FELIX GLOCKER

Der California Consumer Privacy Act

Gesellschaft für Rechtsvergleichung e.V.

Rechtsvergleichung
und Rechtsvereinheitlichung
87

Mohr Siebeck

Rechtsvergleichung und Rechtsvereinheitlichung

herausgegeben von der
Gesellschaft für Rechtsvergleichung e.V.

87

Felix Glocker

Der California Consumer Privacy Act

Ein liberaler Gegenentwurf zur DSGVO für das private Datenschutzrecht

Mohr Siebeck

Felix Glocker, geboren 1992; Studium der Rechtswissenschaft an der Ludwig-Maximilians-Universität München; Wissenschaftlicher Mitarbeiter am Dekanat der Juristischen Fakultät der Ludwig-Maximilians-Universität München; Rechtsreferendariat am OLG München; Rechtsanwalt in München.
orcid.org/0000-0002-7933-9706

ISBN 978-3-16-161941-0 / eISBN 978-3-16-161943-4
DOI 10.1628/978-3-16-161943-4

ISSN 1861-5449 / eISSN 2569-426X (Rechtsvergleichung und Rechtsvereinheitlichung)

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

Zugl.: Diss., Ludwig-Maximilians-Universität München, 2022.

Das Buch wurde von Laupp & Göbel in Gomaringen auf alterungsbeständiges Werkdruckpapier gedruckt und gebunden.

Ulla, Winfrid und Lisa

Vorwort

Die Arbeit wurde von der Juristischen Fakultät der Ludwig-Maximilians-Universität München im Sommersemester 2022 als Dissertation angenommen. Neue Rechtsprechung und Literatur konnten bis Juli 2022 berücksichtigt werden.

Zuerst bedanke ich mich herzlich bei meinem Doktorvater Professor Dr. Martin Franzen für die konstruktive und offene Betreuung sowie die sehr schnelle Erstellung des Erstgutachtens. Professor Dr. Matthias Leistner danke ich für die rasche Erstellung des Zweitgutachtens. Ebenfalls danke ich der Gesellschaft für Rechtsvergleichung e.V. und Professor Dr. Martin Schmidt-Kessel für die Aufnahme in die Schriftenreihe Rechtsvergleichung und Rechtsvereinheitlichung.

Diese Arbeit hat stark von den Erfahrungen mit dem europäischen Datenschutzrecht profitiert, die ich in meiner Teilzeittätigkeit als Datenschutzanwalt bei CMS Hasche Sigle sammeln durfte. Für die stets vertrauensvolle Zusammenarbeit auf Augenhöhe und die Rücksicht auf meine Dissertations-Auszeiten danke ich meinem Mentor Dr. Reemt Matthiesen.

Zahlreiche Freund:innen haben diese Arbeit bereichert, Fehler aufgedeckt und mich von mehr als einem »Holzweg« abgebracht. Matthias Meitner, Julia Karl und Carina Lyko danke ich für das hilfreiche Feedback und ihren treffsicheren Rat. Dr. Anne Brobeil, Ramona Weisenbach und Julia Ciric danke ich für die Gelegenheit zu fachlichen Diskussionen und den Rückhalt, auf den ich mich stets verlassen konnte.

Zuletzt möchte ich mich bei meiner Freundin Lisa Holub und meiner Familie bedanken. Meine Schwester Sophia Glocker hat große Teile dieser Arbeit gegengelesen und mir dadurch aus ihrer naturwissenschaftlichen Perspektive geholfen, viel verklausuliertes Juristendeutsch zu beseitigen. Meine Eltern Ulla Glocker und Dr. Winfrid Glocker haben mich während Studium, Referendariat und Promotion stets vorbehaltlos unterstützt und diese Arbeit mit der ihnen eigenen Genauigkeit und Gewissenhaftigkeit korrekturgelesen (*all errors are my own*, wie man in amerikanischen Aufsätzen zu sagen pflegt). Meiner Freundin Lisa Holub danke ich für die Rücksicht in der Zeit der Mehrfachbelastung durch Job und Promotion, in der sie mir stets mit Liebe und Geduld zur Seite stand. Ihr und meinen Eltern ist diese Arbeit gewidmet.

München, im August 2022 Felix Glocker

Inhaltsübersicht

Vorwort VII
Inhaltsverzeichnis XI
Abkürzungsverzeichnis XIX

Kapitel 1: Einführung 1

A. Das erste umfassende Datenschutzgesetz der Vereinigten Staaten 1
B. Abgrenzung der Fragestellung 3
C. Untersuchungsmethode 4
D. Ausblick auf die folgende Untersuchung 6

Kapitel 2: Hintergrund und Gesetzgebungsgeschichte 7

A. Verfassungsrechtlicher Hintergrund 7
B. Amerikanisches Datenschutzrecht 17
C. Gesetzgebungsgeschichte 30

Kapitel 3: Analyse des CCPA und Vergleich mit europäischem Datenschutzrecht 41

A. Aufbau dieses Kapitels und des CCPA 41
B. Anwendungsbereich 43
C. Verbraucherrechte 81
D. Unternehmenspflichten 150
E. Rechtsdurchsetzung 181
F. Rechtsvergleichendes Fazit 221

Kapitel 4: Schlussfolgerungen aus der Analyse für das europäische Datenschutzrecht 233

A. Angemessenheitsbeschluss für Kalifornien? 233
B. Übernahme der Regelung für finanzielle Anreize in das europäische Datenschutzrecht 241

Kapitel 5: Fazit 277

A. Zusammenfassung der Ergebnisse 277
B. Ausblick 284

Anhang 1: California Consumer Privacy Act 287
Anhang 2: California Consumer Privacy Act Regulations 329
Literatur- und Quellenverzeichnis 351
Sachregister 393

Inhaltsverzeichnis

Vorwort VII
Inhaltsverzeichnis XI
Abkürzungsverzeichnis XIX

Kapitel 1: Einführung 1

A. Das erste umfassende Datenschutzgesetz der Vereinigten Staaten . . . 1
B. Abgrenzung der Fragestellung 3
C. Untersuchungsmethode 4
D. Ausblick auf die folgende Untersuchung 6

Kapitel 2: Hintergrund und Gesetzgebungsgeschichte 7

A. Verfassungsrechtlicher Hintergrund 7

I. Constitution of the United States 7
1. Eingeschränkter Schutz der Privatsphäre 7
2. Grenzen für einzelstaatliche Datenschutzgesetze: Meinungsfreiheit und Dormant Commerce Clause 10
a) First Amendment 10
b) Dormant Commerce Clause 13
II. Constitution of the State of California 15

B. Amerikanisches Datenschutzrecht 17

I. Bund: Datenschutz als Verbraucherschutz 17
1. Langsame Entwicklung des Commons Laws im Deliktsrecht . . . 17
2. Branchenspezifische Datenschutzgesetze 19
3. Federal Trade Commission 24
II. Kalifornien als Vorreiter im Datenschutz 27
III. Fazit 29

C. Gesetzgebungsgeschichte 30

I. Handlungsdruck durch erstes Volksbegehren (2017–2018) 30
II. Kurzes Gesetzgebungsverfahren (2018) 32
III. Korrekturen durch Gesetzesänderungen und Konkretisierung durch die erste Durchführungsverordnung (2018–2020) 34
IV. Volksentscheid Proposition 24 (2019–2020) 35
V. Weitere Gesetzesänderungen und erweiterte Durchführungsverordnung (2021–2022) 38

Kapitel 3: Analyse des CCPA und Vergleich mit europäischem Datenschutzrecht 41

A. Aufbau dieses Kapitels und des CCPA 41
B. Anwendungsbereich 43

I. Kernbegriff der persönlichen Informationen 43
1. Definition 43
a) Darstellung 43
b) Vergleich mit Art. 4 Nr. 1 DSGVO 45
2. Ausnahme für aggregierte und deidentifizierte Informationen . . . 47
3. Ausnahme für öffentliche Informationen 50
a) Darstellung 50
b) Begrenzte Ausnahmen unter der DSGVO 54
II. Rollen 56
1. Verbraucher:innen 56
2. Unternehmen 56
a) Bestimmender Einfluss und Gewinnerzielungsabsicht 56
b) Schwellenwerte 58
c) Konzerngesellschaften und Joint Ventures 62
3. Dienstleister 65
a) Darstellung 65
b) Vergleich mit den Auftragsverarbeitern der DSGVO 68
4. Dritte 71
III. Räumlicher Anwendungsbereich 71
IV. Ausnahmen 74
1. Bereichsausnahmen 74
2. Kollisionsregeln für andere Datenschutzgesetze 76
V. Ergebnis 79

C. Verbraucherrechte 81

I. Widerspruchsrecht gegen Datenhandel 81
1. Ratio legis 81
2. Regelung 82
a) Reichweite 82
b) Ausübung 86
aa) Überblick 86
bb) Individueller Widerspruch 87
cc) Automatisches Widerspruchssignal 89
dd) Vertretung durch Datenschutzagenturen 91
c) Folgen eines Widerspruchs 93
d) Vergleich mit europäischem Datenschutzrecht 94
aa) Nur oberflächliche Gemeinsamkeiten mit Art. 21 DSGVO . 94
bb) Prinzip der Rechtmäßigkeit als funktionales Äquivalent zum Widerspruchsrecht gegen Datenhandel 95
cc) Einwilligungsbasierter Telemediendatenschutz 97
dd) Datenschutzagenturen im Vergleich zu Personal Information Management Systems und Datentreuhand 97
3. Einwilligungsvorbehalt für Minderjährige 98
4. Maßregelungsverbot 100
a) Reichweite 100
b) Ausnahme: Finanzielle Anreize 101
aa) Regelung 101
bb) Auswirkung auf Datenwirtschaft und Kritik 104
c) Vergleich mit europäischem Datenschutzrecht 107
d) Vergleich mit europäischem und deutschem Datenschuldrecht . 108
II. Recht auf Beschränkung sensibler Informationen 109
1. Definition sensibler Informationen 109
a) Darstellung 109
b) Vergleich mit Art. 9, 10 DSGVO 112
2. Reichweite und Ausübung 114
III. Recht auf Auskunft 116
1. Reichweite 116
a) Darstellung 116
b) Vergleich mit Art. 15 DSGVO 122
2. Ausübung 125
a) Darstellung 125
b) Vergleich mit Art. 15 DSGVO 131
3. Inzidentes Recht auf Datenportabilität 133
IV. Recht auf Löschung 134
1. Reichweite 134
a) Ratio legis und Tatbestand 134
b) Weitgefasste Ausnahmen 135

c) Vergleich mit Art. 17 DSGVO . . . 139
2. Ausübung . . . 141
3. Durchführung der Löschung . . . 144
V. Recht auf Berichtigung . . . 145
VI. Ergebnis . . . 147

D. Unternehmenspflichten . . . 150

I. Informationspflichten . . . 150
1. Einleitung und Überblick . . . 150
2. Umfang: Zweistufiges System . . . 151
a) Kurzer Datenschutzhinweis . . . 151
aa) Inhalt . . . 151
bb) Effektivität . . . 154
b) Umfassende Datenschutzerklärung . . . 155
aa) Inhalt für alle Unternehmen . . . 155
bb) Verbraucherrechte-Statistik für besonders große Unternehmen . . . 157
cc) Zugänglichkeit . . . 159
dd) Effektivität . . . 159
c) Vergleich mit Art. 13, 14 DSGVO . . . 160
3. Form und Sprache . . . 163
a) Darstellung . . . 163
b) Vergleich mit Art. 12 DSGVO . . . 164
II. Zweckbindung . . . 166
1. Darstellung . . . 166
2. Vergleich mit Art. 5 DSGVO . . . 168
III. Datenminimierung und Speicherfristbegrenzung . . . 169
1. Darstellung . . . 169
2. Vergleich mit Art. 5 DSGVO . . . 171
IV. Datensicherheit . . . 171
V. Weiterübermittlungs- und Dienstleistervertrag . . . 173
VI. Organisationspflichten . . . 176
1. Trainings- und Dokumentationspflichten . . . 176
2. Risikoanalysen und Datensicherheit-Audits . . . 177
3. Keine weiteren Organisationspflichten . . . 180
4. Ergebnis . . . 180

E. Rechtsdurchsetzung . . . 181

I. Aufsichtsbehörden . . . 181
1. Gewaltenteilung als typisches Element des amerikanischen Verwaltungsaufbaus . . . 181
2. Calilfornia Privacy Protection Agency . . . 182

a) Aufbau als unabhängige Kommission 182
b) Budget und Consumer Privacy Fund 186
c) Verordnungsermächtigung 187
d) Betriebsprüfungen und Ermittlungen 190
e) Bußgelder 191
f) Öffentlichkeitsarbeit und Beratung 194
3. Kalifornischer Attorney General 194
a) Rolle als Vollzugsbehörde 194
b) Verhängung von civil penalties 196
4. District und City Attorneys 198
5. Europäische Aufsichtsbehörden im Vergleich: Rechtssicherheit vor Effektivität 200
II. Begrenztes Privatklagerecht bei Datenpannen 204
1. Sammelklagen wegen Datenpannen vor dem CCPA 204
2. Regelung 208
a) Tatbestand 208
b) Schadensersatzhöhe 211
c) Verfahren 212
d) Kein weitergehendes Privatklagerecht 214
3. Vergleich mit europäischem und deutschem Datenschutzrecht sowie Zivilprozessrecht 216
III. Ergebnis 219

F. Rechtsvergleichendes Fazit 221

I. Privatautonomie statt Paternalismus 221
1. Selbstermächtigung als Ziel des CCPA 221
2. Die DSGVO als Ausdruck der mittelbaren Drittwirkung von Grundrechten 223
3. Bewertung 225
II. Transparenz und freier Informationsfluss 226
III. Exakte, aber fehlerreiche Regelungstechnik 228
IV. Oberflächlicher Einfluss der DSGVO 230

Kapitel 4: Schlussfolgerungen aus der Analyse für das europäische Datenschutzrecht 233

A. Angemessenheitsbeschluss für Kalifornien? 233

I. Maßstab der Angemessenheit 233
II. Materielles Datenschutzrecht 235
III. Umsetzung durch Aufsichtsbehörden, Privatklagerechte und Datenschutzorganisation 238

IV. Zugang von Sicherheitsbehörden 239
V. Gesamtbewertung 240

B. Übernahme der Regelung für finanzielle Anreize in das europäische Datenschutzrecht 241

I. Einleitung: gegenseitiger transatlantischer Austausch 241
II. Regelungsbedarf 243
1. Hintergrund: Leistung gegen Daten im grundrechtsgeprägten europäischen Datenschutz 243
2. Unzureichende Regelung *de lege lata* 245
a) Koppelungsverbot des Art. 7 Abs. 4 DSGVO 245
b) TTDSG und geplante ePrivacy-VO 249
c) Digitale-Inhalte-RL und §§ 327–327u BGB 250
d) Klausel-RL und §§ 305–310 BGB 251
3. Regelungsalternativen *de lege ferenda* im Überblick 254
III. Entwicklung eines Regelungsvorschlags 256
1. Eignung der kalifornischen Lösung 256
2. Regelungsstandort: neuer Art. 8a DSGVO-E 258
a) Verankerung im europäischen oder nationalen Recht? 258
b) Aufnahme in Digitale-Inhalte-RL, Klausel-RL oder DSGVO? . 259
c) Verortung innerhalb der DSGVO 260
3. Inhalt des neuen Art. 8a DSGVO-E »Bedingungen für Datenüberlassungsverträge« 262
a) Absatz 1: Grundsätzliche Zulässigkeit des Datenüberlassungsvertrages 262
b) Absatz 2: Angemessenes Alternativangebot 265
c) Absatz 3: Informationspflichten 265
d) Absatz 4: Bestimmung des Datenwerts 267
e) Absatz 5: Ausnahme für Unternehmer als betroffene Person . . 270
f) Absatz 6: Verhältnis zu Artikel 9 und dem Vertragsrecht der Mitgliedstaaten 270
aa) Satz 1: Verhältnis zu Art. 9 DSGVO 270
bb) Satz 2: Verhältnis zum Vertragsrecht der Mitgliedsstaaten . 272
4. Folgeänderungen 272
IV. Abschließender Regelungsvorschlag 274

Kapitel 5: Fazit 277

A. Zusammenfassung der Ergebnisse 277

I. Hintergrund und Gesetzgebungsgeschichte 277
1. Verfassungsrechtlicher Hintergrund 277

2. Amerikanisches Datenschutzrecht 277
3. Gesetzgebungsgeschichte 278
II. Analyse des CCPA und Vergleich mit europäischem Datenschutzrecht 278
1. Anwendungsbereich 278
2. Verbraucherrechte 279
a) Widerspruchsrecht gegen Datenhandel 279
b) Recht auf Beschränkung sensibler Informationen 280
c) Recht auf Auskunft, Recht auf Löschung und Recht auf Berichtigung 280
3. Unternehmenspflichten 280
4. Rechtsdurchsetzung 281
5. Rechtsvergleichendes Fazit 282
III. Schlussfolgerungen aus der Analyse 283
1. Kein Angemessenheitsbeschluss für Kalifornien 283
2. Übernahme der Regelung finanzieller Anreize 283

B. Ausblick 284

Anhang 1: California Consumer Privacy Act 287
Anhang 2: California Consumer Privacy Act Regulations 329
Literatur- und Quellenverzeichnis 351
Sachregister 393

Abkürzungsverzeichnis

a. A.	am Anfang/andere Ansicht
A. B.	Assembly Bill
a.E.	am Ende
ACLU	The American Civil Liberties Union
AcP	Archiv für die civilistische Praxis
Admin. L. Rev.	Administrative Law Review
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AGB	Allgemeine Geschäftsbedingungen
Am. Bus. L. J.	American Business Law Journal
Am. J. Comp. L.	The American Journal of Comparative Law
Am. J. Public Health	American Journal of Public Health
Am. U. L. Rev.	American University Law Review Forum
Antitrust ABA	American Bar Association Antitrust Law Section
Ark. Code Ann.	Arkansas Code Annotated
B. C. L. Rev.	Boston College Law Review
B. U. L. Rev. Online	Boston University Law Review Online
BAG	Bundesarbeitsgericht
Banking & Financial Services Policy Report	Banking & Financial Services Policy Report
BayDSG	Bayerisches Datenschutzgesetz
BayLDA	*Bayerisches Landesamt für Datenschutzaufsicht*
BayLfD	Bayerischer Landesbeauftragter für den Datenschutz
BayPAG	Gesetz über die Aufgaben und Befugnisse der Bayerischen Polizei
BB	Betriebs-Berater
BDSG	Bundesdatenschutzgesetz
BeckRS	Beck-Rechtsprechung
Berkeley J. Int'l L.	Berkeley Journal of International Law
BGB	Bürgerliches Gesetzbuch
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGH	Bundesgerichtshof
BKartA	Bundeskartellamt
BlnDSG	Berliner Datenschutzgesetz
Boston L. Rev.	Boston University Law Review
Brook. J. Corp. Fin. & Com. L.	Brooklyn Journal of Corporate, Financial & Commercial Law
Brook. J. Int'l L.	Brooklyn Journal of International Law
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik

BT-Drs.	Bundestags-Drucksache
BtMG	Gesetz über den Verkehr mit Betäubungsmitteln
Buffalo L. Rev.	Buffalo Law Review
Bus. Law.	The Business Lawyer
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVwG	Bundesverwaltungsgericht (Österreich)
C. C. R.	California Code of Regulations
C. F. R.	Code of Federal Regulations
Colo. Rev. Stat.	Colorado Revised Statutes
Cal.	California
Cal. 2nd	California Reports, Second Series
Cal. 3rd	California Reports, Third Series
Cal. 4th	California Reports, Fourth Series
Cal. 5th	California Reports, Fifth Series
Cal. App.	California Appellate Reports
Cal. App. 4th	California Appellate Reports, Fourth Series
Cal. App. 5th	California Appellate Reports, Fifth Series
Cal. Bus. & Prof. Code	California Business and Professions Code
Cal. Civ.	Civil Code of the State of California
Cal. Civ. Proc. Code	California Code of Civil Procedure
Cal. Const.	Constitution of the State of California
Cal. Educ. Code	California Education Code
Cal. Elec. Code	California Elections Code
Cal. Evid. Code	California Evidence Code
Cal. Gov. Code	California Government Code
Cal. Ins. Code	California Insurance Code
Cal. L. Rev.	California Law Review
Cal. Lab. Code	California Labor Code
Cal. Pen. Code	Penal Code of California
Cal. Rev. & Tax. Code	California Revenue and Taxation Code
Cal. Stats.	California Statutes
Cardozo Arts & Ent. L. J.	Cardozo Arts & Entertainment Law Journal
Cardozo L. Rev. De Novo	Cardozo Law Review De Novo
Case W. Res. L. Rev.	Case Western Reserve Law Review
Cath. U. J. L. & Tech.	Catholic University Journal of Law and Technology
Cath. U. L. Rev.	Catholic University Law Review
CCPA-2018	California Consumer Privacy Act of 2018 in der Fassung der A. B. 375, 2017–18 Leg. Reg. Sess. (Cal. 2018), Cal. Stats. 2018, ch. 55.
CCZ	Corporate Compliance Zeitschrift
Clev. St. L. Rev.	Cleveland State Law Review
Colo. Tech. L. J.	Colorado Technology Law Journal
Colum. Bus. L. Rev.	Columbia Business Law Review
Colum. J.L. & Arts	Columbia Journal of Law & the Arts
Colum. J.L. & Soc. Probs.	Columbia Journal of Law and Social Problems
Colum. L. Rev.	Columbia Law Review
Colum. L. Rev. Forum	Columbia Law Review Forum
Comm. L. & Pol'y	Communication Law and Policy
Cong.	Congress

COPPA	Children's Online Privacy Protection Act of 2000
Corp.	Corporation
Corp. & Bus. L. J.	Corporate and Business Law Journal
CR	Computer und Recht
CRi	Computer Law Review International
Cybaris Intell. Prop. L. Rev.	Cybaris: An Intellectual Property Law Review
DÄ	Deutsches Ärzteblatt
Denv. L. Rev. Online	Denver Law Review Online
DePaul J. Art Tech. & Intell. Prop. L.	DePaul Journal of Art, Technology & Intellectual Property Law
Data-Governance-VO	Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (DatenGovernance-Rechtsakt)
Dig.	Digesten
Digitale-Inhalte-RL	Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, ABl. L 136 vom 22.5.2019, S. 1–27
DSB	Datenschutz-Berater
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
DSGVO-E(KOM)	Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endg.
DSGVO-E(PARL)	Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))
DSK	Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder
DSRITB	Deutsche Stiftung für Recht und Informatik: Tagungsband Herbstakademie
DSRL	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
DuD	Datenschutz und Datensicherheit
Duke J. Const. L. & Pub. Pol'y Sidebar	Duke Journal of Constitutional Law & Public Policy Sidebar

Duke L. J.	Duke Law Journal
Ecology L. Currents	Ecology Law Currents
EGMR	Europäischer Gerichtshof für Menschenrechte
eIDAS-VO	Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
Empirical Legal Stud.	Empirical Legal Studies
EL	Ergänzungslieferung
EPA	Environmental Protection Agency
EPDL	European Data Protection Law Review
ePrivacy-RL	Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation
ePrivacy-VO-E(KOM)	Vorschlag für eine Verordnung des europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) (COM/2017/010 final – 2017/03 (COD))
ePrivacy-VO-E(PARL)	Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) (COM(2017)0010 – C8-0009/2017 – 2017/0003(COD))
ePrivacy-VO-E(RAT)	Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Mandate for negotiations with EP (ST 6087 2021 INIT – 2017/0003(COD))
EuGH	Gerichtshof der Europäischen Union
Eur. Foreign Aff. Rev.	European Foreign Affairs Review
Europäische Datenschutzkonvention	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EY	Ernst & Young
F. App'x	Federal Appendix
F. Supp.	Federal Supplement
F. Supp. 2d	Federal Supplement, Second Series
F. Supp. 3d	Federal Supplement, Third Series
F.2d	Federal Reporter, Second Series
F.3d	Federal Reporter, Third Series
F.T.C.	Federal Trade Commission Decisions

FCRA	Fair Credit Reporting Act of 1970
Fed. Comm. L. J.	Federal Communications Law Journal
Fed. R. Civ. P.	Federal Rules of Civil Procedure
Fed. Reg.	Federal Register
FERPA	Family Educational Rights and Privacy Act of 1974
Fla. L. Rev.	Florida Law Review
Fla. Stat.	Florida Statutes
Fordham Int'l L. J.	Fordham International Law Journal
Fordham Intell. Prop. Media & Ent. L. J.	Fordham Intellectual Property, Media & Entertainment Law Journal
FTC	Federal Trade Commission
Ga.	Georgia
gem.	gemäß
Geo. L. Tech. Rev.	Geo. L. Tech. Rev.
Geo. Wash. L. Rev.	George Washington Law Review
Geoblocking-VO	Verordnung (EU) 2018/302 des Europäischen Parlaments und des Rates vom 28. Februar 2018 über Maßnahmen gegen ungerechtfertigtes Geoblocking und andere Formen der Diskriminierung aufgrund der Staatsangehörigkeit, des Wohnsitzes oder des Ortes der Niederlassung des Kunden innerhalb des Binnenmarkts und zur Änderung der Verordnungen (EG) Nr. 2006/2004 und (EU) 2017/2394 sowie der Richtlinie 2009/22/EG
GLBA	Gramm-Leach-Bliley-Act (Financial Services Modernization Act of 1999)
Global Privacy Rev.	Global Privacy Review
GRCh	Charta der Grundrechte der Europäischen Union
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
Harv. J.L. & Pub. Pol'y	Harvard Law & Policy Review
Harv. J.L. & Tech.	Harvard Journal of Law & Technology
Harv. L. Rev.	Harvard Law Review
Hastings Const. L.Q.	Hastings Constitutional Law Quarterly
Hastings L. J.	Hastings Law Journal
Hastings Sci. & Tech. L. J.	Hastings Science and Technology Law Journal
HBDI	Hessischer Beauftragter für Datenschutz und Informationsfreiheit
HIPAA	Health Insurance Portability and Accountability Act of 1996
Hofstra L. Rev.	Hofstra Law Review
Hrsg.	Herausgeber
Humanarzneimittel-Prüf-VO	Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG
i. Erg.	im Ergebnis
i. R. d.	im Rahmen der/des
i. S. d.	im Sinne der/des
i. V. m.	in Verbindung mit
IAPP	International Association of Privacy Professionals
ICO	Information Commissioner's Office

Ill. Comp. Stat	Illinois Compiled Statutes
Inc.	Incorporated
Ind. L. Rev.	Indiana Law Review
Ind. L. J. Supp.	Indiana Law Journal Supplement
Inf. Commun. Soc.	Information Communication & Society
International Data Privacy Law	International Data Privacy Law
Internet World Business	Internet World Business
Iowa L. Rev.	Iowa Law Review
IP	Internet Protocol
IPTJL	Intellectual Property & Technology Law Journal
ISJLP	I/S: A Journal of Law and Policy for the Information Society
ITRB	IT-Rechts-Berater
J. Tech. L. & Pol'y	Journal of Technology Law & Policy
JDPP	Journal of Data Protection & Privacy
JI-RL	Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates
JZ	JuristenZeitung
KG	Kammergericht
Klausel-RL	Richtlinie 93/13/EWG des Rates vom 5. April 1993 über mißbräuchliche Klauseln in Verbraucherverträgen
Law & Contemp. Probs.	Law and Contemporary Problems
Law Libr. J.	Law Library Journal
LDI NRW	Landesbeauftragte für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen
Leg., Reg. Sess.	Legislative, Regular Session
LEXIS	LexisNexis
LfD Niedersachsen	Landesbeauftragte für den Datenschutz Niedersachsen
LfD Sachsen-Anhalt	Landesbeauftragter für den Datenschutz Sachsen-Anhalt
LfDI Bremen	Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen
LfDI Rheinland-Pfalz	Landesbeauftragter für Datenschutz und Informationsfreiheit Rheinland-Pfalz
LfDI Saarland	Landesbeauftragte für Datenschutz und Informationsfreiheit Saarland
lit.	littera(e)
LLC	Limited liability company
Loy. Consumer L. Rev.	Loyola Consumer Law Review
Loy. L. A. L. Rev.	Loyola of Los Angeles Law Review
m. w. N.	mit weiteren Nachweisen
Mass. Code Regs.	Code of Massachusetts Regulations
Md. Code Ann. Com. Law	Maryland Code Annotated Commercial Law
Md. L. Rev.	Maryland Law Review

Medienstaatsvertrag HSH	Staatsvertrag über das Medienrecht in Hamburg und Schleswig-Holstein
MedR	Medizinrecht
Mich. L. Rev.	Michigan Law Review
Mich. Tech. L. Rev.	Michigan Technology Law Review
Mich. Telecomm. & Tech. L. Rev.	Michigan Telecommunications and Technology Law Review
Minn. L. Rev.	Minnesota Law Review
MIS Quarterly	Management Information Systems Quarterly
MITSloan	MIT Sloan Managment Review
MMR	Multimedia und Recht
MMR-Beil.	Multimedia und Recht-Beilage
MOModStV	Staatsvertrag zur Modernisierung der Medienordnung in Deutschland
N. C. Banking Inst.	North Carolina Banking Institute
N. D. L. Rev.	North Dakota Law Review
N. Y.	New York Reports
N. Y. Gen. Bus	New York General Business Law
N. Y. Times	New York Times
N. Y. U. Ann. Surv. Am. L.	New York University Annual Survey of American Law
N. Y. U. J. Legis. & Pub. Pol'y	New York University journal of legislation and public policy
N. Y. U. L. Rev.	New York University Law Review
NJW	Neue Juristische Wochenschrift
Notre Dame L. Rev.	Notre Dame Law Review
NVwZ	Neue Zeitschrift für Verwaltungsrecht
Nw. U. L. Rev.	Northwestern University Law Review
NZA	Neue Zeitschrift für Arbeitsrecht
NZG	Neue Zeitschrift für Gesellschaftsrecht
NZKart	Neue Zeitschrift für Kartellrecht
NZM	Neue Zeitschrift für Miet- und Wohnungsrecht
o. Bgr.	ohne Begründung
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OGH	Oberster Gerichtshof
OLG	Oberlandesgericht
Or. L. Rev.	Oregon Law Review
OVG	Oberverwaltungsgericht
Pace Int'l L. Rev.	Pace International Law Review
Pace L. Rev.	Pace Law Review
Pepp. L. Rev.	Pepperdine Law Review
PinG	Privacy in Germany
PwC	Pricewaterhouse Coopers
Quinnipiac Health L. J.	Quinnipiac Health Law Journal
RabelsZ	Rabels Zeitschrift für ausländisches und internationales Privatrecht
RDV	Recht der Datenverarbeitung
Rich. J.L. & Tech.	Richmond Journal of Law & Technology
RIS-Justiz	Rechtssatznummer des österreichischen Rechtsinformatiksystem des Bundes: Judikatur

Rn.	Randnummer
S. Cal. L. Rev.	Southern California Law Review
S.B.	Senate Bill
S.Ct.	Supreme Court Reporter
SächsDSB	Sächsische Datenschutzbeauftragte
Santa Clara High Tech. L. J.	Santa Clara High Technology Law Journal
Seton Hall L. Rev.	Seton Hall Law Review
SMU L. Rev..	SMU Law Review
St. John's L. Rev.	St. John's Law Review
st. Rspr.	ständige Rechtsprechung
StGB	Strafgesetzbuch
Stan. Envtl. L. J.	Stanford Environmental Law Journal
Stan. L. Rev.	Stanford Law Review
Stan. L. Rev. Online	Stanford Law Review Online
Stan. Tech. L. Rev.	Stanford Technology Law Review
Stat.	United States Statutes at Large
StBerG	Steuerberatungsgesetz
StPO	Strafprozeßordnung
Suffolk J. Trial & App. Advoc.	Suffolk Journal of Trial & Appellate Advocacy
Suffolk U. L. Rev.	Suffolk University Law Review
Sup. Ct. Rev.	Supreme Court Review
TCPA	Telephone Consumer Protection Act of 1991
TechReg	Technology and Regulation
Tex.B.J.	Texas Bar Journal
Tex. Bus. & Com. Code Ann.	Texas Business and Commerce Code Annotated (West)
Tex. L. Rev.	Texas Law Review
TKG	Telekommunikationsgesetz
Touro L. Rev.	Touro Law Review
U. Chi. L. Rev.	University of Chicago Law Review
U. Cin. L. Rev.	University of Cincinnati Law Review
U. Dayton L. Rev.	University of Dayton Law Review
U. III. J. L. Tech & Pol'y	University of Illinois Journal of Law Technology & Policy
U. Ill. L. Rev.	University of Illinois Law Review
U. Ill. L. Rev. Online	University of Illinois Law Review Online
U. Pa. L. Rev.	University of Pennsylvania Law Review
U.C. Davis L. Rev.	University of California at Davis Law Review
U.C. Irvine L. Rev.	University of California, Irvine Law Review
U. S.	United States of America/bei Entscheidungen des U. S. Supreme Court: United States Reports
U. S. C.	United States Code
U. S. Const.	Constitution of the United States
U. S. District Court C. D. Cal.	United States District Court for the Central District of California
U. S. District Court N. D. Cal.	United States District Court for the Northern District of California
U. S. District Court N. D. Ga.	United States District Court for the Northern District of Georgia
U. S. District Court S. D. Cal.	United States District Court for the Southern District of California

U. S. District Court W. D. Tex.	United States District Court for the Western District of Texas
U. S. Supreme Court	Supreme Court of the United States
UAbs.	Unterabsatz
UC Irvine L. Rev.	UC Irvine Law Review
UCL	California Unfair Competition Law
UCLA L. Rev.	UCLA Law Review
UK	Vereinigtes Königreich Großbritannien und Nordirland
UKlaG	Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen
Va. Code Ann.	Code of Virginia 1950 Annotated
Va. L. Rev.	Virginia Law Review
Vand. L. Rev.	Vanderbilt Law Review
Verbandsklagen-RL	Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher und zur Aufhebung der Richtlinie 2009/22/EG
Verbraucherrechte-RL	Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG des Rates und der Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 85/577/EWG des Rates und der Richtlinie 97/7/EG des Europäischen Parlaments und des Rates
vorgänge	vorgänge, Zeitschrift für Bürgerrechte und Gesellschaftspolitik
Vt. Stat. Ann. tit.	Vermont Statutes Annotated Title
VuR	Verbraucher und Recht
Wash. J. L. Tech. & Arts	Washington Journal of Law, Technology & Arts
Wash. L. Rev.	Washington Law Review
Wash. Rev. Code	Revised Code of Washington
Wash. U. L. Rev.	Washington University Law Review
Werbe-RL	Richtlinie 2006/114/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über irreführende und vergleichende Werbung
Wis. L. Rev.	Wisconsin Law Review
Wm. & Mary Bus. L. Rev.	William and Mary Business Law Review
Wm. & Mary L. Rev.	William & Mary Law Review
Yale J. L. & Tech.	Yale Journal of Law & Technology
Yale J. on Reg.	Yale Journal on Regulation
Yale L. J.	Yale Law Journal
ZaöRV	Zeitschrift für ausländisches öffentliches Recht und Völkerrecht
ZD	Zeitschrift für Datenschutz
ZEuP	Zeitschrift für Europäisches Privatrecht
ZfA	Zeitschrift für Arbeitsrecht
ZfPW	Zeitschrift für die gesamte Privatrechtswissenschaft
ZHR	Zeitschrift für das Gesamte Handels- und Wirtschaftsrecht
ZPO	Zivilprozessordnung
ZUM	Zeitschrift für Urheber- und Medienrecht

Kapitel 1

Einführung

A. Das erste umfassende Datenschutzgesetz der Vereinigten Staaten

»It is one of the happy accidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory, and try novel social and economic experiments without risk to the rest of the country«

Louis Brandeis, Justice of the U. S. Supreme Court[1]

Das progressive Kalifornien ist in der Internetwirtschaft weltweit führend. Das Bruttoinlandsprodukt des bevölkerungsreichsten und wirtschaftlich stärksten U. S. Bundesstaats Kalifornien wäre für sich genommen das fünftgrößte der Welt.[2] Als Staat des Silicon Valley ist Kalifornien Heimat einiger der größten Technologieunternehmen, die globale Datenströme verwalten. Kalifornien hatte von Anfang versucht, die Gefahren durch massenhafte Datenverarbeitung einzuhegen. So hatte Kalifornien bereits 1972 ein Recht auf Privatsphäre in seine Verfassung aufgenommen und darauf folgend eine dreistellige Anzahl an bereichsspezifischen Datenschutzgesetzen erlassen.[3] Im Zuge des Facebook-Cambridge-Analytica-Skandals Anfang 2018 hat sich die Sorge vor einem Kontrollverlust über die eigenen persönlichen Informationen aber noch massiv verstärkt.

In diesem Klima beschloss Kalifornien das erste umfassende amerikanische Datenschutzgesetz. Das kalifornische Parlament hat im Juni 2018 das Volksbegehren California Consumer Privacy Act (CCPA) unter demselben Namen nahezu unverändert einstimmig angenommen.[4] Im November 2020 hat das kalifornische Volk aufgrund eines zweiten Volksbegehrens der gleichen Bürgerinitiative den CCPA zudem bestätigt und deutlich erweitert. Im weltweit ersten

---

[1] U. S. Supreme Court vom 21.03.1932, *New State Ice Co. v. Liebmann* – ablehnendes Sondervotum *Brandeis*, 285 U. S. 262, 311. Der *topos* von Staaten als Demokratielaboren ist inzwischen st. Rspr. geworden, zuletzt: U. S. Supreme Court vom 23.06.2016, *Fisher v. Univ. of Tex.*, 136 S. Ct. 2198, 2214.

[2] *Fuller*, N. Y. Times, The Pleasure and Pain of Being California, the World's 5th-Largest Economy.

[3] Zur kalifornischen Verfassung siehe Kapitel 2:A.II (ab S. 15) und zum kalifornischen Datenschutzrecht siehe Kapitel 2:B.II (ab S. 27).

[4] Näher zur Gesetzgebungsgeschichte siehe Kapitel 2:C (ab S. 30).

Volksentscheid über ein umfassendes Datenschutzgesetz erzielte der so gestärkte CCPA eine deutliche Mehrheit von 56,2 %.[5] Erklärtes Ziel war es, Verbraucher:innen[6] mehr Kontrolle über ihre persönlichen Informationen zu ermöglichen und sie mithin zu befähigen, großen Technologieunternehmen auf Augenhöhe zu begegnen.[7] So beschloss Kalifornien als erster amerikanischer[8] Bundesstaat ein umfassendes Datenschutzgesetz und setzte so *Louis Brandeis'* Vision von Staaten als Demokratielaboren um.

Als erstes umfassendes Datenschutzgesetz der Vereinigten Staaten wird der CCPA zwangsläufig die amerikanische und weltweite Entwicklung des Datenschutzes beeinflussen. Dies ist besonders für Europa relevant, das bereits über ein umfangreiches Datenschutzrecht verfügt und im vielfältigen Austausch mit den Vereinigten Staaten steht. Das politisch progressive Kalifornien steht Europa sogar noch einmal näher als die restlichen Vereinigten Staaten. Kaliforniens Technologieunternehmen wie Google, Apple oder Meta (früher: Facebook) prägen aufgrund ihrer herausragenden Stellung in der Internetwirtschaft auch den europäischen Datenschutz. So betreffen zahlreiche EuGH-Entscheidungen zum Datenschutz kalifornische Konzerne,[9] und das Modell eines »rücksichtslosen kalifornischen Datenkapitalismus«[10] gilt als zentrale Herausforderung der DSGVO. Eine Reform des heimatlichen Rechts der kalifornischen Technologieunternehmen wird auch deren Einstellung zum Datenschutz weltweit beeinflussen. Umgekehrt müssen auch europäische Unternehmen den CCPA einhalten, wenn sie in Kalifornien tätig sind.[11]

In der deutschen rechtswissenschaftlichen und rechtspolitischen Debatte spielt der CCPA bisher allerdings kaum eine Rolle. Der CCPA wird vor allem verniedlichend als »Mini-DSGVO« eingeordnet,[12] während die DSGVO prätentiös

---

[5] *Cal. Secretary of State*, Statement of Vote: General Election November 3, 2020, S. 66.

[6] Zum Verbraucher:innen-Begriff siehe Kapitel 3:B.II.1 (ab S. 56). Diese Arbeit verwendet geschlechtergerechte Sprache – wie der CCPA selbst, vgl. die Grundsatzentscheidung des kalifornischen Parlaments in ACR 260, 2017–18 Leg., Reg. Sess. (Cal. 2018). Ämter stehen im Genus der jeweils aktuellen Amtsinhaber:innen. Der Gesetzeswortlaut ist vorrangig.

[7] Proposition 24 (Cal. 2020), Sec. 2(H).

[8] Das Adjektiv »amerikanisch« ist gegenüber »US-amerikanisch« vorzugswürdig, weil es kürzer ist und zugleich stets klar ist, wann die Vereinigten Staaten gemeint sind. Dies entspricht auch: *Auswärtiges Amt*, Verzeichnis der Staatennamen für amtlichen Gebrauch, S. 9.

[9] EuGH vom 13.05.2014 – C-131/12, *Google Spain*, ECLI:EU:C:2014:317; vom 06.10.2015 – C-362/14, *Schrems I*, ECLI:EU:C:2015:650; vom 05.06.2018 – C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388; vom 29.07.2019 – C40/17, *Fashion ID, ECLI:EU:C:2019:629*; vom 24.09.2019 – C-507/17, *Google gegen CNIL*, ECLI:EU:C:2019:772; vom 16.07.2020 – C311/18, *Schrems II*, ECLI:EU:C:2020:559; vom 15.06.2021 – C645/19, *Facebook Ireland Limited u. a. gegen Gegevensbeschermingsautoriteit*, ECLI:EU:C:2021:483.

[10] *Roßnagel/Geminn*, Datenschutz-Grundverordnung verbessern, S. 5.

[11] Zu dem räumlichen Anwendungsbereich des CCPA siehe Kapitel 3:B.III (ab S. 71).

[12] *Oberlin*, BvD-NEWS 2/2019, 47, 47; *Salzmann/Schindler*, ZD-Aktuell 06293; *Spies*, ZD-Aktuell 2018, 04318. Ähnlich: *Gemsa*, Internet World Business 14/2018, 22: abgeschwächte Kopie; *Weichert*, DuD 2020, 293, 294: DSGVO habe »Pate« gestanden. Aus amerikanischer

als der weltweite »Goldstandard« bezeichnet wird.[13] Rechtsvergleichende Arbeiten existieren nur in Aufsatzform.[14] Umgekehrt rezipieren amerikanische Rechtswissenschaftler:innen die DSGVO vielfach, wobei aber auch jenseits des Atlantiks eine über den Detailgrad eines Aufsatzes hinausgehende rechtsvergleichende Arbeit fehlt.[15] Vielfach beschreiben amerikanische Aufsätze die DSGVO als *opt-in*-Gesetz, das eine aktive Einwilligung in Datenverarbeitungen fordere, während der CCPA ein *opt-out*-Gesetz sei, der nur ein aktiv auszuübendes Widerspruchsrecht kenne.[16] Die beiden Charakterisierungen als »Mini-DSGVO« oder als *opt-out*-Gesetz widersprechen sich fundamental, sodass sie einer Klärung zugeführt werden sollten.

B. Abgrenzung der Fragestellung

Somit ist naheliegend, den CCPA umfassend zu analysieren. Dabei stellt die Arbeit den Inhalt des CCPA und dessen Durchführungsverordnung vollständig dar, ordnet diesen im amerikanischen Recht ein und untersucht, warum welche Regelungsalternative ergriffen wurde und wie sich der CCPA in der Rechtspraxis auswirkt. Das sonstige amerikanische Verfassungs- und Datenschutzrecht interessiert die Arbeit dagegen nur, soweit es zum Verständnis und zur Einordnung des CCPA erforderlich ist.[17]

Die Arbeit untersucht den CCPA in der durch Proposition 24 geschaffenen Fassung, auch wenn diese erst am 01.01.2023 in Kraft tritt[18] (der CCPA-2018 war

---

Perspektive den CCPA-2018 als »Mini GDPR« beschreibend: *Davis*, 24 N.C. Banking Inst. 499, 516; *Khoury*, Gordon & Rees Scully Mansukhani, California's Mini-GDPR?

[13] *Europäische Kommission*, Data Protection Day 2014: Full Speed on EU Data Protection Reform, MEMO/14/60; *dies.*, Datenschutztag: Europäische Datenschutzregeln sind Goldstandard. Diesen *topos* hat wohl ursprünglich das U. S. Department of Commerce für die Safe-Harbor-Prinzipien geprägt, vgl. zur Begriffsgeschichte *Linxweiler*, rescriptum 2012, 28, 29 f.

[14] Überblicksweise zum gesamten CCPA: *Botta*, PinG 2019, 261–266; *Determann*, ZD 2018, 443–448; *ders.*, ZD 2021, 69–74; *Hoeren/Pinelli*, MMR 2018, 711–716; *Hense/Fischer*, DSB 2019, 26 f.; *Oberlin*, BvD-NEWS 2/2019, 47–53; *Lejeune*, CR 2018, 569–576; *ders.*, ITRB 2021, 13–19; *ders.*, PinG 2021, 25–17. Speziell zum Widerspruchsrecht gegen Datenhandel: *Halim/Klee*, CCZ 2021, 300–305; *Schröder*, DSB 2021, 15–17.

[15] Über eine bloße Gegenüberstellung gehen hinaus: *Chander/Kaminski/McGeveran*, 105 Minn. L. Rev. 1733, 1746–1762; *Marini et al.*, Comparing privacy laws: GDPR v. CCPA, passim; *Kessler*, 93 S. Cal. L. Rev. 99, 103–115; *Park*, 10 UC Irvine L. Rev. 1455, 1473–1489.

[16] *Alexander*, 32 Loy. Consumer L. Rev. 199, 231; *Cahill et al.*, 30 IPTJL 11, 16; *Jazzar*, 70 Case W. Res. L. Rev. 457, 481 f.; *Park*, 10 UC Irvine L. Rev. 1455, 1473–1479; *Resnick*, 46 Brook. J. Int'l L. 277, 298–302.

[17] Eine umfassende Darstellung des amerikanischen Datenschutzrechts findet sich in: *Solove/Schwartz*, Information privacy law, passim. Siehe auch die weiterführenden Fußnoten in Kapitel 2.

[18] Proposition 24 (Cal. 2020), Sec. 31(a).

am 01.01.2020 in Kraft getreten).[19] Proposition 24 ist die logische Fortsetzung des CCPA-2018, welche von der gleichen Bürgerinitiative stammt und zahlreiche Redaktionsfehler des CCPA-2018 korrigiert.[20] Es ist nicht zielführend, sich lange mit Unklarheiten des CCPA-2018 aufzuhalten, der in wenigen Monaten ohnehin außer Kraft treten wird. Bei größeren Änderungen durch Proposition 24 weist der Text allerdings kurz auf die bisherige Rechtslage hin. Ebenfalls bildet die Arbeit den von Proposition 24 vorgesehenen Mindestinhalt der zukünftig zu erweiternden Durchführungsverordnung ab.[21]

Als Vergleichsmaßstab dient das europäische Datenschutzrecht, das angesichts der weltweiten Datenströme häufig ähnliche Probleme und Unternehmen reguliert. Das europäische Datenschutzrecht ist zudem weit entwickelt und global einflussreich, sodass es sich besonders als Vergleichsmaßstab anbietet. Dabei werden DSGVO und BDSG nur knapp dargestellt, da bereits zahlreiche Kommentare, Aufsätze und andere Literatur über deren Auslegungsfragen existieren.[22] Eine allgemeine Abhandlung über die DSGVO würde daher den Rahmen sprengen und hätte begrenzten wissenschaftlichen Wert. Deshalb werden Auslegungsfragen nur insoweit vertieft, als dies für die Rechtsvergleichung bedeutsam ist. Außerhalb des europaweit vereinheitlichen Rechts liegt zur Vereinfachung der Fokus auf dem deutschen Datenschutz- und Datenschuldrecht. Dieses ist angesichts der verhältnismäßig guten Ausstattung der deutschen Aufsichtsbehörden[23] in Europa führend und liegt auch als Heimatrecht des Verfassers nahe. Soweit für die Auslegung der DSGVO bedeutsam, wird aber auch die Anwendung der DSGVO in anderen Mitgliedsstaaten berücksichtigt.

Dieser Vergleich ermöglicht es zu beantworten, inwieweit Kalifornien ein angemessenes Datenschutzniveau gemäß Art. 45 Abs. 1 S. 1 DSGVO erreicht. Angesichts des jahrzehntelangen transatlantischen Austausches im Datenschutzrecht ist es zudem naheliegend zu fragen, inwieweit der europäische Gesetzgeber das kalifornische Recht zum Vorbild nehmen soll.

C. Untersuchungsmethode

Zur Beantwortung dieser Fragen ist die funktionale Rechtsvergleichung das Mittel der Wahl. Dieser Methode liegt das offene und flexibele Prinzip zugrunde,

---

[19] Cal. Civ. Code § 1798.198(a).

[20] Siehe Kapitel 2:C.IV (ab S. 35).

[21] Cal. Civ. Code § 1798.185.

[22] Der Katalog der Deutschen Nationalbibliothek weist z. B. derzeit 992 Treffer für »DSGVO« aus.

[23] *Europäische Kommission*, Commission Staff Working Document: two years of application of GDPR, SWD/2020/115 final, Nr. 2.4: das Gesamtbudget der deutschen Aufsichtsbehörden liege in etwa so hoch wie das Budget der vier nächstgrößeren Aufsichtsbehörden zusammen (Italien, Niederlande, Frankreich und Irland).

das fremde Recht wertungsfrei und losgelöst von den heimatlichen Konzeptionen darzustellen und anschließend anhand funktionaler Äquivalente mit dem heimatlichen Recht qualitativ zu vergleichen.[24] *Kischel* nennt diese Methode zutreffend auch »kontextuale Rechtsvergleichung«, da sie sämtliche Hintergründe des jeweiligen Rechts berücksichtigt.[25] Gerade die fehlende Festlegung auf ein starres Modell ermöglicht es, grundlegende Unterschiede und Gemeinsamkeiten herauszuarbeiten und deren Gründe zu erkennen.[26]

Quantitative Methoden wie die statistische Rechtsvergleichung sind für die Fragestellung nicht geeignet. Zwar haben diese Methoden den Vorteil einer Vereinfachung und bis zu einem gewissen Grad auch einer Objektivierung, der sich besonders bei Massenvergleichen zwischen zahlreichen verschiedenen Rechten positiv auswirkt.[27] Bei einem Einzelvergleich wie der vorliegenden Fragestellung ist allerdings ein qualitativer Vergleich besser geeignet, um die komplexen und vielschichtigen Hintergründe des jeweiligen Rechtes zu ergründen.[28]

Für eine umfassende Analyse des CCPA wertet die Arbeit die amerikanische Literatur, Stellungnahmen der kalifornischen Aufsichtsbehörden und soweit vorhanden auch die Rechtsprechung zum CCPA aus. Dies schließt auch Praxiswerke und Blog-Beiträge ein, um auch einen Einblick in das *law in action* zu erlangen,[29] zumal sich in den Vereinigten Staaten auch anerkannte Rechtswissenschaftler:innen häufig in Blog-Beiträgen zu aktuellen Auslegungsfragen äußern.[30] Die Zitierweise der Arbeit folgt grundsätzlich den in Deutschland üblichen Regeln, um für deutsche Leser:innen verständlich zu bleiben. Nur die Angabe der Fundstelle folgt bei Gesetzen, Rechtsprechung und Aufsätzen dem amerikanischen System,[31] da amerikanische Datenbanken nur diese akzeptieren.

---

[24] Grundlegend: *Zweigert/Kötz*, Einführung in die Rechtsvergleichung, S. 31–47.

[25] *Kischel*, Rechtsvergleichung, § 3 Rn. 199–201.

[26] *Kischel*, Rechtsvergleichung, § 3 Rn. 201; *Michaels* in: Reimann/Zimmermann, The Oxford Handbook of Comparative Law, 339, 362, 364–366; *Zweigert/Kötz*, Einführung in die Rechtsvergleichung, S. 42 f.

[27] *Schreiner*, Die Vermessung des Mietrechts, S. 33; *Siems*, RabelsZ (72) 2008, 354, 383; *Vagts* in: Schweizer/Druey, FS Druey, 595, 604. Vgl. *Porta et al.*, 106 Journal of Political Economy 1113, 1117: mittels statistischer Rechtsvergleichung seien 49 Länder vergleichbar, während bisherige Studien in der Regel nur zwei Länder verglichen hätten.

[28] *Siems*, RabelsZ (72) 2008, 354, 371–373; *Kischel*, Rechtsvergleichung, § 3 Rn. 121.

[29] Gegen eine Beschränkung des Quellenmaterials bei der Rechtsvergleichung: *Kischel*, Rechtsvergleichung, § 3 Rn. 261; *Zweigert/Kötz*, Einführung in die Rechtsvergleichung, S. 33 f.

[30] *Keslowitz*, 2009 Cardozo L. Rev. De Novo 252, 257–271; *Solum*, 84 Wash. U. L. Rev. 1071, 1072 f.

[31] Niedergelegt in *Columbia Law Review et al.*, The Bluebook, passim.

D. Ausblick auf die folgende Untersuchung

Aus der Wahl einer funktionalen, kontextualen Rechtsvergleichung ergibt sich, dass zuerst der Hintergrund des CCPA zu ermitteln ist (Kapitel 2). Dabei wird erläutert, inwieweit die amerikanische und die kalifornische Verfassung die Privatsphäre schützen und Datenschutzgesetze ermöglichen oder verhindern (A). Anschließend gilt es, das sonstige amerikanische Datenschutzrecht zu analysieren (B). Dieses bildet den Kontext der Gesetzgebungsgeschichte des CCPA (C).

Den Kern der Arbeit bildet die Analyse des CCPA und dessen Vergleich mit dem europäischen Datenschutzrecht (Kapitel 3). Die Rechtsvergleichung ist als verzahnter Vergleich gestaltet, der von den Rechtskonzepten des CCPA ausgeht. Das Kapitel bildet den Inhalt des CCPA und dessen Durchführungsverordnung vollständig ab. Dabei wird nach einer kurzen Darstellung des Aufbaus des CCPA (A) zuerst dessen Anwendungsbereich analysiert und verglichen (B). Einen Schwerpunkt bildet die Untersuchung der umfangreichen und detailliert geregelten Verbraucherrechte des CCPA (C). Geringer ausgeprägt ist die Regelung der Unternehmenspflichten, die dementsprechend auch weniger Raum einnimmt (D). Anschließend werden Privatklagerecht und die verschiedenen Aufsichtsbehörden des CCPA behandelt und verglichen (E). Schließlich führt ein Fazit übergreifende Gedanken zusammen (F).

Aufbauend auf diesem Rechtsvergleich werden zwei Folgefragen geprüft (Kapitel 4). Erreicht Kalifornien mit dem CCPA ein angemessenes Datenschutzniveau nach Art. 45 Abs. 1 S. 1 DSGVO (A)? Sollte sich die EU an der umfangreichen Sonderregelung für finanzielle Anreize zur Bereitstellung persönlicher Informationen orientieren und so das stark umstrittene Geschäftsmodell »Leistung gegen Daten« regulieren (B)?

Die Untersuchung rundet ein Fazit ab (Kapitel 5), das Kapitel 2–4 knapp zusammenfasst (A) und anschließend einen Ausblick auf die weitere Entwicklung des Datenschutzrechts in den Vereinigten Staaten bietet (B).

Kapitel 2

Hintergrund und Gesetzgebungsgeschichte

A. Verfassungsrechtlicher Hintergrund

I. Constitution of the United States

1. Eingeschränkter Schutz der Privatsphäre

Die U. S. Constitution kennt kein explizites Recht auf Privatsphäre. Der U. S. Supreme Court leitet aus ihr nur einen ungeschriebenen, schwachen Schutz der Privatsphäre ab.[1] In *Griswold v. Connecticut* (1965) entwickelte er erstmals aus der Gesamtheit des *First, Fourth, Fifth* und *Fourteenth Amendment* ein begrenztes *right to privacy:* die Grundrechte in diesen *Amendments* strahlten so hell, dass ihr Licht auch nicht explizit genannte ähnliche Rechte erfasse.[2] Das streitgegenständliche einzelstaatliche Verbot von Empfängnisverhütung verstoße gegen dieses *right to privacy,* da es den privaten Bereich der Ehe verletze.[3] Später hat er aus dem *right to privacy* in *Lawrence v. Texas* (2003)[4] die Straflosigkeit der Sodomie und in *Obergefell v. Hodges* (2015)[5] das Recht zu gleichgeschlechtlicher Ehe entwickelt. Damit wird deutlich, dass unter dem Schlagwort *right to privacy* in den Vereinigten Staaten damals wie heute auch der Schutz der Selbstbestimmung in privaten Angelegenheiten diskutiert wird[6] (die prominenteste Ausprägung des *right to privacy* als Selbstbestimmung – das Recht auf Schwangerschaftsabbruch – hat der U. S. Supreme Court allerdings wieder aufgehoben[7]).

---

[1] *Cate/Litan*, 9 Mich. Telecomm. & Tech. L. Rev. 35, 39–42; *Ursul*, 52 Suffolk U. L. Rev. 577, 581.

[2] U. S. Supreme Court vom 07.06.1965, *Griswold v. Connecticut*, 381 U. S. 479, 483–485; Umfassend zu dieser Metapher: *Henly*, 15 Hastings Const. L.Q. 81–100.

[3] U. S. Supreme Court vom 07.06.1965, *Griswold v. Connecticut*, 381 U. S. 479, 485 f.

[4] U. S. Supreme Court vom 26.06.2003, *Lawrence v. Texas*, 539 U. S. 558 562–579.

[5] U. S. Supreme Court vom 26.06.2015, *Obergefell v. Hodges*, 576 U. S. 644, 665.

[6] Diese Unterscheidung andeutend: U. S. Supreme Court vom 22.07.1977, *Whalen v. Roe*, 429 U. S. 589, 598–600. Dies ist nicht mit dem deutschen Konzept der allgemeinen Handlungsfreiheit gem. Art. 2 Abs. 1 GG zu verwechseln. Das *right to privacy* ist vielfach schon auf Schutzbereichsebene eingeschränkt. Zur Handlungsfreiheit als Unterfall des *right to privacy*: *Solove*, 154 U. Pa. L. Rev. 477, 557–562.

[7] U. S. Supreme Court vom 22.01.1973, *Roe v. Wade*, 410 U. S. 113, 152–164 aufgehoben durch U. S. Supreme Court vom 24.06.2022, *Dobbs v. Jackson Women's Health Org.*, 2022 U. S. LEXIS 3057, 17–110.

Das *Fourth Amendment* schützt die Privatsphäre am umfassendsten von allen Grundrechten der *Bill of Rights* in der U. S. Constitution.[8] Es gewährt zwar ebenfalls kein umfassendes Recht auf Privatsphäre.[9] Es schützt aber die Privatsphäre gegenüber dem Staat indirekt auf zwei Weisen: Erstens dürfen die Behörden eine *search* (Durchsuchung) nur durchführen, wenn dies objektiv erforderlich ist (insbesondere bei hinreichendem Tatverdacht hinsichtlich einer Straftat).[10] Zweitens muss ein Richter die *search* anordnen.[11] Diese beiden Hürden für *searches* sollen die Privatsphäre des Individuums gegen willkürliche behördliche Entscheidungen schützen[12] und einen Überwachungsstaat verhindern.[13] Das Fourth Amendment erfasst daher auch staatliche Überwachung außerhalb von Strafverfahren.[14]

Search ist nicht nur als Wohnungsdurchsuchung zu verstehen. Vielmehr erfasst dieser Begriff auch eine Vielzahl anderer staatlicher Überwachungsmaßnahmen (»The Fourth Amendment protects people, not places«).[15] Der U. S. Supreme Court hat den zweistufigen *Katz*-Test für das Vorliegen einer *search* entwickelt.[16] Auf der ersten Stufe fragt er, ob das betroffene Individuum subjektiv Privatheit erwartet hatte.[17] Auf der zweiten Stufe prüft er, ob die staatliche Überwachung auch objektiv für die Mehrheit der Gesellschaft in ihre berechtigte Privatheitserwartung eingreifen würde *(reasonable expectation of privacy)*.[18] So erwarte man beispielsweise Privatheit subjektiv wie objektiv, wenn man sich in der eigenen Wohnung mit seiner Familie unterhält.[19] Hingegen könne

---

[8] *Blanke*, 2018 U. Ill. L. Rev. Online 260, 264; *Cate/Litan*, 9 Mich. Telecomm. & Tech. L. Rev. 35, 42.

[9] U. S. Supreme Court vom 18.12.1967, *Katz v. United States*, 389 U. S. 347, 350 f.

[10] U. S. Const. amend. IV.

[11] U. S. Const. amend. IV.

[12] U. S. Supreme Court vom 27.06.1948, *Wolf. v. Colo.*, 338 U. S. 25, 27: »The security of one's privacy against arbitrary intrusion by the police – which is at the core of the Fourth Amendment«; vom 05.06.1967, *Camara v. Municipal Court of the City and County of San Francisco*, 387 U. S. 523, 528; vom 22.06.2018, *Carpenter v. United States*, 138 S.Ct. 2206, 2213.

[13] U. S. Supreme Court vom 22.06.2018, *Carpenter v. United States*, 138 S.Ct. 2206, 2213.

[14] U. S. Court of Appeals 4th Circuit vom 23.05.2017, *Wikimedia Found. v. NSA/Central Sec. Serv.*, 857 F.3d 193, 209 f.

[15] U. S. Supreme Court vom 18.12.1967, *Katz v. United States*, 389 U. S. 347, 351; vom 20.06.1979, *Smith v. Md., 442 U. S. 735*, 739; vom 23.01.2012, *United States v. Jones*, 565 U. S. 400, 406.

[16] Grundlegend: U. S. Supreme Court vom 18.12.1967, *Katz v. United States* – zustimmendes Sondervotum *Harlan*, 389 U. S. 347, 361.

[17] U. S. Supreme Court vom 18.12.1967, *Katz v. United States*, 389 U. S. 347, 351. Diese Stufe spielt nur eine minimale Rolle, da subjektive Erwartungen nur schwer im Nachhinein festgestellt werden können: *Blanke*, 2018 U. Ill. L. Rev. Online 260, 264; *Kerr*, 82 U. Chi. L. Rev. 113–134; *Ohm*, 32 Harv. J.L. & Tech. 357, 361 f.

[18] U. S. Supreme Court vom 18.12.1967, *Katz v. United States*, 389 U. S. 347, 351. Kritisch dazu, dass der U. S. Supreme Court dazu keinerlei Studien berücksichtigt, sondern die Privatheitserwartung selbst würdigt: *Tokson*, 88 Geo. Wash. L. Rev. 1, 27–30.

[19] U. S. Supreme Court vom 18.12.1967, *Katz v. United States* – zustimmendes Sondervotum *Harlan*, 389 U. S. 347, 361.

man bei Unterhaltungen auf öffentlichen Plätzen in der Regel objektiv keine Privatheit erwarten.[20] In öffentlichen Telefonzellen sei daher ein gezieltes Abhören durch die Polizei ohne richterliche Anordnung zulässig.[21] Zudem bestehe keine berechtigte Erwartung von Privatheit bei an Dritten weitergegebenen Informationen *(third party doctrin)*.[22] Diese seien weniger sensibel, weil der Betroffene sie bewusst aus der Hand gibt.[23]

In *Jones v. United States* (2012) und *Carpenter v. United States* (2018) hat der U. S. Supreme Court den *Katz*-Test für elektronische Überwachung weiterentwickelt.[24] Hiernach prüft er anhand einer Gesamtbetrachtung dreier Kriterien, wann staatliche Überwachung in das *Fourth Amendment* eingreift. Erstens berücksichtigt er, wie sensibel die betroffenen Daten sind (»the deeply revealing nature«).[25] Zweitens prüft er die Eingriffsintensität der Überwachung (»depth, breadth, and comprehensive reach«).[26] Drittes Kriterium ist die Eignung zu einer Massenüberwachung (»automatic nature of its collection«).[27] Dieser Prüfungsmaßstab ist explizit auf die moderne elektronische Überwachung zugeschnitten.[28] Darin zeigt sich, dass der U. S. Supreme Court durchaus die Gefahren für die Privatsphäre durch massenhafte digitale Datenverarbeitung sieht.[29]

Auch andere Grundrechte schützen indirekt die Privatsphäre. Das *First Amendment*, das die Meinungsfreiheit regelt, schützt auch das Recht auf anonyme Meinungsäußerung.[30] Das *Third Amendment* verbietet die Einquartierung von Soldaten ohne gesetzliche Grundlage und schützt so die Privatheit der Wohnung.[31] Schließlich hat der Supreme Court schon in *Whalen v. Roe* (1977) angedacht, dass das *Fourteenth Amendment* gegen elektronische Massenüberwachung schützen könnte – wenngleich er diesen Gedanken kaum weiter entwickelt hat.[32]

---

[20] U. S. Supreme Court vom 18.12.1967, *Katz v. United States* – zustimmendes Sondervotum *Harlan*, 389 U. S. 347, 361.

[21] U. S. Supreme Court vom 18.12.1967, *Katz v. United States*, 389 U. S. 347, 349–360; ebenso: zustimmendes Sondervotum *Harlan*, 389 U. S. 347, 361 f.

[22] U. S. Supreme Court vom 20.06.1979, *Smith v. Md.*, 442 U. S. 735, 743–746; U. S. Supreme Court vom 02.04.1984, *United States v. Jacobsen*, 466 U. S. 109, 117.

[23] U. S. Supreme Court vom 20.06.1979, *Smith v. Md.*, 442 U. S. 735, 742.

[24] U. S. Supreme Court vom 22.05.2020, *Jones v. United States,* 529 U. S. 848; vom 22.06.2018, *Carpenter v. United States*, 138 S.Ct. 2206. Diese drei Kriterien aus der Rechtsprechung herausarbeitend: *Tokson*, 88 Geo. Wash. L. Rev. 1, 27–30.

[25] U. S. Supreme Court vom 22.06.2018, *Carpenter v. United States*, 138 S.Ct. 2206, 2215 f., 2223.

[26] Ebd., 2223.

[27] Ebd., 2223.

[28] Ebd., 2215.

[29] *Ohm*, 32 Harv. J.L. & Tech. 357, 399–415.

[30] U. S. Supreme Court vom 07.03.1960, *Talley v. California*, 362 U. S. 60, 64–65; vom 19.04.1995, *McIntyre v. Ohio Elections Comm'n*, 514 U. S. 334, 341 f.

[31] U. S. Const. amend III. Zur Einordnung als Schutz der Privatsphäre: *Ursul*, 52 Suffolk U. L. Rev. 577, 582.

[32] U. S. Supreme Court vom 22.07.1977, *Whalen v. Roe*, 429 U. S. 589, 605. Offenlassend:

2. Grenzen für einzelstaatliche Datenschutzgesetze: Meinungsfreiheit und Dormant Commerce Clause

a) First Amendment

Diesem relativ schwachen Schutz der Privatsphäre stehen beachtliche verfassungsrechtliche Hürden für einzelstaatliche Datenschutzgesetze gegenüber. So schützt die Meinungsfreiheit des *First Amendment* auch das Sammeln und Weitergeben personenbezogener Informationen.

Die Meinungsfreiheit hat im amerikanischen Verfassungsrecht eine überragende Bedeutung, was sich schon darin zeigt, dass sie als erstes Grundrecht im *First Amendment* geregelt ist. Dabei geht sie in der Regel der Privatsphäre vor. Im *marketplace of ideas* sollen Informationen und Ideen frei fließen können.[33] Auch der Informationsaustausch im Wirtschaftsleben ist geschützt. Gesetze, die das freie Sammeln oder Weitergeben von Informationen beschränken, müssen daher ein wichtiges staatliches Interesse verfolgen und eng beschränkt sein. Dies gilt auch für Gesetze der Bundesstaaten, da das *First Amendment* über das *Fourteenth Amendment* auch auf diese anwendbar ist.[34]

Das *First Amendment* schützt auch *commercial speech*. Dieser Begriff umfasst neben Werbung auch jedes Werturteil und jede Tatsachenbehauptung, die durch wirtschaftliche Interessen motiviert sind.[35] Der Supreme Court hat erstmals 1976 den Schutz der *commercial speech* anerkannt.[36] Anfangs betonte er, dass geschäftliche Äußerungen weniger geschützt seien als politische Meinungsäußerungen.[37] Dies hat er über die Jahre immer mehr aufgeweicht. Inzwischen unterscheidet er kaum noch zwischen geschäftlichen und politischen Meinungsäußerungen.[38] Auch das Sammeln und Weitergeben personenbezogener Daten ist als Teil der

---

U. S. Supreme Court vom 19.01.2011, *NASA v. Nelson*, 562 U. S. 134, 144–147. Ein Recht auf Privatsphäre aus dem Fourteenth Amendment hatte bereits zuvor ein Sondervotum entwickelt: U. S. Supreme Court vom 07.06.1965, *Griswold v. Connecticut* – ablehnendes Sondervotum *Black*, 381 U. S. 479, 528.

[33] Näher zu diesem *topos* bei dem Recht auf Löschung, siehe Kapitel 3:C.IV (ab S. 134).

[34] U. S. Supreme Court vom 26.06.2018, *Nat'l Inst. of Family & Life Advocates v. Becerra*, 138 S. Ct. 2361, 2371.

[35] U. S. Supreme Court vom 20.06.1980, *Central Hudson Gas & Elec. v. Public Svc. Comm'n*, 447 U. S. 557, 561. Eine allgemein übliche Definition dieses Begriffs existiert nicht. Zu den verschiedenen Defintionsversuchen: *Thomson*, 47 Colum. J.L. & Soc. Probs. 171, 183 f.

[36] U. S. Supreme Court vom 24.05.1976, *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, 425 U. S. 748, 761–763.

[37] U. S. Supreme Court vom 24.05.1976, *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, 425 U. S. 748, 771. Eingehend dazu auch zustimmendes Sondervotum *Stewart*, 425 U. S. 748, 776.

[38] Kritisch dazu: U. S. Supreme Court vom 26.06.2018, *Nat'l Inst. of Family & Life Advocates v. Becerra* – ablehnendes Sondervotum *Breyer*, 138 S. Ct. 2361, 2382; vom 27.06.2018, *Janus v. AFSCME, Council 31* – ablehnendes Sondervotum *Kagan*, 138 S. Ct. 2448, 2501: »weaponizing the First Amendment«. Umfassend zu der Entwicklung der commercial-speech-Rechtsprechung: *Thomson*, 47 Colum. J.L. & Soc. Probs. 171, 199–205.

commercial speech von der Meinungsfreiheit geschützt.[39] Das *First Amendment* schützt zudem vor Zwang, sich in einer bestimmten Weise zu äußern *(compelled speech)*.[40] Dabei ist allerdings die Pflicht zur Angabe wahrer und neutraler Informationen in der Regel zulässig.[41]

Wie prüft der U. S. Supreme Court Beschränkungen der Meinungsfreiheit? Das amerikanische Verfassungsrecht kennt drei Prüfstufen. Die niedrigste Stufe *(rational basis review)* fragt nur, ob der Staat ein legitimes Interesse verfolgt. Diese Stufe spielt wegen der Bedeutung der Meinungsfreiheit nahezu keine Rolle.[42] Die mittlere Stufe *(intermediate scrutiny)* stellt darauf ab, ob das Gesetz ein wichtiges staatliches Ziel verfolgt und für das Erreichen dieses wichtigen Ziels die Beschränkung erforderlich ist.[43] Die höchste Stufe ist hingegen die *strict scrutiny.* Bei dieser prüft die Rechtsprechung, ob das Gesetz ein zwingendes staatliches Interesse verfolgt, eng auf dieses zwingende Interesse zugeschnitten ist und das mildeste Mittel darstellt.[44] Bei der *strict scrutiny* wird die Verfassungswidrigkeit vermutet,[45] wobei der Staat diese Vermutung nur selten widerlegen kann (»strict in theory, fatal in fact«).[46] Beschränkungen der *commercial speech* prüft der U. S. Supreme Court mit *intermediate scrutiny*.[47] Der *strict scrutiny* unterliegen

---

[39] U. S. Supreme Court vom 23.06.2011, *Sorrell v. IMS Health Inc.*, 564 U. S. 552, 570. Wohl auch: U. S. Supreme Court vom 21.03.1984, *Dun & Bradstreet v. Greenmoss Builders*, 472 U. S. 749, 762.

[40] Grundlegend: U. S. Supreme Court vom 11.03.1934, *W. Va. State Bd. of Educ. v. Barnette*, 319 U. S. 624, 634; dies auf commercial speech erweiternd: U. S. Supreme Court vom 19.04.1995, *Rubin v. Coors Brewing Co*., 514 U. S. 476, 802; vom 08.12.2004, *Johanns v. Livestock Mktg. Ass'n*, 544 U. S. 550.

