ders.*, WRP 2019, 1279 (1283); *Obly*, GRUR 2019, 686 (688f.); für eine durch die DS-GVO unbeeinflusste Aktivlegitimation von Mitbewerber nach dem UWG: *Uebele*, GRUR 2019, 694 (697f.).

⁶ Die luxemburgische Datenschutzbehörde (CNPD) verhängte gegen die europäische Tochter von *Amazon* mit Sitz in Luxemburg ein (nicht rechtskräftiges) Bußgeld in Höhe von 746 Mio. Euro (<https://www.heise.de/news/Datenschutz-Rekordstrafe-von-746-Millionen-Euro-fuer-Amazon-in-Luxemburg-6152051.html>, zuletzt abgerufen am 19.05.2022). Die französische Datenschutzbehörde (CNIL) verhängte 2019 – jeweils nur für Frankreich – eine Strafe von 50 Mio. Euro gegen *Google* (<https://www.heise.de/news/DSGVO-Verstoesse-Conseil-d-Etat-bestaetigt-50-Millionen-Strafe-gegen-Google-4790235.html>, zuletzt abgerufen am 19.05.2022) sowie im Dezember 2020 in Höhe von 100 Mio. Euro gegen *Google* und 35 Mio. Euro gegen *Amazon* (<https://www.heise.de/news/Frankreich-Datenschuetzer-verhaengen-Millionen-Bussgelder-gegen-Google-und-Amazon-4985956.html>, zuletzt abgerufen am 19.05.2022). Der Hamburgische Datenschutzbeauftragte hat wegen Verstößen gegen die DS-GVO im Beschäftigungsverhältnis für Deutschland ein Bußgeld von knapp 35,3 Mio. Euro gegen *Hennes & Mauritz* (H&M) verhängt (<https://www.heise.de/news/DSGVO-Deutsche-Rekord-busse-von-35-3-Millionen-Euro-gegen-H-M-4917437.html>, zuletzt abgerufen am 19.05.2022).

Besonders deutlich wird dies an dem Sachverhalt, der einem Vorlagebeschluss des *ÖOGH* zum *EuGH* zugrunde liegt.⁷ Darin geht es maßgeblich darum, ob *Facebook* (jetzt: *Meta Platforms*) die personenbezogenen Daten der Endnutzer – soweit es sich dabei nicht um besonders sensible personenbezogene Daten handelt – vertragsakzessorisch und somit auf Grundlage des Nutzungsvertrags i. V. m. Art. 6 Abs. 1 lit. b DS-GVO rechtmäßig verarbeiten kann, oder ob insoweit spezifische Einwilligungen der Endnutzer erforderlich sind. Dem Vorlagebeschluss des *ÖOGH* ging ein Urteil des *OLG Wien* voraus, in dem dieses das Profiling für personalisierte Werbung durch *Facebook* auf Grundlage eines in der österreichischen Rechtsordnung nicht ausdrücklich geregelten, also atypischen Schuldverhältnisses für rechtmäßig erachtet hatte. Nach Ansicht des *OLG Wien* ist diese Datenverarbeitung (auch) zur Finanzierung des Angebots von *Facebook* und damit zur Erfüllung dieses atypischen Nutzungsvertrags i. S. d. Art. 6 Abs. 1 lit. b DS-GVO erforderlich.⁸

Die Antwort des *EuGH* auf die nun erfolgte Vorlage des *ÖOGH* wird grundlegende Auswirkungen auf die Geschäftsmodelle der Betreiber von solchen mehrseitigen Plattformen haben, die Datensubjekten digitale Produkte bereitstellen und dieses Angebot finanzieren, indem sie mit Hilfe von personenbezogenen Daten Profile über ihre Endnutzer erstellen und diese im Verhältnis zu ihren Werbekunden für personalisierte Werbeansprache monetarisieren. Abhängig davon, welche datenschutzrechtliche Grundlage der *EuGH* für solche Austauschverhältnisse zwischen Datensubjekten und Verantwortlichen heranzieht, kommt es für die Rechtmäßigkeit dieser Geschäftsmodelle auf die unionsrechtlich vereinheitlichten Anforderung an die datenschutzrechtliche Einwilligung oder auf das lediglich teilweise harmonisierte nationale Vertragsrecht der Mitgliedstaaten an.⁹

Zweitens wird anhand des Vorlagebeschlusses des *ÖOGH* auch deutlich, dass sich das europäische Datenschutzrecht und das nationale Schuldrecht der Mitgliedstaaten auf einem Kollisionskurs befinden. Die europäische DS-GVO ist weder mit dem nationalen Schuldrecht noch den privatrechtlichen Grundprinzipien synchronisiert.

Sprachlich lässt sich diese Dominanz der DS-GVO daran festmachen, dass die schuldrechtlich zutreffende Bezeichnung von personenbezogenen Daten als „Gegenleistung“ einem postmodernen Sakrileg gleichgestellt wird.¹⁰ In voraus-

⁷ *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems [III]*.

⁸ *OLG Wien*, Urt. v. 07.12.2020 (nicht rechtskräftig), GZ 11 R 153/20f, 11 R 154/20b-99 S.27. Diese Ansicht ist nicht überzeugend, hierzu unten: Kapitel 3 C.II.4./5 und III.3.

⁹ Obwohl es wenig überrascht, dass *Meta Platforms* (ehemals: *Facebook*) häufig beklagte Partei ist, birgt dieses Vorlageverfahren die Gefahr, dass der *EuGH* sich die Folgen seiner Entscheidung für andere, kleinere Verantwortliche zu wenig bewusst macht.

¹⁰ *EDSB*, Stellungnahme 4/2017 zu dem Vorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, 14.03.2017, S.10/Nr.17; sowie: Rede von *Giovanni Buttarelli* (ehemaliger EU-Datenschutz-Beauftragter), verfügbar unter

eilender *political correctness* meidet der europäische Gesetzgeber deshalb mittlerweile¹¹ diesen Begriff, ohne dadurch den tatsächlich bestehenden Konflikt zwischen Datenschutz- und Schuldrecht zu lösen.¹² Zwar soll mit dem europäischen Data Act auch die Nutzung von personenbezogenen Daten verbessert werden; wie dieses Ziel sich jedoch mit den Anforderungen der DS-GVO synchronisieren lässt, bleibt einstweilen offen.¹³

Rechtlich bringen Art. 3 Abs. 8 der Richtlinie (EU) 2019/770 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (DID-RL)¹⁴ und § 327q BGB¹⁵ diese Dominanz der DS-GVO zum Ausdruck. Zwar versucht der deutsche Gesetzgeber das nationale Schuldrecht gegenüber der DS-GVO zu immunisieren. Gemäß § 327q Abs. 1 BGB soll die Abgabe einer datenschutzrechtlichen Erklärung des Verbrauchers nach Vertragsschluss die Wirksamkeit des Vertrags unberührt lassen. Weil jedoch per-

https://edps.europa.eu/sites/edp/files/publication/17-01-12_digital_content_directive_sd_en.pdf, zuletzt abgerufen am 19.05.2022 („So, even if some people treat personal data as commodity, under EU law it cannot be a commodity. There might well be market for personal data, just like there is, tragically, a market for live human organs.“)

¹¹ Anders noch *EU-Kommission* Vorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, COM/2015/0634 final. (Art. 3 Abs. 1 des Vorschlags erstreckte den Anwendungsbereich auf „alle Verträge, auf deren Grundlage ein Anbieter einem Verbraucher digitale Inhalte bereitstellt oder sich hierzu verpflichtet und der Verbraucher *als Gegenleistung* einen Preis zahlt oder aktiv eine andere Gegenleistung als Geld in Form *personenbezogener* oder anderer *Daten erbringt*“.

¹² Ohne Bezugnahme auf die zu diesem Zeitpunkt bereits verabschiedete, aber noch nicht umsetzungspflichtige Richtlinie (EU) 2019/770 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (DID-RL) kam das *OLG Wien* zu einer anderen Beurteilung. Danach sei es insbesondere „legitim, dass ein marktwirtschaftlich operierendes Unternehmen, das für bestimmte Dienstleistungen kein Geld verrechnet, im Rahmen der Gesetze auf anders geartete Finanzierungsquellen zurückgreift. [...] Denn nur diese Datenverwertung ermöglicht maßgeschneiderte Werbung, die das von der Beklagten geschuldete „personalisierte Erlebnis“ in wesentlichem Maße prägt und der Beklagten zugleich die für den Aufrechterhaltung der Plattform und die Erzielung eines Gewinns notwendigen Einkünfte verschafft.“ *OLG Wien*, Urt. v. 07.12.2020 (nicht rechtskräftig), GZ 11 R 153/20f, 11 R 154/20b-99 S.28. Zur fehlenden Synchronisierung zwischen DS-GVO und DID-RL, unten Kapitel 3 C.III.2.

¹³ *Europäische Kommission*, Inception of Assessment, Ref. Ares(2021)3527151 v. 28.05.2021, S. 7 (Likely impacts on fundamental rights): „Since personal data [...] fall into the scope of some elements of this initiative (e.g. improving usability of data linked to natural persons), the measure will be designed in a way that fully complies with the existing rules on personal data protection and ePrivacy“.

¹⁴ ABl. v. 22.05.2019, L 136/1. Art. 3 Abs. 8 DID-RL lautet: „Das Unionsrecht betreffend den Schutz personenbezogener Daten gilt für alle personenbezogenen Daten, die im Zusammenhang mit Verträgen gemäß Absatz 1 verarbeitet werden. Insbesondere lässt diese Richtlinie die Verordnung (EU) 2016/679 und die Richtlinie 2002/58/EG unberührt. Im Fall von Widersprüchen zwischen Bestimmungen dieser Richtlinie und dem Unionsrecht zum Schutz personenbezogener Daten ist letzteres maßgeblich.“

¹⁵ Eingeführt durch das Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen v. 25.06.2021, BGBl. 2021 Teil I Nr. 37, 30.06.2021, 2123 ff.

sonenbezogene Daten tatsächlich und rechtlich zunehmend als Leistungsgegenstand behandelt und vereinbart werden und einige der derzeit ökonomisch besonders erfolgreichen Geschäftsmodelle von *GAFAM* und *BAT* – in unterschiedlichem Ausmaß – auf dem Zugang zu personenbezogenen Daten beruhen, entspricht dieser schlichte Abgrenzungsversuch in § 327q Abs. 1 BGB eher einem Wunschdenken, als dem Anspruch, die tatsächliche Realität rechtlich abzubilden.¹⁶