[41] U. S. Supreme Court vom 28.05.1985, *Zauderer v. Office of Disciplinary Counsel of Supreme Court*, 471 U. S. 626, 651; vom 26.06.2018, *Nat'l Inst. of Family & Life Advocates v. Becerra*, 138 S. Ct. 2361, 2372.

[42] Generell die Anwendbarkeit auf die Meinungsfreiheit ablehnend: U. S. Supreme Court vom 14.06.1943, *W. Va. State Bd. of Educ. v. Barnette*, 319 U. S. 624, 639. Einzige Ausnahme, allerdings nur in einem Sondervotum: U. S. Supreme Court vom 21.06.1991, *Barnes v. Glen Theatre* – ablehnendes Sondervotum *Scalia*, 501 U. S. 560, 580. Auch sonst hat das *rational basis review* kaum eine Rolle in der *First Amendment*-Rechtsprechung gespielt: *Bhagwat*, 2007 U. Ill. L. Rev. 783, 784–787.

[43] U. S. Supreme Court vom 23.06.2011, *Sorrell v. IMS Health Inc.*, 564 U. S. 552, 583. Eingehend zur *intermediate scrutiny* i. R. d. First Amendment: *Bhagwat*, 2007 U. Ill. L. Rev. 783, 787–816.

[44] U. S. Supreme Court vom 22.06.1992, *R. A. v. v. St. Paul*, 505 U. S. 377, 382; vom 27.06.2011, *Brown v. Entm't Merchs. Ass'n*, 564 U. S. 786, 799.

[45] U. S. Supreme Court vom 27.06.2011, *Brown v. Entm't Merchs. Ass'n*, 564 U. S. 786, 799; vom 06.07.2020, *Barr v. Am. Ass'n of Political Consultants* – ablehnendes Sondervotum *Breyer*, 140 S. Ct. 2335, 2360.

[46] *Winkler*, 59 Vand. L. Rev. 793, 815 mit einer statistischen Auswertung der untergerichtlichen Rechtsprechung.

[47] U. S. Supreme Court vom 20.06.1980, *Central Hudson Gas & Elec. v. Public Svc. Comm'n*, 447 U. S. 557, 566. Die Mehrheitsmeinung nennt dies zwar nie »intermediate scrutiny«, aber ein zustimmendes Sondervotum: U. S. Supreme Court vom 20.06.1980, *Central Hudson Gas*

dagegen Beschränkungen, die darauf abstellen, wer sich äußert oder was der Inhalt der Äußerung ist *(speaker- or content-based restrictions)*.[48]

In *Sorrell v. IMS Health Inc.* (2011) hat der Supreme Court ein Gesetz Vermonts verworfen,[49] nach dem Apotheken und Krankenversicherungen Daten über die Verschreibungsgewohnheiten nicht für Werbezwecke an Dritte weitergeben durften.[50] In der Vergangenheit hatte die Pharmabranche solche Daten genutzt, um ihre Werbung an die Verschreibungsgewohnheiten des jeweiligen Arztes oder der jeweiligen Ärztin anzupassen.[51] Die Weiterübermittlung dieser Verschreibungsgewohnheiten sei als *commercial speech* geschützt, da die Meinungsfreiheit jedes Sammeln und Verbreiten von Informationen erfasse.[52] Nominelle *ratio legis* des Gesetzes war, die Vertraulichkeit ärztlicher Verschreibungen sicherzustellen.[53] Dies sah der U. S. Supreme Court jedoch als ein vorgeschobenes Motiv: tatsächliches Ziel sei, die Werbung für teure Medikamente zu erschweren, da nur die Weiterübermittlung zu Werbezwecken verboten war.[54] Der Gesetzgeber wolle so individuell an den jeweiligen Arzt oder die jeweilige Ärztin angepasste Werbung verhindern und so mittelbar die Verschreibung teurer Markenmedikamente reduzieren.[55] Ein grundsätzliches Verbot mit Ausnahmen für spezifische, legitime Zwecke sei eventuell mit der Vertraulichkeit ärztlicher Verschreibungen zu rechtfertigen.[56] Dagegen richte sich das Gesetz Vermonts in Wahrheit gegen einen bestimmten Inhalt, nämlich die angebliche Überlegenheit teurer Markenmedikamente.[57] Ein solches inhaltsbezogenes Gesetz unterliege der *strict scrutiny*.[58] Ein wichtiges staatliches

---

& Elec. v. Public Svc. Comm'n – zustimmendes Sondervotum *Blackmun*, 447 U. S. 557, 573. So auch die spätere Rechtsprechung: U. S. Supreme Court vom 23.06.2011, *Sorrell v. IMS Health Inc.*, 564 U. S. 552, 583.

[48] Er legt sich dabei ausdrücklich nicht fest, ob es sich um ein separates Kriterium oder um eine Konkretisierung der *intermediate scrutiny* handelt: U. S. Supreme Court vom 23.06.2011, *Sorrell v. IMS Health Inc.*, 564 U. S. 552, 571.

[49] U. S. Supreme Court vom 23.06.2011, *Sorrell v. IMS Health Inc.*, 564 U. S. 552, 571.

[50] Vt. Stat. Ann. tit. 18, § 4631(d); zu vergleichbaren Gesetzen anderer Bundesstaaten: *Heathcoat*, 15 Quinnipiac Health L. J. 187, 194–196.

[51] *Heathcoat*, 15 Quinnipiac Health L. J. 187, 190–192.

[52] U. S. Supreme Court vom 23.06.2011, *Sorrell v. IMS Health Inc.*, 564 U. S. 552, 570.

[53] Vt. Stat. Ann. tit. 18, § 4631(a).

[54] U. S. Supreme Court vom 23.06.2011, *Sorrell v. IMS Health Inc.*, 564 U. S. 552, 572.

[55] *Heathcoat*, 15 Quinnipiac Health L. J. 187, 190–192.

[56] U. S. Supreme Court vom 23.06.2011, *Sorrell v. IMS Health Inc.*, 564 U. S. 552, 573.

[57] Ebd., 571.

[58] U. S. Supreme Court vom 23.06.2011, *Sorrell v. IMS Health Inc.*, 564 U. S. 552, 571. *Sorell* benutzt hier den Begriff »heightened scrutiny«, zitiert allerdings nur Fälle zur *strict scrutiny*, vgl. *Shah*, 54 Colum. J.L. & Soc. Probs. 93, 110–114. Später hat der U. S. Supreme Court klargestellt, dass *strict scrutiny* bei inhaltsbasierten Beschränkungen von *commerical speech* greift: U. S. Supreme Court vom 06.07.2020, *Barr v. Am. Ass'n of Political Consultants*, 140 S. Ct. 2335, 2347.

Interesse sei nicht ersichtlich, da der Gesetzgeber auch direkt das Verschreibeverhalten regeln könne.[59]

Dagegen hat der U. S. Supreme Court in *Barr v. Am. Ass'n of Political Consultants* (2020) ein Verbot automatisierter kommerzieller Anrufe aufrechterhalten.[60] Das grundsätzliche Verbot sei durch das staatliche Interesse an der Privatsphäre von Verbraucher:innen gerechtfertigt, was der U. S. Supreme Court recht knapp festhält und daher wohl für unproblematisch hält.[61] Die Ausnahme für staatliches Inkasso hat er jedoch verworfen, da sie inhaltsbasiert sei und daher *strict scrutiny* greife: für diese Ungleichbehandlung sei kein zwingendes staatliches Interesse ersichtlich.[62]

Damit wird deutlich, dass umfassende Datenschutzgesetze verfassungsrechtlich weniger problematisch sind als solche, die auf bestimmte Inhalte abzielen.[63] Auch in der Rechtsprechung der Untergerichte ist Datenschutz als wichtiges öffentliches Interesse anerkannt.[64] Ein Verbot der Übermittlung von Informationen ist aber dennoch ein Eingriff in die Meinungsfreiheit, der von einem gewichtigen staatlichen Interesse getragen sein muss. Das *First Amendment* erlaubt damit wohl ein umfassendes Datenschutzgesetz wie den CCPA grundsätzlich.[65] Es führt aber dazu, dass der kalifornische Gesetzgeber diverse »Klippen umschiffen muss«, wenn er nicht die Verwerfung durch ein Bundesgericht[66] riskieren will.

b) Dormant Commerce Clause

Eine weitere Einschränkung erfahren Datenschutzgesetze der Bundesstaaten durch die *dormant Commerce Clause*. Die U. S. Constitution weist die Gesetzgebungskompetenz für den Handel zwischen Bundesstaaten in der *Commerce*

---

[59] U. S. Supreme Court vom 23.06.2011, *Sorrell v. IMS Health Inc.*, 564 U. S. 552, 571, 577.

[60] U. S. Supreme Court vom 06.07.2020, *Barr v. Am. Ass'n of Political Consultants*, 140 S. Ct. 2335.

[61] Ebd., 2348 f.

[62] Ebd., 2344–2347.

[63] *American Law Institute*, Principles of the law, data privacy, § 1 Reporter's Note 7; *Comber*, 89 Geo. Wash. L. Rev. 202, 229; *Hartzog/Richards*, 61 B.C. L. Rev. 1687, 1729–1731; *Richards*, 56 Wm. & Mary L. Rev. 1501, 1521–1524; *Schapiro*, 63 B. C. L. Rev. 2007, 2049; a. A. *Volokh*, 52 Stan. L. Rev. 1049–1124: jedes Datenschutzgesetz verstoße gegen die Meinungsfreiheit (allerdings wohl durch *Sorell* überholt).

[64] U. S. Circuit Court of Appeals D.C. Circuit vom 13.04.2001, *Trans Union Corp. v. FTC*, 245 F.3d 809, 818; U. S. Court of Appeals 9th Circuit vom 08.08.2019, *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1273; U. S. District Court S. D. N. Y. vom 28.09.2016, *Bolter v. Advance Magazine Publisher*, 210 F.Supp.3d 579, 599.

[65] *Comber*, 89 Geo. Wash. L. Rev. 202, 230 f.; *Faison*, 16 Duke J. Const. L. & Pub. Pol'y Sidebar 115, 144; *Palmieri*, 11 Hastings Sci. & Tech. L. J. 37, 52; *Schapiro*, 63 B. C. L. Rev. 2007, 2042–2044. Dies offen lassend: *Kessler*, 93 S. Cal. L. Rev. 99, 115–117.

[66] Jedes Bundesgericht kann Gesetze für verfassungswidrig erklären, vgl. U. S. Supreme Court vom 24.02.1803, *Marbury v. Madison*, 5 U. S. 137, 171–180; vom 26.06.2013, *Hollingsworth v. Perry*, 570 U. S. 693, 705.

Clause dem U. S.-Kongress zu.[67] Bundesstaaten dürfen den zwischenstaatlichen Handel auch dann nicht beeinträchtigen, wenn der U. S. Kongress seine Gesetzgebungskompetenz noch nicht ausgeübt hat und diese gleichsam noch »schläft« (*dormant Commerce Clause*).[68] Bundesstaaten verstoßen in drei Fallgruppen gegen die *dormant Commerce Clause:*[69]

– unmittelbare Diskriminierung von Produkten und Dienstleistungen wegen ihrer Herkunft aus anderen Bundesstaaten[70]
– unangemessene mittelbare Beschränkungen des zwischenstaatlichen Handels[71]
– Regelung vollständig extraterritorialer Sachverhalte[72]

Dabei sind unmittelbare Diskriminierungen und die Regelung extraterritorialer Sachverhalte selten, da die Bundesstaaten sie einfach vermeiden können.[73] Mittelbare unangemessene Beschränkungen des zwischenstaatlichen Handels sind naturgemäß schwieriger zu vermeiden, weshalb diese Fallgruppe die größte Rolle spielt.[74] Die *dormant Commerce Clause* soll dabei verhindern, dass sich ein Bundesstaat protektionistisch isoliert, aber nicht die Autonomie der Bundesstaaten schwächen.[75] Der Supreme Court wägt hier mittels des *Pike*-Test ab: die indirekten Nachteile für den zwischenstaatlichen Handel dürfen nicht die direkten lokalen Vorteile offensichtlich überwiegen.[76]

Der Datenschutz ist als legitimes öffentliches Interesse im Rahmen des *Pike*-Tests anerkannt. So haben beispielsweise der California Supreme Court[77] und ein

---

[67] U. S. Const. Art. I, § 8 cl. 3.

[68] Ursprünglich entwickelt in: U. S. Supreme Court vom 02.03.1824, *Gibbons v. Ogden*, 22 U. S. 1, 189; vom 02.03.1852, *Cooley v. Board of Wardens*, 53 U. S. 299, 318.

[69] Zu der Vergleichbarkeit dieser Fallgruppen mit der Grundfreiheits-Dogmatik des AEUV: *Allmendinger*, 4 Wm. & Mary Bus. L. Rev. 67–110.

[70] U. S. Supreme Court vom 23.06.1978, *City of Philadelphia v. New Jersey*, 437 U. S. 617, 624; vom 23.06.1986, *Maine v. Taylor*, 477 U. S. 131, 138; vom 19.05.2008, *Dep't of Revenue v. Davis*, 553 U. S. 328, 337 f.; U. S. Court of Appeals 5th Circuit vom 27.08.2001, *Ford Motor Co. v. Tex. Dep't of Transp.*, 264 F.3d 493, 499 f.

[71] Supreme Court vom 02.03.1970, *Pike v. Bruce Church Inc.*, 397 U. S. 137, 142; vom 23.06.1982, *Edgar v. MITE Corp.*, 457 U. S. 624, 640; vom 22.05.1984, *South-Central Timber Dev. v. Wunnicke*, 467 U. S. 82, 100.

[72] U. S. Supreme Court vom 03.06.1986, *Brown-Forman Distillers Corp. v. New York State Liquor Auth.,* 476 U. S. 573, 582–584; vom 19.06.1989, *Healy v. Beer Institute, Inc.,* 491 U. S. 324, 335–337; U. S. Court of Appeals 10th Circuit vom 13.07.2015, *Energy & Envtl. Legal Inst. v. Epel*, 793 F.3d 1169, 1171.

[73] *Palmieri,* 11 Hastings Sci. & Tech 37, 50; *Ursul*, 52 Suffolk U. L. Rev. 577, 594.

[74] *Palmieri,* 11 Hastings Sci. & Tech 37, 50; *Ursul*, 52 Suffolk U. L. Rev. 577, 594.

[75] U. S. Supreme Court vom 19.05.2008, *Dep't of Revenue v. Davis*, 553 U. S. 328, 337 f.

[76] U. S. Supreme Court vom 02.03.1970, *Pike v. Bruce Church Inc.*, 397 U. S. 137, 142.

[77] Cal. Supreme Court vom 13.06.2006, *Kearney v. Salomon Smith Barney, Inc.*, 39 Cal. 4th 95, 106 f.

U. S. District Court[78] den California Invasion of Privacy Act[79] unter Anwendung des *Pike*-Tests aufrechterhalten. Dieses Gesetz verbietet es, Telefonate ohne beidseitige Einwilligung aufzuzeichnen, was Call-Center faktisch nur für alle Anrufer umsetzen können (die Vorwahl entspricht wegen Rufnummermitnahmen häufig nicht dem Wohnsitz).[80] Das Datenschutzinteresse der geschützten Personen mit kalifornischem Wohnsitz überwiege etwaige Nachteile für Call-Center aus anderen Bundesstaaten.[81]

Auch sonst haben Gerichte des Bundes und Kaliforniens das Internet regulierende Gesetze nicht schon deshalb an *dormant Commerce Clause* scheitern lassen, weil sie auch Unternehmen mit Sitz außerhalb des Staates erfassen.[82] Daher sind umfassende Datenschutzgesetze der Bundesstaaten ohne Verstoß gegen die *dormant Commerce Clause* möglich, wenn ihr räumlicher Anwendungsbereich auf das nötige Maß beschränkt ist.[83]

II. Constitution of the State of California

Die California Constitution kennt dagegen ein explizites Recht auf Privatsphäre, welches das kalifornische Volk 1972 in einem Volksentscheid eingeführt hat.[84] Dieses steht an prominenter Stelle direkt zu Beginn des ersten Artikels der Verfassung.[85]

Der California Supreme Court unterscheidet zwei Ausprägungen des Rechts auf Privatsphäre: *autonomy privacy* (ähnlich zur Handlungsfreiheit) und *informational privacy*.[86] Die *informational privacy* ist die für den Datenschutz relevante Ausprägung, da sie am ehesten der informationellen Selbstbestimmung entspricht. Der California Supreme Court hat erstmals in *White v. Davis* (1975) definiert, welche Handlungen in die *informational privacy* eingreifen: geheimes Sammeln

---

[78] U. S. District C. D. Cal. vom 08.09.2014, *Ades v. Omni Hotels Mgmt. Corp.*, 46 F. Supp. 3d 999, 1011–1016.

[79] Cal. Pen. Code §§ 630–638.55.

[80] Zumindest bei Mobiltelefonnummern sei nicht festzustellen, aus welchem Staat ein Anruf stammt: U. S. District Court, C. D. California vom 08.09.2014, *Ades v. Omni Hotels Mgmt. Corp.*, 46 F. Supp. 3d 999, 1012.

[81] U. S. District C. D. Cal. vom 08.09.2014, *Ades v. Omni Hotels Mgmt. Corp.*, 46 F. Supp. 3d 999, 1015–1016; Cal. Supreme Court vom 13.07.2006, *Kearney v. Barney*, 39 Cal.4th 95, 106 f.

[82] U. S. Supreme Court vom 21.06.2018, *South Dakota v. Wayfair, Inc.*, 138 S. Ct. 2080, 2095; U. S. Court of Appeals 9th Circuit vom 05.02.2014, *Greater L. A. Agency on Deafness, Inc. v. CNN, Inc.,* 742 F.3d 414, 433.

[83] *Cal. Attorney General*, Summary and Response to Comments Submitted During 45-Day Period, S. 322; *Chander/Kaminski/McGeveran*, 105 Minn. L. Rev. 1733, 1794–1796; *Palmieri*, 11 Hastings Sci. & Tech 37, 49–53; Spivak, 88 U. Cin. L. Rev. 475, 493–514; Ursul, 52 Suffolk U. L. Rev. 577, 599. Zu dem räumlichen Anwendungsbereich siehe Kapitel 3:B.III (ab S. 71).

[84] Umfassend zur Gesetzgebungsgeschichte: *Kelso*, 19 Pepp. L. Rev. 327, 416–443.

[85] Cal. Const. Art. 1, § 1.

[86] Cal. Supreme Court vom 28.01.1994, *Hill v. National Collegiate Athletic Assn.*, 7 Cal. 4th 1, 35.

personenbezogener Informationen; übermäßiges Sammeln und Speichern von nicht erforderlichen persönlichen Informationen; missbräuchliche Verwendung von Informationen, die für einen bestimmten Zweck erhoben wurden und Speicherung unrichtiger Daten.[87]

Darin zeigt sich, dass der California Supreme Court bereits 1975 eine fortschrittliche Auffassung von Datenschutz vertrat, als es in Deutschland noch kein Bundesdatenschutzgesetz gab.[88] Eingriffe in die *informational privacy* prüft der California Supreme Court mittels eines zweistufigen Schemas. Zunächst muss der Eingriff erheblich gegen die berechtigte Privatheitserwartung (*reasonable expectation of privacy)* verstoßen.[89] Auf der zweiten Stufe wägt der California Supreme Court die Interessen beider Parteien ab.[90] Dieses Recht wirkt, anders als die reinen Abwehrrechte gegen den Staat der U. S. Constitution,[91] auch unmittelbar gegen Private.[92]

In *Hill vs. National Collegiate Athletic Assn.* (1995) hat der California Supreme Court anhand dieser Maßstäbe ein Doping-Testsystem für private Sportwettbewerbe aufrechterhalten.[93] Es läge zwar ein erheblicher Eingriff in die Privatsphäre vor, da sich die Sportler:innen bei der Urinabgabe beobachten lassen und offenlegen müssen, welche Medikamente sie nehmen (1. Stufe).[94] Dabei überwiege aber das berechtigte Interesse der National Collegiate Athletic Assn., die einen fairen Wettbewerb sicherstellen müsse (2. Stufe). Darauf aufbauend hat der California Supreme Court in *Hernandez v. Hillsides, Inc. (*2009) eine verdeckte Videoüberwachung für keinen Verstoß gegen das Recht auf Privatsphäre gehalten.[95] Diese Videoüberwachung war durch einen konkreten Anlass motiviert und nur nachts, außerhalb der Geschäftszeiten aktiv.[96] Daher liege kein erheblicher Eingriff in die Privatsphäre vor (1. Stufe).[97] Ansonsten dominieren die Fälle, in denen sich der California Supreme Court mit Eingriffen in

---

[87] Cal. Supreme Court vom 24.03.1975, *White v. Davis*, 13 Cal. 3d 757, 775.

[88] Das BDSG wurde am 27.01.1977 verkündet (BGBl. 1977 I S. 201) und ist am 01.01.1978 in Kraft getreten. (§ 46 BDSG 1977).

[89] Cal. Supreme Court vom 28.01.1994, *Hill v. National Collegiate Athletic Assn.*, 7 Cal. 4th 1, 35–37.

[90] Ebd., 37–39.

[91] Diese als Abwehrrechte nach deutschem Verständnis einordnend: *Schwartz*, 37 Am. J. Comp. L. 675, 679.

[92] Cal. Supreme Court vom 28.01.1994, *Hill v. National Collegiate Athletic Assn.*, 7 Cal. 4th 1, 15–20; vom 03.08.2009, *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287.

[93] Cal. Supreme Court vom 28.01.1994, *Hill v. National Collegiate Athletic Assn.*, 7 Cal. 4th 1, 57.

[94] Ebd., 43, 53.

[95] Cal. Supreme Court vom 03.08.2009, *Hernandez v. Hillsides, Inc.,* 47 Cal. 4th 272, 287.

[96] Ebd., 282.

[97] Ebd., 296 f.

die *informational privacy* durch den Staat auseinandersetzte.[98] Diese betrachtet er als schwerwiegender, wie er schon in *Hill* betonte.[99]

Bei der Auslegung der restlichen California Constitution betont der California Supreme Court zudem stärker die Privatsphäre als der U. S. Supreme Court. So hat er die *third party doctrine* zu dem kalifornischen Äquivalent[100] des *Fourth Amendment* schon seit 1974 abgelehnt.[101]

Mithin steht die California Constitution immer noch in der amerikanischen Tradition eines eher niedrigen Schutzes der Privatsphäre, ist aber wesentlich datenschutzfreundlicher als die U. S. Constitution.

B. Amerikanisches Datenschutzrecht

I. Bund: Datenschutz als Verbraucherschutz

1. Langsame Entwicklung des Commons Laws im Deliktsrecht

Ein deliktsrechtliches *right to privacy* haben zuerst *Warren* und *Brandeis* 1890 in ihrem gleichnamigen Aufsatz entwickelt.[102] Dieser ist einer der einflussreichsten Aufsätze der amerikanischen Rechtswissenschaft und bis heute relevant.[103] So hat der Supreme Court noch nach 130 Jahren im Jahr 2020 *Warren/Brandeis* zitiert.[104] Dieser Aufsatz zeigt auf, dass diverse Ansätze eines *right to privacy* schon immer im Sachen- und Urheberrecht vorhanden waren und man nun nur einen

[98] Cal. Supreme Court vom 24.03.1975, *White v. Davis*, 13 Cal. 3d 757; vom 24.07.1986, *Perkey v. Dep't of Motor Vehicles,* 42 Cal. 3d 185; vom 06.01.1997, *Loder v. City of Glendale*, 14 Cal. 4th 846; vom 17.07.2017, *Lewis v. Superior Court,* 3 Cal.5th 561; vom 26.12.2019, *Matthews v. Beccerra*, 8 Cal. 5th 756.

[99] Cal. Supreme Court vom 28.01.1994, *Hill v. National Collegiate Athletic Assn.*, 7 Cal. 4th 1, 38 f.

[100] Cal. Const. Art. 1, § 13. Dieser entspricht abgesehen von einigen grammatikalischen Anpassungen an den modernen Sprachgebrauch U. S. Const. amend. 4.

[101] Cal. Supreme Court, vom 27.12.1974, *Burrows v. Superior Court*, 529 P.2d 590, 593. Weiterführend zu den Äquivalenten des Fourth Amendment in einzelstaatlichen Verfassungen: *Henderson*, 55 Cath. U. L. Rev. 373, 393–412.

[102] *Warren/Brandeis,* 4 Harv. L. Rev. 193–220.

[103] U. S. Supreme Court vom 21.06.1989, *Florida Star v. B.J.F.,* 491 U. S. 524, 551: »the article widely relied upon in cases vindicating privacy rights«; *Nimmer,* 19 L. and Contemporary Probs. 203, 203; *Reidenberg*, 44 Fed. Comm. L. J. 195, 200.

[104] U. S. Supreme Court vom 29.06.2020, *June Medical Servs. L. L. C. v. Russo* – ablehnendes Sondervotum *Thomas*, 140 S. Ct. 2103, 2150. Vgl. auch das *Warren/Brandeis*-Zitat der Mehrheitsmeinung und beider Sondervoten in: U. S. Supreme Court vom 21.05.2001, *Bartnicki v. Vopper*, 532 U. S. 514, 534, Sondervotum *Breyer,* 532 U. S. 514, 537–540, Sondervotum *Rehnquist*, 532 U. S. 514, 553.

Schritt weiter gehen müsse.[105] Dies ist eine typische Argumentationsstruktur des *common law,* das in kleinen Schritten das Recht induktiv fortentwickelt.[106]

Noch zu Beginn des 20. Jahrhunderts haben nur wenige Gerichte ein solches Recht auf Privatsphäre anerkannt.[107] Die ersten Entscheidungen konzentrierten sich auf das Recht am eigenen Bild.[108] Erstmals hat ein kalifornisches Gericht in *Melvin v. Reid* (1931) Schadensersatz wegen einer Privatsphäreverletzung zugesprochen.[109] Es sprach einer »geläuterten« Prostituierten Schadensersatz wegen eines Boulevard-Artikels zu, der ihre frühere Zeit als Prostituierte und einen damit verbundenen Mordprozess thematisierte.[110] Damit war Kalifornien sogar noch einer der ersten Staaten – 1940 hatten erst 14 der damaligen 48 Bundesstaaten ein solches Recht anerkannt.[111]

Seit der Mitte des 20. Jahrhunderts haben immer mehr Gerichte Schadensersatz bei Privatsphäreverletzungen zugesprochen.[112] Dabei hat sich immer mehr herausgebildet, dass der freie Fluss von Informationen durch ein solches Recht nicht eingeschränkt werden sollte. So hat beispielsweise der U. S. 2nd Circuit Court of Appeals in *Sidis v. FR Pub. Corp.* (1940) betont, dass bereits ein Interesse der Öffentlichkeit an »Klatsch und Tratsch« ausreiche, um umfangreiche Informationen über das Privatleben Unbekannter zu publizieren.[113] Endgültig anerkannt war das Recht auf Privatsphäre erst in den 1970ern[114] – über 80 Jahre nach *Warren/Brandeis'* Aufsatz. Die sich in den 1960ern und 1970ern herausgebildeten vier Deliktstatbestände *intrusion of solitude, public disclosure of*

[105] Allerdings hat sich die vorgeschlagene Lösung eines umfassenden Privatsphäreschutzes angesichts des hohen Stellenwerts der Meinungsfreiheit auch nicht durchgesetzt, vgl. *Whitman*, 113 Yale L. J. 1151, 1202–1211; *Zimmerman*, 68 Cornell L. Rev. 291, 294–299.

[106] Zur Methode des *common laws:* Kischel, S. 243–271.

[107] *Nizer*, 39 Mich. L. Rev. 526, 530 f.

[108] Ga. Supreme Court vom 03.03.1905, *Pavesich v. New England Life Ins. Co.*, 122 Ga. 190; ein solches Recht hatte noch abgelehnt: N.Y. Court of Appeals vom 26.11.1895, *Schuyler v. Curtis*, 147 N.Y. 434 (Der N.Y. Court of Appeals ist der Name des höchsten New Yorker Gerichts, das in Kalifornien und im Bund »Supreme Court« heißt).

[109] Cal. Court of Appeal 4th District vom 28.02.1931, *Melvin v. Reid,* 112 Cal. App. 285. Der Cal. Supreme Court hat die dagegen eingelegte Beschwerde verworfen und erst 1952 explizit das Recht auf Privatsphäre anerkannt: Cal. Supreme Court vom 18.01.1952, *Gill v. Curtis Publishing Co.*, 38 Cal. 2d 273, 276 m. w. N. zu der bis dahin ergangenen untergerichtlichen Rechtsprechung.

[110] Cal. Court of Appeal vom 28.02.1931, *Melvin v. Reid,* 112 Cal. App. 285, 292.

[111] *Nizer*, 39 Mich. L. Rev. 526, 529.

[112] *Richards/Solove*, 98 Calif. L. Rev. 1887, 1892–1895.

[113] U. S. Court of Appeals 2nd Circuit vom 22.07.1940, *Sidis v. FR Pub. Corp,* 113 F.2d 806, 809. Weiterführend zu dieser Entscheidung und ihrem Einfluss auf das *right to privacy*: *Barbas*, 36 Colum. J.L. & Arts 21–70.

[114] In den 1970ern wurde das right to privacy in die Restatements aufgenommen, welche die herrschende Meinung in der amerikanischen Rechtsprechung abbilden: *American Law Institute*, Restatement (Second) of Torts, §§ 652A–E.; zur Vergleichbarkeit mit dem deutschen allgemeinen Persönlichkeitsrecht: *Schwartz/Peifer*, 98 Calif. L. Rev. 1925, 1937–1987; *Whitman*, 113 Yale L. J. 1151, 1180–1211.

private facts, false light und *appropriation*[115] sind wiederum bis heute nahezu unverändert.[116]

Dieser komplexe Prozess des *common law,* anhand von Einzelfällen das Recht induktiv fortzuentwickeln, ist für die sich schnell verändernde moderne Datenverarbeitung zu langsam.[117] Bis sich ein Konsens zwischen verschiedenen Gerichten herausbildet, dauert es Jahrzehnte, während personenbezogene Daten im Zeitalter des Internets in ständig neuer Weise verwendet werden.[118] In der oben diskutierten *Carpenter*-Entscheidung des U. S. Supreme Court haben sich daher mit *Gorsuch*[119] und *Alito*[120] selbst zwei der höchsten amerikanischen Richter dafür ausgesprochen, den Datenschutz dem U. S. Kongress zu überlassen. Das Richterrecht des *common law* spielt im heutigen Datenschutzrecht nur noch bei Sammelklagen wegen Datenpannen eine begrenzte Rolle.[121]

2. Branchenspezifische Datenschutzgesetze

Der U. S. Kongress hat dagegen zahlreiche Datenschutzgesetze erlassen.[122] 1974 hat er sogar ein umfassendes Datenschutzgesetz für den Staat und die Privatwirtschaft erwogen – den Federal Privacy Act.[123] Dieser war für seine Zeit fortschrittlich und enthielt viele Regelungen, die heute international anerkannte Datenschutzstandards bilden: ein Verbot der Übermittlung personenbezogener

---

[115] Grundlegend: *Prosser*, 48 Calif. L. Rev. 383–423. Später aufgenommen in: *American Law Institute*, Restatement (Second) of Torts, §§ 652A–E.

[116] *Richards/Solove*, 98 Calif. L. Rev. 1887, 1904–1907 nennen dies »Fossilization«.

[117] *Blanke*, 2018 U. Ill. L. Rev. Online 260, 265 f.; *Entrikin*, 42 Harv. J.L. & Pub. Pol'y 351, 356 (auch zur Frage, ob das amerikanische Recht überhaupt noch primär Richterrecht ist); *Volokh*, 114 Colum. L. Rev. 879, 942–947.

[118] *Blanke*, 2018 U. Ill. L. Rev. Online 260, 265 f.; *Entrikin*, 42 Harv. J.L. & Pub. Pol'y 351, 356.

[119] U. S. Supreme Court vom 22.06.2018, *Carpenter v. United States* – ablehnendes Sondervotum *Gorsuch,* 138 S.Ct. 2206, 2265.

[120] U. S. Supreme Court vom 22.06.2018, *Carpenter v. United States* – ablehnendes Sondervotum *Alito,* 138 S.Ct. 2206, 2261.

[121] Zu diesen siehe Kapitel 3:E.II.1 (ab S. 204).

[122] Für den nicht-staatlichen Bereich in chronologischer Reihenfolge (Änderungen aufgeführter Gesetze sind nicht separat dargestellt): FCRA (1970), 15 U. S. C. §§ 1681–1681u; Farm Credit Act of 1971, 12 C. F. R. § 618.8300–8330; FERPA (1974), 20 U. S. C. § 1232g, 34 C. F. R. § 99.1–67; Cable Communications Policy Act of 1984, 47 U. S. C. § 551; Computer Fraud and Abuse Act of 1984, 18 U. S. C. § 1030; Cable Communications Policy Act of 1984, 45 U. S. C. § 551; Electronic Communications Privacy Act of 1986, 18 U. S. C. §§ 2510–2523; Video Privacy Protection Act of 1988, 18 U. S. C. § 2710; Computer Matching & Privacy Protection Act of 1988, 5 U. S. C. § 552a; TCPA (1991), 47 U. S. C. § 227; Driver's Privacy Protection Act of 1994, 18 U. S. C. § 2721; HIPAA (1996), 42 U. S. C. § 1320d-2(a), 45 C. F. R. §§ 160, 162, 164; Telecommunications Act of 1996, 45 U. S. C. § 222; Federal Identity Theft and Assumption Deterrence Act of 1998, 18 U. S. C. § 1028; GLBA (1999), 15 U. S. C. §§ 6801–6809; COPPA (2000), 15 U. S. C. § 6501–6506.

[123] Privacy Act of 1974, 5 U. S. C. § 552a.

Informationen an Dritte mit Erlaubnisvorbehalt,[124] ein Auskunftsrecht,[125] ein Berichtigungsrecht[126] und die Pflicht zur Datensicherheit.[127] Dieses Gesetz sollte ursprünglich sowohl für die Privatwirtschaft als auch für den Staat gelten.[128] Im Gesetzgebungsverfahren hat der Kongress allerdings den Anwendungsbereich auf staatliche Datenerhebung in direkt personenbezogenen Akten beschränkt.[129] Der zuständige Senatsausschuss begründete dies damit, dass damals staatliche Datenerhebung die größeren Probleme aufwerfe.[130] Die privatwirtschaftliche Datenverarbeitung solle beobachtet und bei einem festgestellten Missbrauch beschränkt werden.[131] Trotz zahlloser Aufrufe[132] und Gesetzesinitiativen[133] hat

[124] 5 U. S. C. § 552a(b). Diese und die folgenden Vorschriften fanden sich nahezu unverändert auch schon in der Originalfassung von 1974 (Pub.L. 93–579, 88 Stat. 1896).

[125] 5 U. S. C. § 552a(d)(1).

[126] 5 U. S. C. § 552a(d)(2).

[127] 5 U. S. C. § 552a(e)(9),(10).

[128] Gesetzentwurf des Senators Ervin, S. 3418, § 201(a) in: *U. S. Senate, Committee on Government Operations/U. S. House of Representatives, Committee on Government Operations*, Legislative History of the Privacy Act of 1974, S. 13.

[129] 5. U. S. C. § 552a(a)(1) i. V. m. § 551(1). Diese Frage war auch in Deutschland beim ersten BDSG 1976 stark umstritten: BT-Plenarprotokoll 07/250, 17738.

[130] Protokoll des U. S. Senate, Committee on Government Operations vom 20.08.1974, zitiert nach: *U. S. Senate, Committee on Government Operations/U. S. House of Representatives, Committee on Government Operations*, Legislative History of the Privacy Act of 1974, S. 50. Ausführlich zur Gesetzgebungsgeschichte: *Regan*, Legislating Privacy, S. 71–81. Es gab zahlreiche Versuche, diese Einschränkung zurückzunehmen (zuletzt: American Data Dissemination Act of 2019, S. 142, 116th Cong. (2019)).

[131] U. S. Senate, Protokoll des Committee on Government Operations vom 20.08.1974, zitiert nach *U. S. Senate, Committee on Government Operations/U. S. House of Representatives, Committee on Government Operations*, Legislative History of the Privacy Act of 1974, S. 51.

[132] Aus der Rechtswissenschaft monographisch: *American Law Institute*, Principles of the law, data privacy. Ebenso: *Büyüksagis,* 30 Fordham Intell. Prop. Media & Ent. L. J. 139, 182; *Faison*, 16 Duke J. Const. L. & Pub. Pol'y Sidebar 115, 140–145; *Hartzog/Richards*, 61 B.C. L. Rev. 1687, 1738–1760; *Jamison*, 10 Cybaris Intell. Prop. L. Rev. 1, 30–40; *Kraft*, 45 U. Dayton L. Rev. 97, 121–126; *Li*, 4 Notre Dame L. Rev. 2211, 2231–2234; *Shubet,* 48 Hofstra L. Rev. 835, 866–871; a. A. *Byun,* 32 Loy. Consumer L. Rev. 246, 26 f.: ein solches Gesetz werde Bundesstaaten einschränken und so dem Datenschutz letztlich schaden; *Krishnamurthy*, 114 AJIL Unbound 26, 29 f.: branchenspezifischer Ansatz sei flexibler; *Schwartz,* 118 Yale L. J. 902, 927–31: Bundesstaaten würden stärkere Datenschutzgesetze erlassen.

[133] Z. B. (nur solche, die Kongressmitglieder beider Parteien oder die jeweilige Bundesregierung vorgeschlagen haben): Consumer Privacy Protection Act, H.R.296, 99th Cong. (1986); Consumer Privacy Protection Act, S.2606, 106th Cong. (2000); Consumer Privacy Protection Act of 2011, H.R.1528, 112th Cong. (2011); Privacy Bill of Rights Act of 2015, Diskussionsentwurf der Regierung, https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf [perma.cc/LG35-TFNC]; Consumer Online Privacy Rights Act, S.2968, 116th Cong. (2019); American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022),

der Kongress jedoch nie ein umfassendes Datenschutzgesetz für die Privatwirtschaft erlassen.[134]

Stattdessen hat der Kongress wiederholt *ad hoc* auf einen festgestellten Missbrauch reagiert und für die betreffende Branche ein branchenspezifisches Datenschutzgesetz geschaffen.[135] Diese branchenspezifischen Gesetze haben teilweise einen sehr hohen Schutzstandard.[136] Wegen zahlreicher nicht erfasster Branchen und Ausnahmen ist der Schutz dennoch nur lückenhaft.[137] Auch für Unternehmen hat der branchenspezifische Ansatz Nachteile, da sich die Anforderungen ohne erkennbares System von Gesetz zu Gesetz unterscheiden und so erhebliche Rechtsunsicherheit herrscht.[138] Dieser Ansatz ist zudem häufig langsam, da er nur *ex post* bei einer bereits eingetretenen Fehlentwicklung reagiert.[139]

Die branchenspezifischen Gesetze entstanden häufig als Reaktion auf einen öffentlichen Skandal. Beispielsweise hat der Kongress mit dem Video Privacy Protection Act[140] den Umgang mit personenbezogenen Daten von Videoverleihkunden geregelt, weil zuvor Aktivisten die Liste ausgeliehener Filme des für den U. S. Supreme Court nominierten Richters *Robert Bork* veröffentlicht hatten.[141] Er gilt für Videoverleihe aller Art,[142] d. h. auch moderne Videostreamingdienste wie Netflix,[143] und verbietet die Übermittlung von Kundendaten an Dritte mit bestimmten, eng begrenzten Ausnahmen.[144] Zudem müssen Videoverleihdienste personenbezogene Daten löschen, wenn sie nicht mehr erforderlich sind.[145] Darin erschöpft sich jedoch sein Regelungsgehalt: es fehlen insbesondere

---

[134] Zu der Auseinanderentwicklung des transatlantischen Datenschutzes von einer gemeinsamen Basis in den 1970ern bis zu sehr unterschiedlichen Gesetzen in den 1990ern: *Voss,* 2019 U. IlL. J.L. Tech. & Pol'y 405, 412–427.

[135] Eingehend: *Reidenberg,* 44 Fed. Comm. L. J. 195, 209–220. Ebenso: *Adams,* 84 Mo. L. Rev., 1055, 1062; *Bradford*, 107 Nw. U. L. Rev. 1, *22*; *Hoofnagle*, Country Report U. S. for European Commission, S. 1; *Ivers*, 62 B.C. L. Rev. 2573, 2589–2590; *Jamison,* 10 Cybaris Intell. Prop. L. Rev. 1, 3; *Li,* 4 Notre Dame L. Rev. 2211, 2213–2214; *Murray,* 21 Fordham Int'l L.J 932, 945–948; *Pernot-Leplay,* 18 Colo. Tech. L. J. 25, 36.

[136] *Schwartz,* 108 Yale L. J. 902, 911–913.

[137] *Hoofnagle*, Country Report U. S. for European Commission, S. 21; *Li,* 4 Notre Dame L. Rev. 2211, 2213–2231; *Reidenberg*, 44 Fed. Comm. L. J. 195, 219; *Shubet,* 48 Hofstra L. Rev. 835, 841.

[138] *Hoofnagle*, Country Report U. S. for European Commission, S. 22; *Li,* 4 Notre Dame L. Rev. 2211, 2229; *Reidenberg*, 44 Fed. Comm. L. J. 195, 219 f.

[139] *Hoofnagle*, Country Report U. S. for European Commission, S. 1; *Lode,* 94 Ind. L. J. Supp. 41, 56 f.

[140] 18 U. S. C. § 2710.

[141] Der U. S. Senat hat *Robert Bork* letztendlich nicht bestätigt, was allerdings wohl nicht an der Ausleihliste lag, die nur harmlose Filme enthielt. Zur Gesetzgebungsgeschichte: *Urgoti,* 53 U.C. Davis L. Rev. 1689, 1699 f.

[142] 18 U. S. C. § 2710(a)(4).

[143] *Schwartz*, 118 Yale L. J. 902, 937.

[144] 18 U. S. C. § 2710(b)(2).

[145] 18 U. S. C. § 2710(e).

Informationspflichten, Auskunftsrechte oder Datensicherheitspflichten. Er bildet daher ein Beispiel dafür, dass auch innerhalb einer erfassten Branche der Schutz nur lückenhaft ist.

Ein weiteres typisches branchenspezifisches Datenschutzgesetz ist der Gramm-Leach-Bliley-Act (GLBA).[146] Er erfasst Banken,[147] Versicherungen[148] und andere Unternehmen der Finanzbranche.[149] Diese müssen darüber informieren, welche personenbezogenen Informationen von Privatkund:innen sie erheben,[150] an wen sie diese weitergegeben,[151] welche Rechte Privatkund:innen haben[152] und wie personenbezogene Daten geschützt sind.[153] Ebenfalls regelt er ein Widerspruchsrecht gegen die Übermittlung personenbezogener Informationen an Dritte mit auf die Finanzbranche zugeschnittenen Ausnahmen.[154] Die Weiterübermittlung der Kontonummer für Werbezwecke ist dabei explizit verboten.[155]

Der GLBA zeigt die Vor- und Nachteile des branchenspezifischen Ansatzes. So können Besonderheiten der jeweiligen Branche wie die Nutzung von Kontonummern für Werbung berücksichtigt werden. Zusätzlich sind verpflichtende Informationen über Datensicherheit ein Aspekt, der selbst von den Informationspflichten der Art. 13, 14 DSGVO nicht umfasst ist. Allerdings bestehen auch deutliche Schutzlücken. So fehlt ein Auskunftsrecht, und die Definition personenbezogener Informationen ist sehr eng, da sie nicht-öffentliche, direkt personenbezogene Daten über Privatkund:innen erfasst.[156] Zudem regelt er kein Verbot mit Erlaubnisvorbehalt, sondern nur ein Widerspruchsrecht, das Verbraucher:innen umständlich gegen jedes Unternehmen einzeln ausüben müssen.[157]

Ein solches Verbot mit Erlaubnisverbot kennt hingegen der Health Insurance Portability and Accountability Act of 1996 (HIPAA),[158] der den Schutz von Patientendaten regelt. Er schützt Patientendaten nicht allgemein, sondern nur

---

[146] Alternativ auch Financial Services Modernization Act of 1999, Pub.L. 106–102, 113 Stat. 1338. Dessen Datenschutzvorschriften sind in 15 U.S.C. § 6801–6809 kodifiziert. Durchführungsverordnungen (jeweils für verschiedene Adressat:innen): 12 C.F.R. § 1016, 16 C.F.R. § 313, 17 C.F.R. § 160.

[147] 15 U.S.C. § 6809(3)(A) i.V.m. 12 U.S.C. § 1843(k)(4)(A).

[148] 15 U.S.C. §§ 6809(3)(A) i.V.m. 12 U.S.C. § 1843(k)(4)(B).

[149] 15 U.S.C. §§ 6809(3)(A) i.V.m. 12 U.S.C. § 1843(k)(C)–(I).

[150] 15 U.S.C. § 6803(c)(2).

[151] 15 U.S.C. § 6803(a)(1),(c)(4).

[152] 15 U.S.C. § 6802(b)(1)(A),(C).

[153] 15 U.S.C. § 6803(a)(3),(c)(3).

[154] 15 U.S.C. § 6802(b).

[155] 15 U.S.C. § 6802(d).

[156] 15 U.S.C. § 6089(4).

[157] Zu den Schwächen des Gramm-Leach-Bliley-Acts und wie dieser überarbeitet werden sollte: *Soubouti*, 24 N.C. Banking Inst. 527, 534–539.

[158] Pub.L. 104–191, 110 Stat. 1936. Der HIPAA selbst enthält nur eine Verordnungsermächtigung (42 U.S.C. § 1320d-2(a),(b)), die durch eine umfangreiche Durchführungsverordnung des U.S. Department of Health and Human Services ausgefüllt wird (45 C.F.R. §§ 160, 162, 164).

wenn diese entweder eine *covered entity* (Krankenversicherungen, Krankenhäuser, Arztpraxen und ähnliche Unternehmen) oder ein *business associate* (Dienstleister) im Auftrag einer *covered entity* verarbeitet.[159] Die auf seiner Basis erlassene Verordnung verbietet es, Patientendaten zu verarbeiten, wenn nicht eine der eng gefassten Ausnahmen greift.[160] Ebenfalls bestehen Informationspflichten,[161] ein Auskunftsrecht[162] und detaillierte Regelungen zur Datensicherheit.[163] Der Begriff personenbezogener Informationen weicht von dem des GLBA ab, da pseudonymisierte Daten nicht erfasst,[164] dafür aber auch öffentliche personenbezogene Informationen umfasst sind.[165]

Der HIPAA statuiert einen hohen Schutzstandard. Dieser wird auch aktiv durchgesetzt: im Jahr 2020 hat das U. S. Department of Health and Human Services 19 Geldstrafen in einer Gesamthöhe von 13,5 Millionen Dollar verhängt.[166] Auch er enthält aber Lücken. So besteht kein Privatklagerecht, die Erhebung der Patientendaten ist nicht geregelt, und der Adressatenkreis erfasst selbst manche Unternehmen der Gesundheitsbranche nicht.[167]

Weiterhin existieren Gesetze, die speziell Kinder schützen, wie vor allem den Children's Online Privacy Protection Act of 1998 (COPPA).[168] Webseitenanbieter müssen nach diesem Bundesgesetz für die Erhebung, Verwendung und Übermittlung personenbezogener Daten von Kindern unter 13 Jahren[169] die Einwilligung der Eltern einholen.[170] Die personenbezogenen Daten von Kindern müssen besonders sicher aufbewahrt werden.[171] Daneben regelt er spezielle Informationspflichten.[172]

Der COPPA ist ein Beispiel dafür, dass amerikanische Datenschutzgesetze teilweise sehr ambitioniert sind – nach der DSGVO können Daten von Kindern grundsätzlich auch ohne Einwilligung der Eltern verarbeitet werden, wie Art. 6 Abs. 1 S. 1 lit. f DSGVO a.E. stillschweigend voraussetzt.[173] Soweit Art. 8 DSGVO die Modalitäten der Einwilligung bei Diensten der Informationsgesellschaft regelt,

---

[159] 45 C. F. R. § 160.102(a),(b).

[160] 45 C. F. R. § 164.502(a).

[161] 45 C. F. R. § 164.520.

[162] 45 C. F. R. § 164.524.

[163] 45 C. F. R. § 164.302–318.

[164] 45 C. F. R. § 164.514(a),(b).

[165] 45 C. F. R. § 160.103, *protected health information.*

[166] *Adler*, HIPAA Journal, 2020 HIPAA Violation Cases and Penalties.

[167] Zur Kritik am HIPAA: Fang, 4 Geo. L. Tech Rev. 125, 144–148.

[168] 15 U. S. C. §§ 6501–6506. Durchführungsverordnung: 16 C. F. R. § 312.1–13. Weiterführend zu Gesetzgebungsgeschichte und Inhalt: *Hoofnagle,* FTC, S. 193–215.

[169] 15 U. S. C. § 6501(1).

[170] 15 U. S. C. § 6502(b)(1), 16 C. F. R. § 312.5. Dies umgehen große Plattformbetreiber jedoch systematisch, indem sie in ihren AGB die Nutzung durch Kinder unter 13 Jahren ausschließen. Dazu: *Finnegan,* 50 Seton Hall L. Rev. 827, 833–838.

[171] 15 U. S. C. § 6502(b)(1)(D), 16 C. F. R. § 312.8.

[172] 15 U. S. C. § 6502(b)(1)(B), 16 C. F. R. § 312.4.

[173] Rechtsvergleich zwischen COPPA und DSGVO: *Rauda,* MMR 2017, 15–19.

war COPPA Vorbild für die DSGVO.[174] So nannte der Europäische Datenschutzbeauftragte COPPA in seiner Stellungnahme zur Vorbereitung der DSGVO den COPPA als mögliches Vorbild für den Minderjährigenschutz.[175] Die Europäische Kommission griff diesen Vorschlag auf und übernahm im Art. 8 Abs. 1 DSGVO-E(KOM) auch die Altersgrenze des COPPA von 13 Jahren, die erst im Trilog auf 16 Jahre angehoben wurde.[176]

3. Federal Trade Commission

Die Lücken des branchenspezifischen Ansatzes füllt die Federal Trade Commission (FTC). Diese ist eine U. S.-Wettbewerbsbehörde, die neben Kartellrecht auch für Verbraucherschutz zuständig ist. Sie hat sich so sehr zu der wichtigsten Aufsichtsbehörde für die Technologiebranche entwickelt,[177] dass sie informell auch »Federal Technology Commission« genannt wird.[178] Sie stützt sich bei der Durchsetzung von Datenschutz vor allem auf die Generalklausel des FTC Acts: »unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.«[179] Diese offen formulierte Norm, die im wesentlichen seit 1938 unverändert ist,[180] ist heute die zentrale »Schaltstelle« im amerikanischen Datenschutzrecht.[181] Auf ihrer Basis hat die FTC in den letzten 20 Jahren über 500 Verfahren gegen Unternehmen jeder Art und Größe durchgeführt.[182]

Zuerst hat sie sich ab Ende der 1990er-Jahre auf den einfacher zu begründenden *deceptive*-Teil der Generalklausel gestützt. Amerikanische Unternehmen haben um die Jahrtausendwende Datenschutzerklärungen veröffentlicht, um zu zeigen, dass sie sorgfältig mit Kundendaten umgehen, und um als Akt der Selbstregulierung strengere Gesetze zu vermeiden.[183] Wenn ein Unternehmen gegen

---

[174] Ebenso i. Erg.: *Rustad/Koenig*, 71 Fla. L. Rev. 365, 424; *Schantz*, NJW 2016, 1841, 1845; *Schrader*, Datenschutz Minderjähriger, S. 167; *Taeger* in: Taeger/Gabel, DS-GVO Art. 8 Rn. 5.

[175] *Europäischer Datenschutzbeauftragter*, Opinion on the Communication from the Commission »A comprehensive approach on personal data protection in the European Union«, Rn. 91 a.E.

[176] Synopse: *Europäisches Parlament*, 4 column table on the General Data Protection Regulation, Art. 8.

[177] U. S. Court of Appeals 9th Circuit vom 26.02.2018, *FTC v. AT&T Mobility LLC,* 883 F.3d 848, 851: FTC sei »the chief federal agency on privacy policy and enforcement«.

[178] *Hoofnagle,* FTC, S. 25 f.; *Teme*, Privacy Perspectives, With Ramirez, FTC became the Federal Technology Commission.

[179] 15 U. S. C. § 45(a)(1).

[180] Pub. L. No. 75–447, 52 Stat. 111: »unfair or deceptive acts or practices *in commerce*, are hereby declared unlawful.« [Hervorhebung durch den Verfasser].

[181] *Büyuksagis,* 30 Fordham Intel. Prop Media & Ent L. J. 139, 166; *Hoofnagle,* FTC, S. 145; *Laji*, 15 Wash. J.L. Tech. & Arts 1, 18; *Li*, 94 Notre Dame L. Rev. 2211, 2214; *Ormerod,* Privacy Qui Tam, S. 15.

[182] *Ramirez*, Letter describing FTC Enforcement of Privacy Shield, S. 3 (Stand: 2016).

[183] *Hoofnagle,* FTC, S. 154; *Solove/Hartzog*, 114 Colum. L. Rev. 583, 590–595.

seine Datenschutzerklärung verstößt, handelt es nach der FTC *deceptive.*[184] Die dahinter stehende Theorie der FTC ist *notice and choice*. Verbraucher:innen sollen sich informiert *(notice)* für ein Angebot entscheiden und sich dabei für oder gegen bestimmte Aspekte der Datenverarbeitung entscheiden können *(choice)*.[185] Die *notice* soll hinreichend klar in einer Datenschutzerklärung geschildert sein.[186] Auf dieser Basis können sich die Verbraucher:innen für oder gegen eine Nutzung des Angebots entscheiden.[187] Bei schweren Eingriffen müssen die Verbraucher:innen leicht widersprechen können *(opt-out)*.[188] Sonst darf das Unternehmen berechtigt von einer Einwilligung ausgehen. Zudem fokussiert sich die FTC auf Datensicherheit.[189] Auch vage Versprechen, Daten sicher aufzubewahren, hat die FTC zum Anlass genommen, hohe Maßstäbe für Datensicherheit anzulegen. Sie hat über zahlreiche Verfahren die Datensicherheits-Anforderungen immer mehr konkretisiert.[190]

Zunehmend geht die FTC selbst ohne solche Versprechen in der Datenschutzerklärung auf Basis des *unfair*-Teils der Generalklausel vor.[191] *Unfairness* ist schwerer zu begründen, da die FTC einen konkreten, erheblichen Schaden für die Betroffenen nachweisen muss.[192] Sie hat sich insoweit damit beholfen, einen viele Verbraucher:innen betreffenden Schaden »zusammenzurechnen«.[193]

Ihre Kontrollverfahren gegenüber Unternehmen schließt sie fast immer mit einem Vergleich ab.[194] In diesem Vergleich konzentriert sie sich nicht darauf möglichst hohe Bußgelder,[195] sondern darauf umfassende Verbesserungen im Datenschutz zu erreichen.[196] Häufig vereinbaren die FTC und das jeweilige Unternehmen für jeweils 20 Jahre umfangreiche organisatorische Maßnahmen wie

---

[184] Erste Entscheidung: FTC vom 05.02.1999, 127 F.T.C. 94. Seitdem gab es zahlreiche auf *deception* gestützte Verfahren, vgl. die Übersicht in: *Hoofnagle,* FTC, S. 160–166.

[185] *FTC,* Privacy Online: a Report to Congress, S. 7–9. Umfassend zur Entwicklung von *notice and choice: Bietti,* 40 Pace L. Rev. 310, 329–338.

[186] FTC vom 31.08.2009, *Sears Holdings Management Corp.,* 148 F.T.C. 83, 97–98.

[187] *Richards/Hartzog,* 19 Stan. Tech. L. Rev. 431, 434.

[188] *FTC,* Privacy Online: a Report to Congress, S. 9; FTC vom 07.11.2011, *Chitika, Inc.,* 151 F.T.C. 494, 505: bei User-Tracking sei gesonderte *Opt-Out*-Möglichkeit nötig.

[189] *Solove/Hartzog*, 114 Colum. L. Rev. 583, 649 f.

[190] Umfassende Liste der Anforderungen: *Solove/Hartzog*, 114 Colum. L. Rev. 583, 650–655.

[191] *Becker*, 120 Colum. L. Rev. Forum 134, 138 f.

[192] 15 U. S. C. § 45(n): »causes or is likely to cause substantial injury«.

[193] FTC vom 08.05.1986, *Orkan Exterminating Company, Inc.*, 108 F.T.C 263, 321; in jüngeren Entscheidungen unterstellt dies die FTC ohne Begründung, vgl. die diesbezügliche Analyse in *Hoofnagle,* FTC, S. 160–162.

[194] *Becker*, 120 Colum. L. Rev. Forum 134, 144; *Cooper/Kobayashi*, Rethinking the FTC's Current Approach to Data Security, S. 7; S*olove/Hartzog*, 114 Colum. L. Rev. 583, 608–619 (auch zu dem Verfahren und den typischen Elementen eines solchen Vergleichs).

[195] Sie hat ohnehin nur eine sehr begrenzte Bußgeldkompetenz bei erstmaligen Verstößen, vgl. U. S. Supreme Court vom 22.04.2021, *AMG Capital Mgmt., LLC v. FTC*, 141 S. Ct. 1341, 1347–1352.

[196] S*olove/Hartzog*, 114 Colum. L. Rev. 583, 605 f.

regelmäßige Risikobeurteilungen, Vorgaben für die Auswahl von Dienstleistern und unabhängige Audits.[197] So zeigt die FTC auf, was aus ihrer Sicht der optimale Datenschutzstandard ist.[198] Die Wirkung dieser Maßnahmen wird noch dadurch verstärkt, dass sich die FTC auf große Unternehmen konzentriert: Derzeit unterliegen mit Google LLC, Microsoft Corp. und Meta Platforms, Inc. (das frühere Facebook) drei der fünf größten amerikanischen Unternehmen solchen Programmen.[199] Wenn ein Unternehmen gegen den Vergleich verstößt, können massive Geldstrafen folgen[200] – die bisher höchste Geldstrafe lag bei fünf Milliarden Dollar.[201]

Es ist sicher beeindruckend, wie die FTC mit ihrer nicht dafür gedachten[202] Generalklausel und nur sehr geringen Ressourcen von 61 Vollzeitstellen in deren Datenschutzabteilung[203] ein Basisniveau an Datenschutz in den Vereinigten Staaten erreicht hat. Unproblematisch ist der Ansatz der FTC jedoch nicht. So ist es nur schwer möglich, aus einer Reihe von Vergleichen feste Regeln abzuleiten.[204] Unternehmen stehen zudem unter einem deutlichen Druck, einen Vergleich zu akzeptieren, um die negative öffentliche Wirkung eines Gerichtsverfahrens zu vermeiden.[205] Dadurch werden viele Fragen nicht endgültig geklärt[206] (wobei die FTC eine Verordnung zum Datenschutz plant).[207]

Auch zielt die FTC aufgrund ihres Hintergrunds als Wettbewerbsbehörde vor allem darauf ab, die Privatautonomie von Verbraucher:innen über ihre Daten zu stärken. Dies ist problematisch, da Verbraucher:innen kaum selbst überblicken

---

[197] Z. B. FTC vom 13.10.2011, *Google, Inc.*, 152 F.T.C. 435, 454 f.

[198] Kritisch zu den teilweise ungenauen Anforderungen: *Becker*, 120 Colum. L. Rev. Forum 134, 142–144.

[199] Nach Marktkapitalisierung (Muttergesellschaft von Google LLC ist Alphabet, Inc.): *PwC*, Global Top 100 companies by market capitalisation: May 2021, S. 22. Die Verfahren waren im Einzelnen: FTC vom 20.12.2002, *Microsoft Corp.*, 134 F.T.C. 709; vom 13.10.2011, *Google, Inc.*, 152 F.T.C. 435; vom 27.07.2012, *Facebook, Inc.* (2012), 154 F.T.C. 1.

[200] Rechtsgrundlage für solche *civil penalties:* 15 U. S. C. 45(l). Zu dem Rechtsinstitut der *civil penalties* siehe Kapitel 3:E.I.3.b) (ab S. 196).

[201] U. S. District Court D.C. vom 23.04.2020, *United States v. Facebook, Inc.*, 2020 U. S. Dist. LEXIS 72162.

[202] Bis in die 1990er ging die FTC noch davon aus, dass die Generalklausel nicht für Datenschutz geeignet sei: *Jackson,* Oral History Project: Joan Z. Bernstein, S. 240 (*Bernstein* leitete bis 2001 die Verbraucherschutzabteilung der FTC).

[203] *FTC*, Federal Trade Commission Fiscal Year 2022 Congressional Budget Justification, S. 141.

[204] *Becker*, 120 Colum. L. Rev. Forum 134, 142–148; *Hagan,* 2019 Colum. Bus. L. Rev. 735, 756 f.; *Polanco*, 36 Touro L. Rev. 603, 626.

[205] *Becker*, 120 Colum. L. Rev. Forum 134, 144.

[206] *Becker*, 120 Colum. L. Rev. Forum 134, 142–148. Bisherige Gerichtsverfahren: U. S. Court of Appeals 10th Circuit vom 29.06.2009, *FTC v. Accusearch, Inc.*, 570 F.3d 1187: durch FTC gewonnen; U. S. Court of Appeals Ww Circuit vom 24.08.2015, *FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236: durch FTC gewonnen; U. S. Court of Appeals 11th Circuit vom 06.06.2018, *LabMD, Inc. v. FTC*, 894 F.3d 1221: durch FTC verloren.

[207] *FTC*, Trade Regulation Rule on Commercial Surveillance.

können, wie Unternehmen ihre personenbezogenen Informationen verwenden.[208] Datenschutzerklärungen lesen sie typischerweise nicht.[209] Die FTC hat selbst bei massiven Gefahren für Verbraucher:innen nicht den Verstoß selbst für *unfair* gehalten, sondern bloß einen deutlichen Hinweis verlangt, damit sich Verbraucher:innen frei entscheiden können.[210] Diese starke Betonung des Selbstdatenschutzes und der Privatautonomie ist einer der zentralen Aspekte des amerikanischen Datenschutzrechts.

II. Kalifornien als Vorreiter im Datenschutz

Kalifornien verfügt über ein dem FTC-Act ähnliches Gesetz: das kalifornische Unfair Competition Law.[211] Auf seiner Basis geht der kalifornische Attorney General regelmäßig gegen Unternehmen wegen Datenschutzverstößen vor.[212] Er kann sich bei seiner Kontrolltätigkeit daneben auch auf über mehr als 100 Datenschutzgesetze stützen.[213] Diese waren auch schon vor dem CCPA die stärksten Datenschutzgesetze der Vereinigten Staaten.[214] Manche davon verstärken das Bundesrecht – so existieren zum GLBA,[215] HIPAA[216] und COPPA[217] jeweils strengere Versionen im kalifornischen Recht.[218] Aber Kalifornien reguliert auch nicht von Bundesgesetzen abgedeckte Branchen und Bereiche wie Smart TVs,[219]

---

[208] *Solove,* 126 Harv. L. Rev. 1880–1903.

[209] *Hartzog/Richards,* 61 B.C. L. Rev. 1687, 1735; *Obar/Oeldorf-Hirsch,* 23 Inf. Commun. Soc. 128, 135–142: Ergebnis eines Experiments mit einer fiktiven Datenschutzerklärung; *Park*, 10 UC Irvine L. Rev. 1455, 1463. Zu den volkswirtschaftlichen Kosten, die entstehen würden, wenn Verbraucher:innen tatsächlich jede Datenschutzerklärung lesen würden: *McDonald/Cranor*, The Cost of Reading Privacy Policies, 4 ISJLP 543–568.

[210] Z. B. für umfassendes Tracking aller besuchten Webseiten: FTC vom 31.08.2009, *Sears Holdings Management Corp.,* 148 F.T.C. 83.

[211] Cal. Bus. & Prof. §§ 17200–17210.

[212] *Citron,* 92 Notre Dame L. Rev. 747, 755–758.

[213] Liste von 119 kalifornischen Datenschutzgesetzen: *Cal. Attorney General*, Privacy Laws. Detaillierte Übersicht zu diesen: *Determann,* California Privacy Law, Chapter 2.

[214] *Chander/Kaminski/McGeveran*, 105 Minn. L. Rev. 1733, 1784; *Schwartz,* 118 Yale L. J. 902, 939; *Pardau,* 23 J. Tech. L. & Pol'y 68, 88; *Park,* 10 UC Irvine L. Rev. 1455, 1470.

[215] Financial Information Privacy Act (2003), Cal. Fin. Code § 4050–4060.

[216] Confidentiality of Medial Information Act (1981), Cal. Civ. Code §§ 56–56.37.

[217] Privacy Rights for California Minors in the Digital World Act (2013), Cal. Bus. & Prof. Code §§ 22580–22582.

[218] Bundesgesetze verdrängen i. d. R. Gesetze der Bundesstaaten (*Supremacy Clause*, U. S. Const. Art. VI cl. 2). GLBA und HIPPA ermächtigten jedoch jeweils die Bundesstaaten, strengere Regeln zu erlassen (für GLBA: 15 U. S. C. § 6807; für HIPPA: 42 U. S. C. § 1320d-7(a)). COPPA verdrängt zwar an sich widersprechende Gesetze der Bundesstaaten (15 U. S. C. § 6502(d)). Staaten können aber die von COPPA nicht erfassten über-13-Jährigen schützen (*FTC,* Amicus Brief Batman v. Facebook, S. 6–8).

[219] Act concerning Connected televisions, Cal. Bus. & Prof. Code §§ 22948.20–25.

Einzelhandel-Kundenkarten[220] und Mietwagenunternehmen.[221] Zudem gab es bereits vor dem CCPA erste Ansätze allgemein geltender Datenschutzgesetze: z. B. ein Auskunftsrecht über die Verwendung persönlicher Informationen für Werbezwecke[222] und eine Pflicht, Datenschutzerklärungen auf Webseiten zu veröffentlichen.[223]

Kalifornische Gesetze wirken auch häufig über die Grenzen Kaliforniens hinaus. Vor allem übernehmen viele kleinere Bundesstaaten die Gesetze des bevölkerungsreichsten und wirtschaftlich stärksten Bundesstaates Kalifornien.[224] Auch Unternehmen unterstützen häufig eine solche Rechtsübernahme: Unternehmen in anderen Bundesstaaten exportieren ihre Waren oft in den großen kalifornischen Markt und folgen daher ohnehin den kalifornischen Standards.[225] Solche Unternehmen haben einen Anreiz, strengere Regulierung in anderen Bundesstaaten zu unterstützen, weil dann ihre bisher unregulierten Konkurrenten den gleichen Standards folgen müssen (Kalifornien-Effekt).[226] So war beispielsweise Kalifornien in den 1960ern Vorreiter bei der Regulierung von Kfz-Abgasen.[227] Der Bund hat diese Grenzwerte 1970 übernommen, aber gleichzeitig Kalifornien erlaubt, noch strengere Grenzwerte festzusetzen.[228] Kalifornien hat diese Ermächtigung wahrgenommen, was wiederum 12 andere Staaten übernommen haben.[229]

Dieser »Kalifornien-Effekt« hat sich auch bereits im Datenschutzrecht niedergeschlagen.[230] Die von Kalifornien zuerst eingeführte Pflicht, Betroffene bei einer Datenpanne zu benachrichtigen,[231] haben inzwischen alle anderen 49 Bundesstaaten übernommen.[232] Auf der anderen Seite kann ein progressives

---

[220] Supermarkt Club Card Disclosure Act, Cal. Civ. Code §§ 1749.60–66.

[221] Act concerning electronic surveillance in rental cars, Cal. Civ. Code § 1939.23.

[222] Shine the Light Act, Cal. Civ. Code § 1798.83. Zu diesem näher beim Auskunftsrecht siehe Kapitel 3:C.III.1.a) (ab S. 116).

[223] California Online Privacy Protection Act of 2003, Cal. Bus & Prof. Code § 22575.

[224] Grundlegend: *Vogel*, Trading Up, S. 248–270.

[225] Ebd., S. 261–263.

[226] Ebd., S. 260 f.

[227] *Chanin*, 58 N.Y.U. Ann. Surv. Am. L. 699, 713–726; *Vogel*, Trading Up, S. 259.

[228] Clean Air Amendments of 1970, Pub. L. No. 91-604, 84 Stat. 1676. Die Ermächtigung ist kodifiziert in 42 U.S.C. § 7543(b). Die *Trump*-Regierung hatte die für strengere Grenzwerte nötige Genehmigung zurückgezogen, wogegen Kalifornien geklagt hat (U.S. Court of Appeals D.C., *California v. Wheeler*, Case No. 19-1239). Die *Biden*-Regierung hat die Genehmigung wieder erteilt, *EPA*, Reconsideration of a Previous Withdrawal of a Waiver of Preemption, 87 F.R. 14332

[229] 13 C.C.R. §§ 1961.3, 1962.2. Zu den weiteren Staaten: *Vogel*, Trading Up, S. 259.

[230] *Al-Saif,* 14 Wash. J. L. Tech & Arts 77, 95; *Chander/Kaminski/McGeveran*, 105 Minn. L. Rev. 1733, 1742–1744.

[231] Cal. Civ. Code § 1798.82.

[232] *National Conference of State Legislatures*, Security Breach Notification Laws. Kritisch zu dieser Regelungsvielfalt und den damit verbundenen Aufwand für Unternehmen: *Gaglione,* 67 Buffalo L. Rev. 1133, 1149 f.

kalifornisches Gesetz gerade auch den Bund inspirieren, durch einen »faulen Kompromiss« strengere Gesetze der Bundesstaaten zu verhindern. So hatte Kalifornien z. B. ein strenges Gesetz zu Spam-Werbung verabschiedet, nach dem das Zusenden von Werbe-E-Mails nur mit vorheriger ausdrücklicher Einwilligung (*opt-in)* zulässig ist (von engen Ausnahmen abgesehen).[233] Der Bund hat als Reaktion darauf[234] den Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (CAN-SPAM-Act)[235] erlassen, der nur eine Widerspruchsmöglichkeit gegen Werbemails vorsieht (*opt-out*) und zugleich strengere Gesetze der Bundesstaaten ausschließt.[236]

III. Fazit

Das amerikanische Datenschutzrecht zeigt, dass es bei Rechtsvergleichung nicht genügt, nur Gesetze und Urteile zu betrachten.[237] Nicht die lückenhaften Gesetze prägen den amerikanischen Datenschutz, sondern die politisch äußerst geschickt vorgehende FTC. Dieser ist es gelungen, einen datenschutzrechtlichen Mindeststandard zu etablieren, der durch Privatautonomie geprägt ist. Verbraucher:innen sollen sich anhand umfassender Informationen *(notice)* selbstbestimmt für oder gegen bestimmte Datenverarbeitungen entscheiden *(choice)*. Selbst scharfe Kritiker von *notice and choice* halten eine Abkehr von diesem tief im amerikanischen Datenschutzrecht verwurzelten Ansatz für einen zu drastischen Paradigmenwechsel.[238] Dieser Ansatz ist auch derjenige, der neueren Gesetzentwürfen für umfassende Datenschutzgesetze im U. S. Kongress zugrundeliegt – nicht etwa eine Verallgemeinerung branchenspezifischer Gesetze.[239] Daneben fokussiert sich die FTC auf Datensicherheit – ein Thema, das auch durch die unten dargestellten Sammelklagen nach Datenpannen[240] eine erhebliche Bedeutung im amerikanischen Datenschutzrecht erlangt hat.

Die branchenspezifischen Datenschutzgesetze sind demgegenüber bloße *ad-hoc*-Maßnahmen, die sich nicht zu einem Gesamtsystem zusammensetzen. Zwar gehen manche punktuellen Datenschutzanforderungen sogar über die der DSGVO hinaus, wie das Beispiel des Minderjährigenschutz des COPPA zeigt.

---

[233] Restrictions On Unsolicited Commercial E-Mail Advertisers (2003), Cal. Bus. & Prof. Code § 17529.2(a),(b).

[234] So explizit die Erwägungsgründe: 15 U. S. C. § 7701(a)(11).

[235] Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003, Pub.L. 108–187, 117 Stat. 2699, kodifiziert in: 15 U. S. C. § 7704(a)(4)(A). Zu recht kritisch dazu: *Hoofnagle,* FTC, S. 244–249.

[236] 15 U. S. C. § 7707(b).

[237] Vgl. allgemein *Kischel*, Rechtsvergleichung, Rn. 229–234.

[238] *Solove/Schwartz*, ALI Data Privacy: Overview and Black Letter Text, S. 15 f.

[239] Insbesondere Consumer Privacy Protection Act of 2011, H.R.1528, 112th Cong. (2011); Privacy Bill of Rights Act of 2015, Diskussionsentwurf der Regierung, https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf [perma.cc/LG35-TFNC]; Consumer Online Privacy Rights Act, S.2968, 116th Cong. (2019).