Indem § 327q Abs. 3 BGB alle Ersatzansprüche des *Unternehmers* gegen den *Verbraucher* wegen Abgabe einer datenschutzrechtlichen Erklärung ausschließt, die eine Einschränkung der rechtmäßigen Datenverarbeitung bewirkt, hat der deutsche Gesetzgeber zwar zu einem kräftigen Befreiungsschlag ausgeholt, um den gordischen Knoten aus europäischem Datenschutz- und nationalem Schuldrecht zumindest im B2C-Verhältnis zu lösen. Auf den zweiten Blick erinnert dieser Befreiungsversuch des Gesetzgebers jedoch an den verzweifelten Versuch des *Laokoon*, sich aus dem Griff der Schlangen zu befreien. § 327q BGB ist nicht in der Lage, den tatsächlich bestehenden Konflikt zwischen einer jederzeit und grundlos widerruflichen Einwilligung und dem schuldrechtlichen Prinzip des *do ut des* befriedigend aufzulösen.¹⁷ Eine solche Lösung ist aber jedenfalls in Fällen erforderlich, in denen Datensubjekte ihre personenbezogenen Daten bewusst dafür einsetzen, um ihr monetäres Konsumbudget zu schonen (Verbraucher) oder um selbst Gewinne zu erwirtschaften (Unternehmer).

Die Ursache dafür, dass das Datenschutzrecht und das Schuldrecht sich auf Kollisionskurs befinden, ist leicht zu identifizieren. Beginnend mit dem ersten BDSG von 1977¹⁸ beruht das deutsche und im Anschluss hieran das europäische Datenschutzrecht auf einem Verarbeitungsverbot mit Erlaubnisvorbehalt (§ 3 Abs. 1 BDSG von 1977 – jetzt: Art. 6 Abs. 1 und Art. 9 Abs. 1 DS-GVO). Das Schuldrecht hingegen beruht auf einer Erlaubnis mit Verbotsvorbehalt (§§ 311, 241 BGB).¹⁹

¹⁶ Insbesondere dürfte damit auch noch nicht „jedweder Diskussion um eine mögliche Einschränkung des Widerrufsrechts [...] ein Riegel vorgeschoben“ worden sein. So aber: *Spindler*, MMR 2021, 528 (530). Hierzu unten Kapitel 5 C.III.

¹⁷ Zum hier unterbreiteten Vorschlag eines befristeten Ausschlusses der Widerruflichkeit durch teleologische Reduktion von Art. 7 Abs. 3 S. 1 DS-GVO unten Kapitel 5 C.III, sowie zuvor: *Sattler*, JZ 2017, 1036 (1041 f.). Sollte der EuGH der Rechtsauffassung von *Facebook*, des LG Wien und des OLG Wien folgen, würde das Geschäftsmodell von *Facebook* und anderen durch personalisierte Werbung finanzierten Kommunikationsplattformen nicht nur gemäß Art. 6 Abs. 1 lit. b DS-GVO weitgehend den Vorgaben der DS-GVO entgegen, sondern es entstünden auch schwerwiegende Abgrenzungsschwierigkeiten zum Anwendungsbereich der DID-RL bzw. von §§ 327 ff. BGB. Hierzu Kapitel 3 C.III.3.

¹⁸ Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung v. 27.01.1977, BGBl. I Nr. 7 S. 201 ff.

¹⁹ Pointiert: *Engert*, in: Grundmann/Möslein (Hrsg.), *Innovation und Vertragsrecht*, 2020, S. 153 (159: „Datenverarbeitung durch Private wird umstandslos einem staatlichen Grundrechtseingriff gleichgestellt und einem umfassenden Rechtfertigungsgebot unterworfen [...]. Strukturell ist das nichts anderes als eine ins Horizontalverhältnis gekippte, unmittelbare Grundrechtsbindung Privater“).

Kurzum: Bislang ist es weder dem europäischen noch dem – insoweit durch Unionsrecht gebundenen deutschen – Gesetzgeber gelungen, das Datenschutzrecht und das Schuldrecht zu synchronisieren. Auch das dem unternehmerisch handelnden Verantwortlichen gemäß § 327q Abs. 2 BGB eingeräumte, komplexe Kündigungsrecht für den Fall, dass ein als Verbraucher handelndes Datensubjekt die Datenverarbeitung für die Zukunft beendet, ist lediglich ein erster – deutscher – Versuch, diese Kollision abzumildern. Ein *Datenschuldrecht*,²⁰ das auch personenbezogene Daten als Leistungsgegenstand anerkennt und die ökonomische Realität rechtlich abbildet oder sogar gestaltet, lässt sich auf dieser Grundlage jedoch nicht entwickeln.

Es ist eine banale Erkenntnis, dass die Verarbeitung von personenbezogenen Daten ubiquitär ist. Sie ist zentral für Entwicklungen, die derzeit mit den schillernden Chiffren „Big Data“²¹ und „künstliche Intelligenz“ (KI)²² umschrieben werden. Beiden Entwicklungen ist gemeinsam, dass sie die Verarbeitung von personenbezogenen Daten nicht voraussetzen, ihre Vorteile aber insbesondere durch eine Verarbeitung von Daten mit Personenbezug entfalten können.

Zwar sind anonymisierte Daten im Kontext von Big Data und KI nicht wertlos, solange ein abstrakter und damit wissenschaftlicher Erkenntnisgewinn angestrebt wird. Allerdings knüpfen auch der wissenschaftliche, jedenfalls aber der ökonomische Wert von Datenanalysen häufig an den Personenbezug als eine wesentliche semantische Ebene von maschinenlesbar codierter Information (kurz: personenbezogenes Datum) an.²³ Deshalb liegt der Fokus der Arbeit nicht auf der – primär technisch spannenden – Frage, wie eine Verarbeitung von personenbezogenen Daten durch Methoden der Anonymisierung effektiv vermieden oder das Risiko der Verarbeitung durch Pseudonymisierung (Art. 4 Nr. 5 DS-GVO) und Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) verringert werden kann. Vielmehr steht die Frage im Zentrum, inwieweit die Auslegung und Anwendung der DS-GVO eine rechtmäßige und rechtssichere Verarbeitung von personenbezogenen Daten im Privatrechtsverhältnis²⁴ ermöglicht, ohne dabei gegen das gemäß Art. 8 GRCh (Schutz personenbezogener Daten)

²⁰ Begriffsprägend *Schmidt-Kessel*, Daten als Gegenleistung in Verträgen über die Bereitstellung digitaler Inhalte, BMJV, 03.05.2016, https://www.bmjv.de/SharedDocs/Downloads/DE/Praesentationen/05032016_digitalesVertragsrecht_Schmidt_Kessler.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 19.05.2022.

²¹ Aus rechtlicher Perspektive: *Leistner/Antoine/Sagstetter*, Big Data, 2021.

²² Mit technischer Einführung: *Zech*, Entscheidungen digitaler autonomer Systeme: Empfehlen sich Regelungen zu Verantwortung und Haftung?, Gutachten für den 73. Deutschen Juristentag, 2020.

²³ Zum Informationsbegriff: *Wiebe*, in: Fiedler/Ullrich (Hrsg.), Information als Wirtschaftsgut, 1997, S. 93 (99 ff.); *Zech*, Information als Schutzgegenstand, 2012, S. 14 ff./114. f./441.

²⁴ Die Datenverarbeitung im Rahmen von Beschäftigungsverhältnissen (Art. 88 DS-GVO i. V. m. § 26 BDSG) weist Besonderheiten auf und bleibt unberücksichtigt: Hierzu: m. w. N.: *Neighbour*, in: Sassenberg/Faber (Hrsg.), Industrie 4.0 und IoT, 2020, S. 277 ff.; *Forgó/Helfrich/Schneider* (Hrsg.), Betrieblicher Datenschutz, 2019.

und gemäß Art. 7 GRCh (Privatsphäre) zu gewährleistende Untermaßverbot zu verstoßen.

Notwendig ist eine privatrechtssensible Auslegung deshalb, weil zunehmend deutlich wird, dass der europäische Gesetzgeber bei Verabschiedung der DS-GVO die rechtliche und ökonomische Realität in den Mitgliedstaaten nur unzureichend erfasst hat. Die DS-GVO nimmt zu wenig Rücksicht auf die tatsächliche Verwertung der vermögenswerten Bestandteile von Persönlichkeitsrechten, die wiederum eine Verarbeitung von personenbezogenen Daten voraussetzt.²⁵

Die Notwendigkeit, bei dieser privatrechtssensiblen Auslegung und Anwendung der DS-GVO auf die Unionsgrundrechte zurückzugreifen, ist der Vielzahl der unbestimmten Rechtsbegriffe in der DS-GVO geschuldet. Diese erschweren die gerichtliche und behördliche Rechtsanwendung derzeit fundamental. Infolgedessen ist es auch für die Wissenschaft eine zentrale Herausforderung *de lege lata* und – soweit dies nicht mehr möglich ist – auch *de lege ferenda* Vorschläge für die Ausgestaltung eines Datenschuldrechts zu unterbreiten, das die informationelle Privatautonomie der Datensubjekte stärkt, dabei aber die multipolaren Grundrechtskonstellationen hinreichend berücksichtigt.²⁶

Das nachfolgend vorgeschlagene Stufenmodell der Erlaubnistatbestände zur Gewährleistung einer abgestützten informationellen Privatautonomie stellt bereits begrifflich die Privatautonomie und insbesondere die Vertragsfreiheit als ihre wichtigste Ausprägung in den Mittelpunkt. Dabei weicht der Begriff der informationellen Privatautonomie von dem bekannten Begriff der informationellen Selbstbestimmung ab. Letztere ist bereits seit dem *Volkszählungsurteil* des BVerfG²⁷ bekannt.

Diese begriffliche Unterscheidung ist jedoch kein bloßes Glasperlenspiel. Im Gegenteil: Die Gewährleistung einer abgestützten informationellen Privatautonomie ist Ausdruck eines Perspektivenwechsels und dient dazu, Grundannahmen des geltenden Datenschutzrechts kritisch zu hinterfragen, soweit personenbezogene Daten als Gegenstand eines vertraglichen Synallagmas vereinbart werden.