[240] Siehe Kapitel 3:E.II.1 (ab S. 204).

Allerdings erfassen sie viele Branchen nicht und erreichen auch in den regulierten Branchen in der Regel nur einen lückenhaften Schutz.

So kann man konstatieren, dass es zwar in den Vereinigten Staaten zahlreiche Ansätze eines fortschrittlichen Datenschutzrechts gibt, sich diese aber bisher nicht zu einem kohärenten Ganzen zusammensetzen. Daher war es naheliegend, dass ein Bundesstaat diese Lücke füllt und als Experiment ein umfassendes Datenschutzgesetz erlässt.

C. Gesetzgebungsgeschichte

I. Handlungsdruck durch erstes Volksbegehren (2017—2018)

Kalifornien verfügt über starke Elemente direkter Demokratie.[241] Neben vom Parlament initiierten Volksentscheiden – wie denjenigen, der das *right to privacy* in die kalifornische Verfassung eingeführt hat[242] – hat das Volk zahlreiche Gesetze eingebracht.[243] Kalifornische Wähler:innen entscheiden im Durchschnitt über circa 14 kalifornienweite Volksentscheide pro zweijähriger *general election.*[244] Die Schwelle für deren Einbringung liegt niedrig. So beträgt das Unterschriftenquorum nur 5 % der Personen, die bei der jeweils letzten Wahl zum Gouverneur teilgenommen haben[245] (d. h. 1–2 % der Gesamtbevölkerung). Bei der Abstimmung genügt eine einfache Mehrheit.[246] Die einzige inhaltliche Anforderung ist, dass ein Volksentscheid nur ein Thema betreffen darf,[247] was der kalifornische Supreme Court zudem weit auslegt.[248]

Es war naheliegend, dass ein Volksbegehren diesen Mechanismus nutzt, um ein populäres, umfassendes Datenschutzgesetz zu erreichen. Man kann die Geschichte dieses Volksbegehrens leicht als die Geschichte eines einzelnen Mannes erzählen: des Multimillionärs und ehemaligen Immobilienhändlers *Alastair Mactaggart*. Er war zugleich Vorsitzender, primärer Geldgeber und Hauptautor des Volksbegehrens.[249] Dann würde man aber übersehen, dass ohne eine grundsätzliche Sympathie der kalifornischen Bevölkerung für den Datenschutz kein

---

[241] *Kelso*, 19 Pepp. L. Rev. 327, 340–344.

[242] Siehe Kapitel 2:A.II (ab S. 15).

[243] *Carrillo et al.*, 92 S. Cal. L. Rev. 557, 573–588 mit einer Statistik zu verfassungsändernden Volksentscheiden; *Kelso*, 19 Pepp. L. Rev. 327, 340–344.

[244] Zeitraum 2010–2020: *Lucy Burns Institute,* Ballotpedia*,* Number of ballot propositions per decade in California. Volksentscheide werden i. d. R. bei der zweijährlichen *general election* abgestimmt, Cal. Const Art. II § 8(c), Cal. Elec. Code § 1200.

[245] Cal. Const Art. II § 8(b).

[246] Cal. Const. Art. II § 10(a).

[247] Cal. Const § 8(d).

[248] Cal. Supreme Court vom 24.08.2017, *Briggs v. Brown,* 3 Cal. 5th 808, 828.

[249] *Confessore*, New York Times, The Unlikely Activists Who Took On Silicon Valley – and Won: fokussiert sich auf *Mactaggert*. Der Autor begründet diese Fokussierung in einem anderen Beitrag mit den Unterschieden zwischen wissenschaftlichen und journalistischem

Volksbegehren erfolgreich gewesen wäre. Kalifornische Wähler:innen stimmen, wenn sie über ein Thema nichts wissen, typischerweise mit »Nein«.[250] Zumindest eine grundsätzliche Beliebtheit des Themas ist nötig, auch wenn sich Wähler:innen in der Regel nur sehr oberflächlich mit Details auseinandersetzen. Datenschutz ist jedoch auch in der amerikanischen Gesellschaft beliebt: so wünschten sich in einer Umfrage des renommierten *Pew Research Center* 81 % der demokratischen und 70 % der republikanischen Wähler:innen strengere Datenschutzgesetze.[251]

Ein Volksbegehren ermöglicht es Interessengruppen, solche vagen Erwartungen zu einem konkreten Gesetz zu verdichten. Das dem CCPA-2018 zugrundeliegende Volksbegehren hat die erst Anfang 2016 gebildete Bürgerinitiative Californians for Consumer Privacy eingebracht. Diese war klein und hat sich nur für das Volksbegehren gegründet.[252] Den Kern bildeten dabei mit dem Immobilienhändler *Alastair Mactaggart* und dem Finanzkaufmann *Richard Arney* nicht Juristen, sondern zwei Unternehmer ohne frühere Tätigkeit im Datenschutz. Über die genaue Entstehung des Gesetzestextes ist wenig bekannt. *Chris Hoofnagle*, Universitätsprofessor und Direktor des Center for Law & Technology an der University of California, Berkeley, war zumindest als Ideengeber beteiligt.[253] Den konkreten Gesetzestext hat *Alastair Mactaggart* zusammen mit *Ashkan Soltani*, einem bekannten Datenschutzaktivisten und früherem Chief Technologist der FTC,[254] und *Mary Ross*, einer früheren CIA-Analystin und Datensicherheits-Expertin,[255] geschrieben.[256] Dieser Gesetzentwurf trug bereits den Namen »California Consumer Privacy Act« und ist sehr ähnlich zu dem verabschiedeten Gesetz.

Californians for Consumer Privacy reichte im November 2017 diesen Gesetzesentwurf offiziell ein[257] und begann Unterschriften zu sammeln. Daraufhin meldete im Januar 2018 die California Chambers of Commerce – der größte

---

Stil: *Confessore,* The N.Y. Times, Demystifying Online Privacy, Through the Story of the Man Who Took On Silicon Valley.

[250] *Carrillo et al.*, 92 S.Cal. L.Rev. 557, 598.

[251] *Pew Research Center*, Americans and Privacy, S. 43. Vgl. auch: *Gallup News Service,* Facebook, Google and Internet Privacy: von amerikanischen Facebook-Nutzer:innen seien 55 % »Very concerned« und 25 % »Somewhat concerned« über Facebooks Datenverarbeitung.

[252] *Confessore*, N.Y. Times, The Unlikely Activists Who Took On Silicon Valley – and Won.

[253] *Hoofnagle*, Comments on the CCPA.

[254] *Confessore*, N.Y. Times, The Unlikely Activists Who Took On Silicon Valley – and Won. Dieser wurde später Executive Director der California Privacy Protection Agency, siehe Kapitel 3:E.I.2.a) (ab S. 182).

[255] *Hill,* Jezebel, How a Woman Disappears from the History Books.

[256] Es gibt starke Indizien, dass bei der Formulierung auch eine auf Volksbegehren spezialisierte Kanzlei mitgewirkt hat: *Californians for Consumer Privacy*, The Consumer Right to Privacy Act of 2018, S. 1: Eine solche Kanzlei ist als Ansprechpartner für alle Fragen zum Volksbegehren genannt; *Confessore*, N.Y. Times, The Unlikely Activists Who Took On Silicon Valley – and Won: das erste Treffen von *Mactaggart* und *Soltani* fand in deren Kanzlei statt.

[257] *Californians for Consumer Privacy*, The Consumer Right to Privacy Act of 2018 (trotz der Überschrift des Briefes ist der Gesetzestext selbst als »California Consumer Privacy Act of 2018« überschrieben).

Wirtschaftsverband in Kalifornien – das Oppositionskommittee Committee to Protect California Jobs an; Facebook, Google, Microsoft und die größten drei amerikanischen Telekommunikationsbetreiber steuerten einen großen Teil der Finanzierung bei.[258] Das Committee to Protect California Jobs stütze sich vor allem auf die hohen Umsetzungskosten des CCPA-2018 und die Rechtsunsicherheit, die durch ein Privatklagerecht entstehe.[259]

Dieser Gegeninitiative hat allerdings der Cambridge-Analytica-Skandal im März 2018 den »Wind aus den Segeln genommen«. Das Politikberatungsunternehmen Cambridge Analytica hatte personenbezogene Daten von 87 Millionen[260] Facebook-Nutzer:innen (davon 6,7 Millionen Kalifornier:innen)[261] erlangt.[262] Diese Daten waren so detailliert, dass Cambridge Analytica daraus psychografische Profile erstellen und Wahlwerbung individuell ausrichten konnte.[263] Im U. S.-Präsidentschaftswahlkampf 2016 haben die Kandidaten *Ted Cruz* und *Donald Trump* diese Technik genutzt.[264] Dieser Skandal hat das öffentliche Misstrauen gegenüber der Datenverarbeitung großer Unternehmen wesentlich verstärkt.[265]

II. Kurzes Gesetzgebungsverfahren (2018)

In diesem datenschutzfreundlichen Klima konnte Californians for Consumer Privacy einen günstigen Kompromiss abschließen: Das kalifornische Parlament hat ihren Gesetzentwurf weitgehend übernommen. Californians for Consumer Privacy hat im Gegenzug das Volksbegehren zurückgezogen.

Dies war das Ergebnis nicht-öffentlicher Verhandlungen im Mai und Juni 2018. Beteiligt waren zwei kalifornische Parlamentarier (Senator *Hertzberg* und Assembly Member *Chau*),[266] die Chamber of Commerce und Californians for

---

[258] *Cal. Secretary of State*, Cal. Access, Contributions Received by Committee to Protect California Jobs.

[259] *Confessore*, N.Y. Times, The Unlikely Activists Who Took On Silicon Valley – and Won. Zur Skepsis gegenüber einem Privatklagerecht siehe Kapitel 3:E.II.2.d) (ab S. 214).

[260] *Facebook*, About Facebook, An Update on Our Plans to Restrict Data Access on Facebook.

[261] *Facebook*, About Facebook, An Update on Our Plans to Restrict Data Access on Facebook, Anhang »State-by-State Breakdown«.

[262] *Cadwalladr/Graham-Harrison,* The Guardian, Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach; *Rosenberg/Confessore/Cadwalladr,* N.Y. Times, How Trump Consultants Exploited the Facebook Data of Millions.

[263] *Rosenberg/Confessore/Cadwalladr,* N.Y. Times, How Trump Consultants Exploited the Facebook Data of Millions.

[264] *Rosenberg/Confessore/Cadwalladr,* N.Y. Times, How Trump Consultants Exploited the Facebook Data of Millions.

[265] *Slicktext*, One Year After Cambridge Analytica, Survey Reveals Strong Consumer Privacy Fears Remain.

[266] Das kalifornische Parlament besteht aus dem Unterhaus Cal. State Assembly und dem Oberhaus California State Senate, Cal. Const. Art. IV § 1.

Consumer Privacy.[267] *Hertzberg* und *Chau* wollten lieber ein Parlamentsgesetz erreichen, da bei einem erfolgreichen Volksentscheid der CCPA nur noch schwer zu ändern gewesen wäre.[268] Dafür wäre entweder eine mit den Zielen des CCPA inhaltlich kompatible Änderung in Kombination mit einer Mehrheit von 70 % in beiden Parlamentskammern oder ein neuer Volksentscheid erforderlich gewesen.[269] Die Chamber of Commerce hatte eine schlechte Verhandlungsposition. Der CCPA hatte in ihren internen Umfragen sehr gute Ergebnisse erzielt.[270] Eine große Werbekampagne gegen den CCPA hätte das Misstrauen der Bevölkerung im Zuge des Cambridge-Analytica-Skandals potenziell noch verstärkt und wäre zudem wohl nicht erfolgreich gewesen.[271]

Diese gute Verhandlungsposition des Volksbegehrens spiegelt sich im gefundenen Kompromiss wieder. Diesen haben *Hertzberg* und *Chau* als A. B. 375 am 21.08.2018 in das kalifornische Parlament eingebracht.[272] Im einwöchigen Gesetzgebungsverfahren wurde er nur minimal verändert.[273] Das wesentliche Zugeständnis seitens Californians for Consumer Privacy war die Beschränkung des Privatklagerechts auf Datenpannen.[274] Außerdem hat das Parlament Unternehmen eine 30-tägige Abhilfefrist eingeräumt, bevor der kalifornische Attorney General gegen sie vor Gericht vorgehen konnte.[275] Ein weiteres Zugeständnis war die Zulassung von finanziellen Anreizen für die Einwilligung in Datenhandel.[276] Stellenweise wurde der CCPA auch erweitert, insbesondere wurde ein Recht auf Löschung eingeführt.[277]

Beide Kammern des kalifornischen Parlaments (Senate und Assembly) haben den CCPA-2018 am 28.06.2018 einstimmig verabschiedet[278] (dem letzten Tag, an dem ein Zurückziehen des Volksbegehrens möglich war).[279] Am selben Tag hat der kalifornische Gouverneur das Gesetz unterschrieben und Californians for Consumer Privacy das Volksbegehren zurückgezogen.[280]

---

[267] *Confessore*, N.Y. Times, The Unlikely Activists Who Took On Silicon Valley – and Won.

[268] Ebd.

[269] *Californians for Consumer Privac*y, The Consumer Right to Privacy Act of 2018, Sec. 5(a).

[270] *Confessor*e, N.Y. Times, The Unlikely Activists Who Took On Silicon Valley – and Won.

[271] *Confessor*e, N.Y. Times, The Unlikely Activists Who Took On Silicon Valley – and Won; *Fang,* The Intercept, Google and Facebook Are Quietly Fighting California's Privacy Rights Initiative, Emails Reveal.

[272] A. B. 375, 2017–18 Reg. Sess. (Cal. 2018), Stat. 2018, Ch. 55. Dazu: Cal. Legislature, AB 375 History.

[273] Inhaltlich hat das Parlament nur die *data-breac*h-Definition geändert: *Cal. Legislatur*e, AB 375 Version 06/28/18 compared to Version 06/21/18.

[274] Cal. Civ. Code § 1798.150(c).

[275] CCPA-2018, Sec. 3, § 1798.155(c).

[276] Cal. Civ. Code § 1798.125(b).

[277] Cal. Civ. Code § 1798.105.

[278] *Cal. Legislature*, AB 375 Votes.

[279] Volksbegehren dürfen nur bis 131 Tage vor der Abstimmung zurückgezogen werden, Cal. Elec. Code § 9604(b), 9033(b)(2).

[280] *Cal. Secretary of State,* Proponents Withdraw Initiative to Establish New Consumer

III. Korrekturen durch Gesetzesänderungen und Konkretisierung durch die erste Durchführungsverordnung (2018—2020)

Das schnelle Gesetzgebungsverfahren hat zu diversen Redaktionsfehlern und Unklarheiten geführt, welche das kalifornische Parlament durch diverse Gesetzesänderungen bis zum Inkrafttreten des CCPA am 01.01.2020[281] teilweise beseitigt hat. Die verabschiedeten Gesetzesänderungen waren eher kleinere Korrekturen:

- S. B. 1121 hat nur wenige Wochen nach der Verabschiedung des CCPA diverse Rechtschreibfehler und Ungenauigkeiten behoben.[282]
- A. B. 25[283] und A. B. 1281[284] verlängerten die Übergangsfrist für Arbeitsverhältnis und Kommunikation zwischen Unternehmen um jeweils ein Jahr (wobei Proposition 24 diese um ein weiteres Jahr verlängert hat und endgültiges Auslaufdatum der Ausnahme jetzt der 01.01.2023 ist).[285]
- A. B. 874 erweiterte die Ausnahme für Daten aus öffentlichen Registern.[286]
- A. B. 1146 stellte klar, dass die Übermittlung von persönlichen Informationen einer Autowerkstatt an den Autohersteller, soweit für einen Produktrückruf oder Garantieansprüche nötig, kein Datenhandel ist.[287]
- A. B. 1355 erweiterte die Informationspflichten um die Mitteilung, dass Verbraucher:innen über ein Auskunftsrecht und Recht auf Löschung verfügen.[288]
- A. B. 1564 erlaubte Unternehmen für Auskunftsanfragen statt einer gebührenfreien Telefonnummer auch eine Post- und E-Mail-Adresse anzugeben.[289]
- A. B. 713 harmonisierte die Ausnahmen für deidentifizierte Gesundheitsdaten mit dem für die Gesundheitsbranche geltenden Datenschutzgesetz HIPAA.[290]

Substantielle Änderungen hat das Parlament jedoch abgelehnt. Wirtschaftsverbände hatten wiederholt versucht, den CCPA aufzuweichen.[291] Abgelehnte

---

Privacy Rights; Expand Liability for Consumer Data Breaches; *Anderson*, The Sacramento Bee, California's new initiative process.

[281] Cal. Civ. Code § 1798.198(a).

[282] S.B. 1121, 2017–18 Leg., Reg. Sess. (Cal. 2018), Cal. Stats. 2018, Ch. 735, Sec. 8.

[283] A. B. 25, 2017–18 Leg., Reg. Sess. (Cal. 2019), Cal. Stats. 2019, Ch. 763, Sec. 2.3.

[284] A. B. 1281, 2019–20 Leg., Reg. Sess. (Cal. 2020), Cal. Stats. 2020, Ch. 268, Sec. 1.

[285] Cal. Civ. Code § 1798.145(m)(4),(n)(3).

[286] A. B. 874, 2017–18 Leg., Reg. Sess. (Cal. 2019), Cal. Stats. 2019, Ch. 748, Sec. 1. Siehe Kapitel 3:B.I.3 (ab S. 50).

[287] A. B. 1146, 2017–18 Leg., Reg. Sess. (Cal. 2019), Cal. Stats. 2019, Ch. 751, Sec. 1. Siehe Kapitel 3:C.I.2.a) (ab S. 82).

[288] A. B. 1355, 2017–18 Leg., Reg. Sess. (Cal. 2019), Cal. Stats. 2019, Ch. 757, Sec. 1.

[289] A. B. 1564, 2017–18 Leg., Reg. Sess. (Cal. 2019), Cal. Stats. 2019, Ch. 759, Sec. 1. Siehe Kapitel 3:C.III.2.a) (ab S. 125).

[290] A. B. 713, 2019–20 Leg., Reg. Sess. (Cal. 2020), Cal. Stats. 2020, Ch. 171, Sec. 1. Siehe Kapitel 3:B.I.2 (ab S. 47).

[291] *Forsheit,* Technology & Marketing Law Blog, And At the End of the Day, the CCPA Remains Very Much the Same; *Park,* 10 UC Irvine L Rev 1455, 1488; *Romm*, California adopted the country's first major consumer privacy law. Now, Silicon Valley is trying to rewrite it; *Urgoiti,* 53 U.C. Davis L. Rev. 1689, 1692 f.

Gesetzesentwürfe hätten insbesondere eine nahezu vollständige Ausnahme für IP-Adressen und pseudonymisierte Daten eingeführt[292] und Werbetracking von der Datenhandelsdefinition ausgenommen.[293] Auf der Kehrseite hat das kalifornische Parlament auch Gesetzesentwürfe abgelehnt, die den CCPA gestärkt hätten.[294] So ist der CCPA am 01.01.2020[295] weitgehend unverändert in Kraft getreten.

Parallel dazu hat der kalifornische Attorney General die im CCPA vorgesehene Verordnungsermächtigung[296] genutzt und nach einem längeren öffentlichen Verordnungsgebungsverfahren am 14.08.2020 eine Durchführungsverordnung erlassen.[297] Diese Durchführungsverordnung konkretisiert die Informationspflichten,[298] das Verfahren für die Ausübung der Verbraucherrechte[299] und die Zulässigkeit finanzieller Anreize für die Einwilligung in Datenhandel[300]. Sie sorgt dabei durch ihren großem Detailgrad für Rechtssicherheit, verändert den CCPA aber nur unerheblich.

IV. Volksentscheid Proposition 24 (2019—2020)

Diesen inhaltlichen Stillstand hat Californians for Consumer Privacy zum Anlass genommen, ein neues Volksbegehren zu initiieren, um den CCPA-2018 zu reformieren und vor einer Aufweichung zu schützen. Dieses Volksbegehren hat das kalifornische Volk am 03.11.2020 als »Proposition 24« mit einer Mehrheit von 56 % angenommen.[301] Das Änderungsgesetz selbst hieß »California Privacy Rights Act of 2020«, wobei die amtliche Überschrift des novellierten Gesetzes weiterhin »California Consumer Privacy Act« ist,[302] sodass der Name CCPA auch nach Inkrafttreten am 01.01.2023[303] bleiben wird. Proposition 24 stellt sich insgesamt auch mehr als evolutive, logische Fortsetzung des CCPA-2018 dar.

Der Gesetzestext der Proposition 24 ist 2019 in einem transparenten Verfahren unter Beteiligung zahlreicher Interessengruppen entstanden. Zuerst hat

---

[292] A. B. 873, 2019–20 Leg., Reg. Sess. (Cal. 2019).

[293] S.B. 753, 2019–20 Leg., Reg. Sess. (Cal. 2019).

[294] S.B. 561, 2019–20 Leg., Reg. Sess. (Cal. 2019) hätte ein allgemeines Privatklagerecht eingeführt. A. B. 1760, 2019–20 Leg., Reg. Sess. (Cal. 2019) hätte Datenhandel nur bei einer aktiven Einwilligung erlaubt.

[295] Cal. Civ. Code § 1798.198(a).

[296] Cal. Civ. Code § 1798.185. Zu dieser und dem Verordnungsgebungsverfahren siehe Kapitel 3:E.I.2.c) (ab S. 187).

[297] Cal. Office of Administrative Law, Notice of Approval. Kodifiziert in 11 C. C. R. §§ 7000–337. Nach dem CCPA-2018 sollte die Durchführungsverordnung bis spätestens 01.07.2020 in Kraft treten, § 1798.185(a).

[298] 11 C. C. R. §§ 7010–7016.

[299] 11 C. C. R. §§ 7020–7031.

[300] 11 C. C. R. §§ 7080–7081.

[301] *Cal. Secretary of State*, Statement of Vote: General Election November 3, 2020, S. 67.

[302] Cal. Civ. Code, title 1.81.5.

[303] Proposition 24 (Cal. 2020), Sec. 31(a).

Californians for Consumer Privacy im September 2019 einen ersten Entwurf veröffentlicht[304] und an zahlreiche Wirtschaftsverbände, Verbraucherschutzorganisationen und Rechtswissenschaftler:innen verschickt.[305] Daran schlossen sich mehrwöchige Verhandlungen mit Wirtschaftsverbänden und Verbraucherschutzorganisationen an.[306] Diese führten am Ende zu dem Kompromiss, den Californians for Consumer Privacy im November 2019 als endgültigen Gesetzesentwurf eingereicht hat[307] und den am Ende die Wähler:innen angenommen haben.

Der endgültige Gesetzestext der Proposition 24 erweitert die Verbraucherrechte und Unternehmenspflichten deutlich. So erhalten Verbraucher:innen ein Recht auf Beschränkung sensibler Informationen[308] und ein Recht auf Berichtigung.[309] Zudem verpflichtet Proposition 24 Unternehmen auf Datenminimierung, Speicherfristbegrenzung und Datensicherheit.[310] Darüber hinaus enthält Proposition 24 auch viele Klarstellungen und redaktionelle Änderungen.[311]

Vor allem aber stärkt Proposition 24 die Rechtsdurchsetzung, indem es die erste unabhängige Datenschutzbehörde der Vereinigten Staaten geschaffen hat. Die California Privacy Protection Agency verfügt über umfassende Untersuchungs- und Abhilfebefugnisse, insbesondere kann sie Bußgelder in beträchtlicher Höhe verhängen.[312] Zudem kann sie sich auch selbst das Recht schaffen, das sie durchsetzt, da die Verordnungsermächtigung des Attorney General auf sie übergeht.[313] Diese Änderungen lassen einen deutlichen Einfluss der DSGVO erkennen – insoweit war erklärtes Ziel der Proposition 24, einen Angemessenheitsbeschluss zu erlangen.[314]

---

[304] *Californians for Consumer Privacy*, The California Privacy Rights and Enforcement Act of 2020.

[305] *Carson*, The Privacy Advisor, On keynote stage, Mactaggart addresses his »new« CCPA.

[306] *Lapowsky*, Inside the closed-door campaigns to rewrite California privacy law, again. Offener Brief der Verbraucherschutzorganisationen zu diesen Verhandlungen: *American Civil Liberties Union of California et al.*, California Privacy Rights and Enforcement Act – Privacy Coalition Comments. Zuordnung konkreter Änderungen zu bestimmten Autor:innen: *Soltani*, Twitter-Beitrag vom 24.07.2020.

[307] *Californians for Consumer Privacy*, California Privacy Rights and Enforcement Act of 2020, Version 3.

[308] Cal. Civ. Code § 1798.121.

[309] Cal. Civ. Code § 1798.106.

[310] Cal. Civ. Code § 1798.100(a),(c).

[311] Insbesondere die Klarstellung, dass eine Weiterübermittlung für gezielte Werbung Datenhandel ist, siehe Kapitel 3:C.I.2.a) (ab S. 82).

[312] Cal. Civ. Code § 1798.155. Näher zur California Privacy Protection Agency siehe Kapitel 3:E.I.2 (ab S. 182).

[313] Cal. Civ. Code § 1798.185.

[314] *Angwin*, The Markup, Tech on the Ballot: Interview with Ashkan Soltani; *Bracy*, Alastair Mactaggart on California's Prop 24, 43m:00s; *Californians for Consumer Privacy*, Prop 24 Webinar, 13m:00s; *Kohne/Reed/Kurzweil*, Law360, Calif. Privacy Law Resembles, Transcends EU Data Regulation.

Insgesamt waren wohl weder Wirtschaftsverbände noch Verbraucherschutzorganisationen völlig zufrieden mit dem gefundenen Kompromiss. Werbeunternehmen kritisierten die geschaffene Rechtsunsicherheit durch das Angehen einer Gesetzesreform, noch bevor der CCPA-2018 überhaupt am 01.01.2020 in Kraft getreten war.[315] Verbraucherschutzorganisationen nahmen Anstoß an dem weiterhin fehlenden allgemeinen Privatklagerecht und der Zulässigkeit des Geschäftsmodells »Leistung gegen Daten«.[316] Jedoch wollte keine Seite signifikante Geldsummen ausgeben, um Proposition 24 zu verhindern.

Dementsprechend ist Proposition 24 ab der Einreichung des Volksbegehrens ohne größeren Widerstand »durchgesegelt«. Es gab zwar ein Oppositionskommitee, dieses konnte allerdings mit seinen geringen Spenden von insgesamt nur 20.223 $[317] keine wirksame Öffentlichkeitsarbeit gegen Proposition 24 betreiben. Proposition 24 ist es gelungen, trotz der Covid-19-Pandemie 930.983 Unterschriften noch rechtzeitig[318] am 04.05.2020 einzureichen und damit das Unterschriftenquorum von 623.212 Unterschriften deutlich überzuerfüllen.[319] Bis zur Wahl am 03.11.2020 gab es neben Diskussionen in sozialen Medien nur einige Zeitungsartikel für und gegen Proposition 24.[320] Insgesamt war das Interesse der Öffentlichkeit jedoch nur gering ausgeprägt. Nur wenige Wochen vor der Wahl ergab eine unabhängige Umfrage, dass nur 26 % der Wähler:innen

---

[315] *Association of National Advertisers et al.*, Statement of Opposition to Proposition 24: The California Privacy Rights Act of 2020 Ballot Initiative.

[316] *American Civil Liberties Union of California et al.*, California Privacy Rights and Enforcement Act – Privacy Coalition Comments S. 7, 17; *Bensinger*, N.Y. Times, A Privacy Measure That's Hard to Like; *Fowler*, Washington Post, Privacy advocates battle each other over whether California's Proposition 24 better protects consumers; *Reader*, Fast Company, California's Proposition 24 is an ambitious – but controversial – privacy overhaul; *Snow/Conley*, ACLU Northern California, Californians Should Vote No on Prop 24; *Tien/Schwartz/Tskukayama*, Why EFF Doesn't Support California Proposition 24.

[317] *Cal. Secretary of State*, CalAccess: California Consumer and Privacy Advocates Against Prop 24.

[318] Eine Stichprobe der Unterschriften musste bis zum 25.06.2020 ausgezählt sein. Die Countys hatten ursprünglich bis zum 26.06.2020 Zeit, diese Stichprobe zu erstellen. Angesichts der Gefahr, die Frist für die Wahl im November 2020 zu verpassen, hat der Cal. Superior Court Sacramento die Frist für die Countys ebenfalls auf dem 25.06.2020 verkürzt, vgl. Cal. Superior Court Sacramento vom 19.06.2020, *Alastair Mactaggart et al. v. Alex Padilla*, Case No. 34-2020-80003402, https://elections.cdn.sos.ca.gov/ballot-measures/pdf/1879-court-order.pdf [perma.cc/B6TG-RMUJ].

[319] *Californians for Consumer Privacy*, CPRA Ballot Signatures Submitted; *dies.*, CPRA Qualifies for Nov 2020 Ballot. Das Unterschriftenquorum von 623.212 entspricht 5 % der Summe aller Wähler:innen bei der letzten Gouverneurswahl, Cal. Const. Art. II § 8(b).

[320] *Bensinger*, N.Y. Times, A Privacy Measure That's Hard to Like; *Fowler*, Washington Post, Privacy advocates battle each other over whether California's Proposition 24 better protects consumers; *Hertzberg*, Give consumers back their power over data breaches; *Los Angeles Times Editorial Board*, Endorsement: Yes on Prop. 24. It's not perfect, but it would improve online privacy; *San Francisco Chronicle Editorial Board*, Chronicle recommends: Vote no on Prop. 24, a flawed privacy initiative.

Proposition 24 kannten.[321] Die demokratische Partei war neutral, während die republikanische Partei Proposition 24 wegen der mit der California Privacy Protection Agency neu geschaffenen »Bürokratie« ablehnte.[322]

Bei der Wahl am 03.11.2020 hat das kalifornische Volk Proposition 24 mit deutlicher Mehrheit angenommen (56,2 % Ja-Stimmen und 43,8 % Nein-Stimmen).[323] Dabei haben wohl vor allem republikanische Wähler:innen gegen Proposition 24 gestimmt, da nahezu jeder County, in dem Proposition 24 mehr Nein- als Ja-Stimmen erzielt hat, auch mehrheitlich für den republikanischen Präsidentschaftskandidaten *Donald Trump* gestimmt hat.[324]

Ist ein solches Volksbegehren die optimale Lösung für die Novelle eines umfassenden Datenschutzgesetzes? Die Komplexität der Änderung eines solch umfangreichen Gesetzes ist für Wähler:innen kaum in Gänze zu verstehen. Allerdings war Proposition 24 nur erfolgreich, weil Privatsphäre und Datenschutz für Wähler:innen positiv besetzt sind. Natürlich erlaubt der Volksbegehrensprozess den wenigen Initiator:innen des Volksbegehrens, die Details des Gesetzes zu gestalten, da Wähler:innen nur über »Ja« oder »Nein« entscheiden und die Details in der Regel nicht kennen. Allerdings kennen auch Parlamentarier:innen in der Regel nicht jedes Gesetz im Detail. Vielmehr stellt das Parlament bereits auf einer früheren Ebene in Ausschusssitzungen und informellen Absprachen einen ausgewogenen Ausgleich aller beteiligten Interessen sicher. Kalifornische Volksbegehren haben einen starken Anreiz, ebenfalls ein solches Verfahren durchzuführen. Die kalifornische Wählerschaft lehnt traditionell Volksbegehren im Zweifel eher ab. Eine gut finanzierte Opposition konnte historisch nahezu jedes Volksbegehren zum Scheitern bringen, indem sie genug Zweifel säht.[325] Daher versuchen viele Volksbegehren bereits im Vorfeld, alle Interessengruppen soweit zufrieden zu stellen, dass diese keinen Wahlkampf gegen das Volksbegehren betreiben. Wenn dies wie bei Proposition 24 gelingt, führt dies zu einem ausgewogenen Gesetzestext, wie er so ähnlich auch im parlamentarischen Verfahren entstanden wäre.

V. Weitere Gesetzesänderungen und erweiterte Durchführungsverordnung (2021—2022)

Ändern kann den CCPA in der Fassung der Proposition 24 entweder ein neuer Volksentscheid[326] oder das kalifornische Parlament mit einfacher Mehrheit, wenn

---

[321] *Redfield & Wilton Strategies*, Proposition 22, and Proposition 24 Voting Intentions (19-21 September).

[322] *California Republican Party*, Endorsements.

[323] *Cal. Secretary of State*, Statement of Vote: General Election November 3, 2020, S. 67.

[324] *Cal. Secretary of State*, Statement of Vote: General Election November 3, 2020, S. 18–20, 64 f.

[325] *Carrillo et al.*, 92 S. Cal. L. Rev. 557, 598.

[326] Cal. Const. Art. II, § 10(c).

das Parlament die in Proposition 24 festgelegten Bedingungen erfüllt.[327] Eine Änderung durch das Parlament muss mit den Zielen der Proposition 24 vereinbar sein.[328] Kalifornische Gerichte betrachten dabei den Zweck des gesamten Volksentscheides.[329] Zentral ist, dass Änderungen nicht das Datenschutzniveau senken dürfen,[330] dessen Stärkung das zentrale Ziel der Proposition 24 war.[331] Tendenziell legt die Rechtsprechung solche Öffnungsklauseln sehr eng aus – so haben kalifornische Gerichte beispielsweise bereits drei Parlamentsgesetze für nichtig erklärt, weil sie gegen den wortlautgleichen Änderungsmaßstab der 1988 angenommen Proposition 103 verstießen.[332] Zudem darf das kalifornische Parlament den CCPA ändern, um einer gerichtlich festgestellten Unwirksamkeit wegen Verfassungsverstoßes oder einem Verstoß gegen Bundesrecht abzuhelfen.[333]

Bisher hat das kalifornischen Parlament nach Proposition 24 den CCPA nur minimal geändert:

- A. B. 335 hat die klarstellende Ausnahme von der Datenhandelsdefinition und vom Recht auf Löschung für Garantieansprüche und Produktrückrufe von KfZ auf Wasserfahrzeuge erweitert.[334]
- A. B. 694 hat neben grammatikalischen Korrekturen einen Redaktionsfehler der Proposition 24 berichtigt.[335] Proposition 24 sprach an zwei Stellen davon, dass die Verordnungsermächtigung entweder am 01.07.2021 übergeht oder sechs Monate, nachdem die California Privacy Protection Agency dem Attorney General mitgeteilt hat, dass sie ausreichend zur Übernahme der Verordnungsermächtigung bereit ist. An einer Stelle hieß es, dass der frühere der beiden Termine gelten solle, während an der anderen Stelle der spätere der beiden Termine als maßgeblich aufgeführt war.[336] A. B. 694 hat dies im Sinne des späteren Termins aufgelöst.

---

[327] Proposition 24 (Cal. 2020), Sec. 25(a).

[328] Proposition 24 (Cal. 2020), Sec. 25(a).

[329] Cal. Supreme Court vom 14.12.1995, *Amwest Surety Ins. Co. v. Wilson*, 906 Cal.4th 1112, 1261; Cal. Court of Appeal 3rd District vom 26.08.2019, *Howard Jarvis Taxpayers Assn. v. Newsom*, 39 Cal. App. 5th 158, 170; *Carrillo*, SCOCAblog, How California lives with two legislatures.

[330] Proposition 24 (Cal. 2020), Sec. 3(C)(6): »provided that the amendments do not compromise or weaken consumer privacy«.

[331] *Carrillo*, SCOCAblog, How California lives with two legislatures.

[332] Cal. Supreme Court vom 14.12.1995, *Amwest Surety Ins. Co. v. Wilson*, 906 Cal. 4th 1112; Cal. Court of Appeal 2nd District vom 24.06.1998, *Proposition 103 Enforcement Project v. Quackenbush,* 64 Cal. App. 4th 1473; vom 27.09.2005, *Foundation for Taxpayer & Consumer Rights v. Garamendi*, 132 Cal. App. 4th 1354.

[333] Proposition 24 (Cal. 2020), Sec. 25(a) a.E.

[334] A. B. 335, 2021–22 Leg., Reg. Sess. (Cal. 2021), Cal. Stats. 2021 Ch. 700.

[335] A. B. 694, 2021–22 Leg., Reg. Sess. (Cal. 2021), Cal. Stats. 2021 Ch. 525.

[336] Proposition 24 (Cal. 2020), Sec. 21, § 1798.185(d): »latter«; Proposition 24 (Cal. 2020), Sec. 24.7, § 1798.199.40(b): »earlier«.

Diese Mitteilung hat die California Privacy Protection Agency am 21.10.2021 verschickt, sodass die Verordnungsermächtigung am 21.04.2022 auf die California Privacy Protection Agency überging.[337] Proposition 24 sah eine Frist für den Erlass der erweiterten und auf Proposition 24 angepassten Durchführungsverordnung bis zum 01.07.2022 vor, die inzwischen verstrichen ist; an das Fristende ist freilich keine Rechtsfolge geknüpft.[338]

Die California Privacy Protection Agency hat im Juni 2022 einen ersten Entwurf der überarbeiteten und an Proposition 24 angepassten Durchführungsverordnung veröffentlicht.[339] Dieser orientiert sich eng am im Proposition 24 enthaltenen Mindestinhalt der reformierten Durchführungsverordnung[340] Der neue Entwurf präzisiert zwar den CCPA an manchen Stellen, nutzt aber bisher noch nicht die Möglichkeiten der Verordnungsermächtigung, diesen auch zu erweitern und fortzuschreiben[341] – vermutlich wegen des erheblichen Zeitdrucks bis zum Inkrafttreten der Änderungen durch Proposition 24 am 01.01.2023.[342]

[337] Vgl. die wiedergegebene Aussage der Vorsitzenden der California Privacy Protection Agency *Urban* in: *Tam,* Law.com, Experts Weigh in on California Privacy Rights Act Changes.

[338] Das Fristende ergibt sich aus Cal. Civ. Code § 1798.185(d). Näher zu dem komplexen Verordnungsgebungsverfahren siehe Kapitel 3:E.I.2.c) (ab S. 187).

[339] Cal. Privacy Protection Agency, Proposed Regulations.

[340] *Cal. Privacy Protection Agency*, Invitation Preliminary Comments.

[341] Insbesondere die Möglichkeit automatisierte Entscheidung Profiling zu regulieren (Cal. Civ. Code § 1798.185(a)(16))nutzt der Entwurf bisher nicht.

[342] Proposition 24 (Cal. 2020), Sec. 31(a). Die Vorschriften über die Einrichtung der California Privacy Protection Agency sind bereits am 16.12.2020 in Kraft getreten, vgl. Proposition 24 (Cal. 2020), Sec. 31(b), Cal. Const. Art. II, § 10(a).

Kapitel 3

Analyse des CCPA und Vergleich mit europäischem Datenschutzrecht

A. Aufbau dieses Kapitels und des CCPA

Dieses Kapitel analysiert den Gesetzestext des CCPA und dessen Auslegung durch amerikanische Gerichte, Aufsichtsbehörden und die Rechtswissenschaft. Dabei stellt es die jeweiligen Regelungen des CCPA dar, ordnet diese in das amerikanische Recht ein und vergleicht sie mit dem europäischen und deutschen Datenschutzrecht. Dieser einführende Abschnitt gibt einen Überblick über die Systematik des CCPA und der Durchführungsverordnung sowie den Aufbau des sich anschließenden Kapitels.

Der CCPA ist als Datenschutzrecht allein für die Privatwirtschaft Teil des Civil Code of the State of California (Cal. Civ. Code), der das kalifornische Zivilrecht in für das *Common Law* untypischer Detailtiefe kodifiziert.[1] Im Jahre 1872 erhoffte sich Kalifornien, durch die als großen zivilisatorischen Fortschritt begriffene Kodifizierung das amerikanische Zivilrecht nachhaltig zu beeinflussen[2] – wie mit dem CCPA 146 Jahre später das amerikanische Datenschutzrecht. Der CCPA befindet sich in dem Titel 1.81.5 des vierten Teils »Obligations arising from particular transactions« des dritten Abschnitts »Obligations« dieses Gesetzbuches (Cal. Civ. Code §§ 1798.100–1798.199.100). Die Paragrafen hat der Gesetzgeber, wie in kalifornischen Gesetzen üblich, anfangs nur in Fünferschritten vergeben, um Raum für spätere Einfügungen zu lassen.

Der CCPA beginnt – seine Herkunft als Volksbegehren spiegelnd – nicht mit seinem Anwendungsbereich oder Definitionen, sondern mit den »spannenderen« Verbraucherrechten und Unternehmenspflichten in Cal. Civ. Code §§ 1798.100–1798.135. Anschließend regelt der CCPA eingehend die Definitionen in Cal. Civ. Code § 1798.140 und seinen Anwendungsbereich in Cal. Civ. Code §§ 1798.145, 1798.146, 1798.148. Darauf folgen Vorschriften zur Rechtsdurchsetzung in Cal. Civ. Code § 1798.150–1798.160, die das Privatklagerecht und die Bußgeldvorschriften enthalten. Anschließend regelt der CCPA begleitende Vorschriften (Cal. Civ. Code §§ 1798.175–199): unter anderen Kollisionsregeln für andere Gesetze,[3]

---

[1] *Grossman*, 45 Hastings L.J. 617, 625–639.

[2] *Grossman*, 45 Hastings L.J. 617, 625–639.

[3] Cal. Civ. Code § 1798.175 und Cal. Civ. Code § 1798.180, Cal. Civ. Code §§ 1798.92, 1798.194, 196.

die Verordnungsermächtigung für die California Privacy Protection Agency[4] und die Regelungen des Inkrafttretens.[5] Nach diesen »Schlussvorschriften« hat Proposition 24 einen Abschnitt über die neue California Privacy Protection Agency eingefügt (Cal. Civ. Code §§ 1798.199.10–100). Systemwidrig enthält er auch die Befugnis für den kalifornischen Attorney General, gegen Unternehmen auf Verhängung einer *civil penalty* zu klagen.[6] Weiterhin enthält der Gesetzestext der Proposition 24 neben Erwägungsgründen[7] noch einige Schlussvorschriften und Kollisionsregeln zu bestimmten Bundesgesetzen, die nicht im Cal. Civ. Code kodifiziert wurden.[8]

Die Durchführungsverordnung ist demgegenüber wesentlich systematischer aufgebaut. Sie ist in Kapitel 1 »California Consumer Privacy Act Regulations« des Abschnitts 6 »California Privacy Protection Agency« des schlicht als »Law« benannten Titels 11 des California Code of Regulations enthalten (11 C. C. R. §§ 7000–7102). Der Standort im Abschnitt »California Privacy Protection Agency« beruht darauf, dass diese seit dem 21.04.2022 für die Durchführungsverordnung zuständig ist.[9] Sie spezifiziert in acht gut strukturierten Artikeln ihren Anwendungsbereich und zusätzliche Definitionen,[10] die Informationspflichten,[11] den Umgang mit Verbraucherrechten,[12] Anforderungen an Dienstleister,[13] das Identifizierungsverfahren bei Verbraucheranträgen,[14] Umgang mit Unter-16-Jährigen,[15] das Maßregelungsverbot[16] und Dokumentations- und Organisationspflichten.[17] Entsprechend der durch Proposition 24 erweiterten Verordnungsermächtigung wird die nun zuständige California Privacy Protection Agency diese Durchführungsverordnung noch deutlich ausbauen.[18]

Dieser historisch gewachsene Aufbau eignet sich für die Analyse des CCPA nicht, da er sachlich zusammenhängende Regelungen über viele Vorschriften verstreut. Dementsprechend folgt dieses Kapitel dem Aufbau des CCPA nicht. Vielmehr analysiert es zuerst den Anwendungsbereich des CCPA (B), gefolgt von einer Darstellung der Verbraucherrechte (C), der Unternehmenspflichten

---

[4] Cal. Civ. Code § 1798.185.

[5] Cal. Civ. Code §§ 1798.198, 1798.199.

[6] Cal. Civ. Code § 1798.199.90.

[7] Proposition 24 (Cal. 2020), Sec. 2–3.

[8] Proposition 24 (Cal. 2020), Sec. 25–31.

[9] Vgl. die wiedergegebene Aussage der Vorsitzenden der California Privacy Protection Agency *Urban* in: *Tam,* Law.com, Experts Weigh in on California Privacy Rights Act Changes.

[10] 11 C. C. R. §§ 7000–7001.

[11] 11 C. C. R. §§ 7010–7016.

[12] 11 C. C. R. §§ 7020–7031.

[13] 11 C.C.R. §§ 7051.

[14] 11 C. C. R. §§ 7060–7063.

[15] 11 C. C. R. §§ 7070–7072.

[16] 11 C. C. R. §§ 7080–7081.

[17] 11 C. C. R. §§ 7100–7102.

[18] Cal. Civ. Code § 1798.185(d). Siehe Kapitel 3:E.I.2.c) (ab S. 187).

(D) und der Rechtsdurchsetzung (E). Die Analyse schließt ein Fazit ab, das übergreifende Gedanken zusammenführt (F). Eng verzahnt mit der Darstellung der Vorschriften des CCPA werden diese jeweils mit dem europäischen und deutschem Datenschutzrecht verglichen.

B. Anwendungsbereich

I. Kernbegriff der persönlichen Informationen

1. Definition

a) Darstellung

Den Kernbegriff der persönlichen Informationen (»personal information«) definiert der CCPA weit als:[19]

»information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.«

Im zweiten Teil der Definition konkretisiert eine Auflistung von insgesamt 137 Informationsarten den Begriff der persönlichen Informationen.[20] Diese enthält auch indirekt mit einer Person verknüpfte, nicht sensible Informationen, wie IP-Adressen oder primär geschäftliche Informationen.[21] Die nicht abschließende Auflistung soll verdeutlichen, dass der CCPA sämtliche Informationsarten erfasst.[22] Dies ist eine deutliche Abkehr von bisherigen amerikanischen Datenschutzgesetzen, die nur sensible Daten oder direkt personenbezogene Daten geschützt hatten.[23]

Ein Datum[24] ist nach der Definition des CCPA nur eine persönliche Information, wenn es sich entweder auf bestimmte Verbraucher:innen oder bestimmte Haushalte bezieht. Verbraucher:innen sind Personen mit Wohnsitz in Kalifornien.[25] Ein Haushalt ist eine Gruppe zusammenlebender Personen, die gemeinsam Geräte nutzen und so nicht unterschieden werden können.[26] Dieser Haushaltsbezug geht auf eine unternehmensnahe Auslegung früherer Datenschutzgesetze

---

[19] Cal. Civ. Code § 1798.140(v)(1).

[20] Cal. Civ. Code § 1798.140(v)(1)(A)–(L). Die Zahl 137 schließt auch Verweise in anderen Legaldefinitionen ein.

[21] Cal. Civ. Code § 1798.140(v)(1)(A),(I).

[22] *Bukaty*, CCPA Implementation Guide, S. 31; *de la Torre,* Golden Data, Personal information under CPRA.

[23] Z. B. 15 U. S. C. § 6501(8); Cal. Civ. Code § 1798.81.5(d)(1); Fla. Stat. § 501.171(1)(g); zu den jeweiligen Begriffen von HIPAA und GLBA siehe Kapitel 2:B.I.2 (ab S. 19).

[24] Der CCPA behandelt ebenso wie die DSGVO *data* und *information* als Synonyme, vgl. Cal. Civ. Code § 1798.125(a)(2),(b)(1): jeweils »consumer's data« und Cal. Civ. Code § 1798.140(ae)(1)(F): »genetic data«.

[25] Cal. Civ. Code § 1798.140(i). Siehe Kapitel 3:B.II.1 (ab S. 56).

[26] Cal. Civ. Code § 1798.140(q).

zurück: Festnetztelefonnummern seien nicht personenbezogen, da sich diese typischerweise auf einen gesamten Haushalt und nicht auf ein Individuum beziehen.[27] Die Haushaltsbezug-Alternative soll gegen eine solche Interpretation absichern.[28] Sie hat daher letztlich nur klarstellende Wirkung.[29]

Der Verbraucher- oder Haushaltsbezug der Definition ist weitgefasst zu verstehen.[30] Eindeutig ist das Tatbestandsmerkmal »identifies«: so sind Identifizierungsmerkmale wie Name oder Passnummer explizit als Regelbeispiele aufgeführt.[31] Auch eine Information ist umfasst, die darüber hinaus die Verbraucher:innen beschreibt (»describes«), also beispielsweise verhaltensbasierte Schlussfolgerungen zu Präferenzen, Veranlagungen, Einstellungen, Intelligenz, Fähigkeiten und Begabungen.[32] Offener ist »relates to«. Dieser Zusammenhang besteht wohl darin, dass sich Informationen ihrem Zweck nach auf bestimmte Personen beziehen sollen.[33] So sind dauerhafte Kennungen explizit als erfasste Informationsart aufgelistet, selbst wenn diese nur mit einem Gerät verknüpft sind.[34] Beispielsweise enthalten für Verhaltensanalyse genutzte Cookies persönliche Informationen.[35] Darüber hinaus genügt als Auffangtatbestand: »reasonably capable of being associated with, or could reasonably be linked«. Dies ist bei Informationen relevant, die sich zwar ihrem Inhalt oder Zweck nach nicht auf Verbraucher:innen beziehen, diese aber mit vertretbarem Aufwand identifizierbar sind. Dabei ist auch das Zusatzwissen des Unternehmens zu berücksichtigen, wie aus »directly or indirectly« deutlich wird.[36] Dies ist besonders bei Maschinendaten von Bedeutung, bei denen Unternehmen nur indirekt

---

[27] *Sjoera,* 10 questions about the CCPA, answered by the American law scholar Chris Hoofnagle. *Hoofnagle* war an der Ausarbeitung des CCPA beteiligt, siehe Kapitel 2:C.I (ab S. 30).

[28] *Sjoera,* 10 questions about the CCPA, answered by the American law scholar Chris Hoofnagle.

[29] *Ross,* Privacy Perspectives, The CCPA needs clarification. *Ross* war eine der Co-Autoren des CCPA-Volksbegehrens (siehe Kapitel 2:C.I (ab S. 30)).

[30] *Cal. Attorney General,* Opinion No. 20-303, S. 5;*Alza*, 37 Santa Clara High Tech. L. J. 231, 239; *Ballon*, E-commerce & Internet law, S. 26-410; *Booher/Robins*, American Privacy Law at the Dawn of a New Decade, S. 3 f.; *Blanke*, 1 Global Privacy Rev. 81, 89; *Bukaty*, CCPA Implementation Guide, S. 30f; *Cahill et al,* 30 Intellectual Property & Technology Law Journal 11, 12; *de la Torre,* Golden Data, Personal information under CPRA; *Gregg,* 60 Orange County Lawyer 32, 33; *Goldman*, Internet Law, S. 378; *Martin*, 105 Iowa L. Rev. 865, 881 f.; *Popova,* 24 Suffolk J. Trial & App. Advoc. 255, 262.

[31] Cal. Civ. Code § 1798.140(v)(1)(A).

[32] Cal. Civ. Code § 1798(v)(1)(E).

[33] *de la Torre,* Golden Data, Personal information under CPRA. Wohl auch: *Pink*, California Consumer Privacy Act Annotated, § 4:1.3; *Rubinstein,* The Privacy Advisor, A close-up on deidentified data under CCPA.

[34] Cal. Civ. Code § 1798.140(v)(1),(aj).

[35] Cal. Attorney General, Summary and Response to Comments Submitted During 45-Day Period, S. 299.

[36] *Pink*, California Consumer Privacy Act Annotated, § 4:1.5.

bestimmte Verbraucher:innen identifizieren können.[37] »Reasonably« ist dabei ein objektiver Standard, der auf eine verständige Person in der konkreten Situation abstellt.[38] Darin wird deutlich, dass der Personen- oder Haushaltsbezug relativ zu bestimmen ist. Die genauen Konturen sind mangels einschlägiger Rechtsprechung oder einer Konkretisierung durch die Durchführungsverordnung noch nicht festgelegt.[39]

b) Vergleich mit Art. 4 Nr. 1 DSGVO

Der Begriff der personenbezogenen Daten des Art. 4 Nr. 1 DSGVO ist ebenfalls weit zu verstehen.[40] Gesetzgebungstechnisch ist die Definition des CCPA allerdings wesentlich spezifischer und länger als die Definition der DSGVO. Die Definition persönlicher Informationen ist mit 260 Wörter nahezu viermal so lang wie die Definition der personenbezogenen Daten mit 71 Wörtern. Hier wirkt sich aus, dass sich die amerikanische Gesetzesauslegung streng am Wortlaut orientiert. Der Wortlaut ist nach amerikanischen Verständnis sowohl Ausgangspunkt der Auslegung als auch deren Endpunkt, wenn er für sich genommen klar und eindeutig ist.[41] Es existiert zwar ein prominenter Meinungsstreit in der amerikanischen Rechtswissenschaft, ob auch der Gesetzeszweck zu berücksichtigen ist (*textualism* vs. *purposivism)*.[42] Selbst der *purposivism* legt aber Gesetze primär nach ihrem Wortlaut aus und wendet teleologische Methoden nur in Einzelfällen an.[43] Gesetzesauslegung prägt Gesetzgebung. Daher muss der CCPA sehr spezifisch sein, um sein Ziel zu erreichen. Die Auslegung des Europarechts durch den EuGH ist demgegenüber stark am *teleos* orientiert.[44]

---

[37] *Torre, de la*, Golden Data, Personal information under CPRA.

[38] Cal. Supreme Court vom 29.11.2007, *People v. Mendoza,* 42 Cal. 4th 686, 703; zu dieser Rechtsfigur des amerikanischen Rechts, die v.a. im Deliktsrecht entwickelt wurde: *Bertenthal*, 2020 Wis. L. Rev. 85, 98–108: statistische Auswertung von Gerichtsentscheidungen zum Verständnis von »reasonable«; *Zipursky*, 163 U. Pa. L. Rev. 2131, 2132–2153: Überblick über *Reasonableness* in verschiedenen Rechtsgebieten.

[39] Der zweite Entwurf der Durchführungsverordnung enthielt eine Konkretisierung dahingehend, dass IP-Adresse für Webseitenbetreiber i. d. R. keine persönlichen Informationen sein sollen (Cal. Attorney General, CCPA, Text of First Set of Modifications, § 999.302). Der Cal. Attorney General hat sie jedoch nach Kritik vorläufig wieder zurückgezogen (Cal. Attorney General, Summary and Response to Comments Submitted during 2nd 15-Day Comment Period, S. 6).

[40] EuGH vom 20.12.2017 – C-434/16, *Nowak*, ECLI:EU:C:2017:994 Rn. 33 f.

[41] Cal. Supreme Court vom 18.05.2009, *In re Tobacco II Cases*, 46 Cal.4th 298, 316; *Eig*, Statutory Interpretation, S. 3–5.

[42] Umfassende Darstellung des Streitstandes: *Fallon*, 114 Nw. U. L. Rev. 269, 270–297; zu vermittelnden Ansichten: *Grove*, 134 Harv. L. Rev. 265–307.

[43] *Fallon*, 114 Nw. U. L. Rev. 269, 313 f.; *Manning*, 2011 Sup. Ct. Rev. 113, 167 f.

[44] *Gaitanides* in: Groeben/Schwarze/Hatje, Europäisches Unionsrecht, EUV Art. 19 Rn. 42–45; *Riesenhuber in:* Riesenhuber, Europäische Methodenlehre, § 10 Rn. 54.

Dieser Unterschied zeigt sich exemplarisch an den sieben Alternativen für einen Personen- oder Haushaltsbezug des CCPA (»identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly«).[45] Art. 4 Nr. 1 DSGVO nennt dagegen nur das Verb »beziehen«, das nach seinem natürlichen Wortsinn nur direkt personenbezogene Daten erfasst (ebenso in der englischen Sprachfassung: »relates to«).[46] Bei einem allgemeinsprachlichen Verständnis würde der Begriff »beziehen« nicht unmittelbar maschinenbezogene Daten erfassen, aus denen nur mittelbar auf natürliche Personen Rückschlüsse gezogen werden können. Amerikanische Rechtswissenschaftler haben deshalb Art. 4 Nr. 1 DSGVO wortlautgetreu in diesem Sinne interpretiert.[47] Allerdings füllt der EuGH den Personenbezug im Wege teleologischer Auslegung durch die drei Elemente Inhalt, Zweck und Ergebnis aus.[48] Ein Datum ist hiernach personenbezogen, wenn es entweder direkt eine Person betrifft (Inhalt), dazu dient, sie zu beschreiben (Zweck), oder es sich sonst auf ihre Rechte und Freiheiten auswirkt (Ergebnis).[49] Die zuerst genannten zwei Alternativen in der Definition des CCPA (»identifies« und »relates to«) entsprechen in etwa dem Inhaltselement, da sie ebenfalls einen direkten Personenbezug ausdrücken. Die Alternative »describes« entspricht dem Zweckelement. Schließlich ist »Reasonably capable of being associated with or could reasonably be linked« das Äquivalent zum Ergebniselement, da diese Formulierung ebenfalls einen nicht intendierten, faktischen Personenbezug ausdrückt. Darin wird deutlich, dass sich personenbezogene Daten und persönliche Informationen im Ergebnis sehr stark ähneln. Der CCPA muss aber durch eine hochgradig spezifische Sprache jede Eventualität abdecken, während bei der DSGVO die teleologische Auslegung eventuelle Lücken schließen kann.

Ebenfalls durch eine überspezifische Sprache ist zu erklären, dass bei den persönlichen Informationen des CCPA neben einem Personenbezug auch ein Haushaltsbezug ausreicht. Manche folgern aus diesem Haushaltsbezug, dass persönliche Informationen weiter als der Begriff der personenbezogene Daten seien.[50] Allerdings ist bei haushaltsbezogenen Daten nahezu immer auch ein Personenbezug im Sinne des Art. 4 Nr. 1 DSGVO herstellbar. So sind mit

---

[45] Cal. Civ. Code § 1798.140(v)(1).

[46] Vgl. *Artikel-29-Datenschutzgruppe*, WP 136 Personenbezogene Daten, S. 10–14: nach allgemein üblichen Verständnis des Wortes »beziehen« drücke dieses einen direkten Personenbezug aus (ebenso in der englischen Sprachfassung zu »relates to«).

[47] *Blanke*, 1 Global Privacy Rev. 81, 85–88; *Jordan*, Notice and Consent Requirements, S. 11: CCPA umfasse deswegen mehr Informationen.

[48] EuGH vom 20.12.2017, *Nowak*, ECLI:EU:C:2017:994 Rn. 34 f.

[49] Vgl. die Subsumtion in: EuGH vom 20.12.2017, *Nowak*, ECLI:EU:C:2017:994 Rn. 37–39. Näher: *Artikel-29-Datenschutzgruppe*, WP 136 Personenbezogene Daten, S. 10–14; *Klabunde* in: Ehmann/Selmayr, DS-GVO Art. 4 Rn. 9–11.

[50] *Bukaty*, CCPA Implementation Guide, S. 31; *Clark/Haltre*, 18 PDP 7, 7; *Jordan*, Notice and Consent Requirements, S. 12; *Spies*, ZD 2018, 501, 502; *McGruer*, 15 Wash. J. L. Tech. & Arts 120, 144.

Wohnanschrift verknüpfte Informationen personenbezogene Daten, da zumindest die Eigentümer:innen identifizierbar sind.[51] Auch bei Verbrauchsdaten von Strom- und Wasserzählern ist der Personenbezug zu bejahen, da diese Rückschlüsse über das Verhalten der jeweiligen Bewohner:innen erlauben.[52] Insgesamt ist daher der Umfang der persönlichen Informationen des CCPA und der personenbezogenen Daten des Art. 4 Nr. 1 DSGVO in etwa vergleichbar.[53]

2. Ausnahme für aggregierte und deidentifizierte Informationen

Keine persönlichen Informationen sind aggregierte und deidentifizierte Informationen.[54] Der CCPA ist auf diese nicht anwendbar.[55] Sie entsprechen in etwa den anonymen Daten der DSGVO.

Informationen sind aggregiert, wenn sie sich auf eine Gruppe von Verbraucher:innen beziehen und weder mit konkreten Verbraucher:innen oder Haushalten verknüpft sind, noch sich mit verhältnismäßigem Aufwand mit einer natürlichen Person oder einem Haushalt verknüpfen lassen.[56] Die Gruppe muss als anonyme Masse erscheinen.[57]

Zudem kennt der CCPA eine Zwischenstufe zwischen pseudonymen und persönlichen Informationen: die deidentifizierten Informationen. Deidentifizierte Informationen haben ihren Personen- oder Haushaltsbezug dadurch verloren, dass das Unternehmen sämtliche identifizierenden Elemente aus dem jeweiligen Datensatz entfernt hat.[58] Diese Kategorie fand sich bereits im branchenspezifischen Gesetz für die Gesundheitsbranche HIPAA.[59] Allerdings sind die Anforderungen des HIPAA an eine Deidentifizierung wesentlich niedriger, da nur besonders aufgelistete Identifikationsmerkmale entfernt werden müssen,[60] was im europäischen Datenschutzrecht eher einer Pseudonymisierung entspricht. Dagegen sind pseudonyme Informationen unter dem CCPA weiterhin persönliche Informationen. Seine Legaldefinition für Pseudonymisierung[61] stimmt nahezu wortlautgleich der Definition pseudonymer Daten in Art. 4 Nr. 5 DSGVO überein.

---

[51] VGH München vom 13.05.2019 – 4 B 18.1515, NJW 2020, 85 Rn. 46, 43; VG Wiesbaden vom 04.11.2019 – 6 K 460/16.WI –, juris Rn. 46; *Klar/Kühling* in: Kühling/Buchner, DS-GVO Art. 4 Nr. 1 Rn. 13.

[52] Für Stromzähler: BT-Drs. 18/7555, 95; *Kreße* in: Specht/Mantz, Datenschutzrecht, § 17 Rn. 27–32. Für Wasserzähler: *Bauer/Böhle/Ecker*, Bayerische Kommunalgesetze, GO Art. 24 Rn. 75b; *HBDI*, Funkwasserzähler, Nr. 2.

[53] Im Ergebnis ebenso: *Popova,* 24 Suffolk J. Trial & App. Advoc. 255, 262; *de la Torre*, Written testimony for California Senate Judicial Committee.

[54] Cal. Civ. Code § 1798.140(v)(2).

[55] Cal. Civ. Code § 1798.145(a)(6).

[56] Cal. Civ. Code § 1798.140(b).

[57] *Bukaty*, CCPA Implementation Guide, S. 38.

[58] Cal. Civ. Code § 1798.140(m).

[59] 45 C. F. R. § 164.514(a)–(c).

[60] 45 C. F. R. § 164.514(b)(2).

[61] Cal. Civ. Code § 1798.140(aa).

Deidentifizierte Informationen sind demgegenüber in der durch Proposition 24 reformierten Fassung der Definition deutlich enger:[62]

»information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the business that possesses the information:
(1) Takes reasonable measures to ensure that the information cannot be associated with a consumer or household.
(2) Publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision.
(3) Contractually obligates any recipients of the information to comply with all provisions of this subdivision.«

Ausreichend ist dagegen gerade nicht, nur Zuordnungsmerkmale getrennt aufzubewahren. Eine Reidentifizierung muss vielmehr nach objektivem Standard (»reasonably«) praktisch unmöglich sein, auch wenn das Unternehmen Zusatzwissen hinzuzieht.[63] Es reichen jedoch häufig nur geringe Anhaltspunkte, um Verbraucher:innen zu reidentifizieren.[64] So können 87 % der amerikanischen Bevölkerung nur durch Postleitzahl, Geschlecht und Geburtsdatum identifiziert werden.[65] Damit wird der erste Satzteil schon schwer zu erfüllen sein.

Zusätzlich zu dem ersten Satzteil bilden die drei zusätzlich aufgezählten Pflichten gleichsam ein zweites Sicherungsnetz. Die Pflichten sind einem Bericht der FTC entlehnt.[66] Die erste Pflicht setzt angemessene Schutzmaßnahmen voraus, die davon abhängen, wie sensibel die persönlichen Informationen sind.[67] Solche angemessenen Schutzmaßnahmen sind unter anderen das Löschen oder Modifizieren bestimmter Daten in einem Datensatz, das Hinzufügen von Rauschen zu einem Datensatz *(differential privacy)* oder das Hinzufügen künstlicher Daten.[68] Die zweite Pflicht einer Bekanntgabe der Deidentifizierung soll sicherstellen, dass die FTC eine fehlende Deidentifizierung sanktionieren kann.[69] Mit einem solchen expliziten Versprechen handeln Unternehmen bei einem Verstoß irreführend und verletzten so die Generalklausel des FTC Acts.[70] Beim CCPA ist dieser Bestandteil überflüssig, da die Aufsichtsbehörden schon die nicht

---

[62] Cal. Civ. Code § 1798.140(m).

[63] *Bukaty*, CCPA Implementation Guide, S. 40 f.

[64] *Determann,* 26 Mich. Tech L. Rev. 229, 248; *Rubinstein/Hartzog*, *91 Wash. L. Rev.* 703, 710–714; *Rubinstein,* The Privacy Advisor, A close-up on deidentified data under CCPA.

[65] *Sweeney*, Simple Demographics Often Identify People Uniquely, S. 16–20.

[66] *Californians for Consumer Privacy*, The California Privacy Rights and Enforcement Act of 2020, S. 23 (das Volksbegehren mündete später in Proposition 24). Der FTC-Bericht: *FTC,* Protecting Consumer Privacy in an Era of Rapid Change, S. 21 f.

[67] *FTC,* Protecting Consumer Privacy in an Era of Rapid Change, S. 21.

[68] Ebd.

[69] Ebd.

[70] Zu dieser Generalklausel siehe Kapitel 2:B.I.3 (ab S. 24).

ausreichende Deidentifizierung an sich ahnden können.[71] Wohl zur Harmonisierung mit der FTC-Definition hat ihn der Gesetzgeber des CCPA dennoch aufgenommen. Die dritte Pflicht, Empfänger:innen deidentifizierter Informationen eine Reidentifizierung vertraglich zu untersagen, soll die Identität der jeweiligen Verbraucher:innen auch bei einer Weiterübermittlung schützen.[72] Die FTC versteht diese Pflicht auch dahingehend, dass der Vertrag wirksame Vertragsstrafen enthalten und eine regelmäßige Überprüfung vorsehen muss.[73] Damit scheidet eine Veröffentlichung deidentifizierter Daten wohl vollständig aus.

Für die Gesundheitsbranche hatte A. B. 713 Anfang 2021 die Anforderungen an die Deidentifizierung an denjenigen des HIPAA[74] angeglichen. So genüge der niedrigere Maßstab des HIPAA, wenn die deidentifizierten Daten von Patientendaten abgeleitet sind.[75] Es ist allerdings unklar, ob Proposition 24 A. B. 713 verdrängt hat. Proposition 24 erklärt alle nach dem 01.01.2021 verabschiedeten Änderungen des CCPA für unwirksam, wenn diese nicht die Ziele der Proposition 24 fördern.[76] Die auch nur partielle Senkung des Deidentifizierungsstandards widerspricht dessen Reform durch Proposition 24 und der Stärkung des Datenschutzniveaus als wesentliches Ziel der Proposition 24.[77] Daher ist A. B. 713 wohl unwirksam.[78]

Die DSGVO kennt demgegenüber nur die Kategorie der Anonymisierung, die sowohl aggregierte als auch deidentifizierte Daten umfasst. Auf anonyme Daten ist die DSGVO nicht anwendbar (Erwägungsgrund 26 S. 6 der DSGVO). Anonyme Daten sind nach Erwägungsgrund 26 S. 5 der DSGVO Informationen, die keinen direkten oder indirekten Personenbezug mehr aufweisen. Daten sind nur anonym, wenn es angesichts des Aufwands an Zeit, Kosten und Arbeitskraft praktisch unmöglich ist, sie zu reidentifizieren.[79] Diese Kriterien ähneln den Anforderungen an eine Deidentifizierung des CCPA.

Eine zusätzliche Absicherung der Anonymisierung durch technische und organisatorische Maßnahmen kennt die DSGVO nicht explizit. Allerdings muss der Verantwortliche die Anonymisierung fortlaufend auf ihre Wirksamkeit prüfen.[80] Zudem können Vertragsstrafen auch unter der DSGVO die

---

[71] Cal. Civ. Code §§ 1798.155(a), 1798.199.90(a).

[72] *FTC,* Protecting Consumer Privacy in an Era of Rapid Change, S. 21 f.

[73] Ebd.

[74] Zu diesem siehe Kapitel 2:B.I.2 (ab S. 19).

[75] Cal. Civ. Code § 1798.146, 1798.148. Zu den genauen Anforderungen des HIPPA-Deidentifikationsstandards: 45 C. F. R. § 164.514(a)–(c); *Gottlieb/Schreibe,* Computer & Internet Lawyer, May 2020, 6–9.

[76] Proposition 24(Cal. 2020), Sec. 25(a).

[77] Siehe Kapitel 2:C.IV (ab S. 35).

[78] *Determann/Tam*, JDPP 2021, 7, 12.

[79] EuGH vom 20.12.2017 – C-434/16, *Nowak*, ECLI:EU:C:2017:994 Rn. 33 f. Näher zu verschiedenen Anonymisierungstechniken und deren Problemen: *Artikel-29-Datenschutzgruppe*, WP 216 Anonymisierung, S. 5–28.

[80] *Artikel-29-Datenschutzgruppe*, WP 216 Anonymisierung, S. 18; *BfDI*, Anonymisierung,

praktische Unmöglichkeit einer Reidentifizierung durch Zusatzwissen eines Dritten absichern.[81]

3. Ausnahme für öffentliche Informationen

a) Darstellung

Zudem sind bestimmte öffentliche Informationen keine persönlichen Informationen,[82] da diese im amerikanischen Recht als Gemeingut gelten. Dies betrifft Informationen von öffentlichem Interesse, durch Behörden oder in Massenmedien veröffentlichte Informationen oder solche, derer sich Verbraucher:innen bewusst entäußert haben, ohne den Empfängerkreis einzuschränken.

Die Dichotomie zwischen privat und öffentlich ist im amerikanische Verfassungsrecht omnipräsent.[83] Der Staat greift in die durch das *Fourth Amendment* geschützte berechtigte Privatheitserwartung nicht ein, wenn die jeweilige Überwachung einen (auch nur geringen) Bezug zur Öffentlichkeit hat.[84] Bürger:innen haben nach der Rechtsprechung des U. S. Supreme Court keine berechtigte Erwartung von Privatheit, wenn sie private Informationen an Dritte weitergeben – selbst wenn dieser Dritte ihr Telefonanbieter ist (*third party doctrine*).[85] Auch hätten beispielsweise Teilnehmer:innen bei Schulwettkämpfen eine geringere Privatheitserwartung hinsichtlich Drogentests, weil sie sich in der Schulumkleide häufig vor ihren Mitschüler:innen umziehen und so den privaten Bereich ohnehin verlassen.[86] Diese schematische Unterscheidung hat ihre Wurzeln darin, dass das *Fourth Amendment* nach seinem Wortlaut ursprünglich nur gegen Durchsuchungen der Wohnung als Rückzugsort vor dem Staat schützen sollte (»The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, […]«).[87] Es wurde erst später auf weitere Privatsphäreverletzungen erweitert, wobei aber die klare Trennung zwischen einem geschützten privaten und einem ungeschützten öffentlichen Bereich geblieben ist.[88]

S. 6; *Arning/Rothkegel* in: Taeger/Gabel, DS-GVO Art. 4 Rn. 48; *Klabunde* in: Ehmann/Selmayr,DS-GVO Art. 4 Rn. 20; Stürmer, ZD 2020, 626.

[81] *Arning/Rothkegel* in: Taeger/Gabel, DS-GVO Art. 4 Rn. 54.

[82] Cal. Civ. Code § 1798.140(v)(2).

[83] *Hartzog*, 99 Boston L. Rev. 459, 469–494; *Solove*, 154 U. Pa. L. Rev. 477, 496.

[84] Zu dem *Fourth Amendment* siehe Kapitel 2:A.I.1 (ab S. 7).

[85] U. S. Supreme Court vom 21.04.1976, *United States v. Miller*, 425 U. S. 435, 443; vom 20.06.1979, *Smith v. Md.,* 442 U. S. 735, 743–746; vom 02.04.1984, *United States v. Jacobsen*, 446 U. S. 109, 117; a. A. U. S. Supreme Court vom 22.06.2018, *Carpenter v. United States* – ablehnendes Sondervotum *Gorsuch,* 138 S.Ct. 2206, 2268–2269.

[86] U. S. Supreme Court vom 26.01.1995, *Vernonia Sch. Dist. 47J v. Acton,* 515 U. S. 646, 657.

[87] U. S. Const amend. IV. Dazu: *Whitman*, 113 Yale L. J. 1151, 1211 f.

[88] *Whitman*, 113 Yale L. J. 1151, 1212–1216.