Im Zentrum des hier vorgeschlagenen Stufenmodells der Erlaubnistatbestände für das Privatrechtsverhältnis steht die datenschutzrechtliche Einwilligung, die ihrerseits in zwei Stufen ausdifferenziert wird. Infolgedessen ist dieses Stufenmodell in der Lage, eine Synthese aus dem datenschutzrechtlichen Verbot und der schuldrechtlichen Erlaubnis herzustellen und dadurch einem künftiges

²⁵ Zuletzt mit dieser Kritik, jedoch aus Perspektive einer Stärkung von Verbraucherrechten: *Wendehorst*, JZ 2021, 974 (984: „die DSGVO [ist] überhaupt nicht auf den Schutz vermögensrechtlicher Verbraucherinteressen [...] zugeschnitten“).

²⁶ Mit dieser Forderung an die Privatrechtswissenschaft: *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 372.

²⁷ BVerfGE 65, 1 (43) = NJW 1984, 419ff. – *Volkszählung*.

Datenschuldrecht den Boden zu bereiten. Dadurch gewährleistet das nachfolgend vorgeschlagene Stufenmodell der Erlaubnistatbestände die unionsgrundrechtlich verankerte abgestützte informationelle Privatautonomie und ermöglicht die Umsetzung von drei wesentlichen Zielen, ohne dabei den Schutz der Datensubjekte wesentlich zu beeinträchtigen:

Erstens wird die bisherige Kommerzialisierung der vermögenswerten Bestandteile von Persönlichkeitsrechten (wieder) ermöglicht, soweit diese auf eine Verarbeitung von personenbezogenen Daten angewiesen ist.

Zweitens werden personenbezogene Daten – wie von der *EU-Kommission* immer wieder und zuletzt im Kontext des Data Act gefordert – für Innovation und Wachstum im Binnenmarkt nutzbar gemacht, ohne dabei über die Präferenzen der Datensubjekte hinwegzugehen.

Drittens hilft dieses Stufenmodell und insbesondere die kartellrechtsakzesessorische und damit asymmetrische Auslegung und Anwendung des Einwilligungstatbestands dabei, die durch die DS-GVO entstandenen Marktzutrittsbarrieren für KMU zu senken.

II. Forschungsstand

Spätestens seit Anfang der 1970er Jahre fordert der technische Fortschritt im Bereich der automatischen Datenverarbeitung den Schutz des Individuums vor einer Verarbeitung personenbezogener Daten immer wieder heraus.²⁸ Nach einer frühen kritischen Auseinandersetzung mit den ersten deutschen Gesetzen zum Schutz von natürlichen Personen vor einer Verarbeitung von personenbezogenen Daten²⁹ stagnierte das Interesse, das Privatrechtswissenschaftler dem Datenschutzrecht entgegenbrachten.³⁰ Das Feld wurde weitgehend dem Verwaltungs- und insbesondere dem Verfassungsrecht überlassen.³¹

²⁸ Hierzu frühzeitig: *Kilian*, Personalinformationssysteme in deutschen Großunternehmen, 1967; *ders.*, Juristische Entscheidung und Elektronische Datenverarbeitung, 1974; *Steinmüller/Lutterbeck/Malman/Harbort/Kolb/Schneider*, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, 1971, BT Drs. VI/3826; *Steinmüller*, EDV und Recht: Einführung in die Rechtsinformatik und das Recht der Informationsverarbeitung, Juristische Arbeitsblätter 1970; *ders.* (Hrsg.), Informationsrecht und Informationspolitik, 1976.

²⁹ Kapitel 1 A.II.

³⁰ Zu den wenigen Ausnahmen zählen: *Ebnet*, Der Informationsvertrag, 1995; *A. Wagner*, Binäre Information als Gegenstand des Rechtsverkehrs, 1999; *Kilian*, CR 2002, 921 ff.; *Buchner*, Die Informationelle Selbstbestimmung im Privatrecht, 2006; *Unselde*, Die Kommerzialisierung personenbezogener Daten, 2010; *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, 2012; *Sandfuchs*, Privatheit wider Willen?, 2015. Zudem ist *Spiros Simitis*, der erste Hessische Datenschutzbeauftragte und Herausgeber des langjährigen Standardkommentars zum BDSG, von Hause aus Privatrechtswissenschaftler.

³¹ Hierzu: *Sattler*, in: Bakhoum u. a. (Hrsg.), 2018, Personal Data in Competition, Consumer Protection and Intellectual Property Law, 2018, S. 27 ff.

Obwohl einige wissenschaftliche Beiträge einen vermittelnden Ansatz wählen,³² leidet die rechtswissenschaftliche Auseinandersetzung weiterhin unter einem – auch institutionell durch die zahlreichen Datenschutzbehörden begünstigten – Übergewicht der öffentlich-rechtlichen Perspektive. Dennoch hat die privatrechtlich ausgerichtete Forschung gerade in den letzten Jahren wegweisende Untersuchungen hervorgebracht.

Besonders hervorzuheben sind die Arbeiten von *Benedikt Buchner*,³³ *Louisa Specht-Riemenschneider*,³⁴ *Carmen Langhanke*,³⁵ *Philipp Hacker*³⁶ und *Jan Niklas Bunnenberg*.³⁷ Die nachfolgende Analyse profitiert von dieser Forschung und baut hierauf teilweise auf. Dennoch unterscheidet sich das hier vorgeschlagene Stufenmodell der Erlaubnistatbestände und die dadurch gewährleistete abgestützte informationelle Privatautonomie in mehreren wesentlichen Punkten vom bisherigen Forschungsstand.

Der Untersuchungsgegenstand der Arbeiten von *Benedikt Buchner*, *Louisa Specht-Riemenschneider* und *Carmen Langhanke* war das alte BDSG, so dass mit der Anwendbarkeit der DS-GVO – trotz deren weitreichender Kontinuität zur Datenschutz-RL von 1995 – eine Neubewertung erforderlich ist. Zudem gehen alle vorgenannten Autorinnen und Autoren – mit Ausnahme von *Benedikt Buchner* – von einer jederzeitigen und grundlosen Widerruflichkeit der datenschutzrechtlichen Einwilligung aus. Infolgedessen dominiert das Datenschutzrecht das Schuldrecht in einer Weise, die – zumindest im B2B-Verhältnis – nach hier vertretener Ansicht nicht mit dem Verhältnismäßigkeitsgrundsatz vereinbar ist. *Benedikt Buchner* wiederum spart das Verhältnis zwischen Datenschutzrecht und AGB-Recht weitgehend aus.³⁸

Weil alle bisherigen Arbeiten von einer Dominanz des Datenschutzrechts gegenüber dem Schuldrecht ausgehen,³⁹ bleibt – jedenfalls nach hier vertretener Auffassung – nicht viel vom Grundsatz der Privatautonomie, einschließlich der Möglichkeit zur Selbstbindung, übrig.

³² *Masing*, NJW 2012, 2305 ff.; *Kingreen/Kühling*, JZ 2015, 213 ff.; *von Lewinski*, Die Matrix des Datenschutzrechts, 2014.

³³ Die informationelle Selbstbestimmung im Privatrecht, 2006.

³⁴ *Specht*, Die Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012.

³⁵ Daten als Leistung, 2018.

³⁶ Datenprivatrecht, 2020.

³⁷ Privates Datenschutzrecht, 2020.

³⁸ Das ist im Ergebnis wenig schädlich, weil infolge der seit 2018 vorrangig anzuwendenden Grundsätze aus Art. 5 Abs. 1 DS-GVO der AGB-Kontrolle lediglich geringe Bedeutung zukommt. Hierzu: Kapitel 3 C.I.3.; a. A. *Hacker*, Datenprivatrecht, 2020, 417 ff. (430 ff.), sowie *Wendehorst*, JZ 2021, 974 (983 f.).

³⁹ Für eine stärkere Berücksichtigung schuldrechtlicher Grundsätze: *Metzger*, JIPITEC 2017, 2 (6 f.); *ders.*, AcP 216 (2016), 817 (833); *ders.*, in: *Lohsse/Schulze/Staudenmayer* (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, S. 25 (36 ff.).

Jan Niklas Bunnenberg will der Bindungswirkung einer Erklärung von Datensubjekten nur dann gemäß Art. 6 Abs. 1 lit. b DS-GVO (sog. vertragsakzessorische Datenverarbeitung) einen Vorrang vor dem Widerrufsinteresse des Datensubjekts einräumen, wenn das Interesse des Verantwortlichen infolge einer Abwägung im Einzelfall ausnahmsweise überwiegt.⁴⁰ Dieser Ansatz überzeugt systematisch nicht, weil er die beiden Erlaubnistatbestände gemäß Art. 6 Abs. 1 lit. b DS-GVO (vertragsakzessorische Datenverarbeitung) und gemäß Art. 6 Abs. 1 lit. f DS-GVO (Datenverarbeitung infolge einer Interessenabwägung) im Ergebnis vermengt und stets auf eine *ex post*-Interessenabwägung im Einzelfall angewiesen ist.⁴¹

Philipp Hacker ordnet die frei widerrufliche Einwilligung (Art. 7 Abs. 3 S. 1 DS-GVO) als schuldrechtliche Bedingung für die Leistungserbringung durch den Verantwortlichen ein.⁴² Infolgedessen verschmelzen Software und Recht potenziell zu dem von Lawrence Lessig konstatierten „Code is Law“.⁴³ Allerdings soll es dem Verantwortlichen im Fall eines allzu „opportunistischen Widerrufs“ der Einwilligung durch das Datensubjekt ausnahmsweise möglich sein, die Datenverarbeitung auf Grundlage einer Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO fortzusetzen.⁴⁴ Sofern personenbezogene Daten vertraglich als Leistungsgegenstand vereinbart werden, soll deren Verarbeitung gemäß Art. 6 Abs. 1 lit. b DS-GVO rechtmäßig sein, soweit dieses Synallagma einer gerichtlichen Angemessenheitskontrolle standhält.⁴⁵

Obwohl sich die von Hacker und in dieser Arbeit bearbeitete Thematik teilweise überschneidet, wird nachfolgend eine andere Lösung vorgeschlagen. Die Skepsis gegenüber einer gerichtlichen Angemessenheitsprüfung des vertraglichen Synallagmas mündet in den nachfolgend herausgearbeiteten Vorschlag einer abgestützten informationellen Privatautonomie, der im Unterschied zu

⁴⁰ Bunnenberg, Privates Datenschutzrecht, 2020, S. 264 f.