Das *First Amendment* schützt zudem öffentliche Informationen als Grundlage für demokratischen Diskurs.[89] So verstößt selbst ein Gesetz gegen das *First Amendment*, das die Weiterverbreitung des legal erlangten vollen Namens eines Vergewaltigungsopfers verbietet.[90] Alle Bürger:innen sollen ihre Ansichten frei verbreiten können, ohne dass der Staat entscheidet, was falsch, töricht, ungerecht oder schädlich ist, auf dass die beste Idee gewinne.[91]

Ähnlich dazu schützt das amerikanische Deliktsrecht nur private, nicht aber öffentliche Informationen. Das einflussreiche Restatement of Tort hält diesbezüglich schematisch fest: »there is no liability when the defendant merely gives further publicity to information about the plaintiff that is already public.«[92] So haben Gerichte beispielsweise bei der Veröffentlichung privater Nacktfotos ohne Einwilligung der Abgebildeten einen Unterlassensanspruch gegen den erstmaligen Veröffentlicher abgelehnt, weil sich die Nacktfotos bereits über das Internet verbreitet hatten.[93] Auch andere amerikanische Datenschutzgesetze kennen ähnliche Ausnahmen für öffentlich verfügbare Informationen.[94] Dass im öffentlichen Raum nach amerikanischen Verständnis keine Privatsphäre besteht, zeigt sich zudem darin, dass amerikanische Zeitungen üblicherweise den vollen Namen von Verdächtigten und Opfern öffentlicher Hauptverhandlungen nennen.[95]

Ziel der Ausnahme des CCPA ist es, eine risikoreiche gerichtliche Auseinandersetzung um die Vereinbarkeit mit dem *First Amendment* zu verhindern. Vor allem sollte der CCPA nicht unter den strengen Maßstab der *strict scrutiny* fallen, bei dem die Verfassungswidrigkeit vermutet wird.[96] Eine verfassungskonforme Auslegung wäre nicht möglich gewesen, da auch für diese im amerikanischen Recht die Wortlautgrenze gilt.[97] Ein im Hinblick auf das *First Amendment* zu weitreichendes Gesetz ermöglicht es Kläger:innen dieses in Gänze anzugreifen, da solche Gesetze von einer freien Meinungsäußerung abschrecken.[98] Zudem

---

[89] Zu diesem siehe Kapitel 2:A.I.2.a) (ab S. 10).

[90] U. S. Supreme Court vom 03.03.1975, *Cox Broadcasting Corp. v. Cohn*, 420 U. S. 469, 492; vom 21.06.1989, *Florida Star v. B.J.F.*, 491 U. S. 524, 536. Kritisch dazu, ob sich die Rechtsprechung wirklich auf Datenschutzgesetze übertragen lässt: *Kaminski et al.*, 54 Loy. L. A. L. Rev. 157, 175 f.

[91] Grundlegend: U. S. Supreme Court vom 09.03.1964, *New York Times Co. v. Sullivan*, 376 U. S. 254, 298 f.

[92] *American Law Institute*, Restatement of the law Second, Torts, § 652D comment b.

[93] U. S. District Court C. D. Cal. vom 02.11.1998, *Schlessinger v. Internet Entm't Group,* 1998 U. S. Dist. LEXIS 24219, 17–21; U. S. District Court E.D. Mich vom 24.03.2011, *Doe v. Peterson,* 784 F. Supp. 2d 831, 841 f.

[94] GLBA, 15 U. S. C. § 6809(4)(B) i. V. m. 16 C. F. R. § 313.3(p); Cal. Civ. Code § 1798.80(b),(e).

[95] *Blom* in: Khosrow-Pour, Media controversy: breakthroughs in research and practice, 354, 361 f.

[96] Zu diesem Prüfungsmaßstab siehe Kapitel 2:A.I.2.a) (ab S. 10).

[97] U. S. Supreme Court vom 22.05.2000, *Jones v. United States*, 529 U. S. 848, 857; *Eig*, Statutory Interpretation, S. 24 f.

[98] U. S. Supreme Court vom 01.07.2021, *Ams. for Prosperity Found. v. Bonta*, 2021 LEXIS 3569, 29–30.

kann jedes Bundesgericht Gesetze für verfassungswidrig erklären.[99] Daher bestand die Gefahr, dass ein konservatives Bundesgericht den ganzen CCPA für nichtig erklärt hätte, weil dieser auch öffentliche Informationen erfasst. Diesem Risiko wollte sich das Volksbegehren Proposition 24,[100] das diese Ausnahme wesentlich erweitert hat, nicht aussetzen.[101]
Daher nimmt der CCPA folgende Informationskategorien von der Definition der persönlichen Informationen aus:[102]
– Informationen von öffentlichem Interesse, die wahr und legal erlangt sind;
– amtliche Informationen, die amerikanische Behörden veröffentlicht haben;
– Informationen, die Massenmedien publik gemacht haben; oder
– Informationen, derer sich Verbraucher:innen entäußert haben, ohne den Empfängerkreis einzuschränken.

Als Informationen von öffentlichem Interesse (»matter of public concern«) gelten in der Rechtsprechung des U. S. Supreme Court zum *First Amendment* politische, gesellschaftliche oder sonst die Allgemeinheit betreffende Informationen.[103] Diese sind von zentraler Bedeutung für Meinungsfreiheit.[104] Die Rechtsprechung prüft daher Beschränkungen für Informationen von öffentlichem Interesse mit *strict scrutiny*.[105] Einschränkungen bezüglich privater Informationen prüft die Rechtsprechung hingegen nur mit *intermediate scrutiny*.[106]

Amtliche Informationen veröffentlichen amerikanische Behörden in großem Ausmaß auf Anfrage oder in öffentlichen Registern.[107] Von der Veröffentlichung sind allerdings ohnehin Akten ausgenommen, die besonders sensible Informationen über Individuen enthalten, wie Kranken- oder Personalakten.[108] Dadurch findet eine Abwägung zwischen Privatsphäre und Informationsfreiheit bereits bei

---

[99] U. S. Supreme Court vom 24.02.1803, *Marbury v. Madison*, 5 U. S. 137, 171–180; vom 26.06.2013, *Hollingsworth v. Perry,* 570 U. S. 693, 705.

[100] Zu diesem Volksbegehren siehe Kapitel 2:C.IV (ab S. 35).

[101] *Soltani,* Twitter-Beitrag vom 24.07.2020. Diese Einschränkung hat ein Memo des Verfassungrechtlers *Volokh* angeregt, vgl. *Pincus/Nemetz/Volokh,* Memo regarding the CCPA, S. 13. Die genaue Formulierung stammt von der Verfassungsrechtlerin *Kaminski*, vgl. *Soltani,* Twitter-Beitrag vom 24.07.2020.

[102] Cal. Civ. Code § 1798.140(v)(2).

[103] U. S. Supreme Court vom 20.04.1983, *Connick v. Myers*, 461 U. S. 138, 146.

[104] U. S. Supreme Court vom 21.03.1984, *Dun & Bradstreet v. Greenmoss Builders*, 472 U. S. 749, 758; vom 02.03.2011, *Snyder v. Phelps,* 562 U. S. 443, 451.

[105] U. S. Supreme Court vom 07.06.1971, *Cohen v. Cal.*, 403 U. S. 15, 24; vom 25.06.2007, *FEC v. Wis. Right to Life, Inc.,* 551 U. S. 449, 457, 464.

[106] Vgl. U. S. Supreme Court vom 02.03.2011, *Snyder v. Phelps*, 562 U. S. 443, 452: »where matters of purely private significance are at issue, First Amendment protections are often less rigorous«.

[107] Vgl. auf Bundesebene den Freedom of Information Act, 5 U. S. C. § 552; in Kalifornien: California Public Records Act, Cal. Gov. Code §§ 6250–6270.7.

[108] 5 U. S. C. § 552(b)(6),(7)(C); Cal. Gov. Code § 6254(c). Die Ausnahmen werden auch in der Rechtspraxis breit genutzt und sind die am häufigsten angegebenen Ablehnungsgründe: *Kwoka*, 127 Yale L. J. 2204, 2217.

der Entscheidung über die Veröffentlichung statt.[109] Die veröffentlichten Informationen sind Gemeingut.[110] Es besteht daher nach amerikanischer Vorstellung kein öffentliches Interesse mehr daran, ihre Weiterverbreitung zu verhindern.[111] Ein solches Verbot würde deswegen wohl gegen das *First Amendment* verstoßen.[112]

Hinsichtlich der in Massenmedien veröffentlichten persönlichen Informationen mag dem Verbraucher oder der Verbraucherin die Veröffentlichung unrecht sein. Allerdings ist die Pressefreiheit zentral für den öffentlichen Diskurs. Daher prüft die Rechtsprechung Beschränkungen der Pressefreiheit zwar immer noch mit *intermediate scrutiny,* aber in der Sache strenger.[113] Eine Beschränkung der Pressefreiheit biete ein besonderes Missbrauchspotenzial, der nur durch eine eingehende verfassungsrechtliche Prüfung begegnet werden könne.[114] Diese vermeidet der CCPA hiermit.

Überdies sind Informationen ausgenommen, welcher sich der Verbraucher oder die Verbraucherin selbst bewusst entäußert hat und sie nicht auf einen bestimmten Empfängerkreis beschränkt hat.[115] Insofern sind die Verbraucher:innen nicht schutzwürdig, da sie selbst die Information der Öffentlichkeit bereitgestellt haben.[116] Dies spiegelt die *third party doctrine* des U. S. Supreme Courts, nach der eine Person keine berechtigte Erwartung einer Privatsphäre hat, wenn sie Informationen freiwillig Dritten überlässt.[117] Diese Ausnahme ist nicht so weitreichend wie sie *prima facie* scheint. So beschränkt ein Verbraucher im Wirtschaftsverkehr in der Regel das Weitergeben auf einen bestimmten Empfängerkreis, da die Angabe der Empfängerkategorien in der umfassenden Datenschutzerklärung nach dem CCPA verpflichtend ist.[118] Auch bei im privaten Umfeld geäußerten Gedanken ist wohl

---

[109] Cal. Supreme Court vom 02.03.2017, *City of San Jose v. Superior Court*, 2 Cal. 5th 608, 626.

[110] *Pincus/Nemetz/Volokh,* Memo regarding the CCPA, S. 7. Dieses Memo war ein wesentlicher Beweggrund für die Ausgestaltung dieser Ausnahme, vgl. *Soltani,* Twitter-Beitrag vom 24.07.2020.

[111] *Pincus/Nemetz/Volokh,* Memo regarding the CCPA, S. 7.

[112] *Pincus/Nemetz/Volokh,* Memo regarding the CCPA, S. 7.

[113] U. S. Supreme Court vom 14.06.1943, *W. Va. State Bd. of Educ. v. Barnette, 319 U. S. 624*, 633; vom 27.06.1994, *Turner Broad. Sys. v. FCC*, 512 U. S. 622, 640 f.; U. S. Court of Appeals 1st Circuit vom 24.02.2021, *Comcast of Maine/New Hampshire, Inc. v. Mills, 988 F.3d 607*, 611. Näher zur *intermediate scrutiny*: *Bhagwat*, 2007 U. Ill. L. Rev. 783–838.

[114] U. S. Supreme Court vom 27.06.1994, *Turner Broad. Sys. v. FCC*, 512 U. S. 622, 640 f.; U. S. Court of Appeals 1st Circuit vom 24.02.2021, *Comcast of Maine/New Hampshire, Inc. v. Mills*, 988 F.3d 607, 611.

[115] Cal. Civ. Code § 1798.140(v)(2): »information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience«.

[116] *Bukaty*, CCPA Implementation Guide, S. 36.

[117] Für eine Übertragbarkeit der *third party doctrine* auf das *First Amendment:* U. S. Court of Appeals 4th Circuit vom 26.07.2010, *Ostergren v. Cuccinelli,* 615 F.3d 263, 281–283.

[118] Cal. Civ. Code §§ 1798.110(c)(4), 1798.115(c), 1798.130(a)(5)(C), 11 C. C. R. § 7011(c)(1)(G)(1). Siehe Kapitel 3:D.I.2.b)aa) (ab S. 155).

der Empfängerkreis nicht unbestimmt.[119] Damit bleiben Situationen, in denen Verbraucher:innen selbst aktiv am öffentlichen Diskurs teilnehmen.

Schließlich besteht eine Rückausnahme für biometrische Informationen,[120] die ohne Wissen des Verbrauchers gesammelt wurden: diese sind stets persönliche Informationen.[121] Manche Anbieter argumentieren, dass Gesichtserkennung von Bildern aus dem Internet ein Nutzen öffentlicher Informationen und von der Meinungsfreiheit geschützt sei.[122] Der auch für Kalifornien zuständige U. S. Court of Appeals for the 9th Circuit hat jedoch in *Patel v. Facebook* (2020) entschieden, dass ein substanzielles Interesse an Privatsphäre für ein Verbot der Gesichtserkennung auf Basis öffentlicher Informationen besteht.[123] Wenn sich diese Rechtsprechung so fortsetzt, wird diese Rückausnahme wahrscheinlich als verfassungsgemäß beurteilt werden.

b) Begrenzte Ausnahmen unter der DSGVO

Hiergegen behandelt die DSGVO öffentlich zugängliche Daten weiter als personenbezogene Daten. Sie schützt sie nur punktuell geringer. Insbesondere darf ein Verantwortlicher besondere Kategorien personenbezogener Daten verarbeiten, wenn die betroffene Person sie erkennbar offengelegt hat (Art. 9 Abs. 2 lit. e DSGVO). Auch überwiegt bei der Interessenabwägung nach Art. 6 Abs. 1 S. 1 lit. f DSGVO regelmäßig das Interesse an einer Nutzung von personenbezogenen Daten, welche die betroffene Person selbst veröffentlicht.[124] Dies bleibt aber immer eine Frage des Einzelfalls. So können Verantwortliche z. B. ein automatisiertes Sammeln personenbezogener Daten aus sozialen Medien in der Regel nicht auf Art. 6 Abs. 1 S. 1 lit. f DSGVO stützen.[125] Die unzulässige Erhebung öffentlicher Daten ist sogar ein Fokus des aufsichtsbehördlichen

---

[119] Die *First Amendment*-Rechtsprechung geht davon aus, dass bestimmte Diskussionsorte nur begrenzt für den öffentlichen Diskurs bestimmt sind (*nonpublic forum* oder *limited public forum)*: U. S. Supreme Court vom 23.02.1983, *Perry Educ. Ass'n v. Perry Local Educators' Ass'n,* 460 U. S. 37, 46; U. S. Court of Appeals 9th Circuit vom 02.07.2019, *Amalgamated Transit Union Local 1015 v. Spokane Transit Auth.,* 929 F.3d 643, 650–653.

[120] Legaldefinition in Cal. Civ. Code § 1798.140(c).

[121] Cal. Civ. Code § 1798.140(v)(2).

[122] *Hill,* N.Y. Times, Facial Recognition Start-Up Mounts a First Amendment Defense.

[123] U. S. 9th Circuit Court of Appeals vom 08.08.2019, *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1273. Das Gericht hat nur über die prozessuale Vorfrage der Klagebefugnis (*standing*) entschieden und noch keine abschließende Entscheidung getroffen. Weiterführend: *Schwartz/Crocker/Lynch*, ACLU v. Clearview: Brief of Amicus EFF, S. 2–17.

[124] *Artikel-29-Datenschutzgruppe*, WP 217 Berechtigtes Interesse, S. 50 (zwar noch zur DSRL, aber übertragbar auf die DSGVO); *Busse/Dallmann*, ZD 2019, 394, 395; *Golland*, MMR 2018, 130, 133.

[125] *Busse/Dallmann*, ZD 2019, 394, 396 f.; *Solmecke* in: Hoeren/Sieber/Holznagel, MMR-HdB, Teil 21 Rn. 64.

DSGVO-Vollzugs: so verhängen Aufsichtsbehörden häufig Bußgelder wegen Videoüberwachung von öffentlichen Orten und der Nutzung von Dashcams.[126]

Zudem greifen bei öffentlich zugänglichen personenbezogenen Daten sämtliche anderen Rechte und Pflichten der DSGVO. Insbesondere muss der Verantwortliche die betroffene Person nach Art. 14 DSGVO informieren. Dabei muss er gemäß Art. 14 Abs. 2 lit. f DSGVO offenlegen, dass die personenbezogenen Daten aus einer öffentlich zugänglichen Quelle stammen.

Andererseits gestattet Art. 86 DSGVO den Mitgliedsstaaten, personenbezogene Daten aus amtlichen Dokumenten zu veröffentlichen. Besonders die skandinavischen Länder veröffentlichen auch durchaus umfangreiche personenbezogene Daten aus amtlichen Dokumenten[127] und zeigen so, dass die DSGVO auch mit sehr weitgehender Informationsfreiheit vereinbar ist.

Eine vergleichbare Funktion zu den Ausnahmen für Informationen von öffentlichem Interesse und für in Massenmedien publik gemachte Informationen erfüllt die Öffnungsklausel für Journalismus des Art. 85 Abs. 2 DSGVO. Nach diesem Medienprivileg können die Mitgliedstaaten von wesentlichen Teilen der DSGVO abweichen (Art. 5–76 und 85–91 DSGVO), soweit dies erforderlich ist, um den Datenschutz mit der Meinungs- und Informationsfreiheit in Einklang zu bringen. Die deutschen Bundesländer haben die Presse für ihre redaktionelle Arbeit weitgehend von der Einhaltung der DSGVO befreit (bis auf die Pflicht zur Datensicherheit).[128] Stattdessen greift die Selbstregulierung durch den Pressekodex, der in seiner Zif. 5 und 8 detaillierte Sonderregelungen für den redaktionellen Datenschutz enthält.

An der pauschalen Ausnahme für öffentliche Informationen zeigt sich, dass das amerikanische Recht Meinungsfreiheit und öffentlicher Debatte ein wesentlich höheres Gewicht einräumt als das europäische und deutsche Recht. Der öffentliche Diskurs hat nach amerikanischen Verständnis Vorrang gegenüber der Privatsphäre. Die sehr weitgehende Ausnahme des CCPA wird auch kaum kritisiert,[129] was auf eine weitgehende Akzeptanz dieser Unterscheidung hindeutet.

---

[126] *LfD Niedersachsen*, 24. Tätigkeitsbericht 2017–2018, S. 15f; *dies.*, LfD Niedersachsen verhängt Bußgeld über 10,4 Millionen Euro gegen notebooksbilliger.de; *LDI NRW*, 25. Datenschutzbericht 2019, S. 31: »Bußgeldtatbestände waren überwiegend […] und der Einsatz von Dashcams im Straßenverkehr.«; *LfDI Rheinland-Pfalz*, Tätigkeitsbericht zum Datenschutz 2019, S. 35: Bußgelder wegen Dashcams seien Schwerpunkt; *LfD Sachsen-Anhalt,* XVI. Tätigkeitsbericht [2019], S. 75: Videoüberwachung sei Schwerpunkt der Kontrolltätigkeit; *SächsDSB*, Tätigkeitsbericht 2019, S. 126. Die Bedeutung unterstreicht auch: *EDSA*, Leitlinien 3/2019 Videogeräte.

[127] Insbesondere zu Schweden: *Stenbeck/Fält/Reichel* in: Slokenberga/Tzortzatou/Reichel, GDPR and Biobanking, 379, 383 f.

[128] Vgl. u. a. Art. 38 BayDSG, § 19 BlnDSG, §§ 23, 113 MOMod-StV, § 37 Medienstaatsvertrag HSH.

[129] Ausnahme: *Parks*, Unfair Collection, S. 34 f.

II. Rollen

1. Verbraucher:innen

Schutzsubjekte des CCPA sind die Verbraucher:innen (»consumers«), die als *California resident* legaldefiniert sind.[130] *Resident* sind dabei alle Personen, die in Kalifornien ihren gewöhnlichen Aufenthalt oder Wohnsitz haben.[131] Gewöhnlicher Aufenthalt bedeutet, dass sich die jeweilige Person längerfristig in Kalifornien aufhält, wobei es auf einen Domizilwillen nicht ankommt.[132] Eine Person hat ihren Wohnsitz in Kalifornien, wenn sie dort ihren Lebensmittelpunkt hat, selbst wenn sie gewisse Zeit abwesend ist.[133] In der Praxis prüfen Unternehmen diese Eigenschaft anhand der IP-Adresse[134] oder der Postanschrift,[135] was wohl beides zulässig ist. Ein konsumptiver Zweck ist hingegen nicht erforderlich. Vielmehr sind auch berufliche oder gewerbliche Tätigkeiten erfasst.[136] Die Wahl des Begriffs »consumer« verdeutlicht aber, dass der CCPA im Ausgangspunkt ein Verbraucherschutzgesetz ist.

Der Schutzbereich der DSGVO ist demgegenüber erheblich weiter, da sie unabhängig von deren Wohnsitz jede natürliche Person schützt (Art. 1 Abs. 2 DSGVO). Diese nennt die DSGVO betroffene Person (Art. 4 Nr. 1 DSGVO). Ebenso wie beim CCPA sind weder juristische noch verstorbene Personen (Erwägungsgrund 27 S. 1 der DSGVO) geschützt. Dass der CCPA den Schutz auf Personen mit Wohnsitz in Kalifornien einschränkt, soll wahrscheinlich einen Verstoß gegen das verfassungsrechtliche Verbot der Regelung exterritorialer Sachverhalte durch die *dormant Commerce Clause* vermeiden.[137]

2. Unternehmen

a) Bestimmender Einfluss und Gewinnerzielungsabsicht

Das Äquivalent zu dem Verantwortlichen der DSGVO ist das Unternehmen (»business«).[138] Genauso wie ein Verantwortlicher muss das Unternehmen einen bestimmenden Einfluss auf die Verarbeitung haben. Unternehmen sind allerdings nur in Kalifornien kommerziell tätige[139] Organisationen mit Gewinnerzielungsabsicht, nicht aber Behörden oder gemeinnützige Organisationen.

---

[130] Cal. Civ. Code § 1798.140(i).

[131] Cal. Civ. Code § 1798.(140)(i) i.V.m. 18 C.C.R. § 17014.

[132] 18 C.C.R. § 17014(b).

[133] 18 C.C.R. § 17014(c).

[134] *Interactive Advertising Bureau*, IAB CCPA Benchmark Survey: Summary, S. 6.

[135] *Pink*, California Consumer Privacy Act Annotated, § 3:2.1.

[136] Vgl. Cal. Civ. Code § 1798.140(v)(1)(I): »Professional or employment-related information« als Regelbeispiel für persönliche Informationen.

[137] Zu dieser siehe Kapitel 2:A.I.2.b) (ab S. 13).

[138] Cal. Civ. Code § 1798.140(d).

[139] Cal. Civ. Code § 1798.140(d)(1): »does business in the State of California«. Näher beim räumlichen Anwendungsbereich siehe Kapitel 3:B.III (ab S. 71).

Das erste Tatbestandselement ist der bestimmendende Einfluss auf die Verarbeitung, der stark an die Verantwortlichendefinition in Art. 4 Nr. 7 DSGVO erinnert (»alone, or jointly with others, determines the means and purposes of processing«).[140] Dieser Wortlaut enthält ebenso wie Art. 4 Nr. 7 DSGVO einen Anhaltspunkt für gemeinsame Verantwortung (»or jointly with others«). Sonst regelt der CCPA die gemeinsame Verantwortung aber nicht. Insbesondere muss ein Unternehmen für die Übermittlung an gemeinsam Verantwortliche keinen Vertrag über die gemeinsame Verantwortung abschließen (abgesehen von dem für jede Übermittlung persönlicher Informationen an Dritte nötigen allgemeinen Weiterübermittlungsvertrag).[141] Nach dem Wortlaut des CCPA ist zudem unklar, ob gemeinsam verantwortliche Unternehmen auch für Bußgelder oder Schadensersatz haften. Zum Schadensersatz ist bei Datenpannen ein Unternehmen verpflichtet, wobei das Unternehmen allerdings eine eigene Pflichtverletzung begangen haben muss.[142] Ein Bußgeld kann gegen mehrere Personen verhängt werden, wenn diese jeweils einen schuldhaften Tatbeitrag geleistet haben.[143]

Entsprechend der nur knappen Regelung spielt gemeinsame Verantwortung bisher in der amerikanischen Literatur nur eine geringe Rolle und ersichtlich keine Rolle in der Rechtspraxis des CCPA.[144] Wahrscheinlich wird sie auch zukünftig – wie lange im deutschen Datenschutzrecht[145] – ein Schattendasein fristen, da es für sie keinen wirklichen Bedarf gibt.

Der EuGH legt die gemeinsame Verantwortung dagegen weit aus.[146] Dies soll die betroffenen Personen effektiv schützen.[147] Gemeinsam Verantwortliche haften nämlich nach Art. 82 Abs. 2 S. 1, Abs. 4 DSGVO gesamtschuldnerisch. Zudem können Aufsichtsbehörden Bußgelder gegen jeden der Verantwortlichen verhängen[148] (strittig ist, ob eigenes Verschulden erforderlich ist[149]). Zudem müssen gemeinsame Verantwortliche nach Art. 26 DSGVO einen Vertrag abschließen, der die datenschutzrechtlichen Rechte und Pflichten aufteilt.

---

[140] Cal. Civ. Code § 1798.140(d)(1). Die Legaldefinition des »processing« in Cal. Civ. Code § 1798.140(y) entspricht dabei Art. 4 Nr. 2 DSGVO.

[141] Cal. Civ. Code § 1798.140(d). Siehe Kapitel 3:D.V (ab S. 173).

[142] Cal. Civ. Code § 1798.150(1)(A). Siehe Kapitel 3:E.II.2.a) (ab S. 208).

[143] Cal. Civ. Code § 1798.150(1)(A).

[144] Einziger Beitrag hierzu: *Linnea/Gomboa*, The Privacy Advisor, Are there joint controllers under the CCPA?

[145] Zu der Rolle unter dem BDSG a.F., das im Gegensatz zu Art. 2 lit. d DSRL nicht explizit eine gemeinsame Verantwortung vorsah: *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, S. 43–45.

[146] EuGH vom 29.07.2019 – C40/17, *Fashion ID,* ECLI:EU:C:2019:629 Rn. 66.

[147] EuGH vom 05.06.2018 – C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388 Rn. 28; vom 10.07.2018 – C-25/17, *Zeugen Jehovas,* ECLI:EU:C:2018:551 Rn. 66; vom 29.07.2019, *Fashion ID*, ECLI:EU:C:2019:629 Rn. 66.

[148] *Nink* in: Spindler/Schuster, DS-GVO Art. 26 Rn. 21; *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, S. 339 f.

[149] Zum Streitstand: *Bergt* in: Kühling/Buchner, DS-GVO Art. 83 Rn. 34–37.

Weiterhin setzt die Unternehmensdefinition Gewinnerzielungsabsicht voraus.[150] Diese bezieht sich nicht auf die konkrete Verarbeitung, sondern auf das gesamte Unternehmen.[151] Gemeinnützige Organisationen und Behörden sind somit nicht erfasst. Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO kann demgegenüber jede öffentliche oder nicht-öffentliche Stelle sein, unabhängig von einer Gewinnerzielungsabsicht. Ausgenommen sind nur Strafverfolgungsbehörden und Einrichtungen der EU (Art. 2 Abs. 2 lit. d, Abs. 3 DSGVO), für die jeweils vergleichbare Regelungen gelten.[152] Dies spricht dafür, dass der CCPA in seinem Ausgangspunkt ein Verbraucherschutzgesetz ist. Zwar drohen den Grundrechten der Bürger durch die Datenverarbeitung des Staates auch Gefahren – wahrscheinlich selbst im amerikanischen Verständnis sogar größere Gefahren.[153] Genau diese klammert der CCPA aber aus und konzentriert sich auf die Machtasymmetrie zwischen großen Unternehmen und Verbraucher:innen.

b) Schwellenwerte

Dementsprechend enthält die Unternehmensdefinition auch einen Schwellenwert für die Unternehmensgröße. Unternehmen müssen alternativ:[154]
- einen Jahresumsatz von mehr als 25 Millionen Dollar erzielen,
- mit persönlichen Informationen von mehr als 100.000 Verbraucher:innen handeln, oder
- einen Anteil von mehr als 50 % des Datenhandels am Gesamtumsatz erreichen.

Der Jahresumsatz von 25 Millionen Dollar bezieht sich auf das jeweils vorangegangene Kalenderjahr.[155] Einige Stimmen in der deutschen Literatur halten für möglich, dass nur der Umsatz in Kalifornien maßgeblich ist.[156] Der für die Auslegung amerikanischer Gesetze herausragend wichtige Wortlaut[157] enthält jedoch keine solche Einschränkung. Daher gehen die amerikanische Literatur und der kalifornische Attorney General einhellig davon aus, dass der weltweite

---

[150] Cal. Civ. Code § 1798.140(d)(1) a.A.

[151] Cal. Civ. Code § 1798.140(d)(1): »organized or operated for the profit«.

[152] Für die Strafverfolgungsbehörden: JI-RL. Für EU-Einrichtungen: Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG.

[153] Ausführlich dazu: *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 7–25. Vgl. die Debatte zum Federal Privacy Act, siehe Kapitel 2:B.I.2 (ab S. 19).

[154] Cal. Civ. Code § 1798.140(d)(1)(A)–(C).

[155] Cal. Civ. Code § 1798.140(d)(1)(A).

[156] *Hoeren/Pinelli*, MMR 2018, 711, 713 f. offenlassend: *Determann*, ZD 2018, 443, 445; *Lejeune*, CR 2018, 569, 570; *ders.,* ITRB 2021, 13, 13, Fn. 3.

[157] Siehe Kapitel 3:B.I.1.a) (ab S. 43).

Umsatz zählt.[158] Dabei ist nur der Umsatz der jeweiligen Gesellschaft maßgeblich.[159] Diesen hohen Schwellenwert erreichen nur circa 2 % der gewinnorientierten Gesellschaften in Kalifornien.[160]

Der zweite Schwellenwert ist erfasst Unternehmen, die mit persönlichen Informationen von mehr als 100.000 Verbraucher:innen im Jahr handeln.[161] Dieser Schwellenwert war im CCPA-2018 wesentlich niedriger.[162] Es reichten bereits 50.000 Verbraucher:innen. Zudem genügte es, wenn ein Unternehmen nur persönliche Information im Geschäftsbetrieb erhielt, ohne dass sich dies als Datenhandel darstellen musste. Damit waren auch beispielsweise kleine Einzelhandelsunternehmen erfasst, die pro Tag mehr als 137 Kreditkartennummern erhalten.[163] Der kalifornische Attorney General ging dabei davon aus, dass diese Definition 50–75 % der kalifornischen Unternehmen erfasse.[164] Um die Bedenken unverhältnismäßiger Umsetzungskosten[165] für kleine Unternehmen auszuräumen, hat Proposition 24 den Schwellenwert von 50.000 auf 100.000 Verbraucher:innen erhöht.[166] Zudem reicht ein Erhalten persönlicher Informationen nicht mehr, sondern der Schwellenwert ist beschränkt auf Datenhandel (»selling« oder »sharing«).[167] »Selling« erfasst dabei jede Übermittlung und jedes Zugriffgewähren auf persönliche Informationen für eine (weit gefasste) Gegenleistung.[168] »Sharing« ist nicht etwa als bloße Übermittlung zu verstehen, sondern erfasst nur das Übermitteln an Dritte für personalisierte Werbung.[169] Die neue Definition betrifft kleine Unternehmen nicht mehr, außer, wenn sie in

---

[158] *Cal. Attorney General,* Summary and Response to Comments Submitted During 45-Day Period, S. 1; *Chander et al.,* 74 SMU L. Rev. 607, 614; *Davis*, 24 N.C. Banking Inst. 499, 500; *de la Torre,* Golden Data, What is a 'business' under CPRA?; *Pink*, California Consumer Privacy Act Annotated, § 2:6.2[A]; *Shatz/Chylik*, 75 Bus. Law. 1918, 1919; *Terry*, 83 Tex. B. J. 148, 148.

[159] *de la Torre,* Golden Data, What is a 'business' under CPRA?

[160] *Roland-Holst et al,* Standardized Regulatory Impact Assessment: CCPA, S. 23.

[161] Cal. Civ. Code § 1798.140(d)(1)(B).

[162] CCPA-2018, Sec. 3, § 1798.140(c)(1)(B).

[163] *Bracy*, Alastair Mactaggart on California's Prop 24, 28m:38s; *Determann,* California Privacy Law, 2-26a:1.2b; *Roland-Holst et al*, Standardized Regulatory Impact Assessment: CCPA, S. 137.

[164] Cal. Attorney General, Summary and Response to Comments Submitted During 45-Day Period, S. 315 unter Verweis auf *Roland-Holst et al*, Standardized Regulatory Impact Assessment: CCPA, S. 20 f.

[165] So *Baik*, Data Privacy Against Innovation or Against Discrimination?, S. 19 f.; *Byun,* 32 Loy. Consumer L. Rev. 246, 249; *Shatz/Chylik*, 75 Bus. Law. 1917, 1918; *Udeshi*, 14 Brook. J. Corp. Fin. & Com. L., 389, 410; *Yallen*, Loy. L. A. L. Rev. 2020, 787, 817.

[166] Proposition 24 (Cal. 2020), Sec. 14, § 1798.140(d)(1)(B). Zur Motivation, diesen Schwellenwert zu erhöhen: *Bracy,* Alastair Mactaggart on California's Prop 24, 28m:38s; *Californians for Consumer Privacy*, The California Privacy Rights and Enforcement Act of 2020.

[167] Cal. Civ. Code § 1798.140(d)(1)(B).

[168] Cal. Civ. Code § 1798.140(ad). Siehe Kapitel 3:C.I.2.a) (ab S. 82).

[169] Cal. Civ. Code § 1798.140(ah)(1). Siehe Kapitel 3:C.I.2.a) (ab S. 82).

größerem Umfang mit persönlichen Informationen handeln. Überschlagsmäßig dürfte das regelmäßig nur in der Medien-, der IT- und der Werbebranche der Fall sein. Diese machen nur etwa 6 % der Gesamtzahl der kalifornischen Betriebe aus.[170] Dieser Prozentsatz gibt einen gewissen Anhaltspunkt dafür, dass von dieser Alternative nur noch eine kleine Minderheit der kalifornischen Betriebe erfasst ist.[171] Die Alternative gibt zudem kleinen bis mittelgroßen Unternehmen einen Anreiz, Datenhandel zu unterlassen und so die Umsetzungskosten des CCPA zu vermeiden.

Die dritte Alternative ist einschlägig, wenn Unternehmen mehr als 50 % ihres Umsatzes mit Datenhandel erzielen.[172] Sie ist ein Auffangtatbestand für kleine werbefinanzierte Anbieter oder kleine Datenhändler. In der Regel dürften Anbieter, die sich durch Datenhandel finanzieren, auch mit persönlichen Informationen von über 100.000 Verbraucher:innen im Jahr handeln, da der Wert einzelner persönlicher Informationen eher gering ist.[173]

Die DSGVO gilt hingegen für Verantwortliche beliebiger Größe. Die Haushaltsausnahme des Art. 2 Abs. 2 lit. c DSGVO erfasst nur persönliche oder familiäre Tätigkeiten. Sie ist eng auszulegen[174] und umfasst nicht jedes Handeln von Privatpersonen, sondern nur das Privat- oder Familienleben außerhalb des öffentlichen Raums.[175] Auch die punktuellen Ausnahmen für kleine und mittlere Unternehmen sind nur schwach ausgeprägt. So soll das europäische Datenschutzrecht zwar auf die besondere Situation der Kleinstunternehmen und der kleinen sowie mittleren Unternehmen Rücksicht nehmen (Erwägungsgrund 13 der DSGVO). Tatsächlich sind diese aber nur an einer Stelle von den Pflichten der DSGVO explizit ausgenommen: Unternehmen mit weniger als 250 Beschäftigten müssen gem. Art. 30 Abs. 5 DSGVO grundsätzlich kein Verzeichnis der Verarbeitungstätigkeiten führen. Dies gilt jedoch hiernach nicht, wenn diese Unternehmen personenbezogene Daten nicht nur gelegentlich verarbeiten

---

[170] *U. S. Census Bureau*, 2017 SUSB Annual Datasets by Establishment Industry: Unternehmenskategorien 4541 (Online-Shops), 51 (Medien), 5415 (Software), 5418 (Werbung & PR) verfügen über einen Anteil von 6,43 % an der Gesamtzahl der Unternehmen in Kalifornien. Davon haben nur 4 % über 100 Beschäftigte, was nahelegt, dass die Überschneidung mit der ersten Jahresumsatz-Alternative nur gering ist.

[171] Ebenso i. Erg.: *Burt*, NAVEX Global, CPRA: 7 Key Changes to California's Data Privacy Laws; *D'Amico/Rumph*, California Ballot Initiative Signals a Sea Change in US Data Privacy Law but Should Not Be Reason for Fear. Vgl. die Berechnung in Cal. Privacy Protection Agency, Notes on Economic Impact Estimates for Form 399, S. 3–10: 66 % der kleinen Unternehmen seien im Anwendungsbereich, räumt allerdings selbst ein, dass diese Berechnung wegen fehlender Daten die tatsächliche Zahl deutlich überschätze (S. 9).

[172] Cal. Civ. Code § 1798.140(d)(1)(C).

[173] Vgl. *OECD,* Exploring the Economics of Personal Data, S. 25f: gibt Marktpreise für bestimmte persönliche Informationen an.

[174] EuGH vom 10.07.2018 – C-25/17, *Zeugen Jehovas*, ECLI:EU:C:2018:551 Rn. 37; *Gola* in: Gola, DS-GVO Art. 4 Rn. 19–23.

[175] EuGH vom 10.07.2018, *Zeugen Jehovas*, ECLI:EU:C:2018:551 Rn. 42.

– wofür selbst Buchhaltung und Kundenmanagement ausreichen sollen.[176] Daneben müssen nicht-öffentliche Stellen Datenschutzbeauftragte in der Regel[177] erst bestellen, wenn sie mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen (§ 38 Abs. 1 S. 1 BDSG). Indirekt wirkt sich die Größe bei Datenschutz-Folgenabschätzung aus, da solche bei einer großen Anzahl betroffener Personen und eines aggregiert höheren Risikos häufiger durchzuführen sind (Erwägungsgrund 91 S. 1 der DSGVO).[178] Mit den hohen Schwellenwerten für die Anwendbarkeit des CCPA ist dies nicht vergleichbar.

Wie wirkt sich die Beschränkung auf große Unternehmen tatsächlich auf die Risiken für Individuen aus? Aus der Verarbeitung großer Datenmengen durch große Unternehmen erwachsen höhere Gefahren. Mit der Größe der Datenmenge skaliert nahezu jedes Risiko für betroffene Personen. Zudem entstehen aus einer Zentralisierung besondere Gefahren.[179] So können auch *prima facie* belanglose Daten mit anderen personenbezogenen Daten kombiniert werden und so umfassende Persönlichkeitsprofile bilden.[180] Eine Zentralisierung ermöglicht zudem Massenüberwachung durch eine einheitliche »Anlaufstelle« für Sicherheitsbehörden. Die DSGVO berücksichtigt diese höheren Risiken durch Zentralisierung kaum. Vielmehr führt ihr weiter Anwendungsbereich gerade zu einer stärkeren Zentralisierung, da bei kleinen Unternehmen die Umsetzungskosten stärker ins Gewicht fallen.[181] Dies zeigt die Entwicklung auf dem Online-Werbemarkt, bei dem die Einführung der DSGVO zu einer Verdrängung kleiner Anbieter geführt hat.[182]

Gleichzeitig können auch kleine Organisationen Risiken hervorrufen. Eine ständige Videoüberwachung in einem Einzelhandelsgeschäft erzeugt beispielsweise einen starken Überwachungsdruck auf die Beschäftigten, der unabhängig von der Unternehmensgröße ist. Auch Datensicherheit ist für jede Organisation relevant.[183]

---

[176] *Petri* in: NK-DatenschutzR, DS-GVO Art. 30 Rn. 45; *Spoerr* in: BeckOK DatenschutzR, DS-GVO Art. 30 Rn. 24; wohl auch: *DSK*, Kurzpapier Nr. 1 – Art. 30 DS-GVO, S. 1; a. A. *Wolff* in: Schantz/Wolff, Das neue Datenschutzrecht Rn. 863–865.

[177] Ausnahmen in Art. 37 Abs. 1 lit. b, c DSGVO, § 38 Abs. 1 S. 2 BDSG.

[178] *Artikel-29-Datenschutzgruppe*, WP 248 DSFA, S. 11; *Friedewald et al.*, White Paper Datenschutz-Folgenabschätzung, S. 21.

[179] *Specht-Riemenschneider et al.*, MMR-Beil. 2021, 25, 30; *Solove*, 154 U. Pa. L. Rev. 477, 506–511.

[180] Vgl. BVerfG vom 15.12.1983 – 1 BvR 209/83, *Volkszählung*, BVerfGE 65, 1, 45: Es gebe wegen der besonderen Verknüpfungsmöglichkeiten der Informationstechnologie keine belanglosen Daten mehr.

[181] *Lancieri*, Narrowing Data Protection's Enforcement Gap, S. 36 f.; *Lewinski*, Die Matrix des Datenschutzes, S. 85; *Veil*, NVwZ 2018, 686, 692 f. Zu Agreggierung von personenbezogenen Daten als eigenständiges Risiko: *Solove*, 154 U. Pa. L. Rev. 477, 506–511.

[182] *Peukert et al.*, Working Paper: European Privacy Law and Global Markets for Data, S. 20 f.

[183] Ähnlich *Williams*, 53 Ind. L. Rev. 217, 238.

Das kalifornische Recht erreicht hier eine ausgewogene Lösung. Der CCPA gilt zwar selbst nur für große Unternehmen. Gleichzeitig greift aber auch eine Art »Basis-Datenschutz« aus anderen kalifornischen Gesetzen. So müssen nach dem kalifornischen Datensicherheitsgesetz alle Organisationen eine angemessene Datensicherheit wahren.[184] Auch gelten zahlreiche bereichsspezifische Datenschutzgesetze.[185] So darf ein Unternehmen nach kalifornischem Arbeitsrecht beispielsweise keine Videoüberwachung in einem Umkleideraum installieren.[186] Diese sehr spezifischen Pflichten sind wesentlich leichter zu erfüllen, als die offen formulierten Pflichten der DSGVO, deren Erfüllung häufig professionellen Rechtsrat erfordert.[187] Diese Lösung dürfte aber nur schwer zu übernehmen sein, da sie kein abgeschlossenes, kohärentes System darstellt. Zudem reagieren diese bereichsspezifischen Gesetze häufig auf spezifisch amerikanische Probleme wie Identitätsdiebstahl.[188] Dennoch sollten *de lege ferenda* auch im europäischen Datenschutzrecht die datenschutzrechtlichen Pflichten stärker abgestuft sein. Es führt beispielsweise zu keiner größeren Transparenz, Privatpersonen oder Kleinstunternehmen umfassende Informationspflichten aufzubürden, die sie allenfalls durch »Abschreiben« einer abstrakt formulierten Musterdatenschutzerklärung erfüllen können.

c) Konzerngesellschaften und Joint Ventures

Konzerngesellschaften sind ebenfalls Unternehmen, auch wenn nur die jeweilige Mutter- oder Tochtergesellschaft den Schwellenwert erreicht. Dies setzt eine Beherrschung der betreffenden Tochtergesellschaft, ein gemeinsames Auftreten nach Außen und eine Weiterübermittlung persönlicher Informationen zwischen den Konzerngesellschaften voraus.[189]

Das erste Tatbestandsmerkmal Beherrschen (»controls or is controlled«) ist erfüllt, wenn die Muttergesellschaft über mehr als 50 % der Anteile oder Stimmrechte, die Entscheidungsmacht über die Mehrheit der Mitglieder des jeweiligen Leitungsgremium oder sonst über einen bestimmenden Einfluss auf die Geschäftsführung verfügt.[190] Das Kriterium des bestimmenden Einflusses entstammt dem Finanzaufsichtsrecht und setzt einen deutlichen, aber nicht notwendigerweise absoluten Einfluss auf die Entscheidungen der kontrollierten Gesellschaft voraus.[191] Die detaillierten Regelungen aus dem Finanzaufsichts-

---

[184] Cal. Civ. Code §§ 1798.80(a), 1798.81.5(c). Siehe Kapitel 3:D.IV (ab S. 171).

[185] Siehe Kapitel 2:B.I.2 (ab S. 19).

[186] Cal. Lab. Code § 435. Dazu: *Determann*, California Privacy Law, S. 126 f.

[187] *Europäische Kommission*, Commission Staff Working Document: two years of application of GDPR, SWD/2020/115 final, Nr. 5: offene Formulierungen und fehlende Handreichungen der Aufsichtsbehörden führten zu starker Inanspruchnahme externen Rechtsrats.

[188] Zu kalifornischen bereichsspezifischen Regelungen siehe Kapitel 2:B.II (ab S. 27).

[189] Cal. Civ. Code § 1798.140(d)(2).

[190] Cal. Civ. Code § 1798.140(d)(2).

[191] 12 U.S.C. § 1841(a)(2), 12 C.F.R. § 238.22.

recht bilden wohl einen Anhaltspunkt, wie man den bestimmenden Einfluss auslegen könnte.

Das zweite Merkmal eines gemeinsamen Auftretens nach Außen ist erfüllt, wenn durchschnittliche Verbraucher:innen aufgrund eines gemeinsamen Namens oder einer sonstigen Marke davon ausgehen, dass beide Betriebe unter einer gemeinsamen Leitung stehen.[192]

Die Bedeutung des dritten Tatbestandsmerkmals Weiterübermittlung persönlicher Informationen an die Konzerngesellschaft (»with whom the business shares consumers personal data«)[193] ist unklar. »Sharing« ist, wie oben dargestellt, als Übermitteln an Dritte allein für personalisierte Werbung legaldefiniert.[194] Damit wäre nur die konzerninterne Übermittlung für Werbezwecke erfasst. Dieser Redaktionsfehler ist wohl so entstanden, dass Californians for Consumer Privacy im ersten Entwurf von Proposition 24 dieses Tatbestandsmerkmal zur Konzerngesellschafts-Definition hinzugefügt hat und erst im dritten Entwurf die Legaldefinition des »sharing« ergänzt hat.[195] Allerdings berücksichtigt die kalifornische Rechtsprechung bei der historischen Auslegung von Volksbegehren nur die allen Wähler:innen vorliegenden zwei Dokumente: die Zusammenfassung auf dem Stimmzettel und die an alle Haushalte verteilte Wahlbroschüre.[196] Allein diese bildeten den Willen des kalifornischen Volkes als Gesetzgeber ab.[197] Bei teleologischer Auslegung wäre das Ergebnis ebenfalls klar: dieses Kriterium soll nur dagegen absichern, dass Konzerngesellschaften, die in keiner Weise mit persönlichen Informationen in Kontakt kommen, nicht die umfangreichen Pflichten für Unternehmen des CCPA erfüllen müssen. Allerdings ist die teleologische Auslegung im amerikanischen Recht stark umstritten und wird allenfalls zurückhaltend angewendet.[198] Bei einem klaren Wortlaut scheidet nach der Rechtsprechung eine teleologische Auslegung aus, außer wenn das Ergebnis einer wortgetreuen Auslegung absurd ist.[199] Die Schwelle für Absurdität liegt hoch. Selbst Regelungen, die im europäischen Kontext

---

[192] Cal. Civ. Code § 1798.140(d)(2).

[193] Cal. Civ. Code § 1798.140(d)(2).

[194] Cal. Civ. Code § 1798.140(ah)(1).

[195] Erste Version: *Californians for Consumer Privacy*, California Privacy Rights and Enforcement Act, S. 20. Dritte Version: *Californians for Consumer Privacy*, California Privacy Rights and Enforcement Act of 2020, Version 3, S. 29. Die zweite Version enthielt diesbezüglich keine Änderung.

[196] Cal. Supreme Court vom 11.03.1985, *People v. Castro,* 696 P.2d 111, 116 f.; vom 23.06.1988, *Lungren v. Deukmejian*, 755 P.2d 299, 309; vom 01.11.1990, *Taxpayers to Limit Campaign Spending v. Fair Pol. Practices Com.*, 51 Cal. 3d 744, 764 Fn. 10; *Liebert*, 90 Law Libr. J., 27, 36; a. A. *Kelso*, 19 Pepp. L. Rev. 327, 353–358.

[197] Cal. Supreme Court vom 11.03.1985, *People v. Castro,* 696 P.2d 111, 116f; vom 23.06.1988, *Lungren v. Deukmejian*, 755 P.2d 299, 309; vom 01.11.1990, *Taxpayers to Limit Campaign Spending v. Fair Pol. Practices Com*, 51 Cal. 3d 744, 764 Fn. 10.

[198] Siehe Kapitel 3:B.I.1.b) (ab S. 45).

[199] Cal. Supreme Court vom 23.06.1988, *Lungren v. Deukmejian*, 755 P.2d 299, 303 f.

»offensichtliche Redaktionsfehler« wären, legt die Rechtsprechung wortwörtlich aus.[200] Eine Legaldefinitionen ist zu beachten, außer wenn das definierte Wort in einem anderen Kontext benutzt wird.[201] Dabei gilt die Vermutung, dass der Gesetzgeber, wenn er den gleichen Begriff in engem Zusammenhang mehrmals verwendet, an allen Stellen die gleiche Bedeutung intendiert.[202] Zwar könnte man argumentieren, dass die Legaldefinition in dem Kontext der Konzerngesellschaftsdefinition nicht vollständig passend ist. Allerdings verwendet der CCPA direkt im vorhergehenden Satz »sharing consumer's personal information« im Sinne der legaldefinierten Weiterübermittlung für Werbezwecke.[203] Der Wortlaut ist daher eindeutig: Konzerngesellschaften sind nur Unternehmen, soweit sie persönliche Informationen konzernintern für Werbezwecke weitergeben.[204] Diese Interpretation ist auch nicht absurd, da konzerninterne Weitergabe persönlicher Informationen für Werbezwecke übliche Praxis bei Medienkonzernen ist.

Zudem sind *joint ventures*, bei denen zwei Unternehmen jeweils mindestens 40 % der Anteile halten, eigenständige Unternehmen.[205] Persönliche Informationen, die das *joint venture* von einem der Mutterunternehmen erhält, darf es nicht an das andere Mutterunternehmen weitergeben (»shares«).[206] Hier stellt sich wegen der Legaldefinition von »sharing«[207] das gleiche Problem wie bei Konzerngesellschaften.

Schließlich kann jede in Kalifornien geschäftlich tätige juristische oder natürliche Person sich freiwillig dem CCPA durch Mitteilung an die California Privacy Protection Agency unterwerfen und so Unternehmen werden.[208] Dies ist vor allem im Fall eines Angemessenheitsbeschlusses für Kalifornien relevant – dann können durch ein solches Unterwerfen auch kleinere Anbieter die Vorteile des Art. 45 DSGVO erreichen.[209]

Die DSGVO enthält keine Sonderregelungen für die Erstreckung des Verantwortlichenbegriffs. Sie benötigt sie auch nicht, da sie keine Schwellenwerte kennt. Die mögliche Konzernhaftung bei Bußgeldern[210] ist nur entfernt verwandt,

---

[200] U. S. Supreme Court vom 01.06.1987, *CIR v. Asphalt Prods. Co.*, Inc., 482 U. S. 117, 121; vom 25.06.2015, *King v. Burwell* – ablehnendes Sondervotum *Scalia*, 576 U. S. 473, 498–518.

[201] U. S. Supreme Court vom 09.01.1979, *Colautti v. Franklin*, 439 U. S. 379, 391 f.

[202] U. S. Supreme Court vom 18.04.2012, *Mohamad v. Palestinian Auth.*, 566 U. S. 449, 456.

[203] Cal. Civ. Code § 1798.140(d)(1)(C).

[204] Ebenso o.Begr.: *Orrick*, The California Privacy Rights Act (CPRA): Frequently Asked Questions.

[205] Cal. Civ. Code § 1798.140(d)(3).

[206] Cal. Civ. Code § 1798.140(d)(3). Dazu *Friel/Fath*, California Voters Approve Reworking of Landmark Consumer Privacy Law – What CCPA 2.0 Will Mean for Businesses and Consumers: Verbot sei nur nicht total gemeint, sondern solle nur sicherstellen, dass die Übermittlung ein Datenhandel i.S.d. CCPA darstelle.

[207] Cal. Civ. Code § 1798.140(ah)(1).

[208] Cal. Civ. Code § 1798.140(d)(4).

[209] Dies ist der Gesetzeszweck: *Californians for Consumer Privacy*, Annotated Text of the CPRA, § 1798.140(d)(4).

[210] Darstellung des Streitstandes: *Bergt* in: Kühling/Buchner, DS-GVO Art. 83 Rn. 28.

da die Adressatenstellung bei Bußgeldern und nicht die Erstreckung des Anwendungsbereichs der DSGVO selbst betrifft.

3. Dienstleister

a) Darstellung

Der CCPA enthält zwei Begriffe für Dienstleister (»contractor«[211] und »service provider«[212]), die sich sowohl in ihren Voraussetzungen als auch in den daran geknüpften Rechtsfolgen stark ähneln. Die wesentliche Rechtsfolge ist, dass eine Übermittlung an *service provider* und *contractor* kein Datenhandel ist.[213] Damit darf das Unternehmen auch bei einem etwaigen Widerspruch gegen Datenhandel persönliche Informationen an *service provider* und *contractor* übermitteln. Im Gegenzug dürfen sie persönliche Informationen grundsätzlich nur für die Vertragserfüllung nutzen und nicht mit persönlichen Informationen aus anderen Quellen kombinieren.[214] Damit ähneln *service provider* und *contractor* stark den Auftragsverarbeitern der DSGVO. Eine Person kann je nach Rolle, die sie im Bezug auf die konkrete Verarbeitung spielt, entweder *service provider, contractor* oder Unternehmen sein, aber nicht zugleich.[215]

Service provider ist definiert als eine Person, die persönliche Informationen im Auftrag des Unternehmens verarbeitet (»on behalf of a business«).[216] Der *contractor*-Begriff setzt dagegen nur voraus, dass das Unternehmen die persönlichen Informationen zugänglich macht (»makes available«).[217] So wird z. B. ein Wirtschaftsprüfer persönliche Informationen nicht im Auftrag handeln, sondern unabhängig prüfen und damit *contractor* sein.[218] Die meisten Dienstleister sind aber *service provider*.[219]

Service provider und *contractor* müssen grundsätzlich für ein Unternehmen handeln.[220] Anbieter für Nicht-Unternehmen (wie eine Behörde) sind dagegen kein *service provider* oder *contractor*. Wenn allerdings ein Anbieter die

---

[211] Cal. Civ. Code § 1798.140(j)(1).

[212] Cal. Civ. Code § 1798.140(ag)(1).

[213] Siehe Kapitel 3:C.I.2.a) (ab S. 82).

[214] Cal. Civ. Code § 1798.140(j)(1)(A)(i)–(iv),(ag)(A)–(D).

[215] 11 C. C. R. § 7051(f). Missverständlich: U. S. District Court S. D. Cal. vom 12.08.2021, *In re Blackbaud, Inc.,* 2021 U. S. Dist. LEXIS 151831, 15–17: *service provider* könne zugleich *business* sein. Offensichtlich wollte das Gericht nur aussagen, dass die Beklagte in diesem Fall *business* ist und keine generelle Aussage für alle *service provider* treffen, vgl. *Goldman*, Technology & Marketing Law Blog, CCPA Definitions Confuse the Judge in a Data Breach Case-In re Blackbaud.

[216] Cal. Civ. Code § 1798.140(ag)(1).

[217] Cal. Civ. Code § 1798.140(j)(1).

[218] *de la Lama/Hengesbaugh*, The Privacy Advisor, How to know if your vendor is a »service provider« under CCPA.

[219] *Friel/Fath*, Data Counsel, What CCPA 2.0 Will Mean for Businesses and Consumers.

[220] Cal. Civ. Code § 1798.140(j)(1),(ag)(1).

Schwellenwerte für Unternehmen erreicht, ist er auch bei Handeln für ein Nicht-Unternehmen *service provider*.[221] Sonst wäre dieser Anbieter Unternehmen und systemwidrigerweise selbst den Pflichten eines Unternehmens unterworfen.[222]

Die für *service provider* und *contractor* zulässigen Dienstleistungen sind abschließend aufgezählt (»business purposes«).[223] Diese zulässigen Dienstleistungen sind allerdings eher weit gefasst. So genügt, dass es sich um eine Unternehmensdienstleistung handelt (»Performing services on behalf of the business«)[224] oder dass die Nutzung persönlicher Informationen nur vorübergehend ist (»Short-term, transient use«).[225] Explizit aufgeführt sind Qualitätskontrolle, Marktforschung, IT-Dienstleistungen wie das Bereitstellen von Speicherplatz, Fehlerbehebung und Webseitenanalysen.[226] Dabei darf aber kein Profil des Verbrauchers oder der Verbraucherin gebildet werden.[227] Auch nicht-personalisierte Werbung ist grundsätzlich zulässig.[228] Werbung ist nicht-personalisiert, wenn das Unternehmen nur die Informationen aus der aktuellen Interaktion und keine genauen Standortdaten nutzt (gröber als circa 1 km^2).[229] Es wäre demnach möglich, beispielsweise anhand der IP-Adresse den ungefähren Aufenthaltsort San Francisco zu bestimmen und dementsprechend an San Francisco lokal angepasste Werbung anzuzeigen.[230] Die Nutzung der persönlichen Informationen für diese Dienstleistungen muss erforderlich und angemessen sein.[231]

Der *service provider* oder *contractor* darf grundsätzlich keine persönlichen Informationen für eigene Zwecke nutzen.[232] Er darf insbesondere nicht mit den persönlichen Informationen handeln,[233] die erhaltenen persönlichen Informationen nicht außerhalb der Geschäftsbeziehung mit dem Unternehmen nutzen[234]

---

[221] 11 C.C.R. § 7051(a). Diese Vorschrift ist noch nicht an die neue Kategorie des *contractors* angepasst, was allerdings zeitnah zu erwarten ist.

[222] *Cal. Attorney General*, Initial Statement of Reasons, S. 21; *ders.,* Final Statement of Reasons, S. 29 f.

[223] Cal. Civ. Code §§ 1798.140(ad)(1), 1798.140(ah)(1) jeweils i.V.m. § 1798.140(e). Zu dem abschließenden Charakter: *Levi/Healow*, California Consumer Privacy Act: A Compliance Guide, S. 13.

[224] Cal. Civ. Code § 1798.140(e)(5).

[225] Cal. Civ. Code § 1798.140(e)(4).

[226] Cal. Civ. Code § 1798.140(e)(1),(2),(3),(5),(7).

[227] Cal. Civ. Code § 1798.140(e)(4),(6).

[228] Cal. Civ. Code § 1798.140(e)(6). Dies war zum CCPA-2018 in der Praxis umstritten: S. *Haggin*, Wall Street Journal, Facebook Won't Change Web Tracking in Response to California Privacy Law.

[229] Cal. Civ. Code § 1798.140(e)(6). Definiert als die Fläche eines Kreises mit einem Radius von 1850 Fuß (Radius: 563,88 m; Fläche: 998.902,85 m2), Cal. Civ. Code § 1798.140(w). Warum dieser Wert gewählt wurde, ist unklar.

[230] *Californians for Consumer Privacy*, Prop 24 Limits the Tracking of Geolocation.

[231] Cal. Civ. Code § 1798.140(e) a.A.

[232] Cal. Civ. Code § 1798.140(e) a.A.

[233] Cal. Civ. Code §§ 1798.140(j)(1)(A)(i),(ag)(1)(A); 11 C.C.R. § 7051(d).

[234] Cal. Civ. Code §§ 1798.140(j)(1)(A)(iii),(ag)(1)(C).

und nicht mit Daten aus anderen Geschäftsbeziehungen kombinieren.[235] Dies muss das Unternehmen durch Abschluss eines Dienstleistervertrages absichern, der im Zusammenhang mit dem ebenfalls nötigen allgemeinen Weiterübermittlungsvertrag näher dargestellt ist.[236]

Service provider und *contractor* dürfen die überlassenen persönlichen Informationen allerdings für eigene bestimmte Betriebszwecke (*operational purposes)* nutzen.[237] Insoweit ist auch eine Kombination mit persönlichen Informationen aus anderen Geschäftsbeziehung möglich.[238] Ein solches Nutzen persönlicher Informationen für eigene Zwecke muss mit den berechtigten Erwartungen der Verbraucher:innen kompatibel sein und darf nicht über das nötige Maß hinausgehen.[239] Die zulässigen eigenen Betriebszwecke umfassen das Erkennen von unberechtigten Zugriffen, Betrug und sonstigen rechtswidrigen Handlungen sowie Qualitätskontrolle, solange der *service provider* oder *contractor* keine Profile von Verbraucher:innen erstellt.[240] Dagegen ist eine Nutzung für eigene Werbezwecke ausdrücklich ausgeschlossen.[241]

Zudem sind *Service provider* und *contractor* verpflichtet, dem Unternehmen Unterauftragnehmer mitzuteilen und ihnen die wesentlichen Pflichten über einen Unter-Dienstleistervertrag weiterzugeben.[242] Sie müssen bei der Ausübung von Löschanträgen kooperieren.[243] Ebenfalls müssen sie angemessene technische und organisatorische Maßnahmen ergreifen.[244] Gegen sie kann ein Bußgeld oder eine *civil penalty* verhängt werden, allerdings nur wenn sie für den Verstoß verantwortlich sind.[245] Dagegen haften sie nicht für Schadensersatz bei Datenpannen.[246]

Unternehmen haften nicht für Rechtsverstöße des *service providers* oder *contractors,* außer wenn sie zum Zeitpunkt der Übermittlung wussten oder deutliche Anhaltspunkte hatten (»reason to believe«), dass diese beabsichtigten, gegen den CCPA zu verstoßen.[247] *Reason to believe* entstammt dem amerikanischen Strafprozessrecht. Er bezeichnet den Verdachtsgrad, der es Strafverfolgungsbehörden ermöglicht, eine Wohnung zu durchsuchen.[248] Eine überwiegende Wahr-

---

[235] Cal. Civ. Code §§ 1798.140(j)(1)(A)(iv),(ag)(1)(D).
[236] Cal. Civ. Code §§ 1798.140(j)(1)(A),(ag)(1). siehe Kapitel 3:D.V (ab S. 173).
[237] Cal. Civ. Code § 1798.140(e): »for the service provider or contractor's operational purposes«; 11 C.C.R. § 7051(3)–(5).
[238] Cal. Civ. Code §§ 1798.140(j)(1)(A)(iv),(ag)(1)(D).
[239] Cal. Civ. Code § 1798.140(e) a.A.
[240] 11 C.C.R. § 7051(d)(3), (4).
[241] Cal. Civ. Code §§ 1798.140(j)(1)(A)(iv),(ag)(1)(D).
[242] Cal. Civ. Code § 1798.140(j)(2),(ag)(2).
[243] Cal. Civ. Code § 1798.105(c)(3).
[244] Cal. Civ. Code § 1798.130(a)(3)(A) a.E.
[245] Cal. Civ. Code § 1798.155(a), 1798.199.55(b), 1798.199.90(a).
[246] Siehe Kapitel 3:E.II.2.a) (ab S. 208).
[247] Cal. Civ. Code § 1798.145(i)(1).
[248] U.S. Supreme Court vom 15.04.1980, *Payton v. New York*, 445 U.S. 573, 603.

scheinlichkeit ist aber nicht erforderlich; es reichen objektive Anhaltspunkte.[249] Umgekehrt haften *service provider* und *contractor* nicht für Rechtsverstöße des Unternehmens.[250] Diese unternehmensfreundliche klare Abgrenzung birgt die Gefahr, dass die Verbraucher:innen schutzlos gestellt werden.[251]

Insgesamt sind an die Unterscheidung zwischen *service provider* und *contractor* nur minimal unterschiedliche Rechtsfolgen geknüpft.[252] Deshalb werden beide nachfolgend als »Dienstleister« zusammengefasst.

b) Vergleich mit den Auftragsverarbeitern der DSGVO

Der *service provider* entspricht hinsichtlich seiner Voraussetzungen dem Auftragsverarbeiter i.S.d. Art. 4 Nr. 8, 28 Abs. 1 DSGVO, da er ebenso personenbezogene Daten im Auftrag verarbeitet (»on behalf«). Die Kategorie des *contractors* entspricht der eines eigenständigen Verantwortlichen. Die Weiterübermittlung von personenbezogenen Daten an eigenständige Verantwortliche ist in der DSGVO kaum geregelt. Wie bei jeder Verarbeitung personenbezogener Daten muss auch für eine Übermittlung an eigenständige Verantwortliche eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO vorliegen.[253] Die Übermittlung an einen eigenständigen Verantwortlichen in einem Drittstaat muss die Bedingungen der Art. 44–50 DSGVO einhalten – insbesondere bezieht sich ein Modul der Standarddatenschutzklauseln nach Art. 46 Abs. 2 lit. a DSGVO auf Übermittlungen an eigenständige Verantwortliche.[254] Es bestehen aber keine mit Art. 28 DSGVO vergleichbaren speziellen Pflichten für solche Übermittlung an eigenständige Verantwortliche.

Dementsprechend ist die Abgrenzung im Grenzbereich zwischen eigenständiger Verantwortlichkeit und Auftragsverarbeitung stark umstritten. Eigenständiger Verantwortlicher ist, wer selbst die Mittel und Zwecke der Verarbeitung bestimmt (Art. 4 Nr. 7 DSGVO). Zur Abgrenzung werden unscharfe Kriterien wie ein Eigeninteresse an der Verarbeitung, Weisungsgebundenheit oder die Planmäßigkeit des Zugriffs auf personenbezogene Daten diskutiert.[255] Freie Be-

---

[249] U.S. Court Appeals D.C. Circuit vom 18.11.2005, *United States v. Thomas*, 429 F.3d 282, 285 f.; Cal. Court of Appeal 4th District vom 18.08.2011, *People v. Downey*, 198 Cal. App. 4th 652, 660–662.

[250] Cal. Civ. Code § 1798.145(i)(1).

[251] *Miller*, Is the California Consumer Privacy Act the Answer to Price Discrimination?, S. 6.

[252] Zu der beim *contractor* zusätzlich nötigen deklaratorischen Bekräftigung seiner Pflichten (Cal. Civ. Code § 1798.140(j)(B)) siehe Kapitel 3:D.V (ab S. 173).

[253] Für Auftragsverarbeiter ist strittig, ob Art. 28 DSGVO eigenständige Rechtsgrundlage ist, vgl. *Spoerr* in: BeckOK DatenschutzR, DS-GVO Art. 28 Rn. 29–32.

[254] Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, ABl. 2021 L 199, 31, Anhang, jeweils Modul Eins.

[255] *EDSA*, Guidelines 07/2020 Controller Processor, Rn. 74–81; *Hartung* in: Kühling/Buchner, DS-GVO Art. 28 Rn. 26–30, 45–52.

rufe (wie Rechtsanwaltschaft und Ärzteschaft) sind wegen ihrer Unabhängigkeit eigenständige Verantwortliche.[256] Dagegen ist unklar, ob Auftragsverarbeiter ist, wer zufällig Zugang zu personenbezogenen Daten erhält (beispielsweise Reinigungsdienstleister).[257]

Unter dem CCPA ist diese Abgrenzung wesentlich einfacher und pragmatischer, da alle Arten des Zugänglichmachens unter die Kategorie des *contractors* fallen.

Ein wesentlicher Unterschied zur DSGVO ist die klare Abgrenzung der Haftung unter dem CCPA. Der Verantwortliche haftet dagegen gemäß Art. 82 Abs. 1, 2 S. 1 DSGVO für eine Pflichtverletzung seiner Auftragsverarbeiter. Der Verantwortliche kann sich zwar nach Art. 82 Abs. 3 DSGVO von der Haftung befreien, wenn er nachweist, dass er in keiner Weise für den Schaden verantwortlich ist. Dabei wird ihm jedoch Fehlverhalten des Auftragsverarbeiters grundsätzlich zugerechnet.[258] Die Zurechnung ist allein für den Fall umstritten, dass ein Auftragsverarbeiter eigenmächtig gegen rechtmäßige Weisungen des Verantwortlichen verstößt.[259]

Sonst ähneln die Rechte und Pflichten der Dienstleister des CCPA denjenigen der Auftragsverarbeitern der DSGVO. Verantwortliche müssen gemäß Art. 28 Abs. 3 DSGVO mit Auftragsverarbeitern einen Vertrag abschließen, dessen Inhalt mit dem Dienstleistervertrag vergleichbar ist.[260] Ebenso wie der Dienstleister muss der Auftragsverarbeiter nach Art. 32 DSGVO angemessene technische und organisatorische Maßnahmen ergreifen. Auftragsverarbeiter dürfen personenbezogene Daten nach Art. 29 DSGVO nur auf Weisung verarbeiten. Der Begriff der Weisungsgebundenheit ist hier missverständlich. Der Auftragsverarbeitungsvertrag ist nicht wie ein Arbeitsvertrag durch umfangreiche Weisungen des Verantwortlichen ausfüllungsbedürftig. Vielmehr sind die Weisungen in der Praxis im Auftragsverarbeitungsvertrag detailliert festgelegt (wobei sich

---

[256] *EDSA*, Guidelines 07/2020 Controller Processor, Rn. 25; *Ziegenhorn/Fokken*, ZD 2019, 194, 197; *Spoerr* in: BeckOK DatenschutzR, DS-GVO Art. 28 Rn. 25, 25.1. Bei Steuerberater:innen war dies umstritten, bis der deutsche Gesetzgeber ausdrücklich in § 11 Abs. 2 StBerG die eigenständige Verantwortlichkeit normiert hat, vgl. *Hartung* in: Kühling/Buchner, DS-GVO Art. 28 Rn. 47.

[257] Für Auftragsverarbeitung: *Bertermann* in: Ehmann/Selmayr, DS-GVO Art. 28 Rn. 10; *Eßer* in: Eßer/Kramer/Lewinski, DSGVO Art. 4 Rn. 40; *Gabel/Lutz* in: Taeger/Gabel, DS-GVO Art. 28 Rn. 17; *Hartung* in: Kühling/Buchner, DS-GVO Art. 28 Rn. 53; *Petri* in: NK-DatenschutzR, DS-GVO Art. 28 Rn. 22 f.; *Wedde* in: Däubler et al., EU-DSGVO Art. 28 Rn. 29.
Gegen Auftragsverarbeitung: *LfDI Bremen*, Tätigkeitsbericht 2020, S. 49 f. *Gola* in: Gola, DS-GVO Art. 4 Rn. 77; *Lissner*, DSRITB 2016, 401, 414; *Spoerr* in: BeckOK DatenschutzR, DS-GVO Art. 28 Rn. 21b;
Vermittelnd: *EDSA*, Guidelines 07/2020 Controller Processor, Rn. 83.

[258] *Bergt* in: Kühling/Buchner, DS-GVO Art. 82 Rn. 55; *Boehm* in: NK-DatenschutzR, DS-GVO Art. 82 Rn. 24.

[259] Für eine Haftung bei weisungswidrigem Handeln: *Bergt* in: Kühling/Buchner, DS-GVO Art. 82 Rn. 55; *Boehm* in: NK-DatenschutzR, DS-GVO Art. 82 Rn. 24. Dagegen: *Moos/Schefzig* in: Taeger/Gabel, DS-GVO Art. 82 Rn. 83.

[260] Siehe Kapitel 3:D.V (ab S. 173).

der Verantwortliche darüber hinaus häufig das Recht zu Einzelweisungen vorbehält).[261] Entscheidend für Weisungsbindung ist nur, dass der Auftragsverarbeiter auf Anweisung und unter Kontrolle des Verantwortlichen handelt.[262] Ein Handeln unter der Kontrolle entspricht der Pflicht des ausschließlichen Nutzens innerhalb der Geschäftsbeziehung für Dienstleister des CCPA.

Eine Nutzung für eigene Zwecke führt unter der DSGVO dazu, dass der Auftragsverarbeiter Verantwortlicher wird.[263] Sie ist beispielsweise zur Produktverbesserung weit verbreitet, allerdings mangels Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO regelmäßig unzulässig.[264] Hierin unterscheidet sich die DSGVO vom CCPA, der punktuell eine Nutzung zu solchen unproblematischen eigenen *operational purposes* zulässt. Weiterhin kann das Unternehmen neuen Unterauftragnehmern unter dem CCPA nicht widersprechen; der Dienstleister muss diese nur mitteilen.[265] Unter der DSGVO dürfen dagegen Auftragsverarbeiter weitere Unterauftragsverarbeiter nur nutzen, wenn der Verantwortliche je nach Vertrag entweder gesondert eingewilligt hat oder keinen Einspruch gegen die mitgeteilten Unterauftragsverarbeiter erhoben hat (Art. 28 Abs. 2 DSGVO).