⁴¹ Das Interesse des Datensubjekts am Widerruf der Einwilligung (Art. 6 Abs. 1 lit. a i. V. m. Art. 7 Abs. 3 S. 1 DS-GVO) wird mit einer Interessenabwägung (Art. 6 Abs. 1 lit. f DS-GVO) kombiniert und soll anschließend die Fortsetzung der Datenverarbeitung auf Grundlage eines bindenden Vertrags gemäß Art. 6 Abs. 1 lit. b ermöglichen. Hierzu unten Kapitel 3 B.II.

⁴² Hacker, ZfPW 2019, 148 (172 ff.); ders., Datenprivatrecht, 2020, S. 228 f.; so auch Rafal Maňko, Contracts for the supply of digital content and digital services, Bericht des Wissenschaftlichen Dienstes des EU-Parlaments (EPRS) vom 27.11.2017, S. 8 („The report deletes the term *counter-performance*, criticized by the EDPS, and replaces it with the term *condition*“), verfügbar unter http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/614707/EPRS_BRI%282018%29614707_EN.pdf, zuletzt abgerufen am 19.05.2022; EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, v. 04.05.2020, Nr. 37; ähnlich: Riehm, in: Pertot (Hrsg.), Rechte an Daten, 2020, S. 194 f. Hierzu: Kapitel 4 A.II.5.

⁴³ Lessig, Code is law, 1999.

⁴⁴ Hacker, Datenprivatrecht, 2020, S. 278. In diese Richtung auch bereits: Buchner, Die informationelle Selbstbestimmung im Privatrecht, 2006, S. 272 ff.

⁴⁵ Hacker, Datenprivatrecht, 2020, S. 445 ff./473 ff. Zu den Bedenken an einer praktischen Umsetzung dieses Ansatzes: Kapitel 3 C.I.2.e. und C.I.3. Zu den Nachteilen für die unionsweit einheitliche Wirkung der DS-GVO: Kapitel 3 C.II.

Stichwortverzeichnis

- AGB 161, 174
Allgemeines Persönlichkeitsrecht 18, 21, 24, 28, 65, 150, 226, 243, 252, 330, 418
Anonymisierung 131, 287
Anti-Diskriminierungsrecht 34
Anwendungsvorrang 146
artificial neuronal networks 128
Automatisierung 377
Aziz-Test 192
- BAT 1, 109, 111, 118, 134, 198, 235, 239
- Cookies* 282, 322, 388, 390
- Data Act 4, 340
data processing by default 235, 333
data protection by design 124, 407
Daten als Gegenleistung 64, 69, 70, 107, 137, 145, 178, 199, 234, 264, 266, 275, 385, 395
datenbasierter *laesio enormis* 155, 173, 179
Datenportabilität 136, 207, 209, 240, 348, 397, 410
Datenpreis 164, 165
Datenschutz-Dashboard 382
Datenschutz durch Technikgestaltung 124, 151, 377, 406
Datenschutz durch Voreinstellung 124, 151, 408
Datensubjekte
– Aufmerksamkeit 156, 161, 165, 166, 168, 170, 419
– Kinder 85, 130, 215, 316, 327
– Schutz 63, 68, 137, 140, 180, 184, 185, 188, 189, 192, 207, 246, 259, 280, 352, 414
– Unternehmer 236, 319, 325, 417, 418
– Verständnis 422
Datenverarbeitung mit Erlaubnisvorbehalt 64, 414
Datenverarbeitung nach Treu und Glauben 147, 149, 175, 273, 294, 342, 344, 350, 355, 356, 391
Digital Markets Act 117, 283, 312, 326, 332, 342, 384, 409, 420, 421
Digitale Produkte 194, 417
do not track 399
Double Opt-In 134, 392
Drohung 222, 318
DS-GVO und DID-RL 73, 153, 265, 416
- Einwilligung 230, 416
– als Gegenleistung 233
– Disposition über die freie Widerruflichkeit 357
– Disposition über die Widerruflichkeit 241, 259, 268, 272, 273, 275, 276, 288, 330, 332, 333, 339, 341, 342, 343, 344, 345, 346, 347, 348, 352, 353, 354, 355, 420
– Fähigkeit 316
– Freiwilligkeit 298, 306, 419, 420
– Kinder 215, 316, 327
– schlichte 250, 262, 353
– Unionsautonom 212, 268, 354, 418
– Unmissverständlichkeit 184
– Unternehmerische Freiheit 297, 310, 315
– Vertragsakzessorisch 182, 247, 249, 298
– Vorrang 417, 419
– Widerruf 328, 418
– Widerrufsabschluss 334, 420, 421
– Zweckbindung 217
Entscheidungskapazitäten 419
ePrivacy-VO 17, 46, 190, 210, 265, 279, 399
Erlaubnistatbestände
– Interessenabwägung 97, 101, 134, 139, 141, 148, 209, 278, 279, 414, 415

- vertragsakzessorisch 287
- Vertragsakzessorisch 74, 98, 119, 136, 143, 207, 261, 262, 277, 378, 416
- europäisches Mehrebenensystem 100, 145, 186, 211, 268, 270
- fingerprints* 110
- first party tracking* 109
- Flucht ins Schuldrecht 416
- GAFAM 1, 106, 109, 111, 134, 140, 150, 197, 198, 235, 239, 297, 382, 415
- Gatekeeper* 117, 283, 312, 313, 314, 315, 326, 332, 333, 334, 342, 347, 370, 409, 420, 421
- gemeinsame Verantwortlichkeit 78, 338
- geo-tracking* 109
- Grundsätze der Datenverarbeitung 153, 350, 355
- Icons 366, 379
- identifier for advertisers* 109
- information overload* 220, 380, 388, 408
- Informationelle Privatautonomie 414, 415, 417, 418, 421
- Informationsasymmetrie 184
- Informationspflichten 219, 220, 339, 361, 364, 367, 368, 369, 373, 379, 380, 383, 387, 388, 389, 393, 397, 405, 406, 408, 409, 421, 422
- Internet of Things 123, 141, 280, 285, 286, 358, 416
- ius tum pretium* 155, 179
- kartellrechtliche Aufspaltung 420
- kartellrechtsakzessorische Anwendung 234, 303, 311, 312, 313, 314, 315, 325, 327, 333, 342, 354, 369, 396, 409, 420, 422
- Kinder *Siehe* Datensubjekte
- Klausel-RL 149, 155, 161, 174, 211
- Konditionenwettbewerb 168, 186, 273
- Kontroll-Cockpit 280, 381, 422
- Kopplungsverbot 297, 298, 318, 320, 325, 419
- künstliche Intelligenz 416
 - maschinelles Lernen 89, 119, 128, 218, 369
 - machine-learning* *Siehe* künstliche Intelligenz
 - Marktversagen 158, 161, 369
 - mehrseitige Plattformen 109, 118, 166, 235, 301, 325, 330, 334, 415
 - Minderjährige 317, 321
 - Nahfeldkommunikation 110
 - Nutzungsvertrag 147, 186, 197, 199, 203, 373
 - one-pager* 379
 - Personenbezug 80, 96, 127, 130, 131, 133
 - privacy by default* 408
 - privacy nutrition labels* 370
 - privacy paradoxon* 87
 - Privacy Score 361, 421, 422
 - privacy-enhancing-technologies* 359
 - privatrechtssensible Auslegung 230, 354, 413, 414
 - Recht auf informationelle Selbstbestimmung 15, 16, 17, 19, 24, 25, 27, 29, 36, 226, 414
 - Unmittelbare Drittwirkung 22, 28, 29
 - Recht auf Vergessen 54, 56, 207, 242, 410
 - Rechtsgeschäftslehre 263, 268, 269
 - Rechtsmissbrauch 274, 350
 - Re-Identifizierung 131
 - Risikospezifizität 146
 - Sachintegration 146
 - schuldrechtliche Gestattung 181, 250, 256, 257, 260, 261, 262, 269, 270, 288, 330, 331
 - Schuldrechtliche Kontrollmöglichkeit 170, 191, 212
 - schwarze Liste 101, 322, 323
 - Selbstdatenschutz 381
 - Signalling* 240, 369, 376
 - Smart-Home 109
 - social plug-in* 78, 109, 110, 388
 - Sprachassistenten 285
 - Stufenmodell 71, 271, 277, 356, 359, 418
 - Suchmaschinen 62, 236, 239, 291
 - Synallagma 64, 145, 152, 154, 155, 167, 170, 183, 191, 203, 227, 236, 263, 266, 290, 320

- third-party-tracking* 110, 322
Tracking 109, 113, 116, 120, 140, 282, 322, 388
tracking-tools 121
Trainingsdaten 127, 130, 131, 132, 133, 286
Transparenzgebot 174, 177, 184, 188
Transparenzkontrolle 154, 158, 164, 169

Übermaßverbot 237
UGP-RL 317, 318, 319, 321, 322, 323, 328
Unmittelbare Drittwirkung 22, 28, 29, 34, 38, 62, 414

Verarbeitungsverhältnis 20, 45, 66, 413
Verhaltensökonomik 160, 184, 360, 408
Verhaltensregeln 106, 107, 299
Verkehrsschutz 86, 257
Verschlüsselung 84, 375

Vertragsakzessorietät der Datenverarbeitung *Siehe* vertragsakzessorische Datenverarbeitung
vertragsakzessorische Datenverarbeitung 60, 74, 148, 152, 180, 201, 202, 207, 209, 277, 378
Vorratsdatenspeicherung 26, 55

Warenkauf-RL 149
Werbung
– Direktwerbung 77, 78, 90, 95, 100, 107, 282, 295, 374, 398, 406, 415
– Online 196
– Profiling 108, 111, 121, 128, 132, 140, 149, 188, 196, 281, 296, 312, 375, 398, 415

Zielkompatibilität 146, 186
Zweckbindung 30, 40, 407