Insoweit zeigt sich die pragmatischere Herangehensweise des CCPA. Die DSGVO geht von einem klaren Über-/Unterordnungsverhältnis zwischen Verantwortlichen und Auftragsverarbeiter aus. Der Verantwortliche ist »Herr der Daten«,[266] während der Auftragsverarbeiter nur dessen »verlängerter Arm«[267] ist. Der CCPA geht dagegen mehr von einem gleichrangigen Zusammenwirken des Dienstleisters und Unternehmens aus, in der nicht Weisungen, sondern die vertragliche Arbeitsteilung maßgeblich ist. Er passt insoweit besser zu der wirtschaftlichen Realität, in der sich große Auftragsverarbeiter nur schwer an Einzelweisungen kleiner Verantwortlicher anpassen können.

---

[261] Vgl. die Muster in: *Bitkom*, Mustervertragsanlage Auftragsverarbeitung, § 2(2); *Hofmann* in: Nägele/Apel, Beck'sche Online-Formulare IT- und Datenrecht, Muster 2.19 Rn. 10; *Schmidt/Brink* in: *Koreng/Lachenmann,* Formularhandbuch Datenschutzrecht, Muster G.I.4, § 4 Abs. 2.

[262] EuGH vom 22.11.2012 – C-119/12, *Probst,* ECLI:EU:C:2012:748 Rn. 27 zu dem Begriff »auf Weisung« i.S.d. Art. 6 Abs. 5 der ePrivacy-RL, welcher Art. 16, 17 DSRL entspreche (Rn. 25).

[263] Art. 28 Abs. 10 DSGVO legt dies für eigenmächtiges, weisungswidriges Handeln explizit fest. Dies gilt aber genauso auch für eine im Auftragsverarbeitungsvertrag zugelassene Nutzung für eigene Zwecke.

[264] Vgl. die Auswertung von Auftragsverarbeitungsverträgen in: *BlnBDI*, Videokonferenzdienste, S. 16, 20–22, 25, 30 f.

[265] Cal. Civ. Code § 1798.140(j)(2),(ag)(2).

[266] *Conrad/Treeger in: Auer-Reinsdorff/Conrad*, Handbuch IT- und Datenschutzrecht, § 34 Rn. 316; *Martini* in: Paal/Pauly, DS-GVO Art. 28 Rn. 2; *Wächter*, Datenschutz im Unternehmen, Rn. 998.

[267] *Martini* in: Paal/Pauly, DS-GVO Art. 28 Rn. 2.

4. Dritte

Ein Dritter (»third party«) ist jede natürliche oder juristische Person, die weder das Unternehmen ist, mit dem die Verbraucher:innen im direkten Kontakt steht und das persönliche Informationen als Teil seiner Interaktion mit den Verbraucher:innen sammelt, noch als Dienstleister für dieses Unternehmen fungiert.[268]

Eine Person kann dabei zugleich Dritter und Unternehmen sein – auch hinsichtlich derselben Verarbeitung.[269] Dies ist der Fall, wenn das Unternehmen nicht im direkten Kontakt (»Intentionally interacts") mit den Verbraucher:innen steht oder persönliche Informationen außerhalb einer Interaktion mit diesen sammelt.[270] Direkter Kontakt ist z. B. das Aufrufen einer Webseite, das Kaufen einer Ware oder In-Anspruch-Nehmen einer Dienstleistung.[271] Ein bloßes Beobachten ohne aktives Handeln der jeweiligen Verbraucher:innen ist dagegen kein direkter Kontakt.[272] Insbesondere ist ein Unternehmen Dritter, wenn es Videoüberwachung betreibt. Dann steht es nämlich nicht im direktem Kontakt mit Verbraucher:innen – zumindest wenn diese nur zufällig vorbeigehen. Ein Datenhändler, der die Schwellenwerte für Unternehmen erreicht,[273] ist bezüglich der gehandelten persönlichen Informationen Unternehmen und zugleich Dritter. Er ist Unternehmen, weil er für diese Zwecke und Mittel der Verarbeitung festlegt. Zudem ist er Dritter, weil er nicht im direkten Kontakt mit den jeweiligen Verbraucher:innen steht.

Dritter im Sinne des Art. 4 Nr. 10 DSGVO kann hingegen nie zugleich der Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO sein. Vielmehr ist Dritter jede natürliche oder juristische Person außer dem Verantwortlichen, dem Auftragsverarbeiter oder der betroffenen Person. Insoweit ist die Terminologie der DSGVO klarer als diejenige des CCPA.

III. Räumlicher Anwendungsbereich

Der räumliche Anwendungsbereich des CCPA erfasst nur Sachverhalte, die einen gewissen Bezug zu Kalifornien haben. Auf der ersten Stufe muss der CCPA für alle Beteiligten persönlich anwendbar sein. Auf der zweiten Stufe ist die konkrete Verarbeitung ausgenommen, wenn jeder Teil der zusammenhängenden Geschäftstätigkeit außerhalb Kaliforniens stattfindet.[274] Dadurch ist der räumliche Anwendungsbereich des CCPA deutlich enger als derjenige der DSGVO.

Auf der ersten Stufe begrenzt der persönliche auch den räumlichen Anwendungsbereich. So ist der CCPA nur auf Personen mit Wohnsitz oder

---

[268] Cal. Civ. Code § 1798.140(ai).
[269] Dies setzt voraus: Cal. Civ. Code § 1798.100(b): »A business that, acting as a third party«.
[270] Cal. Civ. Code § 1798.140(ai)(1).
[271] Cal. Civ. Code § 1798.140(s).
[272] Cal. Civ. Code § 1798.140(s).
[273] Zu diesen siehe Kapitel 3:B.II.2.b) (ab S. 58).
[274] Cal. Civ. Code § 1798.145(a)(7).

gewöhnlichen Aufenthalt in Kalifornien als Verbraucher:innen anwendbar.[275] Zudem muss das Unternehmen in Kalifornien Geschäfte tätigen (»does business in California«).[276] Dieser Begriff ist nicht im CCPA näher erläutert. Er ist aber als ein Fachbegriff des kalifornischen Steuerrechts legaldefiniert und regelt dessen räumlichen Anwendungsbereich.[277] Im amerikanischen Recht gilt die Vermutung, dass der Gesetzgeber sich an der Legaldefinition eines anderen Gesetzes orientieren wollte, wenn er einen definierten Fachbegriff wortgleich übernimmt.[278] Daher ist davon auszugehen, dass auch in diesem Fall der Gesetzgeber sich an der allgemein bekannten Definition des Steuerrechts orientieren wollte.[279] Nach dieser muss die jeweilige natürliche oder juristische Person mit Gewinnerzielungsabsicht gezielt in Kalifornien kommerziell tätig werden.[280] Ein bloße Kapitalbeteiligung ist nicht ausreichend.[281] Zudem muss sie einen signifikanten Bezug zu Kalifornien haben.[282] Dafür muss sich in Kalifornien entweder die Hauptniederlassung[283] befinden oder das Unternehmen einen der drei indexierten Schwellenwerte für Umsatz, Sachvermögen oder Lohnsumme in Kalifornien erreichen.[284]

Für Dienstleister gibt es keine solche Einschränkung. Auch ein Anbieter ohne Bezug zu Kalifornien kann Dienstleister im Sinne des CCPA sein, wenn er für ein Unternehmen tätig ist.

Auf zweiter Stufe ist eine konkrete Verarbeitung ausgenommen, wenn jeder Teil der Geschäftstätigkeit vollständig außerhalb Kaliforniens stattfindet (»every aspect of that commercial conduct takes place wholly outside of California.«)[285]

---

[275] Siehe Kapitel 3:B.II.1 (ab S. 56).

[276] Cal. Civ. Code § 1798.140(d)(1) a. A.

[277] Cal. Rev. & Tax. Code § 23101.

[278] U. S. Supreme Court vom 24.06.1994, *Shannon v. United States*, 512 U. S. 573, 581.

[279] *Cohen/Hall/Woo*, JD Supra, Key Aspects of the CCPA; *Determann*, California Privacy Law, 2-26a:1.2d; *ders,* ZD 2018, 443, 444; *Illman/Temple*, 75 Business Lawyer 1637, 1637; *Stein/Lisy*, Privacy & Data Security Law News, Doing Business; *Marini u. a.*, Comparing privacy laws: GDPR v. CCPA, S. 9; wohl auch: *Cal. Attorney General*, Summary and Response to Comments Submitted During 45-Day Period, S. 2: »should be given meaning according […] other California law«; *Cosgrove*, The Privacy Advisor, Defining »business« under the law; *Pink*, California Consumer Privacy Act Annotated, § 2:4; a. A. o. Begr. *Levi/Healow*, California Consumer Privacy Act: A Compliance Guide, S. 4: »does business« sei das Gegenteil von »every aspect of that commercial conduct takes place wholly outside of California«.

[280] Cal. Rev. & Tax. Code § 23101(a).

[281] Cal. Supreme Court vom 22.01.1943, *Golden State Theatre & Realty Corp. v. Johnson*, 21 Cal. 2d 493, 495 f.; Cal. Court of Appeal 5th District vom 12.01.2017, *Swart Enterprises, Inc. v. Franchise Tax Bd.*, 7 Cal. App. 5th 497, 503.

[282] Cal. Rev. & Tax. Code § 23101(b).

[283] Cal. Rev. & Tax. Code § 23101(b)(1).

[284] Cal. Rev. & Tax. Code § 23101(b)(2),(c)(1). Zum Umsatzbegriff (»Sales«): Cal. Rev. & Tax. Code § 25120(f). Werte für 2020: Cal. Franchise Tax Board, Doing business in California threshold amounts updated for 2020, u. a. Umsatz von 610.395 $.

[285] Cal. Civ. Code § 1798.145(a)(7).

Dies ist der Fall, wenn weder das Unternehmen noch ein Dritter die persönlichen Informationen in Kalifornien sammelt und nicht innerhalb Kaliforniens mit ihnen handelt.[286] Sammeln ist dabei erst das Übermitteln an das Unternehmen oder einen Dienstleister; unerheblich ist, ob ein Gerät die personenbezogene Information innerhalb Kaliforniens zwischengespeichert hat.[287] Ein Beispiel ist eine Person auf einer Wanderung, die ohne Internetverbindung in Kalifornien ihre Wanderroute aufzeichnet, und diese erst nach Überschreiten der Grenze zu einem Nachbarstaat hochlädt.[288] Dann ist der CCPA auf die Speicherung in Kalifornien, nicht aber auf das Hochladen im Nachbarstaat anwendbar.

Der räumliche Anwendungsbereich der DSGVO ist durch das alternative Niederlassungs- und Marktortprinzip deutlich weiter.[289] So genügt, dass die Verarbeitung personenbezogener Daten entweder im Rahmen der Tätigkeit einer Niederlassung des Verantwortlichen in der EU erfolgt (Art. 3 Abs. 1 DSGVO). Alternativ reicht eine Verarbeitungstätigkeit aus, die im Zusammenhang damit steht, Personen in der EU Waren und Dienstleistungen anzubieten oder deren Verhalten zu beobachten (Art. 3 Abs. 2 DSGVO). Das Marktortprinzip soll Grundrechtsschutz im Internet sicherstellen.[290] Insoweit zeigt sich der grundrechtliche Hintergrund der DSGVO: durch den weiten Anwendungsbereich will der europäische Gesetzgeber unabhängig vom Sitz des Verantwortlichen die nebeneinander anwendbaren[291] Grundrechte auf Privatsphäre und Datenschutz nach Art. 7, 8 GRCh schützen.[292] Der europäische Gesetzgeber ist dabei nur durch das Völkerrecht begrenzt.[293]

Kalifornien darf demgegenüber verfassungsrechtlich den Handel zwischen den Bundesstaaten nicht mehr als nötig beeinträchtigen *(dormant Commerce Clause)*.[294] Dementsprechend genügt unter dem CCPA noch kein bloßes Ausrichten auf den kalifornischen Markt. Vielmehr muss das Unternehmen entweder eine Niederlassung in Kalifornien haben oder zumindest einen erheblichen Umsatz in Kalifornien erzielen. Auch schützt der CCPA nicht wie die DSGVO

---

[286] Cal. Civ. Code § 1798.145(a)(7). Zur Datenhandelsdefinition siehe Kapitel 3:C.I.2.a) (ab S. 82).

[287] Cal. Civ. Code § 1798.145(a)(7) a.E.

[288] *Californians for Consumer Privacy*, Annotated Text of the CPRA, § 1798.145(a)(7).

[289] Ähnlich *Botta*, PinG 2019, 261, 263: DSGVO sei etwas weiter.

[290] *Lewinski* in: Eßer/Kramer/Lewinski, DSGVO Art. 3 Rn. 11.

[291] Vgl. EuGH vom 16.07.2020, *Schrems II,* ECLI:EU:C:2020:559 Rn. 170: Datenverarbeitung »berühre« Art. 7 GRCh und »falle« außerdem unter Art. 8 GRCh. Ebenso: *Franzen*, ZfA 2019, 18, 22 f.; *Marsch*, Das europäische Datenschutzgrundrecht, S. 217–219; *Michl*, DuD 2017, 349, 352f; *Roßnagel*, NJW 2019, 1, 2. a.A. *Selmayr*, ZD 2018, 197, 197.

[292] *Däubler* in: Däubler et al., EU-DSGVO Art. 3 Rn. 16; *Piltz* in: Gola, DS-GVO Art. 3 Rn. 25; *Zerdick* in: Ehmann/Selmayr, DS-GVO Art. 3 Rn. 2.

[293] *Däubler* in: Däubler et al., EU-DSGVO Art. 3 Rn. 16; *Koloßa*, ZaöRV 2020, 791, 798–807 (ausführlich zu exterritorialer Anwendung im Völkerrecht); *Zerdick* in: Ehmann/Selmayr, DS-GVO Art. 3 Rn. 14.

[294] Siehe Kapitel 2:A.I.2.b) (ab S. 13).

jedermann, sondern nur Personen mit Wohnsitz oder gewöhnlichen Aufenthalt in Kalifornien. Durch seinen beschränkten räumlichen Anwendungsbereich regelt der CCPA mithin keine Sachverhalte außerhalb Kaliforniens und minimiert die Auswirkungen auf den Handel zwischen den Bundesstaaten. Daher ist der CCPA mit der *dormant Commerce Clause* vereinbar.[295]

In der Rechtspraxis dürfte der Unterschied jedoch begrenzt sein. Das Marktortprinzip ist nämlich dadurch praktisch begrenzt, dass die Aufsichtsbehörden die DSGVO nur schwer außerhalb der EU durchsetzen können.[296] Um dem abzuhelfen, müssen außereuropäische Verantwortliche zwar einen Vertreter in der EU bestellen (Art. 27 DSGVO). Wenn sie dies jedoch nicht tun, ist dies gemäß Art. 83 Abs. 4 lit. a DSGVO bußgeldbewehrt, aber faktisch regelmäßig nicht durchsetzbar.[297]

IV. Ausnahmen

1. Bereichsausnahmen

Der CCPA enthält mehrere Bereichsausnahmen. Dabei konkretisiert der CCPA den genauen Umfang dieser Ausnahmen nicht. Vielmehr ist als Positivliste aufgeführt, wofür Unternehmen persönliche Informationen verarbeiten dürfen, ohne dass dies dem CCPA widerspricht.

So darf ein Unternehmen persönliche Informationen verarbeiten, wenn es dazu aufgrund eines Gesetzes des Bundes, eines Bundesstaates oder einer Kommune verpflichtet ist.[298] Dies gilt insbesondere für die Herausgabe von Dokumenten im Zivilprozess *(discovery).*[299] Ebenso darf es gerichtlichen und behördlichen rechtsförmlichen Anordnungen nachkommen.[300] Ebenfalls ist eine Übermittlung an Strafverfolgungsbehörden des Bundes, der Bundesstaaten und der Kommunen zulässig, wenn objektiv der Verdacht einer Gesetzesverletzung besteht.[301]

---

[295] *Cal. Attorney General*, Summary and Response to Comments Submitted During 45-Day Period, S. 322; *Chander/Kaminski/McGeveran*, 105 Minn. L. Rev. 1733, 1794–1796; *Palmieri*, 11 Hastings Sci. & Tech 37, 49–53; *Spivak*, 88 U. Cin. L. Rev. 475, 493–514; *Ursul*, 52 Suffolk U. L. Rev. 577, 599; *Weber*, 2 Corp. & Bus. L. J. 188, 198–200; a. A. *Jeevanjee*, 70 Am. U. L. Rev. 75, 120–129.

[296] *Hornung* in: NK-DatenschutzR, DS-GVO Art. 27 Rn. 34.

[297] *Hornung* in: NK-DatenschutzR, DS-GVO Art. 27 Rn. 35; *Piltz* in: Gola, DS-GVO Art. 3 Rn. 27; a. A. *Däubler* in: Däubler et al., EU-DSGVO Art. 27 Rn. 13 f.: Versperren des Zugangs zum Binnenmarkt genauso wirksam wie Bußgeld (Dagegen: Versperren praktisch ebenso nicht durchsetzbar).
Die niederländische Autoriteit Persoonsgegevens hat ein Bußgeld wegen eines Verstoßes gegen Art. 27 DSGVO verhängt, wobei unklar ist, ob dieses vollstreckt wurde, vgl. *Autoriteit Persoonsgegevens* (Niederlande), Dutch DPA imposes fine of €525,000 on Locatefamily.com.

[298] Cal. Civ. Code § 1798.145(a)(1).

[299] U. S. District Court C. D. Cal. vom 28.09.2020, *Will Kaupelis v. Harbor Freight Tools USA, Inc.,* 2020 U. S. Dist. LEXIS 246379, 4–8.

[300] Cal. Civ. Code § 1798.145(a)(1),(2).

[301] Cal. Civ. Code § 1798.145(a)(3).

Solche Strafverfolgungsbehörden können nach dem CCPA auch das Unternehmen anweisen, persönliche Informationen für 90 Tage zu speichern, damit die jeweiligen Behörden einen Gerichtsbeschluss erwirken können.[302] Eine solche Speicherung kann – soweit erforderlich – um weitere 90 Tage verlängert werden.[303] Das Unternehmen muss die persönlichen Informationen nicht löschen, falls die Verbraucher:innen in dieser Zeit einen ansonsten berechtigten Löschantrag stellen; es darf sie aber auch nicht mehr für einen anderen Zweck nutzen.[304] Diese Ausnahme orientiert sich an der entsprechenden Regelung des Electronic Communications Privacy Act des Bundes.[305]

Zudem dürfen Unternehmen persönliche Informationen an eine Behörde bei Gefahr im Verzug mitteilen, wenn eine dringende Gefahr für Leben oder körperliche Unversehrtheit einer natürlichen Person besteht.[306] Dafür muss nach pflichtgemäßer Würdigung der Behörde das Auskunftsersuchen sonst rechtmäßig sein und das Abwarten einer gerichtlichen Entscheidung nicht möglich sein.[307] Eine solche Auskunftsanfrage müssen hochrangige (»high-ranking«) Beschäftigte der jeweiligen Behörde stellen.[308] Die Behörde muss sorgfältig prüfen, ob die Auskunftsanfrage ohne Gefahr rechtmäßig wäre.[309] Zudem muss die Behörde binnen drei Tagen einen entsprechenden Antrag bei dem zuständigen Gericht stellen und die persönlichen Informationen löschen, falls das Gericht den Antrag ablehnt.[310] Diese Schutzmaßnahmen sind amerikanischen Gesetzen zur Telekommunikationsüberwachung nachgebildet.[311] Die Übernahme der Schutzmaßnahmen im Rahmen der Ausarbeitung von Proposition 24 hatte eine Gruppe von Bürgerrechtsorganisationen vorgeschlagen.[312] Der Electronic Communications Privacy Act sieht ebenfalls die Entscheidung durch hochrangige Angestellte vor, die aber zuvor für solche Eilentscheidungen speziell ernannt sein müssen.[313] Die Behörde muss die materielle Rechtmäßigkeit ebenfalls sorgfältig prüfen.[314] Das Erfordernis, binnen drei Tagen eine gerichtliche Anordnung zu beantragen und bei Ablehnung die Daten zu löschen, stammt aus dem kalifornischen Äquivalent zum Electronic Communications Privacy Act.[315]

---

[302] Cal. Civ. Code § 1798.145(a)(2).
[303] Cal. Civ. Code § 1798.145(a)(2).
[304] Cal. Civ. Code § 1798.145(a)(2).
[305] 18 U.S.C. § 2703(f).
[306] Cal. Civ. Code § 1798.145(a)(4).
[307] Cal. Civ. Code § 1798.145(a)(4).
[308] Cal. Civ. Code § 1798.145(a)(4).
[309] Cal. Civ. Code § 1798.145(a)(4).
[310] Cal. Civ. Code § 1798.145(a)(4).
[311] 18 U.S.C. §§ 2510–2523.
[312] *American Civil Liberties Union of California et al.,* California Privacy Rights and Enforcement Act – Privacy Coalition Comments, S. 15.
[313] 18 U.S.C. § 2518(7) a.A.
[314] 18 U.S.C. § 2518(7)(b).
[315] Cal. Penal Code § 1546.1(h).

Schließlich ist eine für die Ausübung oder Verteidigung gegen Rechtsansprüche erforderliche Verarbeitung zulässig.[316] Dies gilt auch vorgerichtlich.[317]

Die DSGVO kennt solche allgemein formulierten Ausnahmen nicht. Vielmehr regelt sie punktuelle Einschränkungen bei bestimmten Pflichten oder Rechten. Insoweit ist die DSGVO genauer als der CCPA. So ist eine Verarbeitung gemäß Art. 6 Abs. 1 S. 1 lit. c DSGVO rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist. Auch besteht in diesem Fall gemäß Art. 17 Abs. 3 lit. b DSGVO kein Recht auf Löschung. Ähnlich zu der Ausnahme für eine Auskunftserteilung an Behörden bei Gefahr für Leib oder Leben ist gem. Art. 6 Abs. 1 S. 1 lit. d DSGVO eine Verarbeitung rechtmäßig, wenn sie erforderlich ist, um lebenswichtige Interessen einer natürlichen Person zu schützen. Bei personenbezogenen Daten, die für die Verteidigung oder Ausübung von Rechtsansprüchen erforderlich sind, besteht das Recht auf Löschung nicht (Art. 17 Abs. 3 lit. e DSGVO); der Verantwortliche darf zu diesem Zweck gemäß Art. 9 Abs. 2 lit. f DSGVO besondere Kategorien personenbezogener Daten verarbeiten. Zudem greift in der Regel bei der Verteidigung oder Ausübung von Rechtsansprüchen die Rechtsgrundlage der berechtigten Interessen des Art. 6 Abs. 1 S. 1 lit. f DSGVO.[318]

Die Auskunft an Behörden bei Gefahr im Verzug regelt allein der CCPA. Eine entsprechende Auskunft ist im europäischen Datenschutzrecht gemäß Art. 6 Abs. 1 S. 1 lit. c DSGVO rechtmäßig, wenn das nationale Recht eine Rechtspflicht enthält. In Deutschland bestehen solche Rechtspflichten im Strafprozessrecht und Polizeirecht.[319] Warum der CCPA an dieser Stelle sein eigentliches Rechtsgebiet Verbraucherschutz verlässt, ist unklar. Am wahrscheinlichsten ist, dass die ursprünglich sehr kurze, bloß klarstellende Ausnahme[320] in Verhandlungen mit Bürgerrechtsorganisationen[321] durch zusätzliche Sicherungen »aufgebläht« wurde.

2. Kollisionsregeln für andere Datenschutzgesetze

Bundesrecht bricht einzelstaatliches Recht (*Supremacy Clause*).[322] Der CCPA enthält dementsprechend für zahlreiche Bundesgesetze Kollisionsregeln. Viele

[316] Cal. Civ. Code § 1798.145(a)(6).

[317] *Friel et al.*, Data Counsel, CCPA Compliance Meets Trade Secret Protection.

[318] EuGH vom 04.05.2017, *Rīgas satiksme,* ECLI:EU:C:2017:336 Rn. 29; EuGH vom 17.06.2021 – C-597/19, M.I.C.M., ECLI:EU:C:2021:492 Rn. 108; *Buchner/Petri* in: Kühling/Buchner, DS-GVO Art. 6 Rn. 147. Vgl. die Beispiele in: *Artikel-29-Datenschutzgruppe*, WP 217 Berechtigtes Interesse, S. 77 f.

[319] Speziell für Telekommunikationsdaten: §§ 100j, 101a StPO, Art. 43 BayPAG. Vgl. dazu auch die JI-RL, die allerdings keine speziellen Pflichten bezüglich Gefahr im Verzug enthält.

[320] *Californians for Consumer Privacy*, The Consumer Right to Privacy Act of 2018, Sec. 4.8 § 1798.107(a)(3).

[321] Einen entsprechenden Vorschlag enthält: *American Civil Liberties Union of California et al.*, California Privacy Rights and Enforcement Act – Privacy Coalition Comments, S. 13 f.

[322] U. S. Const. Art. VI cl. 2.

Datenschutzgesetze des Bundes ermöglichen es den Bundesstaaten, zwar jeweils strengere Gesetze zu erlassen, wovon Kalifornien auch vielfach Gebrauch gemacht hat.[323] Auch strengere kalifornische Gesetze dürfen allerdings nicht den Datenschutzgesetzen des Bundes widersprechen.[324]

Die Kollisionsregeln sind für nahezu alle branchenspezifischen Gesetze gleich aufgebaut: die anderen Gesetze gehen bei der jeweiligen Branche vor, aber nur für die persönliche Informationen, die das branchenspezifische Gesetz erfasst. So geht beispielsweise der GLBA für die Finanzbranche[325] dem CCPA vor, soweit er auf die jeweilige Verarbeitung anwendbar ist.[326] Dieser erfasst nur nichtöffentliche persönliche Informationen, welche die Finanzinstitution über einen Privatkunden im Zusammenhang mit einer Finanzdienstleistung erhoben hat.[327] Privatkunden sind dabei solche, die Geschäfte für persönliche, familiäre oder haushaltsbezogene Zwecke abschließen.[328] Freiberuflich oder gewerblich Tätige sowie Beschäftigte von Kundengesellschaften sind dagegen nicht geschützt.[329] Daher ist der CCPA auf alle sonstigen Aktivitäten eines Finanzinstituts anwendbar und füllt so die Lücken des branchenspezifischen Ansatzes. So erfasst der CCPA unter anderem die Angestellten des Finanzinstituts, freiberuflich tätige Kund:innen und Beschäftigte von Kundengesellschaften.[330]

Kollisionsregeln mit dem gleichen Mechanismus gelten für den HIPAA,[331] den Confidentiality of Medical Information Act,[332] die Federal Policy for the Protection of Human Subjects,[333] den Fair Credit Reporting Act,[334] den California Financial Information Privacy Act,[335] den Federal Farm Credit Act[336] und den Driver's Privacy Protection Act.[337]

Bei einem Teil der Gesetze können Verbraucher:innen auch den Schadensersatz nach einer Datenpanne des CCPA verlangen. Dies betrifft den GLBA, den FCRA, den California Financial Information Privacy Act, den Federal Farm

---

[323] Siehe Kapitel 2:B.II (ab S. 27).

[324] Siehe Kapitel 2:B.II (ab S. 27).

[325] Siehe Kapitel 2:B.I.2 (ab S. 19).

[326] Cal. Civ. Code § 1798.145(e).

[327] 15 U.S.C. § 6809(4),(9).

[328] 15 U.S.C. § 6809(9).

[329] 12 C.F.R. § 1016.1(b)(1).

[330] *Olsen/Davis*, Banking & Financial Services Policy Report, November 2019, 1, 2.

[331] Cal. Civ. Code § 1798.145(c)(1)(A),(B). HIPAA, 42 U.S.C. § 1320d–1320d-9, 45 C.F.R. §§ 160, 162, 164. Zu diesem siehe Kapitel 2:B.I.2 (ab S. 19).

[332] Cal. Civ. Code § 1798.145(c)(1)(A),(B). Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56–56.37.

[333] Cal. Civ. Code § 1798.145(c)(1)(C). Federal Policy for the Protection of Human Subjects, 45 C.F.R. §§ 46.101–124.

[334] Cal. Civ. Code § 1798.145(d). FCRA, 15 U.S.C. §§ 1681–1681u.

[335] Cal. Civ. Code § 1798.145(e). California Financial Information Privacy Act, Cal. Fin. Code § 4050–4060.

[336] Cal. Civ. Code § 1798.145(e). Farm Credit Act, 12 C.F.R. § 618.8300–8330.

[337] Cal. Civ. Code § 1798.145(f). Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721.

Credit Act und den Driver's Privacy Protection Act.[338] Warum diese Rückausnahme nur bei einem Teil der vorrangigen Gesetze gilt, ist unklar und wohl ein Redaktionsfehler.

Die bisher genannten kalifornischen Gesetze sind branchenspezifische Gesetze, die das Äquivalent zu einem jeweiligen Bundesgesetz darstellen. Insoweit will der CCPA nicht in den abgeschlossenen, branchenspezifischen Regelungskomplex eingreifen.

Bei dem kalifornischen Insurance Code weicht er von dem üblichen Kollisionsmechanismus ab, weil zu diesem kein Äquivalent auf Bundesebene besteht.[339] Die California Privacy Protection Agency soll ermitteln, inwieweit der Insurance Code persönliche Informationen schützt und ob dieser Schutz jeweils höher oder niedriger ist.[340] In der Durchführungsverordnung soll sie dann nur die Vorschriften des CCPA für anwendbar erklären, die Verbraucher:innen stärker schützen als der Insurance Code.[341]

Für nicht genannte Gesetze bestehen zwei allgemeine Kollisionsregeln. Der CCPA ist nicht anwendbar, soweit ihn ein vorrangiges Bundesgesetz verdrängt.[342] Er soll möglichst im Einklang mit kalifornischen Datenschutzgesetzen ausgelegt werden; wenn dies nicht möglich ist, gilt das Datenschutzgesetz, das den höheren Schutz bietet.[343]

Die Öffnungsklauseln der DSGVO sind weniger weitreichend als die Kollisionsregeln des CCPA. Sie erlauben den Mitgliedstaaten kein Sonderrecht zu schaffen, sondern nur das europäische Datenschutzrecht zu spezifizieren (Erwägungsgrund 10 S. 5 der DSGVO) und dieses an ihr nationales Recht anzupassen. Teilweise gestatten sie nur die punktuelle Abweichung von einzelnen Rechten und Pflichten. Daher gilt für die jeweiligen Verantwortlichen und die jeweiligen personenbezogenen Daten weiterhin die sonstige DSGVO. Teilweise geben sie dem nationalen Gesetzgeber konkret vor, wie er die Öffnungsklausel ausfüllen soll.[344] So können die Mitgliedstaaten beispielsweise das Mindestalter für eine Einwilligung selbst bestimmen, allerdings nur in dem Bereich von 13 bis 16 Jahren (Art. 8 Abs. 1 S. 2, 3 DSGVO). Andere Öffnungsklauseln sind eher mit den Kollisionsregeln des CCPA vergleichbar, da sie den Mitgliedstaaten ermöglichen, ihr nationales Recht mit der DSGVO zu harmonisieren. Der nationale Gesetzgeber kann z. B. nach Art. 23 DSGVO von den Betroffenrechten der DSGVO für bestimmte Ziele abweichen, ist aber an detaillierte Mindestinhalte

---

[338] Cal. Civ. Code § 1798.145(d)(3),(e),(f).

[339] Cal. Civ. Code § 1798.185(a)(21). Datenschutzspezifische Teile des Insurance Codes: Cal. Ins. Code §§ 791–791.29; 10 C. C. R. § 2689.1–2689.24.

[340] Cal. Civ. Code § 1798.185(a)(21).

[341] Cal. Civ. Code § 1798.185(a)(21). Der bisherige Entwurf der Durchführungsverordnung schweigt hierzu: Cal. Privacy Protection Agency, Proposed Regulations.

[342] Cal. Civ. Code § 1798.196. Proposition 24 (Cal. 2020), Sec. 30 (nicht kodifiziert) wiederholt dies für den COPPA.

[343] Cal. Civ. Code § 1798.175.

[344] *Hornung/Spiecker gen. Döhmann* in: NK-DatenschutzR, Einl. Rn. 227.

gebunden (Art. 23 Abs. 2 DSGVO).[345] Die Mitgliedstaaten können daher die DSGVO im Rahmen der Öffnungsklauseln spezifizieren, aber nur in geringem Maß von ihr abweichen (abgesehen Öffnungsklauseln für bestimmte Bereiche in den Art. 85–91 DSGVO).[346]

Die Kollisionsregeln des CCPA erfüllen demgegenüber einen anderen Zweck. Der CCPA steht in der Normenhierarchie unter den Gesetzen des Bundes. Er muss daher einen Konflikt mit dem Bundesrecht vermeiden, um nicht als unwirksam verworfen zu werden. Dementsprechend nimmt er sich stärker als die DSGVO zurück.

V. Ergebnis

Der Begriff der persönlichen Informationen (»personal information«)[347] des CCPA ähnelt stark den personenbezogenen Daten des Art. 4 Nr. 1 DSGVO. Der Personenbezug ist ebenso wie unter der DSGVO weit auszulegen. Die Ausnahme für aggregierte und deidentifizierte Informationen[348] entspricht den anonymen Daten der DSGVO. Dabei sind aggregierte Informationen Daten über eine Gruppe, ohne dass sich Gruppenmitglieder identifizieren lassen.[349] Deidentifizierte Informationen beziehen sich dagegen auf bestimmte Verbraucher:innen, welche aber durch Entfernung aller Identifizierungsmerkmale praktisch nicht mehr identifizierbar sind.[350] Anders als die DSGVO bei anonymen Daten schützt der CCPA bei deidentifizierten Informationen die Verbraucher:innen vor vorhandenen Restrisiken der Reidentifizierung. Das Unternehmen muss insbesondere vertraglich zur Vertraulichkeit verpflichten, wer solche deidentifizierten Informationen erhält.[351] Ein sehr deutlicher Unterschied zu den personenbezogenen Daten der DSGVO ist die Ausnahme für öffentliche Informationen. Öffentlich frei verfügbare oder noch nicht veröffentliche Informationen, die aber von öffentlichem Interesse sind, stellen keine persönlichen Informationen dar.[352] Dies spiegelt den starken Schutz des öffentlichen Diskurs durch das *First Amendment* und die Dichotomie zwischen privat und öffentlich im amerikanischen Recht. Eine solche klare Trennung zwischen privat und öffentlich kennt das europäische Datenschutzrecht nicht. Es gibt

[345] Wobei nach dem Wortlaut unklar ist, ob diese zwingend oder nur im Regelfall erfüllt werden müssen, vgl. *Koreng* in: Taeger/Gabel, DS-GVO Art. 23 Rn. 57 f.

[346] *Hornung/Spiecker gen. Döhmann* in: NK-DatenschutzR, Einl. Rn. 227; *Monreal,* ZD 2022, 359, 362 f.; *Selmayr/Ehmann* in: Ehmann/Selmayr, DS-GVO Einl. Rn. 82–90; a. A. *Kühling/Martini,* EuZW 2016, 448, 449: Fragmentarischer Charakter durch Öffnungsklauseln; *Pohl*, PinG 2017, 85, 85; offenlassend: Generalanwalt *de la Tour,* Schlussanträge vom 02.12.2021 – C-319/20, *Facebook Ireland*, ECLI:EU:C:2021:979 Rn. 55.

[347] Cal. Civ. Code § 1798.140(v).

[348] Cal. Civ. Code § 1798.140(v)(3).

[349] Cal. Civ. Code § 1798.140(b).

[350] Cal. Civ. Code § 1798.140(m).

[351] Cal. Civ. Code § 1798.140(m)(3).

[352] Cal. Civ. Code § 1798.140(v)(2).

zwar punktuelle Lockerungen für öffentliche Informationen, diese kommen aber nicht der pauschalen Ausnahme des CCPA nahe.

Die betroffene Person nennt der CCPA Verbraucher:in (»consumer«).[353] Trotz dieses an Verbraucherschutzgesetze erinnernden Begriffs sind alle natürlichen Personen mit Wohnsitz oder gewöhnlichem Aufenthalt in Kalifornien erfasst, auch wenn sie zu gewerblichen oder beruflichen Zwecken handeln. Diesen steht das Unternehmen (»business«)[354] gegenüber, welches als primärer Adressat der Pflichten des CCPA das Gegenstück zum Verantwortlichen des Art. 4 Nr. 7 DSGVO bildet. Anders als unter der DSGVO sind nur in Kalifornien tätige Unternehmen ab Erreichen eines gewissen Schwellenwerts erfasst. Der wichtigste Schwellenwert ist ein weltweiter Jahresumsatz von 25 Millionen Dollar.[355] So trifft der CCPA eine weitgehend sachgerechte Beschränkung auf diejenigen Organisationen, deren umfangreiche Datenverarbeitung ein besonderes Risiko birgt. Vergleichbar mit dem Auftragsverarbeiter des Art. 4 Nr. 8, 28 DSGVO kennt der CCPA auch die Rolle eines Dienstleisters (»contractor«[356] und »service provider«[357]). Dienstleister ist, wer persönliche Informationen im Auftrag des Unternehmens verarbeitet (»service provider«) oder wer nur Zugriff auf diese hat (»contractor«). Beide Unterrollen des Dienstleisters treffen nahezu identische Pflichten. Sie müssen mit dem Unternehmen einen Dienstleistervertrag abschließen[358] und Datensicherheit gewährleisten.[359] Primär ist weiter das Unternehmen verantwortlich. Wer weder als Verbraucher:in, als Unternehmen mit direktem Kontakt mit Verbraucher:innen noch als Dienstleister hinsichtlich einer Verarbeitung persönlicher Informationen handelt, ist Dritter (»third party«).[360] Unternehmen, die nicht im direkten Kontakt zu Verbraucher:innen stehen, sind gleichzeitig Unternehmen und Dritte (z. B. bei Videoüberwachung).

Der räumliche Anwendungsbereich leitet sich teilweise aus diesen Rollen ab. So sind nur in Kalifornien geschäftlich tätige Personen Unternehmen[361] und nur natürliche Personen mit Wohnsitz in Kalifornien Verbraucher:innen.[362] Darüber hinaus ist eine Verarbeitung ausgenommen, wenn jeder Teil der diesbezüglichen Geschäftstätigkeit vollständig außerhalb Kaliforniens stattfindet.[363] Damit ist der räumliche Anwendungsbereich deutlich enger als derjenige des Art. 3 DSGVO.

Daneben kennt der CCPA Bereichsausnahmen und Kollisionsregeln für Bundesgesetze. So sind Verarbeitungen aufgrund einer Rechtspflicht, einer gerichtlichen

---

[353] Cal. Civ. Code § 1798.140(i).
[354] Cal. Civ. Code § 1798.140(d).
[355] Cal. Civ. Code § 1798.140(d)(1)(A).
[356] Cal. Civ. Code § 1798.140(j).
[357] Cal. Civ. Code § 1798.140(ag).
[358] Cal. Civ. Code § 1798.140(j)(1),(ag)(1).
[359] Cal. Civ. Code § 1798.130(a)(3)(A).
[360] Cal. Civ. Code § 1798.140(ai).
[361] Cal. Civ. Code § 1798.140(d)(1)(A).
[362] Cal. Civ. Code § 1798.140(i).
[363] Cal. Civ. Code § 1798.145(a)(7).

oder behördlichen Anordnung sowie zur Verteidigung und Ausübung von Rechtsansprüchen ausdrücklich zulässig.[364] Die Kollisionsregeln für Bundesgesetze funktionieren nach einem einheitlichen Schema: Das Bundesgesetz muss sowohl persönlich anwendbar sein als auch die jeweiligen persönlichen Informationen schützen. Dann ist für diese persönlichen Informationen der CCPA unanwendbar, aber für andere persönliche Informationen des jeweiligen Unternehmens anwendbar. Solche Kollisionsregeln greifen für alle Datenschutzgesetze des Bundes und sie begleitende Gesetze Kaliforniens.[365]

C. Verbraucherrechte

I. Widerspruchsrecht gegen Datenhandel

1. Ratio legis

Das Kernrecht des CCPA ist das Widerspruchsrecht gegen Datenhandel (»right to opt-out of sale and sharing«).[366] Ziel ist, die Privatautonomie zu stärken und eine informierte Entscheidung für oder gegen einen Handel mit den eigenen persönlichen Informationen[367] zu ermöglichen. Der CCPA will dabei Verbraucher:innen[368] die Kontrolle über ihre persönlichen Informationen geben, sie aber nicht paternalistisch einschränken.

Diese detaillierte Regelung greift nur bei einem Widerspruch. Dieser Widerspruch ist keine individuelle Einzelfallentscheidung. Vielmehr sollen in der Idealvorstellung des CCPA alle Verbraucher:innen ihren Widerspruch bedenkenlos pauschal erklären können. Die Ausübung dieses Rechts ist nach der gesetzgeberischen Konzeption der Standardfall, die Nicht-Ausübung die Ausnahme. Ungerechtfertigte Nachteile durch diesen pauschalen Widerspruch für Unternehmen[369] fängt der CCPA durch ausgewogene Ausnahmen auf.

Solche pauschalen Widerspruchsrechte sind nicht untypisch für das amerikanische Recht. So regelt der Do-Not-Call Implementation Act einen Widerspruch-Mechanismus für Werbeanrufe.[370] Er ist eine Erfolgsgeschichte. Es sind inzwischen circa 244 Millionen Telefonnummern in dem durch die FTC zentral geführten National Do-Not-Call Registry eingetragen.[371] Werbende dürfen

[364] Cal. Civ. Code § 1798.145(a)(1)–(5).

[365] Cal. Civ. Code § 1798.145(c)–(f).

[366] Cal. Civ. Code § 1798.120.

[367] Zum Begriff siehe Kapitel 3:B.I.1.a) (ab S. 43).

[368] Zum Begriff siehe Kapitel 3:B.II.1 (ab S. 56).

[369] Zum Begriff siehe Kapitel 3:B.II.2 (ab S. 56).

[370] 15 U.S.C. § 6151–6156. Umgesetzt durch die darauf beruhende Telemarketing Sales Rule: 16 C.F.R. § 310.1–9.

[371] *FTC,* Do Not Call: Data Book 2021, S. 5. Wie vielen Personen dies entspricht, ist unklar, da viele Personen sowohl über Mobiltelefone als auch über Festnetztelefone verfügen. Ein Eintrag von Mobiltelefonnummern ist zwar möglich, dürfte aber seltener vorkommen,

die eingetragenen Telefonnummern ohne ausdrückliche Einwilligung nicht anrufen.[372] Weiterhin enthalten die branchenspezifischen Datenschutzgesetze GLBA,[373] FCRA[374] und HIPAA[375] begrenzte *opt-out*-Rechte. Vor allem aber basiert das einflussreiche *notice-and-choice*-Modells der FTC zu weiten Teilen auf einem *opt-out*-Mechanismus.[376]

Ein Verbot mit Einwilligungsvorbehalt *(opt-in)* hat der Gesetzgeber des CCPA erwogen und nur wegen der überragenden Bedeutung der Meinungsfreiheit im amerikanischen Recht verworfen. In *Sorell vs. IMS Health* (2011) hatte der U. S. Supreme Court ein Datenschutzgesetz Vermonts für ungültig erklärt, weil sein *opt-in*-Mechanismus zu stark in die Meinungsfreiheit eingreife.[377] Auch sonst hat der U. S. Supreme Court wiederholt *ipso iure* geltende Verbote verworfen, weil ein *opt-out*-Mechanismus ein milderes Mittel sei. So sei z. B. ein zuerst zu ergreifendes Mittel, religiöse Gemeinschaften zur Beachtung von »No Solicitation«-Schilder zu verpflichten, statt Missionierung an Haustüren generell zu verbieten.[378] Aufgrund dieser Rechtsprechung haben die Initiatoren des ursprünglichen Volksbegehrens von dem anfangs geplanten *opt-in*-Mechanismus zu einem Widerspruchsrecht gewechselt.[379]

2. Regelung

a) Reichweite

Das Widerspruchsrecht gegen Datenhandel ist sehr knapp formuliert:

»A consumer shall have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share that consumer's personal information.«[380]

---

weil Werbetreibende Mobiltelefone ohnehin nur sehr eingeschränkt anrufen dürfen, vgl. 47 C. F. R. § 64.1200(a)(ii). Die FTC löscht regelmäßig nicht mehr vergebene Telefonnummern, 15 U. S. C. § 6155(b).

[372] 16 C. F. R. 310.4(b)(1)(iii)(B).

[373] 15 U. S. C. § 6802(b). Zum GLBA siehe Kapitel 2:B.I.2 (ab S. 19).

[374] 15 U. S. C. § 1681s–3(a)(2)(A).

[375] 45 C. F. R. § 164.510(a)(2). Der HIPAA kennt allerdings auch einen weitreichenden *opt-in*-Mechanismus, siehe Kapitel 2:B.I.2 (ab S. 19).

[376] Siehe Kapitel 2:B.I.3 (ab S. 24).

[377] Siehe Kapitel 2:A.I.2.a) (ab S. 10).

[378] U. S. Supreme Court vom 17.06.2002, *Watchtower Bible & Tract Soc'y of N. Y., Inc. v. Vill. of Stratton*, 536 U. S. 150, 168 f. Ähnlich: U. S. Supreme Court vom 03.05.1943, *Martin v. Struthers*, 319 U. S. 141, 147 f.; vom 20.10.1980, *Vill. of Schaumburg v. Citizens for a Better Env't*, 444 U. S. 620, 637–639. Speziell zum Do-Not-Call Implementation Act: U. S. Court of Appeals 10th Circuit vom 17.02.2004, *Mainstream Mktg. Servs. v. FTC*, 358 F.3d 1228, 1236–1245.

[379] *Angwin*, The Markup, Tech on the Ballot: Interview with Ashkan Soltani; *Solove/Antonipillai*, Talk with Alastair Mactaggart, 14m:10s. Ein späterer (gescheiterter) Gesetzesentwurf sah ebenfalls einen Einwilligungsmechanismus vor: A. B. 1760, 2018–2019 Leg., Reg. Sess. (Cal. 2019), Sec. 7.

[380] Cal. Civ. Code § 1798.120(a).

Für die Reichweite dieses Widerspruchsrechts ist die Legaldefinition der beiden Schlüsselbegriffe *sell* und *share* (zusammenfassend: Datenhandel) sowie deren jeweilige Ausnahmen entscheidend.[381] Der Grundgedanke ist: kommerzielle Verwertung persönlicher Informationen als Wirtschaftsgut ist Datenhandel, bloß operative Übermittlungen an Dritte jedoch nicht.

Die erste Alternative *selling* setzt sich aus zwei Elementen zusammen. Erstens muss das Unternehmen persönliche Informationen an einen Dritten übermitteln, wobei auch ein bloßes Zugänglichmachen genügt.[382] Dritter ist eine juristische oder natürliche Person, die weder das Unternehmen noch ein Dienstleister für dieses Unternehmen ist.[383] Dienstleister sind insbesondere Anbieter für Kundendienst, Zahlungsverkehr, Qualitätskontrolle, Marktforschung oder solche, die nur zufällig und vorübergehend mit persönlichen Informationen in Kontakt kommen.[384] Daher ist eine nebensächliche operative Übertragung persönlicher Informationen kein Datenhandel.

Zweitens muss das Unternehmen die persönlichen Informationen im Rahmen eines gewissen Austauschverhältnisses übermitteln (»for monetary or other valuable consideration«).[385] Der CCPA greift mit *consideration* auf ein komplexes Rechtsinstitut des *common law* zurück, das am ehesten mit einer weit verstandenen Gegenleistung zu vergleichen ist. Ein Vertrag ist nur wirksam, wenn er *consideration* enthält.[386] Der Rechtsgedanke ist, dass sich nicht vertraglich binden will, wer nicht auch etwas aufgibt.[387] Das kalifornische Zivilrecht definiert *consideration* als: »Any benefit conferred […] or any prejudice suffered […] as an inducement to the promisor«.[388] Dies bedeutet, dass die Vertragsparteien den Austausch von Vor- oder Nachteil ausgehandelt haben müssen *(bargained-for exchange)*.[389] *Consideration* ist deutlich weitreichender als das deutsche Konzept des Synallagmas.[390] Ausreichend ist ein indirekter[391] oder minimaler[392] wirtschaftlicher Vorteil. Bei einer Geheimhaltungsvereinbarung ist z. B. das Bereitstellen der Informationen die *consideration* für die Geheimhaltung.[393]

---

[381] Cal. Civ. Code § 1798.140(ad),(ah).

[382] Cal. Civ. Code § 1798.140(ad)(1).

[383] Siehe Kapitel 3:B.II.4 (ab S. 71).

[384] Cal. Civ. Code § 1798.140(e)(4),(5) i. V. m. Cal. Civ. Code § 1798.140(j)(1),(ag)(1).

[385] *De la Torre,* Golden Data, What is a 'sale' under CCPA?; *de la Torre/Rupp*, The Privacy Advisor, What does "valuable consideration" mean under the CCPA?; *Scott/Canter/Tonsager*, The Privacy Advisor, Sale under CCPA.

[386] Cal. Civ. Code § 1550.

[387] *Benedict*, RabelsZ 69 (2005), 1, 18–20; *Peel*, The Law of contract Rn. 3–002.

[388] Cal. Civ. Code § 1605.

[389] Cal. Supreme Court vom 18.03.2010, *Steiner v. Thexton*, 48 Cal. 4th 411, 420.

[390] *Kischel*, Rechtsvergleichung, S. 341.

[391] Cal. Supreme Court vom 24.02.2014, *Ennabe v. Manosa*, 58 Cal. 4th 697, 720–722.

[392] Cal. Supreme Court vom 29.12.1988, *Foley v. Interactive Data Corp*., 47 Cal. 3d 654, 679; *Peel*, The Law of contract Rn. 3–014.

[393] Cal. Superior Court Los Angeles vom 21.11.1977, *Cybertek Computer Products,*

Wie sich das auf den CCPA übertragen lässt, ist noch nicht endgültig geklärt.[394] Jedenfalls genügt die Übermittlung als zwangsläufige Nebenfolge eines Vertrags nicht.[395] So ist der Verkauf und die Abtretung eines Forderungsportfolios nahezu immer verbunden mit der Übermittlung persönlicher Informationen über die jeweiligen Schuldner:innen; diese Übermittlung steht aber nicht in einem auch weit verstandenen Austauschverhältnis mit dem Preis für das Forderungsportfolio.[396] Anders ist dies zu beurteilen, wenn der Käufer das Forderungsportfolio gerade auch kauft, um die Kontaktdaten der Schuldner für seine Werbung oder Marktforschung zu erhalten. Dann ist der Kaufpreis *consideration* für die persönlichen Informationen.

Die Werbebranche hat unter dem CCPA-2018 aus dem Element »for consideration« teilweise geschlossen, dass personalisierte Werbung nicht erfasst sei, da der Preis für das Schalten von Werbung und nicht das Übermitteln persönlicher Informationen gewährt werde.[397] Es ist zweifelhaft, ob dies wirklich überzeugend war,[398] zumal das kalifornische Parlament eine entsprechende Einschränkung der *selling*-Definition verworfen hatte.[399]

Um dieser Ansicht die Basis zu entziehen, hat Proposition 24 für personalisierte Werbung den zusätzlichen Begriff *sharing* eingeführt, an den die gleichen Rechtsfolgen wie *selling* geknüpft sind. Dieser bezeichnet – entgegen des allgemein üblichen Wortsinnes – ausschließlich die Übermittlung für »cross-context behavioral advertising, whether or not for monetary or other valuable consideration«.[400] Ansonsten entspricht die Definition derjenigen des *selling* und führt zu

---

Inc. v. Whitfield, 1977 Cal. App. LEXIS 2140, 7–9; U. S. District Court W. D. Tex. vom 01.04.2009, *Birk v. Hub Int'l Southwest Agency, Ltd.*, 2009 U. S. Dist. LEXIS 50221, 68.

[394] *de la Torre,* Golden Data, What is a 'sale' under CCPA?; *de la Torre/Rupp*, The Privacy Advisor, Valuable consideration; *Duball*, The Privacy Advisor, Are companies using semantics to get around CCPA's »sale« provision?; *Pimentel/Mooney/Zhang*, A Sale, or Not a Sale?; *Scott/Canter/Tonsager*, The Privacy Advisor, Sale under CCPA.

[395] *de la Torre,* Golden Data, What is a 'sale' under CCPA?; *Scott/Canter/Tonsager*, Sale under CCPA; dies offenlassend: *de la Torre/Rupp*, The Privacy Advisor, Valuable consideration.

[396] *de la Torre,* Golden Data, What is a 'sale' under CCPA?

[397] *Network Advertising Initiative,* Classification of Ad-tech Data Flows as *"Sales"* Under the CCPA, S. 6–8. Vgl. *Interactive Advertising Bureau,* IAB CCPA Benchmark Survey: Summary, S. 7: 2/3 der befragten Werbeunternehmen gehen davon aus, dass ihre Werbung *selling* ist; *Mahoney/Fahs/Marti*, The State of Authorized Agent Opt-Outs, S. 17–21: Datenschutzerklärungen von Unternehmen, die angeblich nicht mit persönlichen Informationen handeln.

[398] Personalisierte Werbung als *selling* einordnend: *de la Torre,* Golden Data, The gathering storm; *de la Torre/Rupp*, The Privacy Advisor, Valuable consideration; *Determann,* ZD 2018, 443, 445; *Hoofnagle*, 10 questions about the CCPA; *ders.*, Comments on the CCPA; *Mahoney*, Privacy Perspectives, CPRA promises short-term consumer benefits, long-term uncertainty; *Mahoney/Fahs/Marti*, The State of Authorized Agent Opt Outs, S. 16 f.; wohl auch *Urgoiti*, 53 U.C. Davis L. Rev. 1689, 1691.

[399] S.B. 753, 2019–20 Leg., Reg. Sess. (Cal. 2019), version 04/04/2019, Sec. 1 § 1798.140(t)(E). Dieser Gesetzesentwurf wurde nicht verabschiedet.

[400] Cal. Civ. Code § 1798.140(ah)(1).

den gleichen Rechtsfolgen.[401] »Cross-context behavioral advertising« ist dabei zielgerichtete Werbung, die auf persönlichen Informationen beruht, welche aus anderen Quellen stammt als der aktuellen Interaktion der Verbraucher:innen mit dem jeweiligen Unternehmen, der Webseite oder der Dienstleistung.[402] Der Begriff *sharing* geht auf einen Kompromissvorschlag der Werbebranche in den Proposition 24 vorangehenden Verhandlungen zurück, welche zumindest die negativen Konnotationen des Begriffs *selling* vermeiden wollte.[403] Die Gesetzesänderung ist nur klarstellend, da solche Übermittlungen wohl bereits unter *selling* fielen.[404] Daher werden *selling* und *sharing* nachfolgend als »Datenhandel« zusammengefasst.

Ein Umgehungsverbot fingiert Datenhandel, wenn Unternehmen die Datenhandelsdefinition durch anderweitige Gestaltungen umgehen.[405] So handelt es sich auch um einen Datenhandel, wenn das Unternehmen einen bloßen »Strohmann« zwischenschaltet, um die Datenhandelsdefinition zu umgehen.[406] Auch liegt bei einem Aneinanderreihen von Verträgen, die teilweise keine *consideration* enthalten, insgesamt weiterhin ein Datenhandel vor.[407]

Es bestehen fünf Ausnahmen von der Datenhandelsdefinition. Die ersten drei Ausnahmen sind allgemeiner Natur, die zwei weiteren Ausnahmen branchenspezifisch. Erstens sind kein Datenhandel Übermittlungen an Dritte, welche die Verbraucher:innen bewusst und aktiv auslösen[408] (z. B. durch das Senden einer E-Mail an Dritte). Zweitens darf ein Unternehmen ein Identifikationsmerkmal über Datenhandel widersprechende Verbraucher:innen an Dritte übermitteln, um sicherzustellen, dass dieser Widerspruch auch umgesetzt wird.[409] Drittens ist eine Übermittlung persönlicher Informationen kein Datenhandel, wenn sie Teil einer Unternehmensfusion, eines Unternehmenskaufes (*asset deal*),[410] einer insolvenzrechtlichen Abwicklung oder anderen Unternehmenstransaktionen ist.[411] Dies entbindet das Unternehmen aber nicht von der Zweckbindung: die neuen Eigentümer:innen müssen Verbraucher:innen informieren, wenn sie persönliche Informationen auf eine wesentlich andere Weise nutzen.[412] *Ratio legis* ist, dass

---

[401] Cal. Civ. Code § 1798.120(a).

[402] Cal. Civ. Code § 1798.140(k).

[403] Vorschlagen von *Domenique Shelton Leipzig: Biderman/Shelton Leipzig,* Decrypted Unscripted Episode 38, 27m:23s.

[404] *Determann,* ZD 2021, 69, 71; a. A. (o. Begr.) *Schröder*, DSB 2021, 15, 16.

[405] Cal. Civ. Code § 1798.190.

[406] Cal. Civ. Code § 1798.190(a).

[407] Cal. Civ. Code § 1798.190(b).

[408] Cal. Civ. Code § 1798.140(ad)(2)(A),(ah)(2)(A).

[409] Cal. Civ. Code § 1798.140(ad)(2)(B),(ah)(2)(B).

[410] Der share deal ist ebenfalls kein Datenhandel, da das Unternehmen keine persönlichen Informationen an Dritte übermittelt, sondern nur Anteile an dem Unternehmen übergehen.

[411] Cal. Civ. Code § 1798.140(ad)(2)(C),(ah)(2)(C).

[412] Cal. Civ. Code § 1798.140(ad)(2)(C),(ah)(2)(C). Zur Zweckbindung siehe Kapitel 3:D. II (ab S. 166).

sich in solch komplexen Transaktionen ohnehin nur schwer feststellen lässt, ob die persönlichen Informationen für *consideration* übertragen werden oder sie nur zwangsläufige Nebenfolge ist.[413]

Viertens sind das Übermitteln von Identifikationsmerkmalen über ein KfZ oder Wasserfahrzeug oder dessen Eigentümer:innen von einer Werkstatt an einen Hersteller kein Datenhandel, wenn die Werkstatt mit diesen persönlichen Informationen ausschließlich eine Garantie oder einen Produktrückruf abwickelt.[414] Auch diese Ausnahme dient dazu, die schwierige Abgrenzung zu vereinfachen, wann persönliche Informationen für *consideration* übertragen werden, und ist nur klarstellend.[415] Fünftens besteht kein Widerspruchsrecht, wenn die jeweiligen Verbraucher:innen in eine Nutzung ihrer persönlichen Informationen in einem realen Produkt freiwillig und spezifisch eingewilligt haben und die Rückabwicklung erhebliche Kosten mit sich bringen würde.[416] Regelbeispiel ist ein Foto in einem Schuljahrbuch, welches das Unternehmen bei einem Widerspruch neu drucken müsste.[417] Die Einwilligung muss ähnlich der DSGVO freiwillig, spezifisch und informiert sein.[418] Letztlich ist diese Ausnahme nur eine pauschalisierte Interessenabwägung – die Verbraucher:innen sind bei einer erklärten Einwilligung nicht schutzwürdig, während für das Unternehmen die Rückabwicklung realer Produkte kostenträchtig ist.

Zudem gelten sämtliche Bereichsausnahmen auch für das Widerspruchsrecht gegen Datenhandel. Daher erfasst ein Widerspruch unter anderem auch nicht ein Handeln auf Grund einer gesetzlichen Pflicht oder zur Verteidigung gegen Rechtsansprüche.[419]

b) Ausübung

aa) Überblick

Entscheidend für den praktischen Erfolg von *opt-out*-Mechanismen ist eine niedrige Hürde für Verbraucher:innen.[420] So kann man sich allein dadurch in das National Do-Not-Call Registry eintragen, indem man eine kostenlose Telefonnummer der FTC anruft und seine Registrierung durch Drücken einer Taste bestätigt.[421] Mit einer detaillierten Regelung will der CCPA einen vergleichbar niedrigschwelligen Widerspruch ermöglichen. Der CCPA regelt dementsprechend einen möglichst einfachen individuellen Widerspruch (bb), ein automatisches Widerspruchssignal (cc) und einen Widerspruch durch Datenschutzagenturen (dd).

---

[413] *de la Torre,* Golden Data, What is a 'sale' under CCPA?
[414] Cal. Civ. Code § 1798.145(g)(1),(2).
[415] Vgl. *Cal. Senate Judiciary Comm.*, AB 1146 Bill Analysis, S. 6 f.
[416] Cal. Civ. Code § 1798.145(r).
[417] Cal. Civ. Code § 1798.145(r).
[418] Cal. Civ. Code § 1798.140(h).
[419] Siehe Kapitel 3:B.III (ab S. 71).
[420] *Californians for Consumer Privacy*, Annotated Text of the CPRA, § 1798.135(e).
[421] *FTC*, National Do Not Call Registry.

bb) Individueller Widerspruch

Unternehmen sind verpflichtet, Verbraucher:innen bei der Erhebung persönlicher Informationen auf das Widerspruchsrecht gegen Datenhandel hinzuweisen.[422] Mit persönlichen Informationen von Verbraucher:innen, die es nicht auf das Widerspruchsrecht hingewiesen hat, darf es nicht handeln.[423] Diese Hinweispflicht gilt auch für einen Weiterverkauf, wenn es die persönlichen Informationen selbst aus einem Datenhandel erhalten hat.[424]

Unternehmen müssen mindestens auf zwei Methoden in ihrer Datenschutzerklärung aufmerksam machen, mit denen Verbraucher:innen widersprechen können.[425] Dabei sollen Unternehmen die typische Art der Kontaktaufnahme durch Verbraucher:innen berücksichtigen und einen möglichst niedrigschwelligen Widerspruch ermöglichen.[426] Mindestens eine Widerspruchsmöglichkeit soll an den häufigsten Kommunikationsweg angepasst sein, mit denen Verbraucher:innen sonst mit dem jeweiligen Unternehmen kommunizieren.[427] Die im Zuge des Widerspruchs erhaltenen persönlichen Informationen dürfen sie nur für die Bearbeitung des Widerspruchs nutzen.[428] Unternehmen sollen auch sonst einen Widerspruch nicht behindern. Sie dürfen ihn nicht von der Erstellung eines Accounts abhängig machen oder sonst mehr als die unbedingt nötigen Informationen anfordern.[429] Das Unternehmen muss nicht die Identität des Verbrauchers überprüfen. Es darf nur zusätzliche Unterlagen anfordern, wenn es den Widerspruch anhand klarer und dokumentierter Anhaltspunkte für betrügerisch hält.[430] In diesem Fall ist es gegenüber den Antragstellenden verpflichtet zu begründen, warum es weitere Unterlagen anfordert und gegebenenfalls warum es den Antrag ablehnt.[431]

Das Unternehmen muss auf der Startseite seiner Webseite einen auffälligen Widerspruchslink platzieren.[432] Bei Smartphone-Apps ist das Unternehmen verpflichtet, diesen Link auf seiner Downloadseite zu platzieren, und soll ihn zusätzlich innerhalb der Smartphone-App zugänglich machen.[433] Es muss den Link »Do Not Sell or Share My Personal Information« nennen.[434] Diese Wort-

---

[422] Cal. Civ. Code § 1798.135(c)(2), 11 C.C.R. § 7013.

[423] 11 C.C.R. § 7013(e).

[424] Cal. Civ. Code § 1798.115(d).

[425] 11 C.C.R. § 7026(a).

[426] 11 C.C.R. § 7026(b).

[427] 11 C.C.R. § 7026(a). Es ist unklar, ob diese festgelegten Kontaktmöglichkeiten genutzt werden müssen, da dies anders als bei Auskunfts- und Löschanträgen (11 C.C.R. § 7020(e)) nicht explizit festgelegt ist.

[428] Cal. Civ. Code § 1798.135(c)(6).

[429] Cal. Civ. Code § 1798.135(c)(1).

[430] 11 C.C.R. § 7026(g).

[431] 11 C.C.R. § 7026(g).

[432] Cal. Civ. Code § 1798.135(a)(1).

[433] 11 C.C.R. §§ 7026(a).

[434] Cal. Civ. Code § 1798.135(a)(1).

wahl ist missverständlich. »Share« ist legaldefiniert als Weiterübermittlung an Dritte für bestimmte Werbezwecke.[435] Es ist jedoch damit zu rechnen, dass Verbraucher:innen »share« im Sinne des allgemein üblichen Sprachgebrauchs verstehen: Weiterübermittlung an Dritte für einen beliebigen Zweck. Dies vermittelt den Eindruck, dass das Widerspruchsrecht gegen Datenhandel jede Datenübermittlung an Dritte erfasst – was nicht der Fall ist. So verharmlost die Aufnahme des Wortes »Share« den Datenhandel. Eine bloße Datenweitergabe an Dritte kann aus Sicht eines durchschnittlichen Verbrauchers viele legitime Gründe haben (beispielsweise die Nutzung von Zahlungsdienstleistern). Persönliche Informationen zu verkaufen, ist dagegen an sich schon für viele Verbraucher:innen illegitim. So gingen schon vor Inkrafttreten des CCPA eine Mehrheit der Kalifornier:innen fälschlicherweise davon aus, dass Datenverkauf nur mit ihrer ausdrücklichen Einwilligung zulässig sei.[436] Zudem kann ein Unternehmen diesen Link mit dem ebenfalls nötigen Link »Limit the Use of My Sensitive Personal Information« kombinieren, solange es dafür einen klaren und verständlichen Namen verwendet.[437] Wenn die Verbraucher:innen auf den Link klicken, ist das Unternehmen verpflichtet, das Widerspruchsrecht gegen Datenhandel und wie Verbraucher:innen widersprechen können, leicht verständlich[438] zu erklären.[439] Zudem müssen die Verbraucher:innen unmittelbar auf dieser Seite mittels eines Webformulars widersprechen können.[440]

Auf einen Widerspruchslink können Unternehmen verzichten, wenn sie nicht mit persönlichen Informationen handeln und in ihrer umfassenden Datenschutzerklärung ein Negativattest aufnehmen, dass sie nicht mit persönlichen Informationen handeln.[441] Das Negativattest in der umfassenden Datenschutzerklärung soll der California Privacy Protection Agency und dem Attorney General eine effiziente Kontrolle ermöglichen.[442]

Unternehmen können überdies auf diesen Widerspruchslink verzichten, wenn sie keine finanziellen Anreize für die Einwilligung in Datenhandel anbieten.[443] Finanzielle Anreize bezeichnet dabei die unten geschilderte Regelung des CCPA für »Leistung gegen Daten«.[444] Dies ergibt sich daraus, dass der CCPA Unter-

---

[435] Cal. Civ. Code § 1798.140(ah)(1).

[436] *Hoofnagle/King*, What Californians Understand About Privacy Offline, S. 9–18.

[437] Cal. Civ. Code § 1798.135(a)(3). Zu diesem Link siehe Kapitel 3:C.II.2 (ab S. 114).

[438] 11 C.C.R. §§ 7013(a)(2). Zu diesen für alle Informationspflichten einheitlichen Anforderungen siehe Kapitel 3:D.I.3 (ab S. 163).

[439] 11 C.C.R. §§ 7013(b)(1),(c)(1),(3).

[440] 11 C.C.R. §§ 7013(c)(2), 7026(a).

[441] 11 C.C.R. § 7013(d). Zu der umfassenden Datenschutzerklärung siehe Kapitel 3:D.I.2.b) (ab S. 155).

[442] *Cal. Attorney General,* Initial Statement of Reasons, S. 11: »promotes data governance and accountability by requiring a business to ensure that it complies with its posted policy.«.

[443] So die *ratio legis: Californians for Consumer Privacy*, Annotated Text of the CPRA, § 1798.135(e).

[444] Siehe Kapitel 3:C.I.4.b) (ab S. 101).

nehmen eine Wahlmöglichkeit zwischen einem Widerspruchslink[445] und einem Verzicht auf einen Widerspruchslink[446] einräumt. Nur bei der Wahl eines Widerspruchlinks darf das Unternehmen finanzielle Anreize anbieten.[447] Somit gibt der CCPA einen Anreiz, auf finanzielle Anreize zu verzichten.

Um augenfällig auf das Widerspruchsrecht hinzuweisen, kann das Unternehmen zusätzlich zu dem Widerspruchslink optional folgendes Logo verwenden:[448]

Abbildung 1: Opt-Out Icon

Das Design des Logos soll klarstellen, dass es sich nicht um einen anklickbaren Button, sondern nur um einen Hinweis auf eine Entscheidungsmöglichkeit handelt.[449] Es soll etwa so groß wie andere visuelle Elemente auf der Website sein.[450] Es ist zweifelhaft, ob Unternehmen dieses optionale Logo tatsächlich freiwillig nutzen werden, da sie kein Interesse an vermehrten Widersprüchen haben.

Ein Unternehmen, das mit offline gesammelten persönlichen Informationen handelt, soll direkt bei Erhebung über das Widerspruchsrecht gegen Datenhandel informieren.[451] So ist z. B. ein Unternehmen angehalten, das mit durch Papier-Fragebögen ermittelten persönlichen Informationen handelt, direkt auf dem Fragebogen auf das Widerspruchsrecht gegen Datenhandel hinzuweisen.[452] Einzelhandelsunternehmen sollen ein Schild aufstellen, um darüber zu informieren, dass Verbraucher:innen dem Datenhandel widersprechen können und wie sie dieses Recht ausüben können.[453]

cc) Automatisches Widerspruchssignal

Jedes Unternehmen muss ein automatisches, generelles Widerspruchssignal durch Geräte der Verbraucher:innen akzeptieren.[454] Ein solches Widerspruchssignal kann entweder durch eine Browser-Einstellung ähnlich des Do-Not-Track-Signals ausgelöst werden, aber auch beispielsweise durch eine Option in den Systemeinstellungen eines Smartphones.

---

[445] Cal. Civ. Code § 1798.135(a).

[446] Cal. Civ. Code § 1798.135(b).

[447] Cal. Civ. Code § 1798.135(b). Vgl. Cal. Civ. Code § 1798.135(e) a.E.: »business that elects to comply with subdivision (a) of this Section may respond to the consumer's opt-out consistent with Section 1798.125.« *Section* 1798.125 enthält die Regelung finanzieller Anreize.

[448] 11 C.C.R. § 7013(f)(1).

[449] *Cranor et al.*, User Testing of the Proposed CCPA Do-Not-Sell Icon, S. 2.

[450] 11 C.C.R. § 7013(f)(2).

[451] 11 C.C.R. § 7013(b)(3).

[452] 11 C.C.R. § 7013(b)(3)(A).

[453] 11 C.C.R. § 7013(b)(3)(A).

[454] Cal. Civ. Code § 1798.135(e).

Das automatische Widerspruchssignal muss von jeder Webseite eines Unternehmens beachtet werden. Insoweit ist der CCPA widersprüchlich: Cal. Civ. Code § 1798.135(a) regelt die Pflicht, einen Widerspruchslink prominent zu platzieren.[455] Nach Cal. Civ. Code § 1798.135(b) kann ein Unternehmen auf die Einhaltung des Cal. Civ. Code § 1798.135(a) verzichten, wenn es Verbraucher:innen gestattet (»allows«), mittels eines automatischen, generellen Widerspruchssignals zu widersprechen. Isoliert betrachtet, legt »allows« einen Entscheidungsspielraum des Unternehmens nahe, ob es ein generelles Widerspruchssignal akzeptiert.[456] Cal. Civ. Code § 1798.135(e) regelt aber im Gegensatz dazu ausdrücklich, dass Unternehmen ein automatisches Widerspruchssignal stets beachten müssen. Diesen Widerspruch löst der CCPA selbst auf: Cal. Civ. Code § 1798.135(e) geht nach seinem Wortlaut ausdrücklich Cal. Civ. Code § 1798.135(b) vor. Ein automatisches Widerspruchssignal muss das Unternehmen folglich stets akzeptieren.[457]

Vorbild ist das Do-Not-Track-Signal, das Browseranbieter 2010–2011 als Akt der Selbstregulierung eingeführt hatten.[458] Wenn Webseitenbesucher:innen in ihrem Browser die entsprechende Option aktiviert haben und so das Do-Not-Track-Signal an Webseiten senden, sollen Webseiten auf die Weiterübermittlung personenbezogener Daten an Dritte verzichten.[459] Ausgenommen sind ähnlich dem CCPA operative Dienstleistungen und aggregierte Daten.[460] Webseiten müssen nach dem California Online Privacy Protection Act angeben, ob sie das Do-Not-Track-Signal beachten.[461] Das Do-Not-Track-Signal beachten jedoch die wenigsten Webseiten, sodass es als weitgehend gescheitert gilt.[462]

Der kalifornische Attorney General hatte bei der Erstellung seiner Durchführungsverordnung erwogen, das Do-Not-Track-Signal als automatisches Widerspruchssignal genügen zu lassen, dies aber angesichts der unterschiedlichen Voraussetzungen wieder verworfen.[463] Die Anforderungen an das Widerspruchssignal sind niedrig. Es muss nur klar kommunizieren, dass der jeweilige Verbraucher oder die jeweilige Verbraucherin widersprechen will.[464] Eine vorherige Zertifizierung dieses Signals ist nicht erforderlich. Auch ein standardmäßig

---

[455] Siehe Kapitel 3:C.I.2.b) (ab S. 86).

[456] Diese Ansicht vertretend, ohne Diskussion von Cal. Civ. Code § 1798.135(e): *Rippy*, The Privacy Advisor, Notice obligations and right to opt out.

[457] Ebenso i. Erg.: *Cal. Privacy Protection Agency,* Initial Statement of Reasons, S. 35.

[458] Zur von der FTC angestoßenen Umsetzung: *Corbin*, Internetnews, FTC Mulls Browser-Based Block for Online Ads; *Packer*, Quantable, How Many of Your Users Set »Do Not Track«?

[459] *Mayer/Narayanan/Stamm,* Do Not Track, Nr. 9.1.

[460] *Mayer/Narayanan/Stamm,* Do Not Track, Nr. 9.3.

[461] Cal. Bus. & Prof. Code § 22575(b)(5).

[462] Cal. Attorney General, Initial Statement of Reasons, S. 38.

[463] *Cal. Attorney General*, Summary and Response to Comments Submitted During 45-Day Period, S. 186 f.

[464] 11 C. C. R. § 7026(c)(1).

aktiviertes Widerspruchssignal genügt, da insoweit die Entscheidung ausreicht, einen datenschutzfreundlichen Browser zu wählen.[465]

Unternehmen dürfen nach einem solchen Widerspruchssignal auch nicht mehr mit persönlichen Informationen aus anderen Quellen handeln, wenn sie das Widerspruchssignal einem bestimmten Verbraucher oder einer bestimmten Verbraucherin zuordnen können.[466] Falls eine solche Zuordnung nicht möglich ist, dürfen sie jedenfalls nicht mit Daten bezüglich des jeweiligen Geräts handeln.[467]

Amerikanische Verbraucherschutzorganisationen haben 2020 ein entsprechendes Widerspruchssignal unter dem Namen »Global Privacy Control« entwickelt.[468] Dieses ist als Browser-Erweiterung verfügbar und in dem datenschutzfreundlichen Browser Brave standardmäßig aktiviert.[469] Über 40 Millionen Personen verwenden inzwischen dieses Widerspruchssignal, wobei allerdings unklar ist, wie viele davon kalifornische Verbraucher:innen sind.[470] Zudem akzeptieren gängige Nachrichtenwebseiten wie N.Y. Times und The Washington Post das Widerspruchssignal.[471] Der kalifornische Attorney General hat bereits Webseitenbetreiber formell verwarnt, die das Global Privacy Control-Signal nicht akzeptierten.[472] Ob die gängigen Browser ein solches Widerspruchssignal einbauen werden, ist noch offen. Allerdings gilt Datenschutz durchaus als Werbeargument für Browser.[473]

dd) Vertretung durch Datenschutzagenturen

Für Unternehmen, die nicht primär online tätig sind, ist der bevorzugte Mechanismus des CCPA ein Widerspruch durch Datenschutzagenturen (»authorized agent«).[474] Datenschutzagenturen sind Intermediäre, welche die Verbraucher:innen bei der Rechteausübung unterstützen und auch gewinnorientiert sein können.[475] Verbraucher:innen sollen einmalig eine Datenschutzagentur bevollmächtigen, die dann gegenüber vielen Unternehmen widerspricht. Dies entspricht einem wesentlichen Ziel des CCPA: dem Schaffen eines Marktes für

---

[465] *Cal. Attorney General*, Summary and Response to Comments Submitted During 45-Day Period, S. 186 f.

[466] 11 C.C.R. § 7026(c) a.A.

[467] 11 C.C.R. § 7026(c) a.A.

[468] *Global Privacy Control*, Take Control Of Your Privacy.

[469] *Global Privacy Control*, Take Control Of Your Privacy.

[470] *Global Privacy Control*, GPC Privacy Browser Signal Now Used by Millions and Honored By Major Publishers.

[471] *N.Y. Times*, Privacy Policy, Nr. 1.A.ii; *Washington Post*, Privacy Policy, Do-Not-Track Signals and Similar Mechanisms.

[472] *Cal. Attorney General*, CCPA Enforcement Case Examples.

[473] Vgl. insbesondere *Statt*, The Verge, Apple updates Safari's anti-tracking tech with full third-party cookie blocking.

[474] 11 C.C.R. § 7001(c).

[475] 11 C.C.R. § 7001(c).

Datenschutz.[476] Die neuen Datenschutzagenturen sollen ein Gegengewicht zu den großen datenintensiven Technologie-Unternehmen bilden.

Vorbild ist die Verbraucherschutzorganisation Catalog Choice, die einen Widerspruch gegen physikalische Werbepost erleichtert.[477] Verbraucher:innen können bei Catalog Choice gesammelt angeben, von welchen Firmen sie Werbepost erhalten und bei welchen sie widersprechen wollen. Catalog Choice setzt dann den Widerspruch um. Diese Dienstleistung ist spendenbasiert und für Verbraucher:innen kostenlos.[478]

Eine Datenschutzagentur muss für einen Widerspruch dem Unternehmen nur eine unterschriebene Vollmacht vorlegen.[479] Eine Unterschrift kann auch eine elektronische Signatur nach dem kalifornischen Uniform Electronic Communications Act sein.[480] Eine elektronische Signatur ist dabei – einen Rechtsbindungswillen vorausgesetzt – bereits der »getippte« Name unter einer E-Mail[481] oder das Ankreuzen eines Feldes auf einer Webseite.[482] Diese Vorschrift der Durchführungsverordnung soll verhindern, dass Unternehmen hohe Anforderungen an die Identitätsfeststellung bei dem Widerspruch stellen.[483]

Dieses Modell hat gegenüber einer staatlichen Datenbank wie der National Do-Not-Call Registry den Vorteil, dass es weniger missbrauchsanfällig ist. Es gibt keine zentrale Datenbank, die auch bösgläubige Unternehmen anfragen könnten. Bei der National Do-Not-Call Registry ist das Problem insoweit begrenzt, als es nur wenige Telefonwerbeunternehmen gibt (2021 waren nur 2.512 Telefonwerbeunternehmen für vollen Zugriff auf dieses registriert).[484] Der CCPA ist hingegen auf wesentlich mehr Unternehmen anwendbar. Auch müsste ein entsprechendes Register aller Bürger sensiblere Identifikationsmerkmale enthalten als die isolierte Telefonnummer – typischerweise werden viele Unternehmen einen Verbraucher oder eine Verbraucherin nur mit deren vollen Namen und einem weiteren Merkmal wie dem Geburtstag zuordnen können. Damit steigt das Missbrauchsrisiko nochmals. Überdies wäre solches zentrales Register schwer

---

[476] *Hoofnagle*, Comments on the CCPA: »Creating markets for privacy services was a major goal of the initiative«. *Hoofnagle* war an der Ausarbeitung des CCPA beteiligt, siehe Kapitel 2:C.I (ab S. 30).

[477] *Hoofnagle*, Comments on the CCPA.

[478] *Catalog Choice*, About Us.

[479] 11 C. C. R. § 7026(f).

[480] 11 C. C. R. § 7001(u) i. V. m. Cal. Civ. Code § 1633.2(h).

[481] Cal. Court of Appeals 1st District vom 05.12.2014, *J.B.B. Investment Partners, Ltd. v. Fair*, 232 Cal. App. 4th 974, 988. Allgemein zu elektronischer Form im amerikanischem Recht, auch im Vergleich zur eIDAS-VO: *Determann*, 72 Hastings L. J. 1385, 1422–1432.

[482] U. S. District Court vom 28.02.2014, *Chau v. EMC Corp.*, 2014 U. S. Dist. LEXIS 26381, 13.

[483] *Cal. Attorney General*, Final Statement of Reasons, S. 40.

[484] *FTC,* Do Not Call: Data Book 2021, S. 5.

vereinbar mit der amerikanischen Skepsis vor einem starken Zentralstaat, die sich schon in dem Fehlen eines Melderegisters zeigt.[485]

In der Praxis widersprechen bisher nur wenige Verbraucher:innen, wohl weil bisher die gängigen Browser kein automatisches Widerspruchssignal aussenden und kommerzielle Angebote für Datenschutzagenturen noch fehlen. Auch besteht bisher ein Vollzugsdefizit, das zu rechtswidrig hohen Hürden für Widersprüche führt.[486] Für 2020 gehen Umfragen unter Unternehmen von Widerspruchsraten unter 1 % aus.[487] Derzeit ist es allerdings noch zu früh, die Wirksamkeit dieses Konzepts zu beurteilen.

c) Folgen eines Widerspruchs

Unternehmen können auf einen pauschalen Widerspruch mit einem Wunsch auf Spezifizierung reagieren, wobei die Option, sämtlichen Datenhandel zu untersagen, prominenter als die spezifischeren Optionen sein muss.[488] Sie sind verpflichtet, einen Widerspruch unverzüglich, spätestens jedoch innerhalb von 15 Werktagen umzusetzen.[489] Sofern das Unternehmen persönliche Informationen zwischen Zugang und Umsetzung des Widerspruchs an Dritte im Rahmen eines Datenhandels weitergegeben hat, muss es diese Dritte benachrichtigen und anweisen, eine weitere Nutzung dieser persönlichen Informationen zu unterlassen.[490]

Das Unternehmen muss Dienstleister oder Dritte, die für das Unternehmen persönliche Informationen erheben, anweisen, nicht mit den persönlichen Informationen zu handeln.[491] Der angewiesene Dienstleister oder Dritter darf mit den Daten nicht mehr handeln und sie nur noch für eine der für Dienstleister abschließend aufgezählten zulässigen Dienstleistungen verwenden.[492] Dies erstreckt den Widerspruch auf den Dienstleister und soll so Missbrauch verhindern.[493]

Ein Unternehmen kann nach einem Widerspruch wieder mit persönlichen Informationen handeln, wenn die Verbraucher:innen nach dem Widerspruch freiwillig und spezifisch einwilligen.[494] Eine erneute Bitte um Einwilligung

---

[485] Exemplarisch zu dieser Kritik: *American Civil Liberties Union*, 5 Problems with National ID Cards.

[486] *Gumusel,* Data Subject Right Effectiveness, S. 3–7 mit statistischer Auswertung; *Mahoney/Fahs/Marti*, The State of Authorized Agent Opt Outs, S. 8–16 mit zahlreichen Beispielen.

[487] *Barber*, Privacy Tech, Benchmarking CCPA-related data subject requests; *DataGrail*, The State of CCPA, *Interactive Advertising Bureau*, IAB CCPA Benchmark Survey: Summary, S. 6.

[488] 11 C.C.R. § 7026(d).

[489] 11 C.C.R. § 7026(e). Werktage sind alle Tage außer Sonn- und Feiertage, Cal. Civ. Code §§ 9, 7.

[490] 11 C.C.R. § 7026(e).

[491] Cal. Civ. Code § 1798.135(f).

[492] Cal. Civ. Code § 1798.135(f).

[493] *Californians for Consumer Privacy*, Annotated Text of the CPRA, § 1798.135(f).

[494] Cal. Civ. Code § 1798.120(d).

ist erst zwölf Monate nach dem Zugang des Widerspruchs zulässig,[495] um ein wiederholtes Drängen des Verbrauchers zu einer Einwilligung zu verhindern.

d) Vergleich mit europäischem Datenschutzrecht

aa) Nur oberflächliche Gemeinsamkeiten mit Art. 21 DSGVO

Das Widerspruchsrecht gegen Datenhandel ähnelt nur *prima facie* dem Widerspruchsrecht nach Art. 21 DSGVO. Tatsächlich unterscheidet es sich deutlich. Art. 21 DSGVO hat vor allem die Rolle einer Härtefallregelung, die Einzelfallgerechtigkeit herstellen soll, während die Ausübung des Widerspruchsrecht gegen Datenhandel nach der gesetzgeberischen Konzeption des CCPA der Standardfall ist. Ein solches Widerspruchsrecht gegen Datenhandel existiert in der DSGVO nicht. Weder das allgemeine Widerspruchsrecht (Art. 21 Abs. 1 DSGVO) noch das Widerspruchsrecht gegen Direktwerbung (Art. 21 Abs. 2 DSGVO) sind vergleichbar. Vielmehr übernimmt die Funktion des Widerspruchsrechts gegen Datenhandel das Prinzip der Rechtmäßigkeit nach Art. 5 Abs. 1 lit. a Alt. 1, 6 DSGVO.

Dabei ist die Ausübung beider Widerspruchsrechte durchaus vergleichbar. Der Verantwortliche muss es der betroffenen Person möglichst erleichtern zu widersprechen (Art. 12 Abs. 2 S. 1 DSGVO). Dies ähnelt den spezifischeren Regelungen zur Einlegung des Widerspruchs nach dem CCPA, die ebenfalls auf eine möglichst niedrigschwelligen Widerspruch ausgerichtet sind. Zudem ist ein automatisches Widerspruchssignal bei Diensten der Informationsgesellschaft ausreichend (Art. 21 Abs. 5 DSGVO). In der Praxis spielt diese Norm jedoch bisher kaum eine Rolle[496] und ist nur im Rahmen des Werbewiderspruchs relevant (Art. 21 Abs. 2 DSGVO).[497] Die geringe Rolle von Widerspruchssignalen liegt darin begründet, dass sich der Tatbestand des allgemeinen Widerspruchsrechts gem. Art. 21 Abs. 1 DSGVO kaum durch ein pauschales Widerspruchssignal erfüllen lässt.

Das allgemeine Widerspruchsrecht greift gemäß Art. 21 Abs. 1 S. 1 DSGVO allein, wenn Rechtsgrundlage Art. 6 Abs. 1 S. 1 lit. e, f DSGVO ist und der Widerspruch wegen der besonderen Situation der betroffenen Person begründet ist. Diese besondere Situation muss die betroffene Person detailliert darlegen.[498] Das allgemeine Widerspruchsrecht soll nur die Erforderlichkeit und Interessenabwägung des Art. 6 Abs. 1 S. 1 lit. e, f DSGVO auf die individuelle Situation konkretisieren und so ähnlich einer Härtefallregelung[499] Einzelfallgerechtigkeit

---

[495] Cal. Civ. Code §§ 1798.135(c)(4).

[496] Der soweit ersichtlich einzige Umsetzungsversuch ist das primär für den CCPA entwickelte Global Privacy Control, der jedoch in Europa keine größere Verbreitung gefunden hat: *Global Privacy Control*, Take Control Of Your Privacy.

[497] *Spindler/Dalby* in: Spindler/Schuster, DS-GVO Art. 21 Rn. 16.

[498] *Helfrich* in: Sydow, DSGVO Art. 21 Rn. 61; *Kamin/Braun* in: Ehmann/Selmayr, DS-GVO Art. 21 Rn. 20; *Schulz* in: Gola, DS-GVO Art. 21 Rn. 9; *Veil*, NJW 2018, 3337, 3341; a. A. *Forgó* in: BeckOK DatenschutzR, DS-GVO Art. 21 Rn. 8: bloßer Wunsch genüge.

[499] *Veil*, NJW 2018, 3337, 3341.

herstellen. Dies ist nicht mit dem pauschalen Widerspruchsrecht des CCPA vergleichbar, das alle Verbraucher:innen gegenüber jedem Unternehmen bedenkenlos ausüben sollen.

Eher vergleichbar ist das Widerspruchsrecht gegen Direktwerbung gemäß Art. 21 Abs. 2 DSGVO, das keine besondere Situation der betroffenen Person voraussetzt. Dessen *ratio legis* ist, dass Verantwortliche Direktwerbung zwar auf Art. 6 Abs. 1 S. 1 lit. f DSGVO stützen können (Erwägungsgrund 47 S. 6 der DSGVO), betroffene Personen Direktwerbung dennoch im Einzelfall als belästigend empfinden können.[500] Direktwerbung ist bei systematischer Auslegung im Zusammenhang mit Art. 2 lit. a Werbe-RL jede Äußerung mit dem Ziel der Absatzförderung, bei der Werbende unmittelbaren Kontakt zu der betroffenen Person aufnehmen; dies umfasst keine personalisierte Onlinewerbung.[501] Dieser Werbewiderspruch zielt aber anders als der Datenhandel-Widerspruch des CCPA nicht auf den Kontrollverlust der betroffenen Person ab, sondern auf die Belästigung durch Werbung. Sie knüpft nämlich nicht an die Übermittlung an Dritte an, sondern an die Direktwerbung als besonders belästigende Verarbeitungsart. Die Direktwerbung betrachtet die DSGVO jedoch als grundsätzlich legitim, wie an Erwägungsgrund 47 S. 6 der DSGVO erkennbar ist. Art. 21 Abs. 2 DSGVO soll der betroffenen Person damit nur im Einzelfall eine »Ausflucht« geben.

bb) Prinzip der Rechtmäßigkeit als funktionales Äquivalent zum Widerspruchsrecht gegen Datenhandel

Die Funktion des Widerspruchsrechts gegen Datenhandel übernimmt viel mehr das Prinzip der Rechtmäßigkeit nach Art. 5 Abs. 1 lit. a Alt. 1, 6 DSGVO. Dieses geht auf Art. 8 Abs. 2 S. 1 GRCh zurück, der bereits primärrechtlich festlegt, dass personenbezogene Daten nur aufgrund der Einwilligung der betroffenen Person oder einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden dürfen. Die Rechtsgrundlagen des Art. 6 DSGVO regeln dementsprechend, ob der Verantwortliche für einen bestimmten Zweck personenbezogene Daten verarbeiten darf. Damit treffen sie ähnlich wie das pauschale Widerspruchsrecht des CCPA eine allgemeine Wertung.

Datenhandel ist unter der DSGVO aufgrund einer Einwilligung nach Art. 6 Abs. 1 S. 1 lit. a DSGVO zulässig. Wenn die betroffene Person die Einwilligung in die der *sharing*-Variante des Datenhandels entsprechende Weiterübermittlung an Dritte für personalisierte Werbung verweigert, stützen sich große Teile der Werbe- und Medienbranche auf Art. 6 Abs. 1 S. 1 lit. f DSGVO.[502] Dafür ist Art. 6 Abs. 1

[500] *Forgó* in: BeckOK DatenschutzR, DS-GVO Art. 21 Rn. 21.

[501] *Herbst* in: Kühling/Buchner, DS-GVO Art. 21 Rn. 26; *Kamin/Braun* in: Ehmann/Selmayr, DS-GVO Art. 21 Rn. 47; *Martini* in: Paal/Pauly, DS-GVO Art. 21 Rn. 48; *Munz* in: Taeger/Gabel, DS-GVO Art. 21 Rn. 38; a. A. *Helfrich* in: Sydow, DSGVO Art. 21 Rn. 77: auch personalisierte Werbung sei Direktwerbung.

[502] *Interactive Advertising Bureau*, IAB Europe Transparency & Consent Framework Policies, Appendix A. Dieses *framework* bildet die Grundlage für den Großteil der Onlinewerbung

S. 1 lit. f DSGVO aber keine taugliche Rechtsgrundlage.[503] Zwar ist der höhere erzielbare Werbeumsatz ein berechtigtes Interesse der Medienunternehmen und die Übermittlung an Dritte ist dafür auch erforderlich. Allerdings überwiegen die Interessen der betroffenen Person.[504] So begründet die Übermittlung an Dritte und die damit verbundenen umfangreichen Persönlichkeitsprofile erhebliche Risiken für die betroffene Person. Diese Profile werden weiterverbreitet in einer Weise, die sich schon für den Webseitenbetreiber kaum nachvollziehen lässt.[505] Zudem widerspricht es den vernünftigen Erwartungen der betroffenen Person (Erwägungsgrund 47 S. 1 der DSGVO), wenn der Verantwortliche bei verweigerter Einwilligung nur die Rechtsgrundlage auswechselt.[506] Das schutzwürdige Interesse der betroffenen Person, einen solchen Kontrollverlust zu verhindern, überwiegt gegenüber dem Interesse des Verantwortlichen an geringfügig[507] höheren Werbeumsätzen.

Anders als das pauschale Widerspruchsrecht gegen Datenhandel ist Art. 6 DSGVO aber wesentlich umfassender, da er nicht nur Datenhandel regelt. Damit geht die Einstufung der DSGVO als *opt-in*-Gesetz im Gegensatz zum *opt-out*-Gesetz CCPA fehl.[508] Die DSGVO ist umfassender: jede Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage (Art. 6 Abs. 1 DSGVO), von der die Einwilligung nur eine von vielen ist.

---

in Europa (bis auf Facebook und Google). Die belgische Datenschutzbehörde hat wegen dessen Einsatz ein Bußgeld verhängt: *Autorité de protection des données* (Belgien), Decision Transparency & Consent Framework.

[503] *EDSA,* Leitlinien 05/2020 Einwilligung, Rn. 122 f.; *Autorité de protection des données* (Belgien), Decision Transparency & Consent Framework Rn. 409–423; *DSK*, OH Telemedien 2021, S. 31; *Becker*, CR 2021, 87 Rn. 63–74; *Buchner/Petri* in: Kühling/Buchner, DS-GVO Art. 6 Rn. 153; *Hacker*, Datenprivatrecht, S. 279–281; *Janeček/Malgieri* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 95, 113 f.; *Spindler/Dalby* in: Spindler/Schuster, DS-GVO Art. 6 Rn. 19; *Perlingeri* in: Pertot, Rechte an Daten, 207, 223; a. A. *Tavanti*, RDV 2016, 13, 305 f.; ähnlich *Brendle-Weith*, VuR 2018, 331, 334 f. für den Parallelfall des Adresshandels.

[504] *Becker*, CR 2021, 87 Rn. 74; *DSK*, Orientierungshilfe Telemedien, S. IIf.; *Buchner/Petri* in: Kühling/Buchner, DS-GVO Art. 6 Rn. 153; *Hacker*, Datenprivatrecht, S. 279–281; *Janeček/Malgieri* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 95, 113 f.; *Spindler/Dalby* in: Spindler/Schuster, DS-GVO Art. 6 Rn. 19; *Perlingeri* in: Pertot, Rechte an Daten, 207, 223.

[505] *ICO* (UK), Update report into adtech and real time bidding, S. 20 f.

[506] *EDSA*, Leitlinien 05/2020 Einwilligung, Rn. 122 f.; *Schantz* in: BeckOK DatenschutzR, DS-GVO Art. 5 Rn. 8 (allerdings auf Treu und Glauben nach Art. 5 Abs. 1 lit. a DSGVO gestützt); *Taeger* in: Taeger/Gabel, DS-GVO Art. 6 Rn. 47–49; a. A. *Jahnel* in: Jahnel, DS-GVO Art. 6 Rn. 9 (zumindest bei besonders transparentem Hinweis auf potenziellen Wechsel); *Krusche*, ZD 2020, 232, 235.

[507] *Marotta/Abhishek/Acquisti*, Online Tracking and Publishers' Revenues: An Empirical Analysis, S. 20f: etwa 4 % höhere Einnahmen.

[508] A. A. *Alexander*, 32 Loy. Consumer L. Rev. 199, 231; *Jazzar*, 70 Case W. Res. L. Rev. 457, 481 f.; *Lejeune*, ITRB 2021, 13, 19; *Park*, 10 UC Irvine L. Rev. 1455, 1476–1479; *Resnick*, 46 Brook. J. Int'l L. 277, 299 f.

cc) Einwilligungsbasierter Telemediendatenschutz

Das Telemediendatenschutzrecht der ePrivacy-RL und dessen Umsetzung im TTDSG ist dagegen einwilligungsbasiert und folgt einem *opt-in*-Mechanismus. Eine Einwilligung ist gemäß § 25 Abs. 1 TTDSG erforderlich, wenn der Diensteanbieter Informationen in der Endeinrichtung des Endnutzers speichert (d. h. in der Regel Cookies) oder auf Informationen, die bereits in der Endeinrichtung gespeichert sind, zugreift. Ohne Einwilligung darf der Diensteanbieter nur Informationen speichern oder auf diese zugreifen, wenn dies für einen vom Nutzer ausdrücklich gewünschten Telemediendienst unbedingt erforderlich ist (§ 25 Abs. 2 Nr. 2 TTDSG). Daher ist Datenhandel im Telemedienrecht nur mit Einwilligung möglich.

Die Entwürfe der ePrivacy-VO schwächen diesen Fokus auf die Einwilligung ab. So gestatten die drei Entwürfe der Europäischen Kommission, des Europäischen Parlaments und des Rats jeweils in Art. 8 ePrivacy-VO-E bestimmte als unproblematisch angesehene Dienste ohne Einwilligung. Die einzelnen jeweils erfassten Dienste ähneln der Ausnahme von der Datenhandelsdefinition für Dienstleister des CCPA. Für Dienstleister sind nur bestimmte Dienstleistungen zulässig.[509] Die zulässigen Dienstleistungen sind allerdings wesentlich weiter als die ohne Einwilligung erlaubten Dienste der Entwürfe für die ePrivacy-VO. So enthalten die zulässigen Dienstleistungen des CCPA beispielsweise auch nicht-personalisierte Werbung,[510] die in keinem der Art. 8 ePrivacy-VO-E enthalten ist. Insoweit setzt der CCPA einen Anreiz, nur kontextbasierte Werbung zu nutzen, indem Unternehmen für solche Werbung kein Widerspruchsrecht einräumen müssen.

dd) Datenschutzagenturen im Vergleich zu Personal Information Management Systems und Datentreuhand

In einer gewissen Parallele zu dem globalen automatischen Widerspruchssignal des CCPA sollen bereits nach dem TTDSG Nutzer Dienste zur Verwaltung von Einwilligungen nutzen können (§ 26 Abs. 1 TTDSG). Für diese auch als *Personal Information Management Systems* bekannten Dienste ist allerdings eine zusätzliche Anerkennung des Dienstes durch eine unabhängige Stelle erforderlich, welche die Bundesregierung durch eine noch zu erlassende Rechtsverordnung bestimmen wird (§ 26 Abs. 2 S. 2 TTDSG). Unter dem CCPA ist eine solche Zulassung dagegen nicht erforderlich. Insofern zeigt sich das deutsche Telemedienrecht mehr auf Rechtssicherheit bedacht als der pragmatische CCPA.

Nur geringe Ähnlichkeiten weisen die Datenschutzagenturen mit dem Konzept einer Datentreuhand auf, wie sie insbesondere die Data-Governance-VO als Datenvermittlungsdienste regelt. Diese sollen primär Bereitstellung

[509] Siehe Kapitel 3:B.II.3 (ab S. 65).
[510] Cal. Civ. Code § 1798.140(e)(4).

personenbezogener Daten[511] vermitteln (Art. 10 Abs. 1 lit. b Data-Governance-VO) oder die Bedingungen der Bereitstellung aushandeln (Art. 2 Nr. 15 Data-Governance-VO). Für die Ausübung der Datenschutzrechte haben Datenvermittlungsdienste dagegen nach Art. 12 lit. m Data-Governance-VO vor allem eine beratende Funktion. Auch die oft diskutierte Datentreuhand soll primär bei der Datenerhebung zwischen Datennutzenden und betroffenen Personen vermitteln.[512] Eine Unterstützung bei der Rechtsausübung ist allenfalls ein selten diskutierter Nebenzweck.[513]

3. Einwilligungsvorbehalt für Minderjährige

Unternehmen dürfen mit persönlichen Informationen von Minderjährigen unter 16 Jahren nur mit Einwilligung der Erziehungsberechtigten oder der Minderjährigen handeln (»right to opt-in«).[514] Für Minderjährige bis zum 13. Geburtstag müssen die jeweiligen Erziehungsberechtigten einwilligen; 13- bis 15-Jährige können selbst einwilligen.[515] Das Unternehmen muss auch ohne positive Kenntnis des Alters die Einwilligung einholen, wenn es »willfully disregards the consumer's age«.[516] *Willful disregard* stammt aus dem Strafrecht und entspricht dort in etwa dem deutschen Eventualvorsatz: Wissen um das hohe Risiko und Gleichgültigkeit hinsichtlich des Erfolges.[517]

Ratio legis für diesen Einwilligungsvorbehalt ist, dass Minderjährige besonders schutzwürdig sind.[518] Diese sind typischerweise noch nicht in der Lage, den Hinweis auf das Widerspruchsrecht gegen Datenhandel zu verstehen und selbst aktiv zu widersprechen. Ein Einwilligungsvorbehalt für Minderjährige ist eher mit der Meinungsfreiheit vereinbar als für Volljährige. Die Rechtsprechung erkennt insoweit den Schutz von Minderjährigen als legitimes staatliches Interesse an, das die Grundlage für eng begrenzte staatliche Eingriffe in die Meinungsfreiheit bilden kann.[519]

Dieser Einwilligungsvorbehalt gilt nur, soweit der COPPA nicht anwendbar ist.[520] Unter diesem dürfen Webseitenbetreiber personenbezogene Informationen von Minderjährigen unter 13 Jahren nur erheben, wenn die Erziehungsberechtigten

---

[511] Die Data-Governance-VO ist auch auf nicht-personenbezogene Daten anwendbar, vgl. Art. 1 Abs. 1 i. V. m. Art. 2 Nr. 1 Data-Governance-VO.

[512] *Kühling/Sackmann/Schneider*, Forschungsbericht Datentreuhänder, S. 17f; *Richter*, ZEuP 2021, 634, 642; *Specht-Riemenschneider et al.*, MMR-Beil. 2021, 25, 27.

[513] *Kühling/Sackmann/Schneider*, Forschungsbericht Datentreuhänder, S. 24: es fehle eine diesbezügliche Diskussion in der Literatur.

[514] Cal. Civ. Code § 1798.120(c).

[515] Cal. Civ. Code § 1798.120(c).

[516] Cal. Civ. Code § 1798.120(c).

[517] Cal. Court of Appeals 2nd District vom 30.09.2003, *People v. Pinkston*, 112 Cal. App. 4th 387, 395; vom 13.04.2016, *People v. Weddington*, 246 Cal. App. 4th 468, 486.

[518] Proposition 24 (Cal. 2020), Sec. 2(J).

[519] U. S. Supreme Court vom 27.06.2011, *Brown v. Entm't Merchs. Ass'n*, 564 U. S. 786, 794.

[520] Proposition 24 (Cal. 2020), Sec. 30. Zum COPPA siehe Kapitel 2:B.I.2 (ab S. 19).

einwilligen.[521] Anders als der CCPA schützt er aber 13- bis 15-Jährige nicht (wobei der Kongress mehrmals erwogen hat, den COPPA auf diese zu strecken).[522] Vor allem aber gilt er nur bei positiver Kenntnis des Unternehmens vom Alter des Verbrauchers.[523] Soziale Netzwerke verschließen sich vor einer solchen positiven Kenntnis dadurch, dass sie in ihren AGB die Nutzung durch Unter-13-Jährige verbieten und bei der Registrierung auf die Eigenangabe des Geburtsdatums vertrauen.[524] Es liegt auf der Hand, dass dies kein effektiver Mechanismus ist. So haben sich nach einer Umfrage unter Eltern 41 % der Minderjährigen, die soziale Netzwerke nutzen, bereits vor Erreichen des 13. Lebensjahr das erste Mal angemeldet.[525] Dennoch reicht eine solche Eigenangabe nach Auffassung der FTC als zuständiger Vollzugsbehörde, um positive Kenntnis nach dem Children's Online Privacy Protection Act zu vermeiden.[526] Unter dem CCPA ist dagegen ein Vertrauen auf die reine Eigenangabe des Alters ein *willful disregard* des Alters.[527]

Einwilligung bedeutet eine absichtliche, aktive Bestätigung der Entscheidung für einen Datenhandel.[528] Das Unternehmen muss dabei sicherstellen, dass die einwilligende Person tatsächlich erziehungsberechtigt ist.[529] Die Durchführungsverordnung enthält dafür eine nicht abschließende Liste an Methoden,[530] die der Verordnung der FTC zum COPPA nachgebildet ist.[531] Das Unternehmen muss die aktive Einwilligung eines 13–15-Jährigen sich in einem zweistufigen Prozess bestätigen lassen, diese über ihr Recht auf Widerruf informieren und die Einwilligung dokumentieren.[532] Erziehungsberechtigte sollen ein automatisches Browsersignal setzen können, das die Eigenschaft »minderjährig bis zu 12 Jahre« oder »minderjährig zwischen 13 und 16 Jahren« kommuniziert, damit sich Webseitenbetreiber nicht auf Unwissenheit berufen können.[533] Dieses existiert bisher noch nicht. Ansonsten enthält der CCPA keine besonderen Rechte oder Pflichten bezüglich Minderjährigen.

Die DSGVO schützt ebenfalls punktuell Minderjährige. So sind in der Interessenabwägung nach Art. 6 Abs. 1 S. 1 lit. f DSGVO a.E. die Interessen der betroffenen

---

[521] 15 U.S.C. § 6502(a)(1), 16 C.F.R. § 312.5(a)(1).

[522] Zuletzt: PROTECT Kids Act, H.R. 5573, 116th Cong. (2019–20), Sec. 2(2)(A).

[523] 15 U.S.C. § 6501(4)(B),(10)(A).

[524] *Finnegan*, 50 Seton Hall L. Rev. 827, 833–838.

[525] *Lauricella et al.*, The Common Sense Census: Plugged-In Parents of Tweens and Teens, S. 35.

[526] *FTC,* Children's Online Privacy Protection Rule: Not Just for Kids' Sites.

[527] *Finnegan*, 50 Seton Hall L. Rev. 827, 843 f.

[528] Cal. Civ. Code § 1798.120(c), 11 C.C.R. § 7001(a). Der CCPA verwendet hier mit »affirmative authorization« einen leicht anderen Begriff als »consent«, wobei ersichtlich dasselbe gemeint ist.

[529] 11 C.C.R. § 7070(a)(1).

[530] 11 C.C.R. § 7070(a)(2).

[531] *Cal. Attorney General*, Initial Statement of Reasons, S. 34.

[532] 11 C.C.R. §§ 7071(a) i.V.m. 7028(a).

[533] Cal. Civ. Code § 1798.185(a)(19)(B).

Person explizit höher zu gewichten, wenn diese ein Kind ist. Damit ist auch unter der DSGVO bei Minderjährigen häufiger eine Einwilligung erforderlich.

Diese Einwilligung müssen die Erziehungsberechtigten von Minderjährigen unter 16 Jahren nach Art. 8 Abs. 1 UAbs. 1 S. 2 DSGVO bei Diensten der Informationsgesellschaft entweder selbst erteilen oder der Einwilligung von Minderjährigen zustimmen. Vergleichbar zum CCPA soll dafür keine reine Selbstauskunft des Minderjährigen genügen.[534] Für solche Dienste der Informationsgesellschaft können Minderjährige unter 16 Jahren flankierend ohne weitere Voraussetzungen Löschung ihrer personenbezogenen Daten gemäß Art. 17 Abs. 1 lit. f DSGVO verlangen. Die Dienste der Informationsgesellschaft entsprechen eher den »websites or online services« des COPPA[535] als dem Datenhandel des CCPA.

Neben Art. 8 DSGVO muss der Verantwortliche auch die Informationen nach Art. 13, 14 DSGVO und für die Art. 15–22, 34 DSGVO nötigen Mitteilungen in einer kindgerechten Sprache verfassen, wenn sich die Informationen an Kinder richten (Art. 12 Abs. 1 S. 1 HS. 2 DSGVO). Wie beim CCPA sind diese Sondervorschriften für Minderjährige unter der DSGVO eher punktuell. Ein umfassendes Sonderrecht für Minderjährige kennt weder der CCPA noch die DSGVO.

4. Maßregelungsverbot

a) Reichweite

Das Recht auf Nicht-Maßregelung ist als Recht formuliert (»right of no retaliation«), aber nicht von einem aktiven Handeln abhängig, sondern ein *ipso iure* geltendes Maßregelungsverbot.[536] Das Framing von Verboten als Recht ist für das liberale amerikanische Recht typisch, das mit dieser Benennung den Fokus auf die Privatautonomie richtet.[537]

Das Maßregelungsverbot verbietet jede Benachteiligung wegen der Ausübung von Verbraucherrechten.[538] Unternehmen dürfen deswegen weder die Lieferung von Waren oder Erbringung von Dienstleistungen verwehren, für diese andere Preise verlangen oder eine andere Qualität anbieten.[539] Zudem darf ein Unternehmen eine solche Diskriminierung auch nicht suggerieren.[540] Eine Maßregelung von Beschäftigten, Bewerber:innen oder freien Mitarbeiter:innen

---

[534] *Buchner/Kühling* in: Kühling/Buchner, DS-GVO Art. 8 Rn. 23; *Däubler* in: Däubler et al., EU-DSGVO Art. 8 Rn. 11; *Heckmann/Paschke* in: Ehmann/Selmayr, DS-GVO Art. 8 Rn. 37; *Schrader*, Datenschutz Minderjähriger, S. 154; *Schulz* in: Gola, DS-GVO Art. 8 Rn. 19; *Taeger* in: Taeger/Gabel, DS-GVO Art. 8 Rn. 38; a. A. *Greve* in: Eßer/Kramer/Lewinski, DSGVO Art. 8 Rn. 18; *Plath* in: Plath, DSGVO Art. 8 Rn. 11.

[535] 15 U. S. C. § 6501(10)(A).

[536] Cal. Civil Code § 1798.125.

[537] *Glendon*, Rights talk, passim; *Reidenberg*, 80 Iowa L. Rev. 497, 501.

[538] Cal. Civil Code § 1798.125(a)(1).

[539] Cal. Civil Code § 1798.125(a)(1)(A),(B),(C); 11 C. C. R. § 7080(a).

[540] Cal. Civil Code § 1798.125(a)(1)(D).

aufgrund der Ausübung ihrer durch den CCPA gewährten Rechte ist ebenso verboten.[541]

b) Ausnahme: Finanzielle Anreize

aa) Regelung

Als einzige Ausnahme des Maßregelungsverbots erlaubt der CCPA finanzielle Anreize (»financial incentives«) für das Erheben persönlicher Informationen und die Einwilligung in den Datenhandel.[542] Wenn Verbraucher:innen Datenhandel widersprochen haben, kann das Unternehmen nur mit einer aktiven Einwilligung in Datenhandel wegen finanzieller Anreize weiter mit deren persönlichen Informationen handeln.[543] Damit lässt der CCPA das Geschäftsmodell »Leistung gegen Daten« explizit zu. Er knüpft die Zulässigkeit aber an verbraucherschützende Bedingungen wie detaillierte Informationspflichten und das Anbieten eines angemessenen Alternativangebots. Diese Ausnahme greift ebenfalls für das Recht auf Löschung, aber nicht für das Recht auf Beschränkung sensibler Informationen.[544]

Finanzielle Anreize sind weit definiert als jedes Programm, jeden Vorteil oder jedes anderes Angebot entweder für die Bereitstellung persönlicher Informationen oder die Einwilligung in Datenhandel.[545] Sie können eine direkte Zahlung für die persönlichen Informationen darstellen.[546] Finanzielle Anreize sind aber auch ein Rabatt oder eine bessere Qualität für die erhaltenen persönlichen Informationen.[547] Stellen auch Treueprogramme und Kundenkarten finanzielle Anreize dar, wenn sie Datenhandel beinhalten? Cal. Civ. Code § 1798.135(a)(3) spricht davon, dass das Maßregelungsverbot in Treueprogramme und Kundenkarten nicht verbietet, die »consistent with this title« sind. *Title* bezeichnet dabei den Abschnitt, in dem sich der gesamte CCPA befindet, also auch die Regelung finanzieller Anreize. Der Wortlaut spricht daher dafür, dass Cal. Civ. Code § 1798.135(a)(3) nur klarstellender Natur ist. Finanzielle Anreize sind daher auch Treueprogramme und Kundenkarten, wenn diese Datenhandel beeinhalten.

Die finanziellen Anreize müssen sich am Wert der persönlichen Informationen für das Unternehmen orientieren, der nach dem klaren Wortlaut sowohl Ober- als auch Untergrenze des Wertes der finanziellen Anreize bildet.[548] Durch eine dokumentierte Kalkulation des Datenwerts soll sichergestellt werden, dass

---

[541] Cal. Civil Code § 1798.125(a)(1)(E).

[542] Cal. Civ. Code § 1798.125(a)(2),(b).

[543] Cal. Civ. Code § 1798.125(b)(3).

[544] Cal. Civ. Code § 1798.125(b)(1). Zu finanziellen Anreizen beim Recht auf Löschung siehe Kapitel 3:C.IV.2 (ab S. 141).

[545] 11 C.C.R. § 7001(j).

[546] Cal. Civ. Code § 1798.125(b)(1).

[547] Cal. Civ. Code § 1798.125(b)(1).

[548] Cal. Civ. Code § 1798.125(b)(1): »reasonably related to the value provided to the business by the consumer's data«; 11 C.C.R. § 7080(b).

das Alternativangebot nicht übermäßig teuer ist.[549] Das Unternehmen muss den Datenwert anhand eines nachvollziehbaren Maßstabes berechnen.[550] Die Durchführungsverordnung enthält hierfür ein an der einschlägigen wirtschaftswissenschaftlichen Literatur orientiertes,[551] marktorientiertes Konzept. Dabei ist der durchschnittliche Gewinn des Unternehmens[552] aufgrund der jeweiligen persönlichen Informationen maßgeblich.[553] Das Unternehmen hat einen gewissen Spielraum, Einnahmen und Ausgaben zuzuordnen.[554] Auch den Aufwand für das Angebot finanzieller Anreize darf es berücksichtigen, solange diese Zuordnung »reasonable« ist.[555] Das Unternehmen kann entweder den Wert individuell pro Verbraucher:in[556] oder – praxisrelevanter – als Durchschnitt für Kalifornien oder die Vereinigten Staaten beziffern.[557] Daneben ist auch eine andere Berechnungsweise zulässig, wenn diese zu nachvollziehbaren und zuverlässigen Ergebnisse führt und praktikabel ist.[558] Diese flexibele Methode ist dem Regelungsgegenstand angemessen. Ein klarer, objektiver Standard, personenbezogene Daten zu bewerten, existiert bisher nicht.[559] Die Auswahl einer marktbezogenen Methode ist konsequent, da der Wert persönlicher Informationen vom jeweiligen Kontext abhängt.[560]

Als Auffangtatbestand legt der CCPA zudem fest, dass der Umgang mit finanziellen Anreizen nicht ungerecht, unangemessen, knebelnd oder wuchernd sein darf.[561] Dies betrifft wohl vor allem die Art und Weise, wie finanzielle Anreize angeboten werden, und nicht deren Höhe, die sich ohnehin an dem Wert der persönlichen Informationen orientieren muss.

Zur Erläuterung enthält die Durchführungsverordnung zwei Regelbeispiele. Erstens verstoße das bloße Einräumen einer Wahl zwischen einem Bezahl- und einem Werbemodell bei einem Musikstreamingdienst gegen das Maßregelungsverbot, wenn sich die Kosten des Bezahlmodells nicht am Mehrerlös durch

---

[549] *Cal. Attorney General*, Initial Statement of Reasons, S. 38.

[550] 11 C.C.R. § 7081(a).

[551] Cal. Attorney General, Initial Statement of Reasons, S. 38. Zu alternativen Ansätzen siehe Kapitel 4:B.III.3.d) (ab S. 267).

[552] Zum Unternehmensbegriff siehe Kapitel 3:B.II.2 (ab S. 56).

[553] 11 C.C.R. § 7081(a)(7).

[554] Cal. Attorney General, Initial Statement of Reasons, S. 39.

[555] 11 C.C.R. § 7081(a)(6).

[556] 11 C.C.R. § 7081(a)(1).

[557] 11 C.C.R. § 7081(a)(2),(b).

[558] 11 C.C.R. § 7081(a)(8).

[559] *Hacker* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 47, 53; *Heller* in: Leupold/Wiebe/Glossner, IT-Recht, Teil 6.2 Rn. 9.; *OECD*, Exploring the Economics of Personal Data, S. 10; *Schur*, Die Lizenzierung von Daten, S. 266–268.

[560] Vgl. allgemein: *Hacker* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 47, 53: marktbasierte Maßstäbe seien für staatliche Regulierung besser geeignet; *Solove*, 89 Geo. Wash. L. Rev. 1, 31–33 zur Subjektivität einer solchen Wertbestimmung.

[561] Cal. Civ. Code § 1798.125(b)(4).

die persönlichen Informationen orientieren.[562] Daher ist der Wert der persönlichen Informationen wohl auch bei Bündelangeboten maßgeblich. So dürfte der Musikstreamingdienst nur den Mehrerlös durch die Weitergabe der persönlichen Informationen für Werbung berücksichtigen, nicht aber den gesamten Werbeerlös. Sonst wäre die Bezugnahme auf den Wert der persönlichen Informationen statt des Werbeerlöses sinnlos. Das zweite Regelbeispiel ist ein Lebensmitteleinzelhandelsunternehmen, das Rabatte dafür anbietet, wenn Verbraucher:innen ihre Telefonnummer bereitstellen.[563] Dies verstößt gegen das Maßregelungsverbot, außer wenn sich der Rabatt als finanzieller Anreiz am Wert der persönlichen Informationen orientiert.[564]

Das Unternehmen muss in einer *notice of financial incentive* Verbraucher:innen über die wesentlichen Aspekte des finanziellen Anreizes leicht verständlich[565] informieren.[566] Dies dient dazu, dass sich Verbraucher:innen informiert entscheiden können.[567] Es muss dabei den finanziellen Anreiz und den geplanten Datenhandel prägnant beschreiben.[568] Dabei ist es verpflichtet, die betroffenen Kategorien persönlicher Informationen anzugeben,[569] damit Verbraucher:innen den Umfang des Datenhandels einschätzen können. Vor allem aber muss es den Wert der persönlichen Informationen beziffern und die Herleitung dieses Wertes beschreiben.[570] Die Kenntnis des Marktwerts ihrer persönlichen Informationen soll es Verbraucher:innen ermöglichen, auf gleicher Augenhöhe mit Unternehmen zu verhandeln.[571] Daneben muss das Unternehmen mit seiner dokumentierten Herleitung auch gegenüber der Öffentlichkeit Rechenschaft ablegen.[572] Bisher ist zu beobachten, dass viele Unternehmen in ihrer *notice of financial incentive* nur sehr abstrakt die Herleitung beschreiben.[573] Dies spiegelt eine Skepsis, auch Konkurrenten Einblick in das eigene Geschäftsmodell zu

---

[562] 11 C.C.R. § 7080(d)(1).

[563] 11 C.C.R. § 7080(d)(3).

[564] 11 C.C.R. § 7080(d)(3).

[565] Näher zu den für alle Informationspflichten einheitlichen Anforderungen an die Art und Weise der Information siehe Kapitel 3:D.I.3.a) (ab S. 163).

[566] Cal. Civ. Code § 1798.125(b)(3), 11 C.C.R. § 7016.

[567] 11 C.C.R. § 7016(a)(1).

[568] 11 C.C.R. § 7016(b)(1),(2).

[569] 11 C.C.R. § 7016(b)(2).

[570] 11 C.C.R. § 7016(b)(5).

[571] *Cal. Attorney General*, Initial Statement of Reasons, S. 12. Vgl. allgemein die Erwägungsgründe in Proposition 24 (Cal. 2020), Sec. 2(E).

[572] *Cal. Attorney General*, Initial Statement of Reasons, S. 12.

[573] Z.B.: *Frontier*, California Privacy Policy: »Frontier Airlines values the data of FRONTIERMiles members and Discount Den subscribers because it allows us to track and reward Frontier Airlines passengers«; *Kuiu*, Financial Incentives Terms: »The value of KUIU Rewards Data to KUIU is calculated by determining the approximate additional spending of KUIU Rewards customers against the spending of individuals who are not enrolled in KUIU Rewards«; *RA Sushi*, Notice of Financial Incentive: »We have estimated the value of your registration with us as $30 annually for our Benihana, Samurai, or HARU restaurants and

geben, und ist wohl nur über eine stärkere Rechtsdurchsetzung zu lösen. Mehr operativ ist die verpflichtende Angabe, wie Verbraucher:innen in den finanziellen Anreiz einwilligen und wie sie ihre Einwilligung widerrufen können.[574]

Die Einwilligung ist ähnlich der DSGVO definiert als freiwillige, konkrete, informierte und jederzeit widerrufliche[575] Einverständniserklärung für einen spezifischen Verarbeitungszweck.[576] Die Einverständniserklärung muss eine eindeutige gesonderte Erklärung darstellen, die keine datenschutzfremde Elemente betrifft.[577] Eine Einwilligung ist zudem unwirksam, wenn das Unternehmen sogenannte *dark patterns* benutzt hat.[578] *Dark Patterns* definiert der CCPA als Benutzeroberflächenelemente, die irreführen und manipulieren.[579] Dabei ist nur der Effekt, nicht die Absicht des täuschenden Unternehmens entscheidend.[580] Schließlich ist rein passives Verhalten keine Einwilligung.[581]

bb) Auswirkung auf Datenwirtschaft und Kritik

Das Erfordernis einer solchen aktiven, informierten Einwilligung für finanzielle Anreize wirkt sich vor allem bei wirtschaftlich unausgewogenen Geschäften aus. So birgt z. B. die personalisierte Werbung auf Webseiten erhebliche Risiken für die betroffenen Individuen, hat aber nur einen minimalen Vorteil für Webseitenbetreiber. Zwar kann bei sehr unterschiedlichen Interessen des Publikums verhaltensbasierte Werbung in idealisierten Umständen nahezu doppelt so viel Nachfrage erzeugen.[582] Dem stehen jedoch hohe Kosten für Intermediäre entgegen: bei personalisierter Werbung machen die Personalisierungskosten circa ein Drittel der Gesamtwerbekosten aus.[583] *Marotta/Abhishek/Acquisti* gehen anhand der Analyse eines aktuellen und umfangreichen Datensets davon aus, dass Webseitenbetreiber mit verhaltensbasierter Werbung nur ca. 4 % höhere Einnahmen erzielen.[584] Webseitenbetreiber müssten also, wenn sie weiter verhaltensbasierte Werbung nutzen wollen, finanzielle Anreize in Höhe eines kleinen Bruchteils ihrer durchschnittlichen Werbeeinnahmen anbieten. Zudem legen sie mit diesem Angebot offen, dass es sich um eine wirtschaftliche

---

$20 biannually for our RA Sushi restaurants. These amounts equal the average cost of a meal to guests at our respective restaurants.«.

[574] 11 C. C. R. § 7016(b)(3),(4).

[575] 11 C. C. R. § 7016(b)(3).

[576] Cal. Civ. Code § 1798.140(h).

[577] Cal. Civ. Code § 1798.140(h).

[578] Cal. Civ. Code § 1798.140(h).

[579] Cal. Civ. Code § 1798.140(l).

[580] King/Stephan, 5 Geo. L. Tech. Rev. 251, 268.

[581] Cal. Civ. Code § 1798.140(h).

[582] *Chen/Stallaert*, 38 MIS Quarterly 429, 441.

[583] *Incorporated Society of British Advertisers*, Programmatic Supply Chain Transparency Study, S. 18.

[584] *Marotta/Abhishek/Acquisti*, Online Tracking and Publishers' Revenues: An Empirical Analysis, S. 20 f.

Transaktion handelt (Daten gegen Leistung). Die mit dem CCPA verbundene Intention ist, dass Unternehmen sich wegen dieser Schwierigkeiten für andere Werbeformen entscheiden.

Viele kalifornische Bürgerrechtsorganisationen sehen die Ausnahme für finanzielle Anreize kritisch und betonen, dass Datenschutz ein fundamentales Grundrecht sei.[585] Diese Position findet einen Anhaltspunkt in den »inalienable right« auf Privatsphäre der kalifornischen Verfassung.[586] Bürgerrechtler:innen legen den Fokus nicht auf den wirtschaftlichen Wert persönlicher Informationen, sondern auf die Risiken für die individuelle Privatsphäre.[587] Bürgerrechtsorganisationen sehen Datenschutz daher als unveräußerliches Menschenrecht.[588] Sonst entstehe eine Zwei-Klassen-Gesellschaft zwischen Reichen, die sich Datenschutz leisten können, und Armen, die ihre persönlichen Informationen verkaufen müssen.[589] Daher ist es mit der Einordnung als unveräußerliches Grundrecht kaum vereinbar, persönlichen Informationen einen konkreten Wert zuzuweisen.[590]

Der Gesetzgeber des CCPA behandelt persönliche Informationen hingegen als handelbares Wirtschaftsgut. Proposition 24 nennt zu Beginn ihrer Erwägungsgründe zwar durchaus auch das Recht auf Privatsphäre in der kalifornischen Verfassung.[591] Noch im gleichen Absatz betont Proposition 24 aber, dass für dieses Recht die Kontrolle des Verbrauchers über die Nutzung seiner persönlichen Informationen grundlegend sei.[592] Dieses liberale Verständnis ist auch mit dem verfassungsrechtlichen Recht auf Privatsphäre vereinbar, wie die offizielle Begründung des damaligen verfassungsändernden Volksentscheids hervorhob: »Fundamental to our privacy is the ability to control circulation of personal information«.[593]

---

[585] *American Civil Liberties Union of California et al.*, California Privacy Rights and Enforcement Act – Privacy Coalition Comments, S. 7; *Schwartz/Tien/McSherry*, Electronic Frontier Foundation, How to Improve the California Consumer Privacy Act of 2018; *Snow/Conley*, ACLU Northern California, Californians Should Vote No on Prop 24. Kritik Dritter wiedergebend: *Cal. Senate Judiciary Comm.*, AB 375 Bill Analysis, S. 19; *Bensinger*, N.Y. Times, A Privacy Measure That's Hard to Like; *Greig*, TechRepublic, California voters back new data privacy law beefing up CCPA.

[586] Cal. Const. art. I § 1. Siehe Kapitel 2:A.II (ab S. 15).

[587] So explizit *Lyon/Moerel*, Privacy Perspectives, Why placing a price tag on personal data may harm consumer privacy.

[588] Aus kommunikationswissenschaftlicher Sicht: *Baik,* Data Privacy Against Innovation or Against Discrimination?, S. 25.

[589] *American Civil Liberties Union of California et al.*, California Privacy Rights and Enforcement Act – Privacy Coalition Comments, S. 7; *Bensinger*, N.Y. Times, A Privacy Measure That's Hard to Like; *Greig*, TechRepublic, California voters back new data privacy law beefing up CCPA; *Schwartz/Tien/McSherry*, Electronic Frontier Foundation, How to Improve the California Consumer Privacy Act of 2018.

[590] Zu ähnlichen Bedenken im europäischen Recht W.

[591] Proposition 24 (Cal. 2020), Sec. 2(A).

[592] Proposition 24 (Cal. 2020), Sec. 2(A) a.E.

[593] Proposition 11 (Cal. 1972), Ballot Analysis and Arguments zitiert nach: *Kelso*, 19 Pepp. L. Rev. 327, 480 f.

Der Informationsvorsprung der Unternehmen führe nach den Erwägungsgründen der Proposition 24 dazu, dass Verbraucher:innen den Überblick verlieren, wie Unternehmen mit ihren persönlichen Informationen handeln.[594] Dieses Marktversagen soll durch erhöhte Transparenz gelöst werden. Proposition 24 vergleicht explizit diese Informationspflichten mit Kennzeichnungspflichten im Lebensmittelrecht.[595] Nährwertangaben befähigen Verbraucher:innen, sich informiert zu entscheiden – selbst wenn diese am Ende doch ein ungesundes Produkt auswählen. Genauso können sich unter dem CCPA Verbraucher:innen auch dafür entscheiden, ihre persönlichen Informationen für finanzielle Anreize zu »verkaufen«. Die Idealvorstellung des CCPA ist damit eine von Grund auf liberale: Verbraucher:innen sollen informiert und auf gleicher Augenhöhe mit Unternehmen verhandeln. In den Worten der Erwägungsgründe werden sie so zu »informed counterparties in the data economy«.[596] Primäres Ziel der Proposition 24 war damit nicht, Verbraucher:innen vor jedem Risiko zu schützen, sondern ihnen mehr Kontrolle über ihre persönlichen Informationen zu geben.

Wenn deswegen die persönlichen Informationen reicher Verbraucher:innen anfangs besser geschützt sind, nimmt das der CCPA in Kauf. Dies ist ohnehin ein eher begrenztes Problem: persönliche Informationen Reicher sind mehr wert. Bei der Erhebung persönlicher Informationen geht es in der Regel darum, die Entscheidung des jeweiligen Individuums oder einer Gruppe, der es angehört, zu beeinflussen. Einfluss auf Reiche ist inhärent wertvoller, da diese über mehr Mittel verfügen. Das führt dazu, dass die Befürchtung der Bürgerrechtsorganisationen, Arme würden mit ihren Daten und Reiche mit Geld zahlen, nicht realistisch ist. Ein solches System wäre inhärent instabil, da nur Nutzer, deren Daten nicht werthaltig sind, sich für das Modell »Leistung gegen Daten« entscheiden würden. Diese Instabilität auszulösen, ist gerade auch ein Motiv des CCPA. Wenn sich immer mehr Verbraucher:innen gegen eine Monetarisierung ihrer persönlichen Informationen entscheiden, wird langfristig das Geschäftsmodell »Leistung gegen Daten« zurückgehen. Mit *Soltani, Hoofnagle* und *Mactaggart* haben drei der wichtigsten Autoren und Ideengeber für die Ausarbeitung der Proposition 24 betont, dass die Ausnahme für finanzielle Anreize zukünftig wahrscheinlich nicht mehr nötig sein werde.[597] Der CCPA erzwingt das Ende von »Leistung gegen Daten« aber nicht, sondern baut auf die freie Entscheidung der Verbraucher:innen.

---

[594] Proposition 24 (Cal. 2020), Sec. 2(F).

[595] Proposition 24 (Cal. 2020), Sec. 2(G).

[596] Proposition 24 (Cal. 2020), Sec. 2(G).

[597] *Angwin*, The Markup, Tech on the Ballot: Interview with Ashkan Soltani; *Bracy*, The Privacy Advisior Podcast, Alastair Mactaggart on California's Prop 24, 24m:55s; *Hoofnagle*, Comments on the CCPA. Zu ihrer jeweiligen Rolle siehe Kapitel 2:C.I (ab S. 30) und siehe Kapitel 2:C.IV (ab S. 35).

c) Vergleich mit europäischem Datenschutzrecht

Das Maßregelungsverbot des CCPA ist mit dem Grundsatz von Treu und Glauben nach Art. 5 Abs. 1 lit. a Alt. 2 DSGVO und dessen Ausprägung in Art. 12 Abs. 2 DSGVO vergleichbar.[598] Der Verantwortliche soll nach Art. 12 Abs. 2 DSGVO die Ausübung der Rechte gemäß Art. 15–22 DSGVO erleichtern. Er darf insbesondere betroffene Personen nicht an der Ausübung ihrer Rechte hindern, indem er sie irreführt oder mit zusätzlichen Kosten belastet.[599]

Der Grundsatz von Treu und Glauben nach Art. 5 Abs. 1 lit. a Alt. 2 DSGVO füllt Lücken, die Art. 12 Abs. 2 DSGVO lässt. Dieser Grundsatz geht auf Art. 8 Abs. 2 GRCh zurück und unterstreicht als Ausprägung des Verhältnismäßigkeitsgrundsatzes die grundrechtliche Determinierung des europäischen Datenschutzrechts. Der Verantwortliche muss Rücksicht auf die Interessen der betroffenen Person nehmen.[600] Der Verantwortliche darf nicht das Vertrauen der betroffenen Person missbrauchen oder ihre Fehlvorstellungen ausnutzen.[601] Art. 5 Abs. 1 lit. a Alt. 2 DSGVO ist damit ein selbstständig durchsetzbarer Auffangtatbestand.[602] Dies kommt einem Maßregelungsverbot sehr nahe. So ist eine Maßregelung von betroffenen Personen für die Ausübung ihrer Rechte nach Art. 15–22 DSGVO zugleich ein Verstoß gegen Art. 5 Abs. 1 lit. a Alt. 2 DSGVO, da der Verantwortliche nicht mit der gebotenen Rücksicht handelt.

Die Regelung finanzieller Anreize hat dagegen kein Äquivalent in der DSGVO. Noch am ehesten ist das Koppelungsverbot des Art. 7 Abs. 4 DSGVO vergleichbar.[603] Hiernach ist bei der Freiwilligkeit der Einwilligung im »größtmöglichen Umfang« zu berücksichtigen, ob der Verantwortliche die Vertragserfüllung davon abhängig macht, dass die betroffene Person in eine für die Vertragserfüllung nicht erforderliche Verarbeitung einwilligt. Dies spiegelt die grundsätzliche Skepsis des europäischen Gesetzgebers gegenüber diesem Geschäftsmodell »Leistung gegen Daten«, das zwar Ausdruck der Privatautonomie, aber mit einem stark grundrechtlich geprägten Datenschutz nur schwer vereinbar ist.[604] Das Koppelungsverbot war im Gesetzgebungsverfahren heftig umstritten, sodass am Ende nur der kryptische Art. 7 Abs. 4 DSGVO aufgenommen wurde.[605] Eine eingehende Sonderregelung für das Geschäftsmodell »Leistung gegen Daten« existiert nicht.

---

[598] *Davis*, 24 N.C. Banking Inst. 499, 522.

[599] *Eßer* in: Eßer/Kramer/Lewinski, DSGVO Art. 12 Rn. 20.

[600] *Schantz* in: BeckOK DatenschutzR, DS-GVO Art. 5 Rn. 8; *Spindler/Dalby* in: Spindler/Schuster, DS-GVO Art. 5 Rn. 5; *Weichert* in: Däubler et al., EU-DSGVO Art. 5 Rn. 18.

[601] *Schantz* in: BeckOK DatenschutzR, DS-GVO Art. 5 Rn. 8.

[602] *Herbst* in: Kühling/Buchner, DS-GVO Art. 5 Rn. 17; *Kramer* in: Eßer/Kramer/Lewinski, DSGVO Art. 5 Rn. 13. a. A. *Härting*, Datenschutz-Grundverordnung, Rn. 89.

[603] Siehe Kapitel 4:B.II.2.a) (ab S. 245).

[604] Siehe Kapitel 4:B.II.1 (ab S. 243).

[605] Siehe Kapitel 4:B.II.2.a) (ab S. 245).

Auch im Telemediendatenschutz fehlt eine Regelung für das Geschäftsmodell »Leistung gegen Daten«. Die Einwilligung für die Speicherung von Informationen (insbesondere Cookies) in der Endeinrichtung des Endnutzers muss gemäß § 25 Abs. 1 S. 2 TTDSG nach den Vorgaben der DSGVO erfolgen. Daher gilt das unzureichende Koppelungsverbot (Art. 7 Abs. 4 DSGVO) ebenso für die Einwilligung nach dem TTDSG.

d) Vergleich mit europäischem und deutschem Datenschuldrecht

Die Digitale-Inhalte-RL und deren Umsetzung in §§ 327–327u BGB enthält ebenfalls keine befriedigende Lösung für Zulässigkeit von »Leistung gegen Daten«. Erwägungsgrund 24 S. 3 der Digitale-Inhalte-RL spricht die ambivalente Haltung des europäischen Gesetzgebers zu diesem Geschäftsmodell besonders deutlich aus: er erkenne zwar »in vollem Umfang« an, dass Datenschutz »ein Grundrecht ist und daher personenbezogene Daten nicht als Ware betrachtet werden können«. Dennoch behandelt die Digitale-Inhalte-RL »Leistung gegen Daten« implizit durchaus als zulässig.

Die Regelungen der Digitale-Inhalte-RL und §§ 327–327u BGB sind nach § 312 Abs. 1a BGB und Art. 3 Abs. 1 UAbs. 2 Digitale-Inhalte-RL auf Verträge anwendbar, bei denen der Verbraucher[606] personenbezogene Daten bereitstellt oder deren Bereitstellung zusagt. Davon ausgenommen sind hiernach für die Vertragserfüllung oder zur Erfüllung rechtlicher Anforderungen erforderliche Verarbeitungen personenbezogener Daten. Diese Definition erinnert an die finanziellen Anreize des CCPA. Genauso wie diese ist sie weit zu verstehen. So sind genauso wie bei dem CCPA[607] auch nicht nur »typenreine« Angebote erfasst, sondern auch Angebote, bei denen der Verbraucher teilweise einen Preis zahlt und teilweise die Bereitstellung personenbezogener Daten zusagt.[608] Anders als unter dem CCPA sind Cookies nicht umfasst, da bei einem bloßen Webseitenbesuch der Rechtsbindungswille fehle (Erwägungsgrund 25 S. 3 der Digitale-Inhalte-RL). Dies ist konsequent, da die Digitale-Inhalte-RL weitgehend nur Regelungen zu Leistungsstörungen enthält, die für Webseitenbesuche kaum geeignet sind.

Inhaltlich enthält die Digitale-Inhalte-RL und die §§ 327–327u BGB nur an die Verbrauchergüterkauf-RL erinnernde Leistungsstörungsrechte für solche Verträge.[609] Die Zulässigkeit überlassen sie dem Datenschutzrecht, das aber hierzu auch keine eingehende Lösung enthält. *De lege ferenda* sollte der europäische Gesetzgeber die Zulässigkeit des Geschäftsmodell »Leistung gegen Daten« regeln. Die Regelung finanzieller Anreize bietet hierzu ein gut geeignetes Vorbild.[610]

---

[606] Insoweit nicht geschlechtergerecht formuliert wegen des Gesetzeswortlauts.

[607] Cal. Civ. Code § 1798.125(b)(1): »different price«.

[608] Erwägungsgrund 67 S. 3 der Digitale-Inhalte-RL.

[609] Näher siehe Kapitel 4:B.II.2.c) (ab S. 250).

[610] Siehe Kapitel 4:B (ab S. 241)..

II. Recht auf Beschränkung sensibler Informationen

1. Definition sensibler Informationen

a) Darstellung

Seit Proposition 24[611] kennt der CCPA ein Recht auf Beschränkung sensibler Informationen (»right to limit use and disclosure of sensitive personal information«).[612] Dieses ist ähnlich dem Widerspruchsrecht gegen Datenhandel als Recht ausgestaltet, das Verbraucher:innen pauschal gegenüber jedem Unternehmen ausüben sollen.

Die Unterscheidung zwischen sensiblen und nicht-sensiblen persönlichen Informationen hat deutliche Vorläufer im amerikanischen Datenschutzrecht. So hat sich die Rechtsprechung bei Auskunftsverlangen unter dem Freedom of Information Act häufig daran orientiert, ob die herausverlangten Dokumente sensible personenbezogene Informationen enthalten.[613] Zudem stellt der Biometric Information Privacy Act, den der Bundesstaat Illinois bereits 2008 verabschiedet hat, hohe Anforderungen an die Nutzung biometrischer Informationen.[614] Er verbietet es privaten Stellen, biometrische Informationen an Dritte zu übermitteln, außer wenn der Betroffene eingewilligt hat oder die private Stelle dazu gesetzlich oder aufgrund einer gerichtlichen Anordnung verpflichtet ist.[615] Er war Grundlage vielfacher Sammelklagen, bei denen die Kläger:innen teils Schadensersatz in dreistelliger Millionenhöhe erstritten.[616] Auch Florida, Texas und Washington haben für biometrische Informationen ähnliche Gesetze verabschiedet (Kalifornien hat sich dem angeschlossen, allerdings erst nach der Abstimmung über Proposition 24).[617]

Der CCPA schützt demgegenüber nicht nur biometrische Informationen, sondern umfassender sensible Informationen (»sensitive personal information«).[618] Der Begriff ist weit gefasst. Zuerst muss eine sensible Information immer auch persönliche Information sein.[619] Damit gilt insbesondere auch die Ausnahme für öffentliche Informationen.[620] Die geschützten Informationsarten kann man wie folgt kategorisieren: höchstpersönliche Information, genetische oder

---

[611] Zu diesem Volksbegehren siehe Kapitel 2:C.IV (ab S. 35).

[612] Cal. Civ. Code § 1798.121.

[613] *U. S. Department of Justice*, Guide to the Freedom of Information Act: Exemption 6, S. 480–482 m. w. N.

[614] 740 Ill. Comp. Stat. § 14/1–25.

[615] 740 Ill. Comp. Stat. § 14/15(b).

[616] Insbesondere U. S. Court of Appeals 9th Circuit vom 08.08.2019, *Patel v. Facebook, Inc.*, 932 F.3d 1264 mit einer Schadensersatzsumme von 650.000.000 $. Vgl. die diesbezügliche Rechtssprechungsauswertung in *Haley*, 95 Wash. L. Rev. 1193, 1232–1236.

[617] California Genetic Information Privacy Act, Cal. Civ. Code § 56.18–186; Florida Protecting DNA Privacy Act, Fla. Stat. § 760.40, 817.5655. Ohne Namen: Tex. Bus. & Com. Code Ann. § 503.001; Wash. Rev. Code § 40.26.020.

[618] Cal. Civ. Code § 1798.140(ae).

[619] Cal. Civ. Code § 1798.140(ae) a. A.

[620] Cal. Civ. Code § 1798.140(ae)(3). Zu dieser siehe Kapitel 3:B.I.3 (ab S. 50).

biometrische Informationen, Identitätsdiebstahl ermöglichende Informationen, genaue Standortdaten und Kommunikationsinhalte.

Als höchstpersönliche Informationen sind besonders diskriminierungsanfällige Informationen durch die Definition umfasst. Zuerst sind die Informationen umfasst, welche rassische oder ethnische Herkunft, die Religion, die Weltanschauung und die Gewerkschaftszugehörigkeit offenlegen.[621] Weiterhin sind persönliche Informationen ebenfalls sensible Informationen, wenn sie das Unternehmen im Hinblick auf Gesundheit, Sexleben oder sexueller Orientierung erhebt und analysiert.[622]

Ebenfalls sind »genetic data« erfasst.[623] Diese sind im CCPA nicht näher bestimmt. Andere amerikanische Gesetze definieren den parallelen Begriff »genetic information« als das Ergebnis eines Gentests des Individuums oder seiner Familienmitglieder, eine Häufung von Krankheiten bei Familienmitgliedern oder die Tatsache der Inanspruchnahme von Gentests oder genetischer Beratung.[624] Dies gibt zumindest einen gewissen Anhaltspunkt, wobei eine abweichende Beurteilung durch Gerichte aufgrund der schwächeren Rolle der systematischen Auslegung möglich ist.

Weiterhin sind biometrische Informationen sensible Informationen, wenn das Unternehmen sie dazu nutzt, bestimmte Verbraucher:innen zu identifizieren.[625] Biometrische Informationen sind im CCPA legaldefiniert als physiologische, biologische oder verhaltensbasierte Merkmale, die allein oder in Kombination mit anderen Merkmalen dazu genutzt werden können, bestimmte Verbraucher:innen zu identifizieren.[626] Dies konkretisiert der CCPA noch durch 17 Regelbeispiele (unter anderem Fingerabdruck und Gangmuster).[627]

Zudem sind folgende sensible Informationen geschützt, weil sie einen Identitätsdiebstahl ermöglichen:[628]

- Sozialversicherungsnummer[629]
- Ausweisnummer eines Führerscheins, sonstigem staatlichen Ausweises oder Passes[630]
- Kombination aus einem Benutzerkonto, Bankkonto, EC-Kartennummer oder Kreditkartennummer mit den dafür erforderlichen Passwort, PIN oder sonstigen Zugangsdaten[631]

---

[621] Cal. Civ. Code § 1798.140(ae)(1)(D).

[622] Cal. Civ. Code § 1798.140(ae)(2)(B),(C).

[623] Cal. Civ. Code § 1798.140(ae)(1)(F).

[624] Genetic Information Nondiscrimination Act of 2008, 29 USC § 1191b(d)(6); HIPAA, 45 C.F.R. § 160.103.

[625] Cal. Civ. Code § 1798.140(ae)(2)(A).

[626] Cal. Civ. Code § 1798.140(c).

[627] Cal. Civ. Code § 1798.140(c).

[628] Proposition 24 (Cal. 2020), Sec. 2(H): »allowing consumers to limit businesses' use of their sensitive personal information to help guard against identity theft«.

[629] Cal. Civ. Code § 1798.140(ae)(1)(A).

[630] Cal. Civ. Code § 1798.140(ae)(1)(A).

[631] Cal. Civ. Code § 1798.140(ae)(1)(B).

Identitätsdiebstahl ist in den Vereinigten Staaten ein wesentlich weiter verbreitetes Problem als in der EU. Amerikanische Unternehmen können Kund:innen nicht mittels eines zuverlässigen staatlichen Personalausweises identifizieren, sondern müssen sich auf die unsichere Identifizierung durch Angabe persönlicher Informationen verlassen. Die Einführung eines Personalausweises ist immer wieder auf große Widerstände gestoßen, da Bürger:innen eine Massenüberwachung durch ein zentrales Personalregister befürchteten.[632] Stattdessen füllt die Rolle eines Identitätsnachweises faktisch die Sozialversicherungsnummer aus, die dafür aber wenig geeignet ist.[633] So kennt jeder, gegenüber dem sich die Verbraucher:innen mit der Sozialversicherungsnummer identifiziert haben, nun diese und kann mit ihr eine andere Identität vortäuschen. Auch wird häufig mit der Kreditkartennummer gezahlt, ohne dass eine PIN oder die Vorlage der konkreten Kreditkarte erforderlich wäre.[634] Pro Jahr werden daher circa 10 % der amerikanischen Bevölkerung Opfer eines Identitätsdiebstahls.[635] Dies betrifft vor allem den Missbrauch einer Kreditkarte oder eines Bankkontos, in einem Zehntel der Fälle (also insgesamt 1 %) allerdings auch das Nutzen persönlicher Informationen für einen Vertragsschluss im Namen des Opfers.[636] Dementsprechend spielt Identitätsdiebstahl eine große Rolle in der amerikanischen Datenschutzdebatte. Viele Datenschutzgesetze schützen speziell Sozialversicherungsnummern.[637] Identitätsdiebstahl ist ein so universelles Problem, dass amerikanische Politiker:innen Identitätsdiebstahl nutzen, um Bürger:innen die Bedeutung des Datenschutzes näher zu bringen.[638]

Die nächste Kategorie sensibler Informationen sind genaue Standortdaten (»precise geolocation«): Daten, die den Aufenthaltsort bestimmter Verbraucher:innen näher als circa 1 km² eingrenzen, und die ein Gerät automatisch erzeugt.[639] Die Begrenzung auf 1 km² soll verhindern, dass Unternehmen Bewegungsprofile von Nutzern erzeugen.[640] Dementsprechend bezieht sich der Begriff auf den aktuellen Aufenthaltsort des Verbrauchers, nicht aber auf dessen

---

[632] Exemplarisch zu dieser Kritik: *American Civil Liberties Union*, American Civil Liberties Union, 5 Problems with National ID Cards.

[633] *Marcus*, 68 Duke L. J. 555, 563–565.

[634] *Hadar*, Washington Post, Think your credit card is safe in your wallet?

[635] *Harrell*, U. S. Department of Justice: Victims of Identity Theft, 2016, S. 1; Vgl. zur Entwicklung in 2017–2019: *FTC*, Consumer Sentinel Network Data Book 2020, S. 15.

[636] *Harrell*, U. S. Department of Justice: Victims of Identity Theft, 2016, S. 5.

[637] Cal. Civ. Code §§ 1749.64, 1798.85(a); Cal. Civ. Proc. Code § 674(a)(6); Cal. Gov. Code § 27301(a); Cal. Lab. Code § 226(a)(7).

[638] *Dodd*, Virtual Town Hall – The Future of Privacy, 29m:40s. *Dodd* hat mit *Chau* und *Hertzberg* den CCPA-2018 in das kalifornische Parlament eingebracht.

[639] Definiert als die Fläche eines Kreises mit einem Radius von 1850 Fuß (Radius: 563,88 m; Fläche: 998.902,85 m²), Cal. Civ. Code § 1798.140(w). Warum dieser Wert gewählt wurde, ist unklar.

[640] *Californians for Consumer Privacy*, Prop 24 Limits the Tracking of Geolocation. Zu der zulässigen Nutzung ungenauer Ortsdaten für nicht-personalisierte Werbung siehe Kapitel 3:B.II.3 (ab S. 65).

Wohnort: die bloße Postanschrift ist nicht erfasst.[641] Standortdaten gelten im amerikanischen Recht als besonders missbrauchsanfällig. Daher schützt der Children's Online Privacy Protection Act speziell Standortdaten,[642] und ein einflussreicher FTC-Bericht von 2012 erwähnt »precise geolocation« in seiner Definition sensibler Daten.[643] Der CCPA übernimmt an anderen Stellen explizit Teile des Children's Online Privacy Protection Acts[644] und dieses FTC-Berichts,[645] sodass ein Einfluss auch hier nahe liegt.

Weiterhin sind sensible Informationen der Inhalt der Briefpost, E-Mails und sonstigen Textnachrichten des Verbrauchers, wenn das Unternehmen nicht selbst intendierter Empfänger der Nachricht ist.[646] Nicht erfasst sind dagegen Metadaten. Auch der Electronic Communications Privacy Act trifft eine solche Unterscheidung zwischen geschützten Kommunikationsinhalten und ungeschützten Metadaten.[647]

Bei allen sensiblen Informationen ist Auswertungsabsicht erforderlich, damit das Beschränkungsrecht greift.[648] So sind z. B. Videoüberwachungsbilder keine sensiblen Informationen, selbst wenn sich aus der Aufnahme einer Brillenträgerin die Gesundheitsinformation Fehlsichtigkeit schließen lässt.[649] Dies soll die California Privacy Protection Agency in der neuen Durchführungsverordnung noch konkretisieren, um nur nebensächliche, zufällige Verarbeitungen sensibler Informationen auszuschließen und gleichzeitig eine Umgehung des Beschränkungsrechts zu verhindern.[650]

b) Vergleich mit Art. 9, 10 DSGVO

Dagegen erfasst Art. 9 DSGVO nach der Rechtsprechung des EuGH auch Informationen, die nur mittels gedanklicher Ableitung oder unter Rückgriff auf Zusatzwissen Rückschlüsse auf besondere Kategorien personenbezogener Daten erlauben.[651] Damit ist die Reichweite des Art. 9 DSGVO deutlich weiter, da zahlreiche Informationen Rückschlüsse auf Daten im Sinne des Art. 9 Abs. 1

---

641 Cal. Civ. Code § 1798.185(a)(13).

642 16 C. F. R. 312.2 (9).

643 *FTC*, Protecting Consumer Privacy in an Era of Rapid Change, S. 59.

644 Bei dem Einwilligungsvorbehalt für Minderjährige siehe Kapitel 3:C.I.3 (ab S. 98).

645 Bei der Definition deidentifizierter Informationen, siehe Kapitel 3:B.I.2 (ab S. 47).

646 Cal. Civ. Code § 1798.140(ae)(a)(E).

647 18 U. S. C. § 2511(1)(C)–(E).

648 Cal. Civ. Code § 1798.121(d).

649 *Californians for Consumer Privacy*, Annotated Text of the CPRA, § 1798.121(d).

650 Cal. Civ. Code § 1798.185(a)(19)(C).

651 EuGH vom 01.08.2022 – C-184/20, *Vyriausioji tarnybinės etikos komisija*, ECLI:EU:C:2022:601, Rn. 122–127; OLG Frankfurt a. M. vom 06.09.2018 – 16 U 193/17, GRUR 2018, 1283 Rn. 56 (jedenfalls für Gesundheitsdaten); *Albers/Veit* in: BeckOK DatenschutzR, DS-GVO Art. 9 Rn. 21–22; *Frenzel* in: Paal/Pauly, DS-GVO Art. 9 Rn. 8 f.; a. A. VG Mainz vom 24.09.2020 – 1 K 584/19.MZ, ZD 2021, 336 Rn. 29; *Britz/Indenhuck/Langerhans*, ZD 2021, 559, 562 f. (unter zusätzlicher Berücksichtigung objektiver Kriterien); *Majetek/Mäusezahl*, ZD

DSGVO erlauben (z. B. im vom EuGH entschiedenen Fall: vom Namen des Lebenspartners oder der Lebenspartnerin auf die sexuelle Orientierung).

Die besonderen Kategorien des Art. 9 Abs. 1 DSGVO stimmen sonst in weiten Teilen mit den sensiblen Informationen des CCPA überein. So umfassen beide Definitionen Informationen, aus welchen die rassische oder ethnische Herkunft, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie Daten zum Sexualleben und der sexuellen Orientierung, Gesundheitsdaten, genetische und biometrische Daten. Diese Begriffe entlehnt der CCPA offensichtlich aus der DSGVO, da der Wortlaut nahezu vollständig übereinstimmt.

Die einzige im CCPA fehlende Kategorie sind politische Meinungen. Diese gelten in den Vereinigten Staaten nicht als besonders sensibel – so können auch Private das Wählerregister einsehen, das Angaben zur bevorzugten Partei enthält.[652] Im Gegensatz dazu waren bereits vor Inkrafttreten der DSRL politische Meinungen in Datenschutzgesetzen europäischer Staaten übereinstimmend als sensible personenbezogene Daten besonders geschützt.[653] Hier wirkt sich die größere Transparenz als Leitmotiv des CCPA aus.

Ebenso kennt der CCPA keine mit Art. 10 DSGVO vergleichbare Regelung. Eine solche wäre mit der weitgehenden Transparenz in amerikanischen Strafprozessen nicht vereinbar. So sind die Akten aus Strafverfahren grundsätzlich öffentlich einsehbar (mit Ausnahme der Jugendstrafverfahren),[654] und jeder kann den Wohnort von Sexualstraftäter:innen in einem öffentlichen Register nachsehen.[655]

Hingegen erfasst Art. 9 Abs. 1 DSGVO keine einen Identitätsdiebstahl ermöglichende Informationen. Hierin wirkt sich aus, dass Identitätsdiebstahl in Europa weniger verbreitet ist. In Europa ermöglichen Personalausweise eine zuverlässige Identifizierung, ohne personenbezogene Daten abzugleichen. Erwägungsgrund 75 der DSGVO nennt zwar Identitätsdiebstahl als Risiko unter vielen anderen. Dieses Risiko spielt aber nur eine geringe Rolle. Wenn Identitätsdiebstahl in der Literatur diskutiert wird, dann aus technischer Perspektive (Benutzerverwaltung)[656] und aus rechtlicher Perspektive vor allem im Stellvertretungsrecht.[657]

Genaue Standortdaten umfasst Art. 9 Abs. 1 DSGVO ebenso nicht. Sie gelten allerdings als besonders risikobehaftet, was als Faktor in der Interessensabwägung

---

2019, 551, 552 f.; *Mester* in: Taeger/Gabel, DS-GVO Art. 9 Rn. 10; *Schneider/Schindler*, ZD 2018, 463, 467; *Spindler/Dalby* in: Spindler/Schuster, DS-GVO Art. 9 Rn. 4.

[652] Cal. Elec. Code §§ 2194(a)(3).

[653] *Ellger*, Datenschutz im grenzüberschreitenden Datenverkehr, S. 410.

[654] Cal. Rules of Court, Rule 2.503(a). Ausnahme für Jugendstrafverfahren: Cal. Rules of Court, Rule 5.552.

[655] Cal. Sex Offender Registration Act, Cal. Pen. Code § 290–294.

[656] *Jandt/Steidle*, Datenschutz im Internet, Rn. 376–382; *Schmedt*, DÄ 2020, 7, 7. Vgl. aus technischer Sicht: *BSI*, Die Lage der IT-Sicherheit in Deutschland 2021, S. 24–26.

[657] Sog. Handeln unter fremden Namen, dazu *Spindler* in: Spindler/Schuster, BGB § 164 Rn. 4 f.

gemäß Art. 6 Abs. 1 S. 1 lit. f DSGVO und in der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO zu berücksichtigen ist.[658] Für Telekommunikationsanbieter enthält § 13 TTDSG eine Sondervorschrift, die Art. 9 ePrivacy-RL umsetzt: sie dürfen Standortdaten nur auf Basis einer Einwilligung oder anonymisiert für Dienste mit Zusatznutzen verarbeiten.

Auch regeln § 3 TTDSG und Art. 5 Abs. 1 ePrivacy-RL für Telekommunikationsanbieter eine besondere Vertraulichkeit der – auch von den sensiblen Informationen des CCPA erfassten – Kommunikationsinhalte. Art. 9 DSGVO nennt dagegen keine Kommunikationsinhalte, da sie im Bereich der Vertraulichkeit der Telekommunikation nur nachrangig gegenüber der ePrivacy-RL anwendbar ist (Art. 95 DSGVO).

Insgesamt orientiert sich der CCPA zwar an der Definition besonderer Kategorien personenbezogener Daten des Art. 9 Abs. 1 DSGVO, passt diese aber durch zusätzliche Kategorien an das amerikanische Recht an. Die Definition sensibler Informationen des CCPA ist damit deutlich weitergehend. Besonders Zugangsdaten als Unterfall der einen Identitätsdiebstahl ermöglichenden Informationen betreffen jedes Unternehmen, das ein Kundenkonto anbietet.

2. Reichweite und Ausübung

Verbraucher:innen sollen das Recht auf Beschränkung sensibler Informationen pauschal gegenüber jedem Unternehmen leicht ausüben können. Die Ausübung ist parallel zu dem Widerspruchsrecht gegen Datenhandel ausgestaltet.[659] Unternehmen müssen einen Link »Limit the Use of My Sensitive Information« prominent auf ihrer Webseite platzieren.[660] Jedes Unternehmen ist verpflichtet, einen Beschränkungsantrag durch ein automatisches Beschränkungssignal zu akzeptieren.[661] Ebenso können Datenschutzagenturen im Auftrag der Verbraucher:innen das Recht ausüben.[662]

Nach Ausübung des Beschränkungsrechts ist das Unternehmen auf bestimmte unproblematische Nutzungen beschränkt. Dann darf ein Unternehmen sensible Informationen nur noch nutzen oder weitergeben, soweit dies aus Sicht durchschnittlicher Verbraucher:innen erforderlich ist für die:

– Vertragserfüllung[663]
– Qualitätssicherung/Produktverbesserung[664]

---

[658] *Artikel-29-Datenschutzgruppe*, WP 185 Geolokalisierungsdienste, passim; *Scheja* in: Taeger/Gabel, DS-GVO Art. 35 Rn. 20; ähnlich zu Kontaktverfolgungs-Apps: *EDSA*, Leitlinien 04/2020 Kontaktnachverfolgung Rn. 9–23.

[659] Zu diesem siehe Kapitel 3:C.I.2.b) (ab S. 86).

[660] Cal. Civ. Code § 1798.135(a)(2).

[661] Cal. Civ. Code § 1798.135(e).

[662] Cal. Civ. Code § 1798.135(e).

[663] Cal. Civ. Code § 1798.121(a).

[664] Cal. Civ. Code § 1798.121(a) i. V. m. Cal. Civ. Code § 1798.140(e)(8).

– Gewährleistung der Sicherheit und Integrität[665]
– Nutzung einer Unternehmensdienstleistung (z. B. Zahlungsdienstleister)[666]
– nur kurzfristige und vorübergehende Nutzung (ohne dauerhafte Speicherung)[667]

Neben diesen spezifischen Ausnahmen greifen die allgemeinen Bereichsausnahmen des CCPA, insbesondere Verteidigung gegen Rechtsansprüche oder Erfüllung einer Rechtspflicht.[668] Das Unternehmen muss zudem Dienstleister anweisen, ihre Verarbeitung persönlicher Informationen ebenso zu beschränken.[669]

Darüber hinaus ist eine Nutzung nur zulässig, soweit die Verbraucher:innen aktiv und freiwillig einwilligen.[670] Eine Gewährung finanzieller Anreize für diese Einwilligung ist nicht zulässig.[671] Sie würde gegen das Maßregelungsverbot verstoßen.[672] Die Ausnahme für finanzielle Anreize vom Maßregelungsverbot erfasst gerade nur das Widerspruchsrecht gegen Datenhandel und das Recht auf Löschung, nicht aber das Recht auf Beschränkung sensibler Informationen.[673] Ob dies wirklich intendiert war, ist unklar. Dennoch nimmt der CCPA einen beachtlichen Teil der persönlichen Informationen von einer Kommerzialisierung aus.

Die Anforderungen an die Nutzung besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 1, 2 DSGVO sind wesentlich höher. Die Verarbeitung der besonderen Kategorien ist hiernach nur zulässig, wenn die betroffene Person ausdrücklich einwilligt (Art. 9 Abs. 1 lit. a DSGVO) oder wenn eine der eng gefassten Ausnahmen des Art. 9 Abs. 1 lit. b–j DSGVO vorliegt. Die Mehrheit dieser engen Ausnahmen setzen ein verhältnismäßiges Gesetz voraus, das den Eingriff explizit gestattet (Art. 9 Abs. 1 lit. b, g–j).

Dagegen greift das Recht auf Beschränkung sensibler Informationen nur, wenn es die Verbraucher:innen ausüben. Insoweit wirkt sich der höhere Stellenwert der Meinungsfreiheit aus, die auch die Weitergabe persönlicher Informationen schützt.[674] Die zulässigen Nutzungsarten des CCPA sind zudem wesentlich weiter, da insbesondere die Vertragserfüllung genügt.[675] Die Ausnahmen des CCPA sind anders als bei Art. 9 Abs. 2 DSGVO nicht an ein Gesetz geknüpft, sondern beschreiben jeweils bestimmte Nutzungsarten ohne großes Missbrauchspotenzial. Gerade in diesem Gesetzesvorbehalt als typisches Element der Grundrechtsdogmatik zeigt sich, dass die DSGVO in weiten Teilen eine mittelbare

---

665 Cal. Civ. Code § 1798.121(a) i. V. m. Cal. Civ. Code § 1798.140(e)(2).
666 Cal. Civ. Code § 1798.121(a) i. V. m. Cal. Civ. Code § 1798.140(e)(5).
667 Cal. Civ. Code § 1798.121(a) i. V. m. Cal. Civ. Code § 1798.140(e)(4).
668 Siehe Kapitel 3:B.IV.1 (ab S. 74).
669 Cal. Civ. Code § 1798.121(c).
670 Cal. Civ. Code § 1798.121(b) a.E.
671 Zu finanziellen Anreizen siehe Kapitel 3:C.I.4.b) (ab S. 101).
672 Cal. Civ. Code § 1798.125(a)(1).
673 Cal. Civ. Code § 1798.125(b)(1).
674 Siehe Kapitel 2:A.I.2.a) (ab S. 10).
675 Kritisch dazu, dass diese unter der DSGVO fehlt: *Schneider*, ZD 2017, 303, 305 f.

Drittwirkung der Grundrechte regelt.[676] Der CCPA beschränkt sich dagegen vor allem darauf, Missbrauch zu verhindern.

Dennoch sind die Anforderungen des CCPA für sensible Informationen höher als bei Art. 6 DSGVO. So haben zwar die Rechtsgrundlagen der Einwilligung (Art. 6 Abs. 1 S. 1 lit. a DSGVO), der Vertragserfüllung (Art. 6 Abs. 1 S. 1 lit. b DSGVO) und der Rechtspflicht (Art. 6 Abs. 1 S. 1 lit. c DSGVO) jeweils ein Äquivalent in einer Ausnahme vom Beschränkungsrecht oder in einer allgemeinen Bereichsausnahme des CCPA.[677] Allein Art. 6 Abs. 1 S. 1 lit. d DSGVO ist ein Grenzfall. Diese Rechtsgrundlage hat zwar kein direktes Äquivalent im CCPA. Sie kommt allerdings der Ausnahme für eine Notfallauskunft an eine Behörde, wenn eine natürliche Person in einer Gefahr für Leib oder Leben ist, zumindest nahe.[678]

Vor allem aber kann der Verantwortliche auch auf Grundlage einer Interessensabwägung nach Art. 6 Abs. 1 S. 1 lit. f DSGVO personenbezogene Daten verarbeiten, die wesentlich weiter ist als die zulässigen Nutzungsarten des CCPA für sensible Informationen. Diese zulässigen Nutzungsarten des CCPA sind nur akzessorisch zur Vertragserfüllung (wie Kundendienst) und kaum »dehnbar«. Demgegenüber dürfen Verantwortliche auf Basis der Interessenabwägung nach Art. 6 Abs. 1 S. 1 lit. f DSGVO auch personenbezogenen Daten verarbeiten, wenn dies nicht unmittelbar für die Vertragserfüllung erforderlich ist – wie bei der explizit als zulässig deklarierten Direktwerbung (Erwägungsgrund 47 S. 7 der DSGVO).

III. Recht auf Auskunft

1. Reichweite

a) Darstellung

Das Auskunftsrecht des CCPA ist umfassend. Unternehmen müssen zahlreiche Informationen über ihre Nutzung persönlicher Informationen mitteilen und die konkreten persönlichen Informationen vorlegen (»right to access«).[679] Verbraucher:innen sollen durch Zugriff auf ihre persönlichen Informationen Kontrolle über diese erlangen.[680] Zudem beugt die so geschaffene Transparenz Missbrauch vor oder lässt ihn zumindest sichtbar werden.[681]

---

[676] *Veil*, NVwZ 2018, 686, 689.

[677] Art. 6 Abs. 1 S. 1 lit. a DSGVO: Cal. Civ. Code § 1798.121(b); Art. 6 Abs. 1 S. 1 lit. b DSGVO: Cal. Civ. Code § 1798.121(a) a. A.; Art. 6 Abs. 1 S. 1 lit. c DSGVO: Cal. Civ. Code § 1798.145(a)(1).

[678] Cal. Civ. Code § 1798.145(a)(4).

[679] Cal. Civ. Code §§ 1798.110(a),(b), 1798.115(a),(b).

[680] So die Erwägungsgründe in Proposition 24 (Cal. 2020), Sec. 3(A)(1). Vgl. zum Verhältnis datenschutzrechtlicher Auskunftsrechte zum *topos* der Kontrolle über die eigenen Daten: *Mahieu*, 2021 TechReg 62, 64–73.

[681] *Alpert*, 120 Colum. L. Rev. 1215, 1228.

Dieser Transparenzgedanke ist in der amerikanischen Rechtstradition weit verbreitet,[682] hat aber bisher nur zu begrenzten Auskunftsansprüchen gegen den Staat geführt. Der Federal Privacy Act regelt ein beschränktes Akteneinsichtsrecht gegenüber Bundesbehörden.[683] Dieses erfasst allerdings nur Akten über die jeweilige Person, die nach den Namen oder einem anderen Identifikationsmerkmal der Person geordnet sind.[684] Dieses nur gering ausgeprägte Auskunftsrecht hat dazu geführt, dass die Informationsfreiheitsgesetze[685] auch für Auskunftsanträge gegenüber dem Staat im privaten Interesse erhebliche Bedeutung gewonnen haben. Diese sind zwar für die demokratische Kontrolle des Staats durch die Öffentlichkeit gedacht – nicht dafür, dass Individuen Informationen über sich selbst anfordern. Tatsächlich stellen die große Mehrheit der Informationsfreiheitsanträge Individuen im eigenen Interesse.[686] Dies führt angesichts der darauf nicht zugeschnittenen Informationsfreiheitsgesetze dazu, dass Behörden unvollständig oder verzögert antworten.[687]

Für private Stellen bestehen außerhalb des CCPA nur noch engere Auskunftsansprüche. Individuen können Einsicht verlangen in Krankenakten,[688] Schülerakten[689] und Wirtschaftsauskunftei-Akten.[690] Diese gelten aber jeweils nur für Akten über die jeweilige Person und sind daher eher Akteneinsichtsrechte. Das Auskunftsrecht des Cable Communications Policy Act gegenüber Kabelfernsehanbietern umfasst zwar auch andere personenbezogene Informationen.[691] Es ist aber dennoch auf Akten zugeschnitten, weil es nur in Person ausgeübt werden kann.[692] Noch am ehesten mit dem Auskunftsrecht des CCPA vergleichbar ist das Auskunftsrecht für Direktwerbung des kalifornischen Shine the Light Act.[693] Privatkund:innen[694] können hiernach von einem Unternehmen Auskunft darüber verlangen, ob das Unternehmen deren Daten an Dritte für Direktwerbung übermittelt hat.[695] Wenn das Unternehmen Daten für Direktwerbung weitergegeben

---

[682] Siehe Kapitel 3:F.II (ab S. 226).

[683] 5 U. S. C. § 552a(b).

[684] 5 U. S. C. § 552a(d)(1) i. V m. § 552a(a)(4).

[685] Freedom of Information Act, 5 U. S. C. § 551–559; California Public Records Act, Cal. Gov. Code § 6520.

[686] *Alpert*, 120 Colum. L. Rev. 1215, 1237 f.; *Kwoka*, 127 Yale L. J. 2204, 2218–2243 mit einer umfassenden statistischen Auswertung.

[687] *Kwoka*, 127 Yale L. J. 2204, 2243–2255.

[688] HIPAA, 45 C. F. R. § 164.524(a)(1). Zum HIPAA Siehe Kapitel 2:B.I.2 (ab S. 19).

[689] FERPA, 20 U. S. C. § 1232g(a)(1)(A), 34 C. F. R. §§ 99.10–12.

[690] FCRA, 15 U. S. C. § 1681g(a).

[691] 47 U. S. C. § 551(d).

[692] 47 U. S. C. § 551(d).

[693] Cal. Civ. Code § 1798.83. Weiterführend zum faktischen Leerlaufen dieses Gesetzes: *Thomas/Hoofnagle*, Exploring Information Sharing through California's »Shine the Light« Law.

[694] Definition in Cal. Civ. Code § 1798.83(e)(1).

[695] Cal. Civ. Code § 1798.83(a).

hat, muss es zudem mitteilen, welche Kategorien an personenbezogenen Daten es übermittelt hat und an wen (samt deren Adresse).[696]

Das Auskunftsrecht des CCPA gilt dagegen unabhängig vom Verarbeitungszweck und erfasst deutlich mehr Informationen. Regelungstechnisch ist es in zwei Rechte aufgeteilt: einem Auskunftsrecht über die Erhebung und einem Auskunftsrecht über den Datenhandel.[697] Die Unterscheidung beruht wohl darauf, dass die Initiatoren des ursprünglichen Volksbegehrens die geschaffene Transparenz in der »Schattenwirtschaft« des Datenhandels durch ein eigenes Recht hervorheben wollten.[698] Bei beiden Rechten muss das Unternehmen größtenteils dieselben Informationen mitteilen (so erfasst z. B. das Auskunftsrecht über die Erhebung auch Informationen über die Weiterübermittlung an Dritte). Daher wird im Folgenden – wie in der Durchführungsverordnung[699] – nicht mehr zwischen beiden Auskunftsrechten unterschieden.

Zunächst muss ein Unternehmen die konkreten persönlichen Informationen mitteilen, die es über die jeweiligen Verbraucher:innen erhoben hat.[700] Dabei ist ein Unternehmen verpflichtet, auch bei Dienstleistern gespeicherte, persönliche Informationen bereitzustellen[701] und ein leicht verständliches Format zu wählen.[702] Ein Unternehmen darf aber bestimmte missbrauchsanfällige persönliche Informationen nicht übermitteln, um einen Identitätsdiebstahl zu verhindern.[703] Dies sind Sozialversicherungsnummern, Führerscheinnummern, staatliche Personenkennziffern, Krankenversicherungsnummern, Bankkontonummern, Passwörter, Sicherheitsfragen und deren Antworten sowie biometrische Informationen.[704] Stattdessen sollen Unternehmen bei diesen persönlichen Informationen schlagwortartig den Typ der erhobenen persönlichen Information angeben.[705] An solchen Informationen haben Verbraucher:innen typischerweise kein Interesse, da sie ohnehin über sie verfügen. Zudem birgt eine Übermittlung an Antragstellende immer das Risiko einer Fehlidentifizierung. Diese Liste der missbrauchsanfälligen persönlichen Informationen orientiert sich an denjenigen

---

[696] Cal. Civ. Code § 1798.83(a)(1),(2).

[697] Cal. Civ. Code §§ 1798.110, 1798.115.

[698] Vgl. den ursprünglichen Entwurf, der beschreibt, wie wenig Verbraucher:innen über den Handel mit ihren Daten wissen, und das Auskunftsrecht über Datenhandel als Lösung hierfür präsentiert: *Californians for Consumer Privacy*, The Consumer Right to Privacy Act of 2018, Sec. 2(E), 3(B).

[699] Regelungstechnisch geschickt durch eine Legaldefinition des »Request to know«, die auf beide Rechte verweist: 11 C. C. R. § 7001(r).

[700] Cal. Civ. Code §§ 1798.110(a)(5), 1798.130(a)(3)(B)(iii).

[701] Cal. Civ. Code § 1798.130(a)(3)(A).

[702] Cal. Civ. Code § 1798.130(a)(3)(B)(iii).

[703] 11 C. C. R. § 7024(d). Vgl. zur Auswahl der persönlichen Informationen: *Cal. Attorney General*, Initial Statement of Reasons, S. 25.

[704] 11 C. C. R. § 7024(d).

[705] 11 C. C. R. § 7024(d).

Informationen, bei denen Unternehmen in Kalifornien eine Datenpanne melden müssen.[706]

Überdies muss ein Unternehmen über folgendes informieren:

- Kategorien der erhobenen[707] persönlichen Informationen.[708] Dabei muss es die Kategorien der Regelbeispiele in der Definition für persönliche Informationen verwenden.[709] Dies erzielt eine ausreichende Genauigkeit, da die einzelnen Regelbeispiele (137) und nicht deren Oberbegriffe (12) maßgeblich sind.[710]
- Kategorien der Quellen, aus denen es die persönlichen Informationen erhalten hat[711]
- Zweck der Erhebung (schlagwortartig)[712]
- Für jede Kategorie persönlicher Informationen separat, inwieweit es diese an welche Kategorie von Dienstleistern oder Dritten weitergegeben hat.[713] Die gewählten Kategorien müssen aussagekräftig sein.[714] Weiterhin ist es verpflichtet, den Zweck einer solchen Weiterübermittlung kurz zu beschreiben.[715]
- Bei automatisierter Entscheidungsfindung und Profiling eine allgemeinverständliche Erklärung, welche Logik dieser Entscheidungsfindung zugrunde liegt und wie sich diese im konkreten Fall des Verbrauchers auswirken.[716] Profiling ist wie in Art. 4 Nr. 4 DSGVO definiert als jedes Auswerten persönlicher Aspekte, insbesondere das Analysieren oder Vorhersagen des Verhalten eines Verbrauchers.[717] Den genauen Umfang der diesbezüglich offenzulegenden Informationen und der Profilingdefinition soll die California Privacy Protection Agency in der Durchführungsverordnung konkretisieren.[718]

Gerade in den Informationen über automatisierte Entscheidungsfindung zeigt sich der Transparenzgedanke des CCPA: eine solche ist von außen nur schwer

---

[706] *Cal. Attorney General*, Initial Statement of Reasons, S. 26. Diese sind festgelegt in: Cal. Civ. Code § 1798.82(h).

[707] Erheben (»collect«) ist weit definiert und erfasst jedes Erhalten persönlicher Informationen, unabhängig von der Quelle, Cal. Civ. Code § 1798.140(f).

[708] Cal. Civ. Code §§ 1798.110(a)(1), 1798.115(a)(1), 1798.130(a)(3)(B)(ii), 11 C.C.R. § 7024(j)(1).

[709] Cal. Civ. Code § 1798.130(c).

[710] Ebenso wohl *Cal. Attorney General*, Summary and Response to Comments Submitted During 45-Day Period, S. 121: Beispiel »purchase history« für eine Kategorie persönlicher Informationen und nicht der Oberbegriff »commercial information« (Cal. Civ. Code § 1798.140(v)(1)(D)).

[711] Cal. Civ. Code §§ 1798.110(a)(2), 1798.130(a)(3)(B)(ii), 11 C.C.R. § 7024(j)(2).

[712] Cal. Civ. Code § 1798.110(a)(3), 1798.130(a)(3)(B)(ii), 11 C.C.R. § 7024(j)(2),(c).

[713] Cal. Civ. Code §§ 1798.110(a)(4), 1798.115(a)(2),(3), 1798.130(a)(3)(B)(ii), 11 C.C.R. § 7024(j)(5),(f).

[714] 11 C.C.R. § 7024(11).

[715] Cal. Civ. Code §§ 1798.110(a)(3), 1798.130(a)(3)(B)(ii), 11 C.C.R. § 7024(j)(3).

[716] Cal. Civ. Code § 1798.185(a)(16).

[717] Cal. Civ. Code § 1798.140(z).

[718] Cal. Civ. Code § 1798.185(a)(16).

zu durchblicken. Der Zwang, die dahinterstehende Logik zu erklären, erzeugt einen Rechtfertigungsdruck, nur sachgerechte Kriterien zu verwenden.[719] Ob ein solcher Druck tatsächlich entsteht oder ob sich Unternehmen in Allgemeinplätze flüchten können, hängt davon ab, wie die California Privacy Protection Agency die Durchführungsverordnung diesbezüglich ausgestalten wird.

Dieses umfassende Auskunftsrecht schränkt der CCPA durch detaillierte Ausnahmen ein, die Interessen des Unternehmens und anderer Verbraucher:innen dienen. Diese sind pauschalisiert: wenn eine Ausnahme greift, muss das Unternehmen nicht mehr abwägen. Bei Eingreifen einer Ausnahme ist das Unternehmen verpflichtet, die Gründe für die Ablehnung eines Auskunftsantrags mitzuteilen.[720] Bei einer nur teilweisen Ablehnung müssen Unternehmen die Informationen, die nicht von der Ausnahme erfasst sind, dennoch mitteilen und die nur begrenzte Auskunft begründen.[721] Die Ausnahmen dienen drei Zwecken: der Reduktion des Verwaltungsaufwands, dem Geheimhaltungsinteresse des Unternehmens oder den Interessen anderer Verbraucher:innen.

Um den Verwaltungsaufwand[722] zu reduzieren, muss ein Unternehmen Informationen nicht nochmals mitteilen, die es in den zuvor bereitgestellten, umfassenden Datenschutzerklärung bereits erteilt hat.[723] Das Unternehmen darf aber nur auf einen Abschnitt der Datenschutzerklärung verweisen, wenn sämtliche darin enthaltenen Informationen für den konkreten Verbraucher oder die konkrete Verbraucherin relevant sind.[724] Ein Unternehmen kann bei offensichtlich unbegründeten oder – insbesondere im Fall häufiger Wiederholung – exzessiven Anträgen entweder ein angemessenes Entgelt verlangen oder den Antrag ablehnen.[725] Als Konkretisierung der häufigen Wiederholung können Verbraucher:innen nur alle zwölf Monate Auskunft verlangen.[726] Parallel dazu ist ein Auskunftsantrag grundsätzlich so auszulegen, dass er sich nur auf die in den letzten zwölf Monaten vor Zugang erhobenen oder gehandelten persönlichen Informationen bezieht.[727] Wenn ein Verbraucher oder eine Verbraucherin dies ausdrücklich verlangt, muss das Unternehmen allerdings auch Auskunft hinsichtlich eines früheren Zeitraums erteilen.[728] Dies gilt nur dann nicht, wenn das Unter-

---

[719] Vgl. allgemein: *Kim/Routledge*, Why a Right to an Explanation of Algorithmic Decision-Making Should Exist, S. 13–27.

[720] Cal. Civ. Code § 1798.145(h)(2), 11 C.C.R. § 7024(e).

[721] 11 C.C.R. § 7024(e) a.E.

[722] *Californians for Consumer Privacy*, California Privacy Rights and Enforcement Act, S. 9; *Cal. Attorney General*, Initial Statement of Reasons, S. 19.

[723] Cal. Civ. Code § 1798.110(b), 11 C.C.R. § 7024(i).

[724] 11 C.C.R. § 7024(i).

[725] Cal. Civ. Code § 1798.145(h)(3).

[726] Cal. Civ. Code § 1798.130(b).

[727] Cal. Civ. Code § 1798.130(a)(2)(B), 11 C.C.R. § 7024(h).

[728] Cal. Civ. Code § 1798.130(a)(2)(B).

nehmen die länger zurückliegenden Informationen unmöglich zur Verfügung stellen kann oder dies nur mit unangemessenen hohem Aufwand möglich ist.[729]

Ein Unternehmen kann Archive außen vorlassen, wenn diese nur wegen einer gesetzlichen Aufbewahrungspflicht bestehen, schwer zugänglich sind und es diese nicht für den laufenden Geschäftsbetrieb nutzt (insbesondere nicht für Datenhandel).[730] In einem solchen Fall muss es aber über die Existenz eines solches Archivs informieren und abstrakt beschreiben, welche persönlichen Informationen darin möglicherweise enthalten sind.[731] Zudem sind bestimmte technische Informationen wie Systemprotokolle ausgenommen, soweit diese keine für Verbraucher:innen relevante Informationen enthalten – dies soll noch in der Durchführungsverordnung präzisiert werden.[732]

Andere Ausnahmen sind dadurch gerechtfertigt, dass das Unternehmen ein gewichtiges Geheimhaltungsinteresse an den ausgenommenen Informationen hat. Erstens sind alle Informationen ausgeschlossen, die unter ein Zeugnis- oder Aussageverweigerungsrecht des kalifornischen Rechts fallen.[733] Diese hat Kalifornien – untypisch für das *common law* – abschließend kodifiziert.[734] Der Umfang der kalifornischen Zeugnisverweigerungsrechte ist mit §§ 52–55 StPO, §§ 383, 384 ZPO vergleichbar und weicht nur in Details ab.[735]

Zweitens soll die California Privacy Protection Agency noch in die Durchführungsverordnung aufnehmen, dass ein Unternehmen keine Geschäftsgeheimnisse mitteilen muss.[736] Geschäftsgeheimnisse sind im kalifornischen Uniform Trade Secrets Act definiert als Informationen jeder Art, deren Geheimhaltung einen eigenständigen wirtschaftlichen Wert hat und die angemessenen Geheimhaltungsmaßnahmen unterliegt.[737] Diese Definition ähnelt der Geschäftsgeheimnis-Definition im deutschen Geschäftsgeheimnisgesetz, da die deutsche Definition auf das amerikanische Mustergesetz Uniform Trade Secrets Act zurückzuführen ist.[738]

Drittens ist ein Unternehmen nicht verpflichtet, persönliche Informationen offenzulegen, die es zur Wahrung der Informationssicherheit erzeugt hat.[739] Dies soll das Sicherheitskonzept des Unternehmens schützen und für Verbraucher:innen irrelevante Informationen ausschließen (beispielsweise technische Logdateien).[740]

---

[729] Cal. Civ. Code § 1798.130(a)(2)(B).

[730] 11 C.C.R. § 7024(c).

[731] 11 C.C.R. § 7024(c)(4).

[732] Cal. Civ. Code § 1798.185(a)(14).

[733] Cal. Civ. Code § 1798.145(b).

[734] Cal. Evid. Code § 911.

[735] Vgl. Cal. Evid. Code §§ 900–1070, 1115–1128, 1152.

[736] Cal. Civ. Code § 1798.185(a)(3).

[737] Cal. Civ. Code § 3426.1(d).

[738] *Partsch/Rump*, NJW 2020, 118, 119. Der Uniform Trade Secrets Act ist ein Mustergesetz, das auch in anderen Bundesstaaten existiert.

[739] Cal. Civ. Code § 1798.130(a)(3)(B)(iii).

[740] *Californians for Consumer Privacy*, Annotated Text of the CPRA, Cal. Civ. Code § 1798.130(a)(3)(B)(iii).

Viertens greift eine Ausnahme für Prüfungssituationen: ein Unternehmen muss Informationen nicht mitteilen, soweit durch die Informationen ein Prüfling Vorteile gegenüber anderen Prüflingen erlangen würde.[741] Dies gilt nur für Prüfungen, die im Rahmen einer staatlich anerkannten Ausbildung abgenommen werden oder die Eignung für eine solche Ausbildung feststellen sollen.[742] Dies schützt sowohl das Unternehmen als auch die anderen Prüflinge.

Ebenfalls im Interesse Dritter erstreckt sich das Auskunftsrecht nicht auf persönliche Informationen, die anderen natürlichen Personen gehören (»personal information about the consumer that belongs to […] another natural person«).[743] Damit sind nur persönliche Informationen ausgeschlossen, die im Konto anderer Verbraucher:innen gespeichert sind (wie E-Mails in einem fremden Postfach).[744] Im Gegensatz dazu sind persönliche Informationen, die sich auch auf andere Personen beziehen, grundsätzlich erfasst.

Allerdings hat Proposition 24 eine Ausnahme für haushaltsbezogene Informationen eingeführt, die das Unternehmen keiner konkreten Person im Haushalt zuordnen kann.[745] So soll verhindert werden, dass einzelne Verbraucher:innen aus einem Haushalt Informationen über andere Mitglieder ihres Haushaltes erlangen.[746] Diese Ausnahme ist übermäßig weit gefasst, da sie selbst bei gemeinsamen Handeln eines Haushalts einen Auskunftsanspruch ausschließt. Ein Ausgleich wäre möglich gewesen: der kalifornische Attorney General hatte in der Durchführungsverordnung bereits ausgewogen geregelt, wie Haushalte Auskunftsansprüche gemeinsam ausüben können (nach Einreichen der Proposition 24, aber vor der Abstimmung).[747] Diese Vorschrift der Durchführungsverordnung wird mit Inkrafttreten der Proposition 24 nun unwirksam.

Schließlich darf die Ausübung des Auskunftsrechts nicht die Rechte und Freiheiten anderer natürlicher Personen beeinträchtigen (»shall not adversely affect the rights and freedoms of other natural persons«).[748] Dieser Auffangtatbestand ist Art. 15 Abs. 4 DSGVO entlehnt, schränkt diesen aber deutlich ein, da er nur Interessen anderer natürlicher Personen erfasst – nicht aber juristischer Personen wie Unternehmen.

b) Vergleich mit Art. 15 DSGVO

Der Verantwortliche muss nach Art. 15 Abs. 1 DSGVO ähnliche Informationen über die Verarbeitungstätigkeit mitteilen. Allein die Informationen über einen Drittlandstransfer nach Art. 46 Abs. 2 DSGVO, welche das Auskunftsrecht

---

[741] Cal. Civ. Code § 1798.145(q)(2),(3)(B).
[742] Cal. Civ. Code § 1798.145(q)(2),(3)(A).
[743] Cal. Civ. Code § 1798.145(k).
[744] *Californians for Consumer Privacy*, California Privacy Rights and Enforcement Act, S. 33.
[745] Cal. Civ. Code § 1798.145(p). Zum Haushaltsbezug siehe Kapitel 3:B.I.1.a) (ab S. 43).
[746] *Californians for Consumer Privacy*, California Privacy Rights and Enforcement Act, S. 34.
[747] 11 C.C.R. § 7031.
[748] Cal. Civ. Code § 1798.145(k).

der DSGVO nach Art. 15 Abs. 2 DSGVO erfasst, muss das Unternehmen unter dem CCPA weder beauskunften noch proaktiv[749] mitteilen. Allerdings regelt der CCPA ohnehin Drittlandstransfers nicht. Ansonsten muss das Unternehmen nach dem CCPA aufschlüsseln, welcher Empfänger welche Kategorien persönlicher Informationen erhält, während nach der DSGVO eine pauschale Angabe aller Empfänger genügt. Näher ist dies in der folgenden Tabelle dargestellt:

Informationsart	*Erfasst nach CCPA[750]*	*Erfasst nach DSGVO*
Zwecke der Verarbeitung	Ja	Ja[751]
Kategorien der personenbezogenen Daten	Ja (vorgegebene Kategorien)	Ja (frei gewählte Kategorien)[752]
Empfänger	Ja (frei gewählte Kategorien aufgeschlüsselt nach Kategorien der persönlichen Informationen)	Ja (konkret oder frei gewählte Kategorien)[753]
Quellen	Ja (vorgegebene Kategorien)	Ja (konkret)[754]
Speicherfrist	Nein (aber in Informationspflichten)[755]	Ja[756]
Datenschutzrechte	Nein (aber in Informationspflichten)[757]	Ja[758]
Drittlandstransfer	Nein	Ja[759]
Logik einer automatisierten Entscheidungsfindung	Ja	Ja[760]

Tabelle 1: Unterschiede der Auskunftsrechte zwischen CCPA und DSGVO

[749] Zu den Informationspflichten siehe Kapitel 3:D.I (ab S. 150).
[750] Für die jeweiligen Fundstellen siehe Kapitel 3:C.III.1.a) (ab S. 116).
[751] Art. 15 Abs. 1 lit. a DSGVO.
[752] Art. 15 Abs. 1 lit. b DSGVO.
[753] Art. 15 Abs. 1 lit. c DSGVO. Es ist strittig, ob ein Wahlrecht besteht: Paal in: Paal/Pauly, DS-GVO Art. 15 Rn. 26 m. w. N. zum Streitstand.
[754] Art. 15 Abs. 1 lit. g DSGVO. Zur Auslegung als konkrete Quellenangabe: Dix in: NK-DatenschutzR, DS-GVO Art. 15 Rn. 24.
[755] Cal. Civ. Code § 1798.100(a)(3). Siehe Kapitel 3:D.I.2.a)aa) (ab S. 151).
[756] Art. 15 Abs. 1 lit. d DSGVO.
[757] Cal. Civ. Code §§ 1798.110(c)(5), 1798.130(a)(5)(A), 11 C.C.R. § 7011(c)(1)(A),(2)(A),(3)(A),(4)(A). Siehe Kapitel 3:D.I.2.b)aa) (ab S. 155).
[758] Art. 15 Abs. 1 lit. e, f DSGVO.
[759] Art. 15 Abs. 2 DSGVO.
[760] Art. 15 Abs. 1 lit. h DSGVO.

Größere Unterschiede bestehen bei den offenzulegenden, konkreten personenbezogenen Daten. Auch unter der DSGVO muss der Verantwortliche über die verarbeiteten personenbezogenen Daten informieren (Art. 15 Abs. 1 HS 2 DSGVO a. A.) und eine »Kopie« der konkreten personenbezogenen Daten bereitstellen (Art. 15 Abs. 3 S. 1 DSGVO). Der Detaillierungsgrad und das Verhältnis zwischen Art. 15 Abs. 1 und 3 DSGVO ist jedoch stark umstritten. Einigkeit besteht zumindest darin, dass Stammdaten wie Name, Kontaktdaten oder direkt auf die jeweilige Person bezogene Akten (wie Patientenakten)[761] bereitzustellen sind.[762] Ob interne Vermerke und zurückliegende Korrespondenz mit der betroffenen Person zu beauskunften sind, ist dagegen stark umstritten.[763] Das österreichische Bundesverwaltungsgericht, das finnische Itä-Suomen hallinto-oikeus und der BGH haben die Reichweite des Art. 15 Abs. 3 DSGVO dem EuGH vorgelegt.[764]

Der Ausschluss für missbrauchsanfällige Informationen, die Identitätsdiebstahl ermöglichen, hat kein Äquivalent unter Art. 15 DSGVO. Das Auskunftsrecht darf gem. Art. 15 Abs. 4 DSGVO die Rechte und Freiheiten »anderer« Personen nicht beeinträchtigen, dies gilt aber nicht für die betroffene Person. Die Öffnungsklausel des Art. 23 lit. i Alt. 1 DSGVO ermöglicht zwar den Mitgliedstaaten, das Auskunftsrecht zum Schutz der betroffenen Person zu beschränken. Deutschland hat von dieser Öffnungsklausel nur für Patientenakten Gebrauch gemacht, bei denen der Verantwortliche die Auskunft gem. § 630g Abs. 1 S. 1 Alt. 1 DSGVO aus therapeutischen Gründen verwehren kann.[765]

---

[761] Erwägungsgrund 63 S. 2 der DSGVO.

[762] Diese Minimalansicht vertretend: *LfDI Rheinland-Pfalz*, Tätigkeitsbericht zum Datenschutz 2019, S. 46f; *Zikesch/Sörup*, ZD 2019, 239, 240–243.

[763] Für extensive Auslegung: BGH vom 15.06.2021 – VI ZR 576/19, BeckRS 2021, 16831 Rn. 24–28; LAG Baden-Württemberg vom 20.12.2018, NZA-RR 2019, 242 Rn. 177 f.; OVG Münster vom 08.06.2021 – 16 A 1582/20, NRWE.de Rn. 96–144; *EDSA*, Guidelines 01/2022 Right of access, Rn. 25; *Bäcker* in: Kühling/Buchner, DS-GVO Art. 15 Rn. 40f; *Engeler/Quiel*, NJW 2019, 2201, 2203; *Korch/Chatard*, NZG 2020, 893, 895f; *Kremer*, CR 2017, 560, 563f; *Lembke*, NJW 2020, 1841, 1843f; *Schmidt-Wudy* in: BeckOK DatenschutzR, DS-GVO Art. 15 Rn. 85.

Für restriktive Auslegung: LAG Niedersachsen vom 09.06.2020 – 9 Sa 608/19, NZA-RR 2020, 571 Rn. 45; vom 22.10.2021 – 16 Sa 761/20, BeckRS 2021, 32008 Rn. 182; *Franzen*, NZA 2020, 1593, 1594; *Wybitul/Brams*, NZA 2019, 672, 674–676; *Zikesch/Sörup*, ZD 2019, 239, 240–243.

[764] BVwG (Österreich) vom 09.08.2021 – W211 2222613-2/12, Az. beim EuGH: C-487/21, *Österreichische Datenschutzbehörde und CRIF*, InfoCuria, Fragen 1, 2; Itä-Suomen hallinto-oikeus (Finnland) vom 22.09.2021 – 02034/20/1204, Az. beim EuGH: C-579/21 *Pankki S.*, InfoCuria, Frage 1; BGH vom 29.03.2022 – VI ZR 1352/20, Az. beim EuGH: C-307/22, FT, GRUR-RS 2022, 9584, Frage 3; vgl. noch zur DSRL, die kein explizites »Recht auf Kopie« kannte:EuGH vom 17.07.2014 – C-141/12, *YS u. a.*, ECLI:EU:C:2014:2081 Rn. 54–58.

[765] Die Frage, ob dieser mit der Art. 23 Abs. 1 lit. i DSGVO vereinbar ist, hat der BGH dem EuGH vorgelegt: BGH vom 29.03.2022 – VI ZR 1352/20, Az. beim EuGH: C-307/22, FT, GRUR-RS 2022, 258, Frage 2. Weiterführend: *Bäcker* in: Kühling/Buchner, DS-GVO Art. 23 Rn. 30; *Piltz/Zwerschke*, MedR 2021, 1070, 1074 f.; *Wagner* in: MükoBGB, BGB § 630g Rn. 4–6.

Diese Vorschrift ist allerdings kaum mit der Ausnahme für missbrauchsanfällige Informationen vergleichbar, da sie vor Gesundheitsgefahren[766] und nicht vor Identitätsdiebstahl schützen soll. Soweit ersichtlich, hat kein Mitgliedstaat Art. 23 lit. i Alt. 1 DSGVO genutzt, um Identitätsdiebstahl vorzubeugen. Hierin zeigt sich erneut das als geringer wahrgenommene Risiko eines Identitätsdiebstahls in Europa.[767]

Vergleichbar sind die Ausnahmen beider Auskunftsrechte hingegen, soweit sie dazu dienen, den Verwaltungsaufwand zu reduzieren und Interessen des Unternehmens und Dritter zu wahren. Die Ausnahme für offensichtlich unbegründete oder exzessive Anträge (Art. 12 Abs. 5 S. 2 DSGVO) hat der CCPA sogar wortlautgleich übernommen.[768] Zudem darf gem. Art. 15 Abs. 4 DSGVO das Auskunftsrecht[769] nicht Rechte und Freiheiten anderer Personen beeinträchtigten. Diese Ausnahme hat der CCPA ebenfalls übernommen, allerdings nur für natürliche Personen.[770] Für Geheimhaltungsinteressen von Unternehmen regelt der CCPA zu Art. 15 Abs. 4 DSGVO vergleichbare spezifischere Ausnahmen (beispielsweise für Geschäftsgeheimnisse). Auch ähneln die Ausnahmen des CCPA für Zeugnisverweigerungsrechte § 29 Abs. 1 S. 2 BDSG und für schwer zugängliche Archive § 34 Abs. 1 Nr. 2 BDSG.

2. Ausübung

a) Darstellung

Das Auskunftsrecht des CCPA soll leicht auszuüben sein, aber nicht zusätzliche Gefahren für Verbraucher:innen hervorrufen. Dementsprechend regelt der CCPA eingehend das Auskunftsverfahren anhand eines risikobasierten Ansatzes.[771] Zuerst müssen die Verbraucher:innen einen Auskunftsantrag über eine der dafür festgelegten Kontaktmöglichkeiten stellen. Dessen Eingang muss das Unternehmen bestätigen und über das weitere Vorgehen informieren. Danach schließt sich das ausführlich geregelte Identifizierungsverfahren an, das Identitätsdiebstahl verhindern soll. Schließlich legt der CCPA auch fest, bis wann und wie Unternehmen die Auskunft erteilen sollen. Das Verfahren ist überaus spezifisch geregelt.

---

[766] BT-Dr. 17/10488, 26.

[767] Siehe Kapitel 3:C.II.1.a) (ab S. 109).

[768] Cal. Civ. Code § 1798.145(h)(3).

[769] Art. 15 Abs. 4 DSGVO verweist insoweit missverständlich nur auf Art. 15 Abs. 3 DSGVO, gemeint ist aber auch Art. 15 Abs. 1 DSGVO, vgl. *Lembke*, NJW 2020, 1841, 1844.

[770] Cal. Civ. Code § 1798.145(k).

[771] So explizit *Cal. Attorney General*, Initial Statement of Reasons, S. 17: »risk-based approach«.

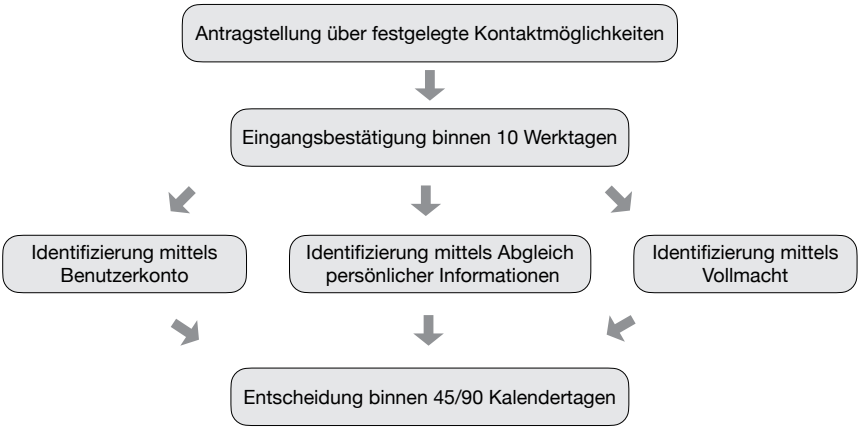

Abbildung 2: Ablauf des Auskunftsverfahrens

Das Verfahren beginnt damit, dass Verbraucher:innen Auskunft beantragen. Sie können dies ausschließlich über die vom Unternehmen in der umfassenden Datenschutzerklärung festgelegten, leicht zugänglichen Kontaktmöglichkeiten.[772] Diese Standardisierung reduziert den Umsetzungsaufwand für Unternehmen. Diese müssen mindestens zwei Kontaktmöglichkeiten zur Verfügung stellen.[773] Die Auswahl der Kontaktmöglichkeiten muss sich daran orientieren, wie Verbraucher:innen mit dem Unternehmen typischerweise in Kontakt treten.[774] So soll ein Unternehmen, das hauptsächlich persönlich vor Ort mit Verbraucher:innen interagiert, auch vor Ort einen Auskunftsantrag ermöglichen (z. B. durch ein direkt im Geschäft auszufüllendes Papierformular).[775] Falls ein Unternehmen einen Auskunftsantrag auf einem dafür nicht vorgesehen Weg erhält, kann es nach seiner Wahl auf die zulässigen Kontaktmöglichkeiten verweisen oder den Auskunftsantrag direkt bearbeiten.[776]

Zwei Kontaktmöglichkeiten sind für die meisten Unternehmen vorgegeben: Erstens muss ein Unternehmen es Verbraucher:innen ermöglichen, über seine Webseite einen Auskunftsantrag zu stellen, wenn es ohnehin über eine Webseite verfügt.[777] Dies dürfte auf nahezu alle Unternehmen im Sinne des CCPA zutreffen, da die Unternehmensdefinition kleine Gesellschaften ausschließt.[778] Unternehmen

[772] Cal. Civ. Code §§ 1798.130(a)(1)(A), 1798.140(n), 11 C.C.R. § 7020(a). Zu der umfassenden Datenschutzerklärung siehe Kapitel 3:D.I.2.b)aa) (ab S. 155).

[773] Cal. Civ. Code § 1798.130(a)(1)(A), 11 C.C.R. § 7020(a).

[774] 11 C.C.R. § 7020(c).

[775] 11 C.C.R. § 7020(c).

[776] 11 C.C.R. § 7020(e).

[777] Cal. Civ. Code § 1798.130(a)(1)(B).

[778] Dazu siehe Kapitel 3:B.II.2.b) (ab S. 58).

sollen diesen Zugang über ihre Webseite als Selbstbedienungsservice ausgestalten, mit dem Verbraucher:innen direkt eine vollständige Kopie ihrer persönlichen Informationen herunterladen können, was allerdings nicht verpflichtend ist.[779]

Zweitens muss ein Unternehmen eine gebührenfreie Telefonnummer für Auskunftsanträge anbieten.[780] Es kann diese Telefonnummer nur dann durch eine E-Mail-Adresse ersetzen, wenn es ausschließlich online tätig ist und die persönlichen Informationen direkt bei den jeweiligen Verbraucher:innen erhebt.[781] Die Einschränkung auf direkt erhobene persönliche Informationen soll Verbraucher:innen schützen, deren persönliche Informationen offline erhoben wurden und die mit dem Internet und E-Mails nicht vertraut sind.[782] Hintergrund dieser Ausnahme ist, dass eine gebührenfreie Telefonnummer für ein reines Online-Unternehmen aufwendiger einzurichten ist.[783]

Ein Unternehmen muss binnen 10 Werktagen[784] den Eingang des Auskunftsantrags bestätigen und darüber informieren, wie das Unternehmen den Antrag bearbeiten wird.[785] Dabei soll das Unternehmen den Antrag möglichst auf dem gleichen Weg, wie der Antrag gestellt wurde, bestätigen (beispielsweise bei einem telefonischen Antrag direkt am Telefon).[786] Das Unternehmen muss in der Bestätigung darüber informieren, wie es den Verbraucher oder die Verbraucherin identifizieren und wann es in etwa vollständig antworten wird.[787]

Der CCPA regelt die Identifizierung umfassend, um dem Risiko eines Identitätsdiebstahls vorzubeugen. Für einen Vertragsschluss im fremden Namen benötigen Kriminelle persönliche Informationen der jeweiligen Person. Der CCPA will verhindern, dass Betrüger:innen bereits erlangte Daten durch eine Auskunft mit weiteren Informationen anreichern.[788] Auch sonstige Risiken für Verbraucher:innen aus einer unberechtigten Offenlegung soll eine zuverlässige Identifizierung verhindern (beispielsweise Stalking). Unternehmen sollen im Zweifel die Betrugsprävention gegenüber einer Offenlegung priorisieren.[789] Daher muss das Unternehmen wirtschaftlich vertretbare Maßnahmen ergreifen, um Verbraucher:innen zu identifizieren.[790] Gleichzeitig soll der Aufwand des Verbrauchers möglichst gering sein.[791]

---

[779] 11 C.C.R. § 7024(g).

[780] Cal. Civ. Code § 1798.130(a)(1)(A), 11 C.C.R. § 7020(a).

[781] Cal. Civ. Code § 1798.130(a)(1)(A); 11 C.C.R. § 7020(a).

[782] *Cal. Senate Judiciary Committee*, Cal. Senate Judiciary Committee: AB 1564, S. 6. Die Ausnahme wurde mit A.B. 1564 eingeführt.

[783] *Cal. Senate Judiciary Committee*, Cal. Senate Judiciary Committee: AB 1564, S. 4–6.

[784] Werktage sind alle Tage außer Sonn- und Feiertage: Cal. Civ. Code §§ 9, 7.

[785] 11 C.C.R. § 7021(a).

[786] 11 C.C.R. § 7021(a).

[787] 11 C.C.R. § 7021(a).

[788] Vgl. die Erwägungsgründe in CCPA-2018, Sec. 2(f).

[789] *Cal. Attorney General*, Initial Statement of Reasons, S. 31.

[790] Cal. Civ. Code § 1798.140(ak).

[791] *Cal. Attorney General*, Initial Statement of Reasons, S. 15.

Ein Unternehmen hat einen gewissen Spielraum, wie es Verbraucher:innen identifiziert, muss aber folgende Prinzipien beachten.[792] Es soll berücksichtigen, welche Informationen es bereitstellen muss, wie sensibel diese sind und welchen Wert sie haben.[793] Dabei gelten insbesondere persönliche Informationen, für die nach dem kalifornischen Datenpannenmeldegesetz eine Meldepflicht besteht, als besonders sensibel.[794] Die meisten dieser Informationen dürfen sie ohnehin nicht im Klartext mitteilen, sondern nur schlagwortartig umschreiben.[795] Neben der Art der persönlichen Informationen muss ein Unternehmen auch das Risiko für Verbraucher:innen in Betracht ziehen: die potenzielle Schadenshöhe und die Wahrscheinlichkeit, das bösgläubige Dritte die mitzuteilenden Informationen erlangen wollen.[796] Falls Verbraucher:innen persönliche Informationen bereitstellen sollen, um sich zu identifizieren, muss das Unternehmen bewerten, inwieweit diese leicht gefunden oder fingiert werden können.[797] Schließlich soll es auch praktische Erwägungen beachten, beispielsweise wie Verbraucher:innen hauptsächlich das Unternehmen kontaktieren und welche Technologie zur Verfügung steht.[798] Die Identifizierung muss für Verbraucher:innen kostenlos sein.[799] Eventuelle Auslagen der Verbraucher:innen hat das Unternehmen zu ersetzen.[800]

Zur Identifizierung darf ein Unternehmen grundsätzlich nur ihm bereits bekannte persönliche Informationen abfragen und mit den bereits bekannten Informationen abgleichen.[801] Dies soll dem Grundsatz der Datenminimierung dienen.[802] Wenn eine Identifizierung sonst unmöglich ist, kann es dennoch weitere persönliche Informationen abfragen.[803] Solche weiteren persönlichen Informationen darf es nur für die Identifizierung nutzen und muss sie anschließend sobald wie möglich löschen.[804] Darüber hinaus soll es die im kalifornischen Datenpannenmeldegesetz genannten sensiblen Daten möglichst nicht abfragen.[805]

Bei Verbraucher:innen, die bereits über ein passwortgeschütztes Benutzerkonto bei dem Unternehmen verfügen, ist die Identifizierung durch eine Sondervorschrift

---

[792] 11 C.C.R. § 7060(a).

[793] Cal. Civ. Code § 1798.185(a)(14), 11 C.C.R. § 7060(b)(3)(A).

[794] 11 C.C.R. § 7060(a)(3)(A); vgl. Cal. Civ. Code § 1798.82(h). Wobei viele dieser Informationen ohnehin schon nicht im Klartext mitgeteilt werden dürfen, Siehe Kapitel 3:C.III.1.a) (ab S. 116). Im Klartext mitgeteilt werden dürfen die vom kalifornischen Datenpannemeldegesetz erfassten Patienten- oder Krankenversicherungsdaten.

[795] Siehe Kapitel 3:C.III.1.a) (ab S. 116).

[796] 11 C.C.R. § 7060(b)(3)(B),(C).

[797] 11 C.C.R. § 7060(b)(3)(D).

[798] 11 C.C.R. § 7060(b)(3)(E),(F).

[799] Cal. Civ. Code § 1798.130(a)(2)(A): »free of charge«, 11 C.C.R. § 7060(d).

[800] 11 C.C.R. § 7060(d).

[801] 11 C.C.R. § 7060(b)(1),(c).

[802] *Cal. Attorney General*, Initial Statement of Reasons, S. 30.

[803] 11 C.C.R. § 7060(c).

[804] 11 C.C.R. § 7060(c).

[805] 11 C.C.R. § 7060(b)(2), Cal. Civ. Code § 1798.81.5(d). Zu diesen Informationen siehe Kapitel 3:E.II.2.a) (ab S. 208).

erleichtert.[806] Hintergrund ist, dass die Identifizierung über ein Benutzerkonto sowohl sicher als auch leicht für die Verbraucher:innen ist. Allerdings dürfen Verbraucher:innen nicht gezwungen sein, nur für einen Auskunftsantrag ein Konto anzulegen.[807] Verbraucher:innen sollen ihr Passwort erneut eingeben und gelten danach als identifiziert.[808] Falls das Unternehmen Anhaltspunkte für eine missbräuchliche Nutzung des Benutzerkontos hat, muss es die Identifizierung mittels Benutzerkonto durch zusätzliche Maßnahmen absichern.[809] Dabei soll es sich an der Vorschrift für eine Identifizierung ohne Benutzerkonto orientieren.[810]

Die Vorschrift für eine Identifizierung ohne Benutzerkonto ist nach einem risikobasierten Ansatz ausgestaltet.[811] Sie unterscheidet zwei Stufen nötiger Sorgfalt: mittlere Sicherheit für die Offenlegung der Kategorien persönlicher Informationen[812] und hohe Sicherheit für die Offenlegung der konkreten persönlichen Informationen.[813] Mittlere Sicherheit gilt als erfüllt, wenn Unternehmen zwei ihnen bekannte, für eine zuverlässige Identifizierung geeignete Informationen abgleichen.[814] Diese Informationen können jeder Art sein. So kann z. B. eine geeignete Information bei einem Einzelhandelsunternehmen, das eine Kaufhistorie speichert, der Geldbetrag des letzten Einkaufs sein.[815] Allerdings sind leicht zu erlangende Informationen ungeeignet (beispielsweise der Name oder Daten aus öffentlichen Registern).[816] Hohe Sicherheit setzt zwei Bedingungen voraus. Erstens müssen die Verbraucher:innen drei dem Unternehmen bekannte, von diesem für eine zuverlässige Identifizierung ausgewählte Informationen benennen.[817] Zweite Voraussetzung ist, dass Verbraucher:innen eine eidesstattliche Erklärung über ihre Identität vorlegen.[818] Diese kann auch elektronisch erfolgen (z. B. als E-Mail).[819] Das Unternehmen muss die eidesstattliche Erklärung im Original aufbewahren.[820]

Statt des vorgeschlagenen Verfahrens können Unternehmen Verbraucher:innen jeweils auch auf eine andere Weise identifizieren, wenn diese gleich sicher ist. So kann ein Smartphone-App-Anbieter Verbraucher:innen beispielsweise

---

[806] 11 C. C. R. § 7061.
[807] Cal. Civ. Code § 1798.130(a)(2).
[808] 11 C. C. R. § 7061(a).
[809] 11 C. C. R. § 7061(b).
[810] 11 C. C. R. § 7061(b).
[811] 11 C. C. R. § 7062(a).
[812] 11 C. C. R. § 7062(b).
[813] 11 C. C. R. § 7062(c). *Vgl. Cal. Attorney General*, Initial Statement of Reasons, S. 18: konkrete persönliche Informationen seien sensibler als Kategorien derselben.
[814] 11 C. C. R. § 7062(b).
[815] 11 C. C. R. § 7062(e)(1).
[816] *Guzzetta/Manukyan*, 62 Orange County Lawyer 40, 44.
[817] 11 C. C. R. § 7062(c).
[818] 11 C. C. R. § 7062(c).
[819] 11 C. C. R. § 7001(u) i. V. m. Cal. Civ. Code §§ 1633.2(h), 1633.11(b)). Siehe Kapitel 3:C.I.2.b)dd) (ab S. 91).
[820] 11 C. C. R. § 7062(c).

identifizieren, indem er eine Benachrichtigung in seiner Smartphone-App auslöst, auf die Verbraucher:innen in der App antworten müssen.[821]

Bei Antragstellung über Datenschutzagenturen kann das Unternehmen entweder verlangen, dass diese eine (elektronisch) unterschriebene Vollmacht des Verbrauchers vorlegt, oder Verbraucher:innen direkt zur Identifizierung oder Bestätigung der Vollmacht kontaktieren.[822] Ein Unternehmen muss sich auf die Vorlage der besonderen Vollmacht *power of attorney* verlassen und darf in diesem Fall die Verbraucher:innen nicht mehr direkt zur Identifizierung kontaktieren.[823] *Power of attorney* kann trotz ihres Namens auch Nicht-Anwälten erteilt werden, unterliegt aber strengen Formvorschriften.[824] Datenschutzagenturen sind verpflichtet, die erhaltenen persönlichen Informationen sicher aufzubewahren und nur zur Erfüllung des Auskunftsanspruchs zu nutzen.[825]

Falls das Unternehmen kein Identifizierungsverfahren einrichten kann, das ausreichend sicher und wirtschaftlich vertretbar ist, darf es Auskunftsanträge ablehnen.[826] Es muss den Antragsstellenden mitteilen, dass es den Antrag ablehnt und warum.[827] Überdies ist das Unternehmen verpflichtet, die Unmöglichkeit einer Identifizierung in seiner Datenschutzerklärung offenzulegen und zu begründen.[828] Die Begründungspflicht soll die Kontrolle durch die Aufsichtsbehörden erleichtern und Situationen aufzeigen, in denen eine ausreichend sichere Identifizierung nicht möglich ist.[829] Dieser öffentliche Rechtfertigungsdruck reduziert das Missbrauchsrisiko erheblich. Spätestens nach zwölf Monaten muss es erneut prüfen, ob es nicht doch ein angemessenes Identifizierungsverfahren einrichten kann.[830]

Das Unternehmen ist verpflichtet, den Auskunftsantrag abzulehnen, wenn die Identifizierung misslingt.[831] Falls die Identifizierung keine hohe, aber eine mittlere Sicherheit erreicht, soll es nur die Kategorien persönlicher Informationen, aber nicht die konkreten persönlichen Informationen mitteilen.[832]

Die Frist für eine Entscheidung über den Auskunftsantrag beträgt 45 Kalendertage ab dessen Zugang.[833] Das Unternehmen kann sie auf insgesamt bis zu 90 Kalendertage verlängern, wenn dies aufgrund der Komplexität oder Anzahl der Anträge nötig ist.[834] Verbraucher:innen sind binnen 45 Kalendertagen ab Zugang

---

821 11 C.C.R. § 7060(e)(2).
822 11 C.C.R. § 7063(a).
823 11 C.C.R. § 7063(b).
824 Cal. Prob. Code §§ 4120–4130.
825 11 C.C.R. § 7063(c),(d).
826 11 C.C.R. § 7062(g).
827 11 C.C.R. § 7062(g).
828 11 C.C.R. § 7062(g).
829 Cal. Attorney General, Initial Statement of Reasons, S. 33.
830 11 C.C.R. § 7062(g).
831 11 C.C.R. § 7062(f).
832 11 C.C.R. § 7024(a).
833 Cal. Civ. Code § 1798.130(a)(2)(A), 11 C.C.R. § 7021(b).
834 Cal. Civ. Code §§ 1798.130(a)(2)(A), 1798.145(h)(1), 11 C.C.R. § 7021(b).

des Antrags über eine solche Verlängerung und deren Gründe zu informieren.[835] Wenn es dem Antrag nachkommt, ist das Unternehmen verpflichtet, die persönlichen Informationen in einer sicheren Weise übermitteln.[836] Eine Ablehnung muss ein Unternehmen unverzüglich, spätestens aber innerhalb der 45/90-Tage-Frist, mitteilen sowie über deren Gründe und über ein (freiwilliges) unternehmensinternes Beschwerderecht informieren.[837] Bei einer Ablehnung soll das Unternehmen der Antwort seine Datenschutzerklärung beifügen, damit Verbraucher:innen zumindest eine abstrakte Beschreibung seiner Erhebung und Nutzung persönlicher Informationen erhalten.[838]

b) Vergleich mit Art. 15 DSGVO

Demgegenüber regelt das Recht auf Auskunft des Art. 15 DSGVO kein spezifisches Verfahren, sondern normiert das abstrakte Ziel, dass der Verantwortliche der betroffenen Person die Ausübung ihres Auskunftsrechts »erleichtert« (Art. 12 Abs. 2 S. 1 DSGVO). Dementsprechend liegt der Fokus der DSGVO mehr auf einer leichten Ausübung des Auskunftsrechts als einer über alle Zweifel erhabenen Identifizierung. Der Verantwortliche darf zwar bei begründeten, nachgewiesenen Zweifeln zusätzliche Informationen anfordern, um die Identität zu bestätigen (Art. 12 Abs. 6 DSGVO) und bei Unmöglichkeit der Identifizierung auch den Auskunftsantrag ablehnen.[839] Der Verantwortliche trägt jedoch die Darlegungs- und Beweislast für Zweifel an der Identität.[840] Die Literatur diskutiert Risiken aus einer fehlenden Identifizierung kaum und hält verbreitet sogar eine routinemäßige Identitätsprüfung für unzulässig.[841] Auch die Leitlinien der Aufsichtsbehörden zielen hauptsächlich auf eine möglichst leichte Antragstellung.[842] Eine zu schwere Antragstellung ist gemäß Art. 83 Abs. 5 lit. b DSGVO bußgeldbewehrt. Damit ist eine zuverlässige Identifizierung für den Verantwortlichen

---

[835] Cal. Civ. Code §§ 1798.130(a)(2)(A), 1798.145(h)(1), 11 C.C.R. § 7021(b).

[836] 11 C.C.R. § 7024(f).

[837] Cal. Civ. Code § 1798.145(h)(2).

[838] 11 C.C.R. § 7024(b).

[839] *Heckmann/Paschke* in: Ehmann/Selmayr, DS-GVO Art. 12 Rn. 26.

[840] *Heckmann/Paschke* in: Ehmann/Selmayr, DS-GVO Art. 12 Rn. 26.

[841] So *Bäcker* in: Kühling/Buchner, DS-GVO Art. 12 Rn. 30; *Paal/Hennemann* in: Paal/Pauly, DS-GVO Art. 12 Rn. 72; a. A. *Engeler/Quiel*, NJW 2019, 2201, 2205; *Kremer*, CR 2016, 560, 566 f.

[842] *Agencia Española Protectección Datos* (Spanien), Resolución De Procedimiento Sancionador, Expediente Nº: PS/00003/2021, S. 26–29: Bußgeld wegen Anfordern von Ausweiskopien; *Autoriteit Persoonsgegevens* (Niederlande), DPA fines DPG Media for unnecessarily requesting copies of identity documents; *BayLDA*, Tätigkeitsbericht 2013/2014, S. 77: Forderung von geschwärzten Ausweiskopien selbst bei sensiblen Daten allenfalls ausnahmsweise zulässig; *ICO* (UK), What should we consider when responding to a request? (erschienen noch vor dem »Brexit«); ähnlich *Artikel-29-Datenschutzgruppe*, WP 242 Datenübertragbarkeit, S. 16 zum parallelen Recht auf Datenübertragbarkeit.

nicht nur mit Aufwand verbunden, sondern führt im Gegenteil sogar zu einem höheren Bußgeldrisiko.

Daraus folgt, dass Verantwortliche in der Praxis im Zweifel auf eine zuverlässige Identifizierung verzichten. Die IT-Sicherheitsforscher *Pavur/Knerr* haben bei 150 Verantwortlichen Auskunftsanträge nach Art. 15 DSGVO für eine Person gestellt, die bei diesen Verantwortlichen tatsächlich ein Benutzerkonto hatte, aber dabei eine dem Verantwortlichen unbekannte E-Mail-Adresse verwendet.[843] 24 % der Verantwortlichen teilten die personenbezogenen Daten ohne jede Identifizierung mit, 16 % forderten zur Identifizierung nur öffentlich verfügbare Informationen und nur 39 % verlangten eine wirksame Identitätsfeststellung.[844] Teilweise teilten Unternehmen selbst sensible Daten wie Passwörter im Klartext ohne Identifizierung mit.[845]

Eine solch unzureichende Identifizierung führt zu erheblichen Risiken für betroffene Personen.[846] Erstens besteht das Risiko einer unerwünschten Kontaktaufnahme, insbesondere bei Personen des öffentlichen Lebens und Stalking-Opfern.[847] Zweitens nimmt auch in Europa durch das Internet das Risiko eines Identitätsdiebstahls zu.[848]

Diesem Risiko kann man unter der DSGVO aber auch *de lege lata* gerecht werden. Eine solche Auslegung ist mit Art. 12 Abs. 6 DSGVO vereinbar: Berechtigte Zweifel an der Identität setzen eine gewisse gedankliche Vorprüfung voraus. Dies entspricht auch Erwägungsgrund 57 S. 1 der DSGVO, nach dem Verantwortliche alle vertretbare Mittel zur Identifizierung nutzen sollen. Um diese Mittel zu konkretisieren, könnte der Europäische Datenschutzausschuss seine bestehende Leitlinie zum Auskunftsrecht erweitern.[849] Leitlinien sind als Instrument des *soft law* ein gut geeignetes Mittel, um dieses Problem zu lösen, da der Verantwortliche schon zur Risikovermeidung ein von diesem vorgeschlagenes Verfahren in der Regel übernehmen wird. Hierfür bildet die ausgewogene Sonderregelung des CCPA eine hilfreiche Vorlage. Das grundsätzliche Prinzip des CCPA, Informationen abzufragen, die nur der betroffenen Person bekannt sind, ist auch für Europa praktikabel. Die vom CCPA vorgesehene Authentifizierung durch ein Benutzerkonto entspricht zudem ohnehin Erwägungsgrund 57 S. 3 der DSGVO. Auch die Unterscheidung zwischen mittlerer und hoher Sicherheit ist sinnvoll, da nicht jeder Auskunftsanspruch gleich sensibele Information

---

[843] *Pavur/Knerr*, GDPArrrrr: Using Privacy Laws to Steal Identities, S. 2–4.

[844] *Pavur/Knerr*, GDPArrrrr: Using Privacy Laws to Steal Identities, S. 5–7.

[845] *Pavur/Knerr*, GDPArrrrr: Using Privacy Laws to Steal Identities, S. 7 f.

[846] *Cormack*, EPDL 2016, 15, 16–19; *Engeler/Quiel*, NJW 2019, 2201, 2205.

[847] Vgl. LG Bonn vom 11.11.2020, *1&1*, BeckRS 2020, 35663 Rn. 46. Im vorliegenden Sachverhalt hatte eine Stalkerin unzureichende technische und organisatorische Maßnahmen für die Authentifizierung bei einer Kundendienst-Hotline ausgenutzt.

[848] *Bundesamt für Sicherheit in der Informationstechnik*, Die Lage der IT-Sicherheit in Deutschland 2021, S. 24–26.

[849] Diese äußert sich derzeit vor allem zu unzulässigen, nicht zu zulässigen Identifizierungsmethoden, vgl. *EDSA*, Guidelines 01/2022 Right of access, Rn. 64–78.

betrifft. Ergänzend sollte eine solche Leitlinie auch festlegen, dass die Vorlage eines Personalausweis für hohe Sicherheit genügt – der CCPA verhält sich allein deshalb nicht dazu, da die Vereinigten Staaten über keinen nationalen Personalausweis verfügen.

3. Inzidentes Recht auf Datenportabilität

Das Auskunftsrecht enthält indirekt auch ein Recht auf Datenportabilität. Die Auskunft muss das Unternehmen nämlich bereitstellen »to the extent technically feasible, in a structured, commonly used, machine-readable format, which also may be transmitted to another entity at the consumer's request without hindrance«.[850] Dies gilt für alle erhobenen persönlichen Informationen.[851]

Dieser Wortlaut ähnelt stark Art. 20 Abs. 1 DSGVO. Dessen Tatbestand ist allerdings enger, da das Recht auf Datenübertragbarkeit nicht für alle personenbezogenen Daten greift, sondern nur, wenn die Verarbeitung auf einer Einwilligung oder einem Vertrag beruht (Art. 6 Abs. 1 S. 1 lit. a, b DSGVO) und die Verarbeitung mittels automatisierter Verfahren erfolgt. Ansonsten stimmt der Wortlaut überein, was dafür spricht, dass sich der Gesetzgeber des CCPA insoweit an der DSGVO orientiert hat.

Warum hat der CCPA dieses Rechtsinstitut übernommen? Datenportabilität ist eng mit Selbstbestimmung verknüpft. Erwägungsgrund 68 S. 1 der DSGVO nennt dabei explizit eine »bessere Kontrolle über die eigenen Daten« als Motiv des Art. 20 DSGVO. Diese Kontrolle ist ein Kernmotiv des CCPA[852] und weit verbreitet im amerikanischen Datenschutzrecht. So zielt vor allem das Auskunftsrecht des HIPAA auch auf Datenportabilität ab.[853] Hiernach müssen die Auskunftsverpflichteten die Patientendaten in einem Format nach Wahl des Individuums bereitstellen und auf dessen Wunsch auch direkt an einen Dritten übermitteln.[854]

Die fehlende Beschränkung des CCPA auf die Rechtsgrundlagen Vertrag oder Einwilligung lässt sich wohl damit erklären, dass der CCPA kein Verbot mit Erlaubnisvorbehalt regelt. Die Begrenzung auf technische Realisierbarkeit des CCPA entspricht wohl der Beschränkung auf automatisierte Verfahren des Art. 20 Abs. 1 DSGVO. Typischerweise ist nämlich nur bei einem automatisiertem Verfahren ein strukturiertes, maschinenlesbares Format möglich, da manuell erhobene personenbezogene Daten nicht strukturiert genug sind. Daher sind beide Rechte im Ergebnis wohl vergleichbar weit.[855]

---

[850] Cal. Civ. Code § 1798.130(a)(3)(A)(iii).

[851] *Jerome*, 33 Antitrust ABA 96, 98.

[852] So die Erwägungsgründe an insgesamt acht Stellen: CCPA-2018, Sec. 2(a),(g)–(i), Proposition 24 (Cal. 2020), Sec. 2(A),(G),(H),(J), 3(A)(1)(2).

[853] *American Law Institute*, Principles of the law, data privacy, § 9 Reportes's Note 5.

[854] 45 C.F.R. § 164.524(c)(2)(i),(c)(3)(ii).

[855] A.A. *Jerome*, 33 Antitrust ABA 96, 98: CCPA sei wohl weiter.

Bisher ist das Datenportabilitätsrecht unter dem CCPA allerdings praktisch bedeutungslos, da keine interoperablen Formate existieren.[856] Art. 20 DSGVO scheitert in der Praxis ebenfalls mangels solcher Formate.[857] Das Recht auf Datenportabilität stellt sich damit beidseits des Atlantiks als attraktive, aber in der bisherigen Ausgestaltung wirkungslose Idee dar.

IV. Recht auf Löschung

1. Reichweite

a) Ratio legis und Tatbestand

Das Recht auf Löschung im CCPA[858] ist ein Novum im amerikanischen Recht. Es ist aber deutlich begrenzter als das Recht auf Vergessenwerden des Art. 17 DSGVO. Es dient nicht primär dem Schutz der Persönlichkeit, sondern der Kontrolle über die eigenen persönlichen Informationen. Vor allem ist das Recht auf Löschung der persönlichen Informationen beschränkt, welche das Unternehmen direkt bei dem Verbraucher oder der Verbraucherin erhoben hat. Weiterhin greifen zahlreiche, teilweise sehr weitgehende Ausnahmen.

Ein Recht auf Löschung ist im amerikanischen Recht ungleich problematischer, weil die Meinungsfreiheit eine hohe Stellung genießt.[859] Informationen sollen auf dem *marketplace of ideas* frei fließen.[860] Ungehinderte Meinungsfreiheit sei ein hohes Gut, weil sie dem öffentlichen Diskurs ermöglicht, Überzeugungen zu bewerten und zu vergleichen, damit sich die besten Ideen durchsetzen.[861] Die beste Lösung für anstößige Äußerungen sei nicht Zensur, sondern engagierte Gegenrede.[862] Fehlvorstellungen seien dagegen darin begründet, dass Bürger:innen noch weitere Informationen benötigten, um sich ein vollständiges

---

[856] Vgl. die wiedergegebene Äußerung der Leiterin der Datenschutzabteilung des kalifornischen Attorney General *Stacy Schesser* in: *FTC*, Data To Go: An FTC Workshop on Data Portability: Transcript, S. 21; vgl. *Lancieri*, Narrowing Data Protection's Enforcement Gap, S. 21: Recht auf Datenportabilität wirkungslos, weil übertragene Daten häufig veraltet.

[857] *Europäische Kommission*, Commission Staff Working Document: two years of application of GDPR, SWD/2020/115 final, Nr. 4: »Operators note that there are sometimes difficulties in providing the data in a structured, commonly used machine-readable format (due to the lack of standard)«; *Dix* in: NK-DatenschutzR, DS-GVO Art. 20 Rn. 1; *Kühling/Martini*, EuZW 2016, 448, 450 f.; *Sattler* in: Pertot, Rechte an Daten, 49, 81–83; a. A. wohl *Paal* in: Paal/Pauly, DS-GVO Art. 20 Rn. 6.

[858] Cal. Civ. Code § 1798.105.

[859] Zur Meinungsfreiheit siehe Kapitel 2:A.I.2.a) (ab S. 10).

[860] Zur Herkunft dieses *topos: Larson*, 18 Comm. L. & Pol'y 91, 112–114.

[861] Grundlegend: U. S. Supreme Court vom 10.11.1919, *Abrams v. United States* – ablehnendes Sondervotum *Holmes*, 250 U. S. 616, 630.

[862] U. S. Supreme Court vom 16.05.1927, *Whitney v. Cal.* – ablehnendes Sondervotum *Brandeis*, 274 U. S. 357, 377; vom 28.06.2012, *United States v. Alvarez*, 567 U. S. 709, 727 f.

Bild machen zu können.[863] In einem liberalen Staat sei die richtige Antwort auf irrationale Äußerungen die rationale Erwiderung, auf uniformierte Behauptungen die aufgeklärte Widerrede und auf glatte Lügen die Wahrheit.[864] Ideen und Informationen der Öffentlichkeit wieder zu entziehen, ist damit nicht vereinbar.[865]

Dementsprechend gab es im amerikanischen Recht bisher nur sehr begrenzte Löschungsrechte. Wirtschaftsauskunfteien müssen falsche Einträge löschen, was allerdings eher dem Unterfall eines Korrekturrechts entspricht.[866] Kalifornien hatte immerhin 2015 ein Recht auf Löschung für Minderjährige eingeführt.[867] Es ist aber auf im Internet veröffentlichte Beiträge begrenzt, welche die Minderjährigen selbst eingestellt haben.[868]

Das Recht auf Löschung im CCPA ist ähnlich dazu auf persönliche Informationen beschränkt, die das Unternehmen direkt bei dem Verbraucher oder der Verbraucherin erhoben hat.[869] Direkt erhoben sind persönliche Informationen, welche die Verbraucher:innen selbst dem jeweiligen Unternehmen zugänglich gemacht haben oder die das Unternehmen aus der Beobachtung ihres Verhaltens geschlossen hat.[870] Grund für die Einschränkung auf direkt erhobene persönliche Informationen ist die Meinungsfreiheit.[871] Wenn Verbraucher:innen selbst persönliche Informationen bereitstellen, können sie selbst über ihre Äußerung disponieren. Wenn aber Dritte persönliche Informationen dem Unternehmen übermitteln, ist dies bereits eine von der Meinungsfreiheit geschützte Äußerung.[872] Das Recht auf Löschung soll nur Verbraucher:innen bei der Kontrolle ihrer persönlichen Informationen unterstützen. Es soll sich aber nicht für einen allgemeinen Ehrschutz zweckentfremden lassen.

b) Weitgefasste Ausnahmen

Zahlreiche Ausnahmen schränken das Recht auf Löschung noch weiter ein. Bei allen Ausnahmen muss das Unternehmen über die weitere Speicherung informieren und diese begründen.[873] Die Begründungspflicht soll Unternehmen dazu anhalten, die Ausnahmen restriktiv zu nutzen und Verbraucher:innen ermöglichen,

---

[863] U. S. Supreme Court vom 10.11.1919, *Abrams v. United States* – ablehnendes Sondervotum *Holmes*, 250 U. S. 616, 630.

[864] U. S. Supreme Court vom 28.06.2012, *United States v. Alvarez*, 567 U. S. 709, 727.

[865] *Larson*, 18 Comm. L. & Pol'y 91, 112–114; *Richards*, 56 Wm. & Mary L. Rev. 1501, 1531–1533.

[866] 15 U. S. C. § 1681i(5)(A)(i).

[867] S.B. 568, 2013-2014 Leg., Reg. Sess. (Cal. 2013), Cal. Stats. 2013 ch. 336, Sec. 1, kodifiziert in Cal. Bus. & Prof. Code § 22581(a).

[868] Cal. Bus. & Prof. Code § 22581(b)(2).

[869] Cal. Civ. Code § 1798.105(a).

[870] Cal. Civ. Code § 1798.140(f).

[871] *Chander/Kaminski/McGeveran*, 105 Minn. L. Rev. 1733, 1754–1755; *Jerome*, 33 Antitrust ABA 96, 99.

[872] Siehe Kapitel 2:A.I.2.a) (ab S. 10).

[873] 11 C. C. R. § 7022(f)(1).

ihr Recht auf Löschung effektiv zu verfolgen.[874] Das Unternehmen darf die weiter gespeicherten persönlichen Informationen nur für den in der Ausnahme genannten Zweck nutzen und muss nicht von der Ausnahme erfasste persönliche Informationen löschen.[875]

Es bestehen Ausnahmen für die Ausübung der Meinungsfreiheit, für betriebliche Interessen des Unternehmens und Forschung sowie eine unscharfe Ausnahme für berechtigte Interessen und Rechte des Unternehmens.

Angesichts der hohen Bedeutung des *First Amendments* greift eine explizite Ausnahme für die Meinungsfreiheit: ein Unternehmen kann persönliche Informationen weiter speichern, soweit dies für die Ausübung der eigenen Meinungsfreiheit erforderlich ist oder um sicherzustellen, dass andere Verbraucher:innen ihr Recht auf Meinungsfreiheit ausüben können.[876] Was heißt nun Meinungsfreiheit ausüben (»exercise free speech«)? Die Ausnahme erfasst wohl nicht die bloße Weiterübermittlung persönlicher Informationen an Dienstleister oder Datenhandel, obwohl eine solche Weiterübermittlung eine geschützte Äußerung im verfassungsrechtlichen Sinne wäre. Gesetze sind nach amerikanischem Verständnis so auszulegen, dass keine Vorschrift überflüssig ist.[877] Bei einem begründeten Löschantrag verpflichtet der CCPA ein Unternehmen, Dienstleister und Dritte anzuweisen, persönliche Informationen zu löschen, wenn sie diese vom Unternehmen erhalten haben.[878] Dies wäre überflüssig, wenn die Meinungsfreiheits-Ausnahme persönliche Informationen erfassen würde, die das Unternehmen an Dienstleiter und Dritte weitergegeben hat.

Die Reichweite der Meinungsfreiheits-Ausnahme ist dadurch eingeschränkt, dass bestimmte öffentliche Informationen ohnehin keine persönlichen Informationen im Sinne des CCPA sind.[879] Dies sind insbesondere legal erlangte Informationen von öffentlichem Interesse und in Massenmedien veröffentlichte Informationen.[880] Die Ausnahme für öffentliche Informationen reduzieren die praktische Relevanz der Meinungsfreiheits-Ausnahme deutlich. Ein Löschantrag einer Politikerin gegenüber einer Tageszeitung über für sie inkriminierende Informationen wäre beispielsweise schon deshalb unbegründet, weil legal erlangte Informationen von öffentlichem Interesse keine persönlichen Informationen sind.

---

[874] *Cal. Attorney General*, Initial Statement of Reasons, S. 20; *ders.*, Final Statement of Reasons, S. 57.

[875] 11 C.C.R. § 7022(f)(1),(2).

[876] Cal. Civ. Code § 1798.105(d)(4). Kritik im Gesetzgebungsverfahren an der Offenheit dieser Formulierung *Cal. Senate Judiciary Comm.*, AB 375 Bill Analysis, S. 16; ebenso später: *Kessler*, 93 S. Cal. L. Rev. 99, 117.

[877] Cal. Supreme Court vom 26.04.2004, *State Farm Mutual Automobile Ins. Co. v. Garamendi*, 32 Cal. 4th 1029, 1045. Ebenso auf Bundesebene: U. S. Supreme Court vom 06.04.2009, *Corley v. United States*, 556 U. S. 303, 314; vom 21.02.2018, *Rubin v. Islamic Republic of Iran*, 138 S. Ct. 816, 824 f.

[878] Cal. Civ. Code § 1798.105(b).

[879] Cal. Civ. Code § 1798.140(v)(2). Siehe Kapitel 3:B.I.3 (ab S. 50).

[880] Cal. Civ. Code § 1798.140(v)(2).

Die Meinungsfreiheits-Ausnahme greift aber, wenn in einem sozialen Netzwerk eine andere Person den Beitrag des Verbrauchers oder der Verbraucherin weiterverbreitet. Dann würde eine Löschung des weiterverbreiteten Beitrags auch im Profil der anderen Person gegen deren Meinungsfreiheit verstoßen.[881] Ebenfalls ist denkbar, dass die Meinungsfreiheits-Ausnahme die Nutzung persönlicher Informationen in kommerzieller Werbung erfasst, die ohnehin deliktsrechtlich geregelt ist.[882]

Weitere Ausnahmen dienen den betrieblichen Interessen des Unternehmens. So müssen Unternehmen persönliche Informationen nicht löschen, wenn diese für die Durchführung eines noch bestehenden Vertrages erforderlich sind.[883] Auch können Unternehmen die für eine Garantie oder einen potenziellen Produktrückruf nötigen persönlichen Informationen weiter aufbewahren, damit Verbraucher:innen bei potenziell gefährlichen Produkten zu erreichen sind.[884] Ebenso sind die für Sicherheit und Integrität und zur Fehlerbehebung zwingend erforderlichen persönlichen Informationen (insbesondere Logdaten)[885] ausgenommen.[886] Unternehmen müssen die von einer gesetzlichen Aufbewahrungspflicht erfassten persönlichen Informationen nicht löschen.[887] Insbesondere muss ein Unternehmen persönliche Informationen nicht löschen, wenn es eine behördliche Anordnung zur weiteren Speicherung nach dem California Electronic Communications Privacy Act[888] erhalten hat.[889] Auch sind persönliche Informationen ausgenommen, die Unternehmen nur im Auftrag eines anderen Verbrauchers oder einer anderen Verbraucherin verwalten.[890] Daneben gelten alle Bereichsausnahmen des CCPA, die insbesondere die Ausübung oder Verteidigung gegen Rechtsansprüche erfassen.[891]

Wenn Verbraucher:innen zuvor informiert, freiwillig und spezifisch eingewilligt[892] hatten, können sie zudem in zwei Situationen keine Löschung mehr

---

[881] *Schwartz/Tien/McSherry*, Electronic Frontier Foundation, How to Improve the California Consumer Privacy Act of 2018. ähnlich *Ballon*, E-commerce & Internet law, S. 26-417; *Bukaty, CCPA* Implementation Guide, S. 81.

[882] Sog. *appropriation*, vgl. zur diesbezüglichen deliktsrechtlichen Rechtsprechung *American Law Institute*, Restatement of the law, second, Torts, § 652C; *Prosser*, 48 Calif. L. Rev. 383, 401–407.

[883] Cal. Civ. Code § 1798.105(d)(1).

[884] Cal. Civ. Code § 1798.105(d)(1). Zur ratio legis: *Cal. Senate Judiciary Comm.*, AB 1146 Bill Analysis, S. 6.

[885] *Bukaty*, California Consumer Privacy Act (CCPA), S. 80.

[886] Cal. Civ. Code § 1798.105(d)(2).

[887] Cal. Civ. Code §§ 1798.105(d)(8), 1798.145(a)(1).

[888] Cal. Pen. Code § 1546–1546.4. Zu dessen Gesetzgebungsgeschichte und Umfang: *Gassner*, 12 U.C. Irvine L. Rev. 267, 309–311.

[889] Cal. Civ. Code § 1798.105(d)(5).

[890] Cal. Civ. Code § 1798.145(k).

[891] Zu diesen siehe Kapitel 3:B.IV.1 (ab S. 74).

[892] Einwilligungsdefinition: Cal. Civ. Code § 1798.140(h).

verlangen: bei physikalisch fixierten persönlichen Informationen[893] und für Forschungszwecke genutzten persönlichen Informationen.[894] *Ratio legis* beider Ausnahmen ist, dass Verbraucher:innen schutzwürdig sind, wenn sie informiert eingewilligt haben, während das Unternehmen erhebliche Nachteile aus einer Löschung erleiden würde. Erstens kann das Unternehmen daher ein bereits hergestelltes reales Produkt weiter nutzen, wenn es für dessen Herstellung in Vertrauen auf die Einwilligung des Verbrauchers erhebliche Summen ausgegeben hat und ein Löschen der persönlichen Informationen daher wirtschaftlich nicht vertretbar wäre.[895] Regelbeispiel ist ein Schuljahrbuch.[896] Zweitens können die Verbraucher:innen keine Löschung verlangen, wenn sie in die Nutzung ihrer persönlichen Informationen für Forschung eingewilligt hatten und die Löschung es unmöglich machen oder wesentlich erschweren würde, die Forschung fertigzustellen.[897] Forschung umfasst dabei sowohl wissenschaftliche Grundlagenforschung als auch angewandte Forschung, solange diese auf eine Veröffentlichung der jeweiligen Ergebnisse abzielt.[898] Hingegen genügen bloße statistische Auswertungen im Eigeninteresse nicht.[899] Das Unternehmen muss die persönlichen Informationen für die Forschungsausnahme pseudonymisiert speichern und darf sie nur, soweit dies für die Forschung nötig ist, reidentifizieren und sie gegen ein unberechtigtes Reidentifizieren technisch und organisatorisch schützen.[900] Nach vollständiger Auswertung muss das Unternehmen die Forschungsdaten endgültig deidentifizieren oder aggregieren.[901]

Schließlich bilden zwei sehr weite Ausnahmen Auffangtatbestände, deren Bedeutung noch nicht geklärt ist. So ist die weitere Speicherung persönlicher Informationen für interne Zwecke zulässig, wenn diese den berechtigten Erwartungen der Verbraucher:innen im Rahmen ihrer Beziehung mit dem Unternehmen entspricht und mit den Umständen der Erhebung vereinbar ist.[902] Dieser Auffangtatbestand ist sehr unscharf: entweder ist er redundant oder übermäßig weit. Man könnte argumentieren, dass sein Regelungsgehalt bereits von den anderen Ausnahmen erfasst ist, da diese umfassend sind und insbesondere auch die für Vertragserfüllung nötigen persönlichen Informationen erfassen.[903] Eine darüber hinausgehende Auslegung würde die Bedeutung des ohnehin schon engen Recht auf Löschung noch weiter minimieren, entspricht aber dem maßgeblichen Wortlaut. Eine weitere Ausnahme erlaubt dem Unternehmen eine

[893] Cal. Civ. Code § 1798.145(r).
[894] Cal. Civ. Code § 1798.105(d)(6).
[895] Cal. Civ. Code § 1798.145(r).
[896] Cal. Civ. Code § 1798.145(r).
[897] Cal. Civ. Code § 1798.105(d)(6).
[898] Cal. Civ. Code § 1798.140(ab).
[899] *Gassner*, 12 U.C. Irvine L. Rev. 267, 311.
[900] Cal. Civ. Code § 1798.140(ab)(3),(4).
[901] Cal. Civ. Code § 1798.140(ab)(2).
[902] Cal. Civ. Code § 1798.105(d)(7).
[903] *Jerome*, 33 Antitrust ABA 96, 99.

Aufbewahrung, die nötig ist »to […] exercise another right provided for by law«.[904] Die genaue Bedeutung ist unklar[905] – zumal *right* im amerikanischen Recht inflationär verwendet wird.[906] Die weitere Bedeutung wird sich erst in der weiteren Rechtspraxis zeigen. Jedenfalls geben diese beiden übermäßig weiten Ausnahmen einen großen Spielraum, Löschanträge abzulehnen.[907]

c) Vergleich mit Art. 17 DSGVO

Das Recht auf Löschung des Art. 17 DSGVO reicht deutlich weiter.[908] Der Tatbestand enthält deutlich weniger Ausnahmen und regelt ein Recht auf Vergessenwerden, das mit dem amerikanischen Verständnis der Meinungsfreiheit unvereinbar wäre. Im Gegensatz zum CCPA schützt Art. 17 DSGVO primär nicht die Privatautonomie, sondern die Persönlichkeitsentfaltung der betroffenen Person.

Art. 17 DSGVO erfasst im Gegensatz zum CCPA nicht nur personenbezogene Daten, welche die betroffene Person selbst bereitgestellt hat. Vielmehr müssen Verantwortliche grundsätzlich sämtliche personenbezogenen Daten löschen, wenn eine der sechs Fallgruppen des Art. 17 Abs. 1 DSGVO vorliegt. Diese Fallgruppen setzen nicht voraus, dass der Verantwortliche die personenbezogenen Daten direkt bei der betroffenen Person erhoben hat. Damit ermöglicht die DSGVO der betroffenen Person, ihre Grundrechte auf Achtung des Privatlebens nach Art. 7 GRCh und auf Datenschutz nach Art. 8 GRCh auch gegenüber Dritten selbstständig durchzusetzen.[909] Diese Grundrechte schützen die selbstbestimmte Persönlichkeitsentfaltung gegenüber der Datenverarbeitung Dritter.[910]

Dieser umfassende Persönlichkeitsschutz kommt vor allem in dem Recht auf Vergessenwerden zum Ausdruck. Dieses hat zwei Ausprägungen: erstens

---

[904] Cal. Civ. Code § 1798.105(d)(4).

[905] *Pardau*, 23 J. Tech. L. & Pol'y 68, 108.

[906] *Glendon*, Rights talk, passim; *Reidenberg*, 80 Iowa L. Rev. 497, 501. Dazu im Kontext des ebenfalls als Recht formulierten Maßregelungsverbots siehe Kapitel 3:C.I.4.a) (ab S. 100).

[907] So zum ähnlichen Auffangtatbestand des CCPA-2018: *Cohen/Hall/Woo*, JD Supra, Key Aspects of the CCPA; *Hintze*, 14 Wash. J.L. Tech. & Arts 103, 130; *Jerome*, 33 Antitrust ABA 96, 99; *Li*, 32 Loy. Consumer L. Rev. 177, 187; *Pardau*, 23 J. Tech. L. & Pol'y 68, 108; *Park*, 10 UC Irvine L. Rev. 1455, 1485; *Palmieri*, 11 Hastings Sci. & Tech. L. J. 37, 46; *Stuenkel*, 19 Colo. Tech. L. J. 429, 441.

[908] *Chander/Kaminski/McGeveran*, 105 Minn. L. Rev. 1733, 1754–1755; *Fang*, 4 Geo. L. Tech. Rev. 125, 173; *Nicola/Pollicino*, The Balkanization of Data Privacy Regulation, S. 41; wohl auch: *Park*, 10 UC Irvine L. Rev. 1455, 1484; a. A. (CCPA und DSGVO seien gleich weitreichend) *Clark/Halpert*, 17 PDP 7, 7; *Cohen/Hall/Woo*, JD Supra, Key Aspects of the CCPA; *Davis*, 24 N.C. Banking Inst. 499, 519.

[909] EuGH vom 13.05.2014 – C-131/12, *Google Spain*, ECLI:EU:C:2014:317 Rn. 81; vom 24.09.2019 – C136/17, *GC u. a.*, ECLI:EU:C:2019:773 Rn. 59; vom 24.09.2019 – C-507/17, *Google gegen CNIL*, ECLI:EU:C:2019:772 Rn. 45; BVerfG vom 06.11.2019 – 1 BvR 276/17, *Recht auf Vergessen II*, NJW 2020, 314, Rn. 99 f.; BGH vom 27.07.2020, NJW 2020, 3436, Rn. 26–28.

[910] BVerfG vom 06.11.2019 – 1 BvR 276/17, *Recht auf Vergessen II*, NJW 2020, 314, Rn. 101.

sind Suchmaschinenbetreiber als unabhängige Verantwortliche neben Webseitenbetreibern verpflichtet, Einträge aus ihrem Index zu löschen, wenn die Voraussetzungen des Art. 17 Abs. 1, 3 DSGVO vorliegen.[911] Zweitens müssen Verantwortliche, die personenbezogene Daten veröffentlicht haben, weitere Verantwortliche über das Verlangen der betroffenen Person, alle Links oder Kopien ihrer personenbezogenen Daten zu löschen, soweit wie möglich informieren (Art. 17 Abs. 2 DSGVO).

Ein solches Recht auf Vergessenwerden widerspricht dem amerikanischen Verständnis von Meinungsfreiheit fundamental. Daher ist das Recht auf Vergessenwerden bereits seit den DSGVO-Entwürfen und dem *Google-Spain*-Urteil des EuGH[912] in der amerikanischen Rechtswissenschaft auf scharfe Kritik gestoßen.[913] Diese reichte von Vergleichen mit Orwell's 1984[914] bis zur Bezeichnung als »biggest threat to free speech on the Internet in the coming decade.«[915] Bezeichnend ist, wie selbstverständlich der Meinungsfreiheits-Verstoß für amerikanische Rechtswissenschaftler:innen ist, die in der Regel apodiktisch von einem klaren Verstoß gegen die Meinungsfreiheit ausgehen.[916] Dem liegt zugrunde, dass nach amerikanischem Verständnis die Lösung für solche Konflikte gerade nicht die staatliche Unterdrückung von Tatsachen ist, sondern deren Einordnung durch den öffentlichen Meinungskampf. Das insoweit weniger liberale europäische Recht scheut sich dagegen nicht, nach einer Abwägung auch Ideen und Tatsachen dem öffentlichen Diskurs zu entziehen.

Die daraus resultierenden Unterschiede in der Praxis sollten allerdings nicht überbewertet werden. Das Recht auf Vergessenwerden ist dadurch stark eingeschränkt, dass die Persönlichkeitsrechte der betroffenen Person gemäß Art. 17 Abs. 3 lit. a DSGVO mit der Meinungsfreiheit abzuwägen sind. Dabei ist insbesondere auch das Informationsinteresse der Öffentlichkeit zu berücksichtigen.[917] Die Persönlichkeitsrechte der betroffenen Person sind auch nicht

---

[911] EuGH vom 13.05.2014 – C-131/12, *Google Spain*, ECLI:EU:C:2014:317 Rn. 80–88; EuGH vom 24.09.2019 – C136/17, *GC u. a.*, ECLI:EU:C:2019:773 Rn. 60; vom 24.09.2019 – C-507/17, *Google gegen CNIL*, ECLI:EU:C:2019:772 Rn. 44; BGH vom 27.07.2020 – VI ZR 405/18*, NJW 2020, 3436*, Rn. 17–19.

[912] EuGH vom 13.05.2014 – C-131/12, *Google Spain*, ECLI:EU:C:2014:317.

[913] *Bennett*, 30 Berkeley J. Int'l L. 161, 164–168 m. w. N. auch zu Reaktionen in der amerikanischen Presse; *Criscione*, 32 Pace Int'l L. Rev. 315, 337–358; *Determann*, 2012 Stan. Tech. L. Rev. 7, Rn. 19; *ders.*, 6 International Data Privacy Law 244, 248; *Rosen*, 64 Stan. L. Rev. Online 88, 88; *Schwartz/Tien/McSherry*, Electronic Frontier Foundation, How to Improve the California Consumer Privacy Act of 2018.

[914] *Determann*, 2012 Stan. Tech. L. Rev. 7, Rn. 19.

[915] *Rosen*, 64 Stan. L. Rev. Online 88, 88.

[916] *Determann*, 2012 Stan. Tech. L. Rev. 7 Rn. 19; *Rosen*, 64 Stan. L. Rev. Online 88, 88.

[917] EuGH vom 13.05.2014 – C-131/12, *Google Spain*, ECLI:EU:C:2014:317 Rn. 81; vom 24.09.2019 – C136/17, *GC u. a.*, ECLI:EU:C:2019:773 Rn. 66; BVerfG vom 06.11.2019 – 1 BvR 276/17, *Recht auf Vergessen II*, NJW 2020, 314, Rn. 110.

generell vorrangig.[918] Allgemein ist die Ausgestaltung des Art. 17 DSGVO als Recht auf Vergessenwerden vor allem Symbolpolitik.[919]

Die sonstigen Ausnahmen der Art. 17 Abs. 3 lit. b–e DSGVO sind enger als diejenigen des CCPA. So sind zwar Art. 17 Abs. 3 lit. b, d, e DSGVO mit den Ausnahmen des CCPA für Aufbewahrungspflichten und zur Verteidigung von Rechtsansprüchen sowie mit der Forschungsausnahme vergleichbar.[920] Allerdings fehlen in der DSGVO die weitgefassten Ausnahmen des CCPA für berechtigte Interessen bei interner Nutzung durch das Unternehmen, für dinglich fixierte oder für Produktrückrufe erforderliche persönliche Informationen und für die Ausübung von Rechten jeder Art.[921] Die Ausnahme für die öffentliche Gesundheit in Art. 17 Abs. 3 lit. c DSGVO hat dagegen kein Äquivalent im CCPA – wohl weil für Gesundheitsdaten das branchenspezifische Datenschutzgesetz HIPAA ohnehin vorrangig anwendbar ist.[922]

Das engere Recht auf Löschung wird bis zu einem gewissen Grad dadurch aufgewogen, dass unter dem CCPA Unternehmen ebenfalls dazu verpflichtet sind, typisierte Speicherfristen bei Zweckfortfall festzulegen.[923] Speicherfristen sind in der Praxis entscheidender als das Recht auf Löschung, das betroffene Personen in Deutschland und Verbraucher:innen in Kalifornien nur selten ausüben.[924]

2. Ausübung

Das Recht auf Löschung des CCPA können Verbraucher:innen weitgehend in derselben Weise wie dessen Auskunftsrecht ausüben.[925] Unternehmen bestimmen ebenso wie für das Auskunftsrecht mindestens zwei Kontaktmöglichkeiten, die in der Regel eine gebührenfreie Telefonnummer und ein Webformular beinhalten müssen.[926] Unternehmen sollen bei einer Antragstellung über Webformulare einen zweistufigen Prozess verwenden, bei dem Verbraucher:innen zuerst einen

---

[918] BGH vom 27.07.2020, NJW 2020, 3436 Rn. 41. Unklar dazu: EuGH vom 24.09.2019, *GC et al.*, ECLI:EU:C:2019:773 Rn. 66: »im Allgemeinen« würden Interessen der betroffenen Person überwiegen, allerdings im Kontext von besonderen Kategorien personenbezogener Daten.

[919] *Schantz*, NJW 2016, 1841, 1845; *Worms* in: BeckOK DatenschutzR, DS-GVO Art. 17 Rn. 3.

[920] Cal. Civ. Code §§ 1798.105(d)(6), 1798.145(a)(1),(5).

[921] Cal. Civ. Code §§ 1798.105(d)(4),(7), 1798.145(g),(r).

[922] Cal. Civ. Code § 1798.145(c)(1)(A). Zu diesem selbst siehe Kapitel 2:B.I.2 (ab S. 19). und zu dessen vorrangigen Geltung siehe Kapitel 3:B.IV.2 (ab S. 76).

[923] Cal. Civ. Code § 1798.100(a). siehe Kapitel 3:D.III.1 (ab S. 169).

[924] So gibt die größte Suchmaschine Google für 2020 nur ca. 25.000 Löschanträge aus Deutschland an: *Google*, Entfernung von Inhalten gemäß europäischem Datenschutzrecht. Für den CCPA gibt Google nur 276 Löschanträge im Jahr 2020 an: *Google*, CCPA Transparency Report. Andere Statistiken verzeichnen im Durchschnitt ca. 50 Löschanträge pro 1.000.000 Verbraucher:innen in Kalifornien: *Barber*, Privacy Tech, Benchmarking CCPA-related data subject requests.

[925] Zu der Ausübung des Auskunftsrechts siehe Kapitel 3:C.III.2.a) (ab S. 125).

[926] Cal. Civ. Code § 1798.130(a)(1)(A); 11 C.C.R. § 7020(b).

Löschantrag abschicken und ihn anschließend bestätigen (*double-opt-in*-Verfahren).[927] Dies soll Verbraucher:innen vor einer versehentlichen, unwiderruflichen Löschung ihrer persönlichen Informationen schützen.[928] Ein solcher zweistufiger Prozess ist allerdings für Unternehmen freiwillig, damit Unternehmen dasselbe Verfahren für Löschanträge nach dem CCPA und der DSGVO nutzen können (es bestanden Bedenken, dass ein zweistufiges Verfahren dem Erleichterungsgebot des Art. 12 Abs. 2 S. 1 DSGVO widerspricht).[929] Das Unternehmen kann bei der Antragstellung fragen, ob die Verbraucher:innen nur einen Teil der persönlichen Informationen löschen wollen, solange das Unternehmen die Option, sämtliche persönlichen Informationen zu löschen, am prominentesten präsentiert.[930]

Die Anforderungen an das Identifizierungsverfahren entsprechen dem des Auskunftsanspruchs.[931] Dies soll nicht wie beim Auskunftsrecht Identitätsdiebstahl vermeiden, sondern den unberechtigten Verlust persönlicher Informationen verhindern. Ob dabei eine mittlere oder hohe Sicherheit der korrekten Identifizierung genügt, hängt davon ab, wie sensibel die zu löschenden persönlichen Informationen sind.[932] So ist bei dem Regelbeispiel Löschung von Familienfotos hohe Sicherheit erforderlich, bei dem Regelbeispiel Löschung des Browserverlaufs nur mittlere Sicherheit.[933]

Wenn das Unternehmen den Löschantrag ablehnt, muss es über das Widerspruchsrecht gegen Datenhandel informieren und fragen, ob der Verbraucher oder die Verbraucherin zumindest dem Datenhandel widersprechen will.[934] Dies soll Verbraucher:innen, die keinen Löschanspruch haben, zumindest ermöglichen, die Weiterverbreitung ihrer persönlichen Informationen zu verhindern.[935]

Das allgemeine Maßregelungsverbot des CCPA schützt Verbraucher:innen vor Benachteiligungen jeder Art, wenn sie ihr Recht auf Löschung ausüben.[936] Das Unternehmen kann finanzielle Anreize für eine weitere Speicherung anbieten,[937] was wegen der weit gefassten Ausnahmen für das Recht auf Löschung nur von begrenzter Relevanz ist. Finanzielle Anreize sind hauptsächlich dann relevant, wenn Verbraucher:innen einem Datenhandel zwar nicht widersprechen, aber Löschung verlangen. Regelbeispiel ist ein Bekleidungsgeschäft, das einen Gutschein von 5 $ entzieht, wenn Verbraucher:innen die Löschung ihrer persönlichen Informationen verlangen.[938] Dann verstößt das Entziehen des Gutscheins gegen

---

927 11 C.C.R. § 7020(d).
928 *Cal. Attorney General*, Initial Statement of Reasons, S. 16.
929 *Cal. Attorney General*, Final Statement of Reasons, S. 22.
930 11 C.C.R. § 7022(h).
931 Zu diesem siehe Kapitel 3:C.III.2.a) (ab S. 125).
932 11 C.C.R. § 7062(d).
933 11 C.C.R. § 7062(d).
934 11 C.C.R. § 7022(g).
935 *Cal. Attorney General*, Initial Statement of Reasons, S. 29 f.
936 Cal. Civ. Code § 1798.125(a)(1). Siehe Kapitel 3:C.I.4.a) (ab S. 100).
937 Cal. Civ. Code § 1798.125(a)(2),(b)(1).
938 11 C.C.R. § 7080(d)(2).

das Maßregelungsverbot, außer wenn der Gutscheinwert von 5 $ dem Wert der persönlichen Informationen entspricht und das Unternehmen die sonstigen Anforderungen an finanzielle Anreize eingehalten hat.[939]

Das Recht auf Löschung nach Art. 17 DSGVO üben betroffene Personen ebenso wie das Recht auf Auskunft nach Art. 15 DSGVO aus. Insoweit müssen Verantwortliche die Antragstellung nach Art. 12 Abs. 2 DSGVO möglichst erleichtern, während es keine detaillierten Regelungen für eine Identifizierung gibt.[940]

Bei Art. 17 DSGVO ist strittig, ob nach dieser Norm auch eine Löschpflicht ohne Verlangen der betroffenen Person besteht.[941] Dafür spricht der Wortlaut des Art. 17 Abs. 1 DSGVO a. A. (»und der Verantwortliche ist verpflichtet«).[942] Allerdings ist weder der konkrete-individuelle Maßstab[943] noch alle Fallgruppen des Art. 17 DSGVO[944] für eine automatische Löschung nach Speicherfristen geeignet. Daher ist es wohl überzeugender, die Pflicht, regelmäßig automatisch zu löschen, direkt aus Art. 5 Abs. 1 lit. c DSGVO herzuleiten.[945] In der Sache wirkt sich der Meinungsstreit kaum aus, da Speicherfristen nach beiden Ansichten unstrittig abstrakt-typisiert festzulegen sind.[946] Damit ähnelt im praktischen Ergebnis auch die Ansicht, die Speicherfristen auf Art. 17 DSGVO stützt, der separaten Pflicht des CCPA, typisierte Speicherfristen für den Zweckfortfall festzulegen.[947]

---

[939] 11 C. C. R. § 7080(d)(2).

[940] Siehe Kapitel 3:C.III.2.b) (ab S. 131).

[941] Für eine Löschpflicht: Handbuch IT- und Datenschutzrecht, § 34 Rn. 614; *Dix* in: NK-DatenschutzR, DS-GVO Art. 17 Rn. 6; *Franzen* in: Franzen/Gallner/Oetker, Europäisches Arbeitsrecht, EU (VO) 2016/679 Art. 17 Rn. 1; *Herbst* in: Kühling/Buchner, DS-GVO Art. 17 Rn. 35–47; *Hornung/Wagner*, ZD 2020, 223, 226; *Mennts/Hinzpeter* in: Taeger/Gabel, DS-GVO Art. 17 Rn. 84; *Nolte/Werkmeister* in: Gola, DS-GVO Art. 17 Rn. 9; *Paal* in: Paal/Pauly, DS-GVO Art. 17 Rn. 20; *Stürmer*, ZD 2020, 626, 628.
Gegen eine Löschpflicht: *Däubler* in: Däubler et al., EU-DSGVO Art. 17 Rn. 10; *Hornung/Wagner*, ZD 2020, 223, 228; *Kamin/Braun* in: Ehmann/Selmayr, DS-GVO Art. 17 Rn. 67; *Kamlah* in: Plath, DSGVO Art. 17 Rn. 6; *Peuker* in: Sydow, DSGVO Art. 17 Rn. 43.

[942] *Herbst* in: Kühling/Buchner, DS-GVO Art. 17 Rn. 8; *Stollhoff* in: Eßer/Kramer/Lewinski, DSGVO Art. 17 Rn. 36; *Peuker* in: Sydow, DSGVO Art. 17 Rn. 43.

[943] VG Wiesbaden vom 11.01.2021 – 6 K 1045/20.WI, ZD 2021, 230 Rn. 3; *Herbst* in: Kühling/Buchner, DS-GVO Art. 17 Rn. 17: »Prüfung in jedem Einzelfall«; *Worms* in: BeckOK DatenschutzR, DS-GVO Art. 17 Rn. 26.

[944] Insbesondere Art. 17 Abs. 1 lit. f DSGVO. Insoweit für eine teleologische Reduktion des Art. 17 DSGVO eintretend: *Herbst* in: Kühling/Buchner, DS-GVO Art. 17 Rn. 16.

[945] VG Karlsruhe vom 06.07.2017 – 10 K 7698/16, ZD 2017, 543. Rn. 18; *Dix* in: NK-DatenschutzR, DS-GVO Art. 17 Rn. 6; *Peuker* in: Sydow, DSGVO Art. 17 Rn. 43; *Plath* in: Plath, DSGVO Art. 5 Rn. 16.

[946] VG Karlsruhe vom 06.07.2017 – 10 K 7698/16, ZD 2017, 543. Rn. 18 »typisierte Regelprüffristen für wiederkehrende Vorgänge«; *Conrad* in: *Auer-Reinsdorff/Conrad*, Handbuch IT- und Datenschutzrecht, § 34 Rn. 617; *Plath* in: Plath, DSGVO Art. 5 Rn. 18.

[947] Siehe Kapitel 3:D.III.1 (ab S. 169).

3. Durchführung der Löschung

Bei einem begründeten Löschantrag muss das Unternehmen die persönlichen Informationen dauerhaft und vollständig löschen.[948] Als Löschung genügt es, die persönlichen Informationen zu deidentifizieren oder aggregieren und so den Personenbezug zu entfernen.[949]

Daten in Archiven oder Back-ups muss das Unternehmen erst löschen, wenn es diese das nächste Mal nutzt oder wiederherstellt.[950] Die vorherige gezielte Löschung einer Datei im Archiv ist häufig technisch unmöglich oder sehr aufwendig für Unternehmen – hat aber nur einen geringen Vorteil für Verbraucher:innen, da seine Daten nicht genutzt werden.[951] Anders als beim Auskunftsrecht erfasst das Recht auf Löschung aber nicht nur die in den letzten zwölf Monaten erhobenen persönlichen Informationen, sondern alle persönlichen Informationen unabhängig von deren Alter.[952]

Die Löschung muss das Unternehmen dem Verbraucher oder der Verbraucherin bestätigen.[953] Zudem ist verpflichtet, für spätere Kontrollen durch Aufsichtsbehörden die Löschanträge und seine Antworten 24 Monate aufzubewahren.[954] Es kann den Löschantrag auch dauerhaft dokumentieren, soweit dies nötig ist, damit die persönlichen Informationen gelöscht bleiben.[955]

Auch nach Art. 17 DSGVO muss der Verantwortliche die personenbezogenen Daten dauerhaft und endgültig löschen.[956] Regelungstechnisch ist Art. 17 DSGVO weniger spezifisch: so ist nicht festgelegt, wie Verantwortliche die Löschung durchführen sollen. Es gibt, anders als unter dem CCPA, keine explizite Ausnahme für Back-ups, allerdings wird eine gewisse Verzögerung der Löschung bei Back-ups allgemein als zulässig angesehen.[957] Anonymisierung ist auch unter der DSGVO eine Löschung, da *ratio legis* des Art. 17 DSGVO das Verhindern einer weiteren Verarbeitung personenbezogener Daten (Erwägungsgrund 65 S. 2 der DSGVO), nicht jedoch von Daten jeder Art ist.[958]

---

[948] 11 C.C.R. § 7022(b)(1).

[949] 11 C.C.R. § 7022(b)(1),(2). Siehe Kapitel 3:B.I.2 (ab S. 47).

[950] 11 C.C.R. § 7022(c).

[951] *Cal. Attorney General*, Initial Statement of Reasons, S. 20, *ders.*, Summary and Response to Comments Submitted During 45-Day Period, S. 153.

[952] *Stine/Kilian*, Computer & Internet Lawyer, May 2020, 3, 3.

[953] 11 C.C.R. § 7022(d).

[954] 11 C.C.R. §§ 7101(a), 7022(e).

[955] 11 C.C.R. § 7022(e).

[956] *Herbst* in: Kühling/Buchner, DS-GVO Art. 17 Rn. 37–40.

[957] *ICO* (UK), Right to erasure, Do we have to erase personal data from backup systems? (erschienen noch vor dem »Brexit«); *IHK Nürnberg f*ür Mittelfranken, Fragen an das BayLDA zur Ausgestaltung der DSGVO in der Praxis, Wie lösche ich DSGVO-konform Daten von Festplatten?; *Kamin/Braun* in: Ehmann/Selmayr, DS-GVO Art. 17 Rn. 36.

[958] *BfDI*, Anonymisierung, S. 8 f.; Österreichische Datenschutzbehörde vom 05.12.2018 – DSB-D123.270/0009-DSB/2018, D.3; *Meents/Hinzpeter* in: Taeger/Gabel, DS-GVO Art. 17

V. Recht auf Berichtigung

Der CCPA enthält ein mit Art. 16 DSGVO vergleichbares Recht auf Berichtigung.[959] Berichtigung ist ein dem amerikanischen Datenschutzrecht nicht fremder Gedanke, der sich in der Ausrichtung des amerikanischen Datenschutzes auf die Privatautonomie gut einfügt. So enthielten schon 1973 die unverbindlichen, aber einflussreichen »Fair Information Practice Principles« des U. S. Department of Health, Education & Welfare ein Berichtigungsrecht.[960] Bundesbehörden verpflichtet der Data Quality Act dementsprechend die Qualität und Integrität von Daten zu wahren (allerdings ohne zwischen personenbezogenen und nicht-personenbezogenen Informationen zu unterscheiden).[961] Zudem beinhalten zahlreiche branchenspezifische Datenschutzgesetze ein Recht auf Berichtigung. So regelt der HIPAA ein umfassendes Berichtigungsrecht für Patientenakten oder Krankenversicherungsakten.[962] Ähnliche Berichtigungsrechte bestehen auch gegenüber Wirtschaftsauskunfteien,[963] Kabelfernsehanbietern,[964] öffentlich finanzierten Schulen[965] und Bundesbehörden.[966]

Das mit Proposition 24[967] eingeführte Berichtigungsrecht erstreckt diese branchenspezifischen Berichtigungsrechte auf sämtliche Unternehmen. Verbraucher:innen können die Berichtigung aller unrichtigen persönlichen Informationen verlangen.[968] Dafür muss das Unternehmen wirtschaftlich vertretbare Anstrengungen unternehmen (»use commercially reasonable efforts«), um die Informationen zu korrigieren.[969] Wirtschaftlich vertretbare Anstrengungen bedeutet nicht, dass ein Unternehmen jedes mögliche Mittel ergreifen muss.[970] Vielmehr ist eine Berichtigung wirtschaftlich nicht vertretbar, wenn sie mit unangemessenen

---

Rn. 75; *Stürmer*, ZD 2020, 626, 628 f.; wohl auch *Thüsing/Rombey*, ZD 2021, 548, 551; a. A. *Roßnagel*, ZD 2021, 188–192 unter Verweis auf den Wortlaut und bestehende Restrisiken.

[959] Cal. Civ. Code § 1798.106.

[960] *U. S. Department of Health, Education & Welfare*, Records, Computers and the Rights of Citizens, S. 41; 1998 ebenso: *FTC*, Privacy Online: a Report to Congress, S. 9.

[961] Treasury and General Government Appropriations Act for Fiscal Year 2001, Pub.L. 106–554, 114 Stat. 2763A-154, Sec. 515. Umgesetzt in: Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies, 67 Fed. Reg. 369.

[962] 45 C. F. R. § 164.256.

[963] FCRA, 15 U. S. C. § 1681i.

[964] Cable Communications Policy Act, 47 U. S. C. § 551(d).

[965] FERPA, 20 U. S. C. § 1232g(a)(2).

[966] Privacy Act, 5 U. S. C. § 552a(d)(2).

[967] Zu diesem Volksbegehren siehe Kapitel 2:C.IV (ab S. 35).

[968] Cal. Civ. Code § 1798.106(a).

[969] Cal. Civ. Code § 1798.106(c).

[970] Vgl. Cal. Court of Appeal 3rd District vom 24.05.2012, *California Pines Property Owners Assn. v. Pedotti*, 206 Cal. App. 4th 384, 394 zur Formulierung »best efforts«. Diese entspricht »commercially reasonable efforts«: Cal. Court of Appeal 2nd District vom 03.03.2016, *Goldsholle v. Internet Brands, Inc.*, 2016 Cal. App. Unpub. LEXIS 1556, 23–24.

Kosten verbunden ist.[971] Dabei sind die Zwecke der Verarbeitung und der Art der persönlichen Informationen zu berücksichtigen.[972] Eine Berichtigungspflicht besteht nicht, wenn die Berichtigung unmöglich oder nur mit unangemessenem Aufwand möglich wäre.[973] Dies soll die California Privacy Protection Agency noch in der Durchführungsverordnung konkretisieren.[974]

Weiterhin muss das Unternehmen keine persönlichen Informationen korrigieren, die es nur im Auftrag anderer natürlicher Personen speichert.[975] Öffentlich verfügbare Informationen sind ohnehin keine persönlichen Informationen.[976] Darüber hinaus gelten alle Bereichsausnahmen des CCPA.[977]

Dieses Recht können Verbraucher:innen auf dieselbe Weise wie das Recht auf Löschung ausüben.[978] Dabei enthält der neue Verordnungsentwurf der California Privacy Protection Agency eine Verfahrensregelung, um die Richtigkeit der jeweiligen persönlichen Informationen festzustellen und Betrug zu verhindern.[979] Hiernach muss das Unternehmen im Einzelfall die Richtigkeit prüfen und dabei die Quelle der persönlichen Informationen berücksichtigen; dabei kann es auch Belege von den Verbraucher:innen anfordern.[980] Bei Gesundheitsdaten haben die Verbraucher:innen das Recht, einen schriftlichen Zusatz von bis zu 250 Wörtern zu ihrer jeweiligen Akte hinzuzufügen, wenn sie diese für unvollständig oder unrichtig halten.[981] Dies ähnelt dem Berichtigungsrecht des HIPAA, bei dem Patient:innen ebenfalls nach einer Ablehnung des Berichtigungsantrags verlangen können, eine ergänzende Erklärung in die jeweilige Akte aufzunehmen.[982] Das Berichtigungsrecht des CCPA füllt Lücken bei Gesundheitsdaten, wenn HIPAA nicht anwendbar ist.[983] Ansonsten verdrängt der vorrangige HIPAA diese Regelung.[984]

Art. 16 S. 2 DSGVO regelt hingegen ein allgemeines Recht auf Vervollständigung. Allerdings greift das Vervollständigungsrecht nur, wenn die personenbezogenen Daten im Hinblick auf den konkreten Verarbeitungszweck unrichtig oder lückenhaft

---

[971] Vgl. Cal. Court of Appeal 3rd District vom 24.05.2012, *California Pines Property Owners Assn. v. Pedotti*, 206 Cal. App. 4th 384, 394.

[972] Cal. Civ. Code § 1798.106(a).

[973] Cal. Civ. Code § 1798.185(a)(8)(A).

[974] Cal. Civ. Code § 1798.185(a)(8)(A).

[975] Cal. Civ. Code § 1798.145(k).

[976] Cal. Civ. Code § 1798.140(v)(2). Siehe Kapitel 3:B.I.3 (ab S. 50).

[977] Siehe Kapitel 3:B.IV.1 (ab S. 74).

[978] Cal. Civ. Code §§ 1798.106(3), 1798.130(a)(1),(2),(3), 1798.140(ak).

[979] Cal. Privacy Protection Agency, Proposed Regulations, § 7023. Die Verordnungsermächtigung enthält bereits Vorgaben für dieses Verfahren: Cal. Civ. Code § 1798.185(a)(8)(B),(C).

[980] Cal. Privacy Protection Agency, Proposed Regulations § 7023(b),(d).

[981] Cal. Civ. Code § 1798.185(a)(8)(D).

[982] 45 C. F. R. § 164.256(d)(2).

[983] Zum persönlichen Anwendungsbereich des HIPAA: 45 C. F. R. § 160.102(a).

[984] Cal. Civ. Code § 1798.145(c)(1)(A). Zu diesem selbst siehe Kapitel 2:B.I.2 (ab S. 19). und zu dessen vorrangiger Geltung siehe Kapitel 3:B.IV.2 (ab S. 76).

sind.[985] Die Abgrenzung zwischen lückenhaften und unrichtigen Daten ist ohnehin fließend, sodass der Unterschied nicht überbewertet werden sollte.

Auch sonst sind die Unterschiede zwischen beiden Berichtigungsrechten minimal. So ist Art. 16 DSGVO zwar nicht auf wirtschaftlich vertretbare Anstrengungen beschränkt, exzessive Anträge[986] kann der Verantwortliche jedoch ablehnen oder für ihre Erfüllung ein angemessenes Entgelt verlangen (Art. 12 Abs. 5 DSGVO).

Die DSGVO kennt eine *ipso iure* geltende Berichtigungspflicht (Art. 5 Abs. 1 lit. d DSGVO). Diese ist jedoch in der Praxis weitgehend irrelevant,[987] da wirtschaftlich rational handelnde Verantwortliche schon ein Eigeninteresse an möglichst korrekten personenbezogenen Daten haben (abgesehen von Teilen des Boulevardjournalismus, auf welchen die DSGVO ohnehin wegen des Medienprivilegs des Art. 85 DSGVO weitgehend unanwendbar ist).[988]

Obwohl die Unterschiede in der Praxis keine größere Rolle spielen dürften, liegt beiden Berichtigungsrechten doch eine unterschiedliche Regelungsphilosophie zu Grunde. In Europa ist ein Berichtigungsrecht bereits primärrechtlich in Art. 8 Abs. 2 S. 2 GRCh vorgesehen. Es soll die betroffene Person davor schützen, dass sich andere ein falsches Bild über sie machen.[989] Daher regelt die DSGVO auch eine Berichtigungspflicht, um solchen Risiken bereits präventiv zu begegnen. Das Berichtigungsrecht des CCPA soll dagegen Verbraucher:innen die Kontrolle über ihre eigenen persönlichen Informationen ermöglichen. Die fehlende Berichtigungspflicht fügt sich in das Bild ein, dass der CCPA einen starken Fokus auf Verbraucherrechte legt und Unternehmenspflichten eher untergeordnet behandelt.

VI. Ergebnis

Die Verbraucherrechte lassen sich in zwei Gruppen einteilen: das Widerspruchsrecht gegen Datenhandel und das Recht auf Beschränkung sensibler Informationen als globale Rechte auf der einen Seite sowie das Auskunfts-, Löschungs- und Berichtigungsrecht als individuelle Rechte auf der anderen Seite. Die globalen Rechte sollen alle Verbraucher:innen leicht und möglichst automatisiert ausüben können. Der Gesetzgeber hätte die globalen Rechte auch als Verbot mit Einwilligungsvorbehalt fassen können (*opt-in)*, hat sich aber wegen eines möglichen Verstoßes gegen die Meinungsfreiheit dagegen entschieden.

---

[985] OVG Hamburg vom 27.05.2019 – 5 Bf 225/18.Z, NVwZ 2019, 1532 Rn. 22; *Paal* in: Paal/Pauly, DS-GVO Art. 16 Rn. 18 m. w. N.

[986] Für ein Verständnis von »exzessiv« als besonders aufwendig: OLG Hamm vom 15.11.2021 – 20 U 269/21, BeckRS 2021, 40312 Rn. 9; *Korch/Chatard*, NZG 2020, 893, 896.

[987] *Schantz* in: BeckOK DatenschutzR, DS-GVO Art. 5 Rn. 27: »Richtigkeit der verarbeiteten Daten wird datenschutzrechtlich eher wenig Aufmerksamkeit geschenkt«. Ebenso vor Inkrafttreten der DSGVO: *Hoeren*, ZD 2016, 459, 459.

[988] Zum Medienprivileg siehe Kapitel 3:B.I.3.b) (ab S. 54).

[989] *Schantz* in: BeckOK DatenschutzR, DS-GVO Art. 5 Rn. 27.

Das Widerspruchsrecht gegen Datenhandel (»right to opt-out«)[990] soll Verbraucher:innen in die Lage versetzen zu verhindern, dass Unternehmen ihre persönlichen Informationen kommerziell verwerten. Datenhandel (»selling«[991] und »sharing«)[992] ist dabei weit definiert als jede Weiterübermittlung persönlicher Informationen an Dritte im Gegenzug zu einem auch nur geringen, indirekten Vorteil. Ungerechtfertigte Nachteile durch diesen pauschalen Widerspruch fängt der CCPA durch ausgewogene Ausnahmen auf, die insbesondere Übermittlungen an Dienstleister erlauben.

Verbraucher:innen sollen möglichst leicht widersprechen können. Ein individueller Widerspruch muss durch einen auffälligen Widerspruchslink auf der Webseite des Unternehmens jederzeit möglich sein.[993] Vor allem aber ermöglicht ein automatisches Widerspruchssignal gegenüber jeder besuchten Webseite einen pauschalen Widerspruch.[994]

Datenhandel ist auch nach dem Widerspruch zulässig, wenn der Verbraucher aufgrund finanzieller Anreize in ihn einwilligt.[995] Unternehmen müssen offenlegen, wie viel die persönlichen Informationen wert sind und wie sie diesen Wert berechnet haben.[996] Der Wert der finanziellen Anreize muss ungefähr dem Wert der persönlichen Informationen entsprechen.[997] Das Unternehmen ist verpflichtet, eine Nutzung des Angebots auch ohne diese finanziellen Anreize zu ermöglichen.[998] Ansonsten dürfen Unternehmen Verbraucher:innen nicht diskriminieren, weil diese Datenhandel widersprochen haben.[999]

Unternehmen dürfen mit persönlichen Informationen eines Minderjährigen unter 16 Jahren nur mit Einwilligung handeln, weil diese besonders schutzbedürftig sind (»right to opt-in«).[1000] Für Minderjährige bis zum 13. Lebensjahr müssen die jeweiligen Erziehungsberechtigten einwilligen; 13- bis 15-Jährige können selbst einwilligen.[1001]

Die DSGVO kennt kein Widerspruchsrecht gegen Datenhandel und regelt die Zulässigkeit von »Leistung gegen Daten« nur unzureichend. Dieses Geschäftsmodell steht in einem Spannungsverhältnis zum Koppelungsverbot des Art. 7 Abs. 4 DSGVO, dessen Inhalt nebulös ist. Das Schuldrecht regelt das Geschäftsmodell »Leistung gegen Daten« nur oberflächlich. Die Digitale-Inhalte-RL erwähnt in ihrem Erwägungsgrund 24 S. 1 kurz die Zulässigkeit dieses

---

990 Cal. Civ. Code § 1798.120.
991 Cal. Civ. Code § 1798.140(ad).
992 Cal. Civ. Code § 1798.140(ah).
993 Cal. Civ. Code § 1798.135(a)(1), 11 C.C.R. § 7026(a).
994 Cal. Civ. Code § 1798.135(e), 11 C.C.R. § 7026(c).
995 Cal. Civ. Code § 1798.125(b).
996 11 C.C.R. § 7016(b)(2),(5).
997 Cal. Civ. Code § 1798.125(a)(2),(b)(1), 11 C.C.R. § 7080(b).
998 Cal. Civ. Code § 1798.125(b)(3).
999 Cal. Civ. Code § 1798.125(a)(1).
1000 Cal. Civ. Code § 1798.120(c).
1001 Cal. Civ. Code § 1798.120(c).

Geschäftsmodells und definiert es in Art. 3 Abs. 1 UAbs. 1 Digitale-Inhalte-RL, regelt aber nur Leistungsstörungen solcher Verträge. Insoweit besteht eine Regelungslücke, die *de lege ferenda* durch eine Übernahme der Regelung des CCPA für finanzielle Anreize gefüllt werden sollte.[1002]

Das zweite globale Recht ist das Recht auf Beschränkung sensibler Informationen (»right to limit use and disclosure of sensitive personal information«).[1003] Dieses schützt ähnliche Daten wie Art. 9 DSGVO, wobei es um bestimmte, einen Identitätsdiebstahl ermöglichende Informationen erweitert ist.[1004] Anders als Art. 9 Abs. 1 DSGVO gilt die beschränkte Nutzung sensibler Daten nicht *ipso iure*, sondern nur, wenn Verbraucher:innen dieses Recht ausüben. Dann dürfen Unternehmen die sensiblen Informationen nur für die Vertragserfüllung und bestimmte sekundäre Zwecke nutzen,[1005] die allerdings deutlich weiter als Art. 9 Abs. 2 DSGVO ist. Die Ausübung ist parallel zu dem Widerspruchsrecht gegen Datenhandel möglichst leicht gestaltet.

Das Auskunftsrecht (»right to access«)[1006] ist zwar nicht auf eine leichte Ausübung gerichtet, ist aber dennoch ein weitreichendes Instrument, um Transparenz herzustellen. Das Unternehmen ist verpflichtet, die konkreten persönlichen Informationen sowie mit Art. 15 Abs. 1 DSGVO vergleichbare Metainformationen über die Verarbeitung mitzuteilen. Die zu beauskunftenden persönlichen Informationen muss das Unternehmen in einer interoperablen Form bereitstellen – was aber wie das Recht auf Datenübertragbarkeit gemäß Art. 20 DSGVO bisher totes Recht ist. Detailliert geregelte Ausnahmen schützen die Interessen des Unternehmens, Dritter sowie auch des Verbrauchers oder der Verbraucherin. Dabei ist das Identifizierungsverfahren ausführlich geregelt,[1007] um Identitätsdiebstahl zu verhindern.

Das Recht auf Löschung des CCPA[1008] ist wegen der hohen Bedeutung der Meinungsfreiheit im amerikanischen Recht deutlich enger als Art. 17 DSGVO. Es ist nicht auf Schutz des eigenen Bildes in der Öffentlichkeit, sondern auf Kontrolle der eigenen persönlichen Informationen ausgerichtet. Daher erfasst es nur bei den jeweiligen Verbraucher:innen direkt erhobene Informationen, die weder von öffentlichem Interesse noch öffentlich frei verfügbar sind. Zudem greifen weit gefasste Ausnahmen. Ein Recht auf Vergessenwerden, wie es Art. 17 DSGVO in begrenzten Maß statuiert, wäre mit dem amerikanischen Verständnis eines freien Informationsflusses im *marketplace of ideas* unvereinbar.

Der CCPA regelt schließlich wie zahlreiche andere amerikanische Datenschutzgesetze ein Recht auf Berichtigung.[1009] Dieses ist in seiner näheren Aus-

---

[1002] Siehe Kapitel 4:B (ab S. 241).
[1003] Cal. Civ. Code § 1798.121.
[1004] Definition in: Cal. Civ. Code § 1798.140(ae).
[1005] Cal. Civ. Code § 1798.121(a).
[1006] Cal. Civ. Code §§ 1798.110(a),(b), 1798.115(a),(b).
[1007] Cal. Civ. Code § 1798.140(ak); 11 C.C.R. § 7060–7063.
[1008] Cal. Civ. Code § 1798.105.
[1009] Cal. Civ. Code § 1798.106.

gestaltung dem Recht auf Berichtigung in Art. 16 DSGVO nachempfunden. Es unterscheidet sich von diesem nur in Details.

D. Unternehmenspflichten

I. Informationspflichten

1. Einleitung und Überblick

Transparenz ist ein Kernprinzip des CCPA.[1010] Verbraucher:innen sollen sich informiert für oder gegen bestimmte Unternehmen entscheiden können.[1011] Zudem ermöglicht die geschaffene Transparenz Interessengruppen, Medien, Wissenschaft und Aufsichtsbehörden, missbräuchlich handelnde Unternehmen zur Rechenschaft zu ziehen.[1012]

Transparenz ist ein Grundpfeiler des amerikanischen Rechts.[1013] Schon die Verfassungsväter betonten den hohen Wert frei verfügbarer Informationen für den öffentlichen Diskurs.[1014] Der spätere Richter am U. S. Supreme Court *Brandeis* fasste das amerikanische Verständnis der Transparenz bereits 1914 prägnant zusammen: »Sunlight is said to be the best of disinfectants; electric light the most efficient policeman«.[1015] Das amerikanische Recht hat dementsprechend neben umfangreichen Informationsfreiheitsgesetzen für staatliche Einrichtungen[1016] zahlreiche Informationspflichten für Wirtschaftsunternehmen entwickelt. Diese Entwicklung begann 1933 im Kapitalmarktrecht[1017] und erstreckt sich mittlerweile auf nahezu jedes Rechtsgebiet.[1018]

Im amerikanischen Datenschutzrecht bestanden dementsprechend bereits vor dem CCPA umfassende Informationspflichten. Kalifornien verpflichtete bereits seit 2003 Webseiten, Datenschutzerklärungen zu veröffentlichen.[1019] Auch enthalten zahlreiche branchenspezifische Datenschutzgesetze Informationspflichten.[1020] Vor allem aber zeigt sich der Fokus auf Transparenz im *notice-and-choice*-Modell

---

[1010] *Buresh*, 6 IJICL 257, 275; *Chander/Kaminski/McGeveran*, 105 Minn. L. Rev. 1733, 1750 f.

[1011] Proposition 24 (Cal. 2020), Sec. 2(G).

[1012] *Cal. Attorney General*, Summary and Response to Comments Submitted During 45-Day Period, S. 221, 232.

[1013] *Fung/Graham/Weil*, Full disclosure: the perils and promise of transparency, S. 19–34; *Kwoka*, 127 Yale L. J. 2204, 2211.

[1014] *Fung/Graham/Weil*, Full disclosure: the perils and promise of transparency, S. 24.

[1015] *Brandeis*, Other people's money, and how the bankers use it, S. 92.

[1016] Siehe Kapitel 3:C.III.1.a) (ab S. 116).

[1017] Securities Act of 1933, Pub.L. 73–22, 48 Stat. 74.

[1018] *Fung et al.*, Full disclosure, S. 24–34.

[1019] California Online Privacy Protection Act of 2003, A. B. 68, 2002–03 Leg., Reg. Sess. (Cal. 2003), kodifiziert in Cal. Bus & Prof. Code § 22575.

[1020] Zu den Informationspflichten des GLBA, des HIPAA und des COPPA siehe Kapitel 2:B.I.2 (ab S. 19).

der FTC. Nach diesem müssen Unternehmen Verbraucher:innen über eine Datenverarbeitung informieren (*notice)* und zumindest eine Widerspruchsmöglichkeit einräumen (*choice)*. Dieses Modell hat sich in der amerikanischen Rechtspraxis weitgehend durchgesetzt, ist aber wegen häufig langer, unverständlicher und schwammiger Datenschutzerklärungen umstritten.[1021]

Der CCPA baut auf dem *notice-and-choice*-Modell auf, soll aber auch dessen Probleme lösen. Er erwähnt in seinen Erwägungsgründen mithin explizit lange, komplexe und unklare Datenschutzerklärungen.[1022] Als Reaktion darauf regelt er ein zweistufiges System:[1023] auf der ersten Ebene enthält ein kurzer Datenschutzhinweis die wichtigsten Informationen für Verbraucher:innen. Dieser Datenschutzhinweis soll den Verbraucher:innen ermöglichen, sich informiert für oder gegen einen Vertragsschluss mit dem jeweiligen Unternehmen zu entscheiden. Auf der zweiten Ebene schafft eine umfassende Datenschutzerklärung Transparenz für die Öffentlichkeit als Ganzes. Daneben bestehen Informationspflichten für das Widerspruchsrecht gegen Datenhandel und bei dem Angebot finanzieller Anreize.[1024]

2. Umfang: Zweistufiges System

a) Kurzer Datenschutzhinweis

aa) Inhalt

Den kurzen Datenschutzhinweis (»notice at collection«) muss das Unternehmen bei Erhebung der persönlichen Informationen bereitstellen.[1025] Er soll vergleichbar zu einer Lebensmittel-Zutatenliste eine informierte Entscheidung über den Vertragsschluss mit dem jeweiligen Unternehmen ermöglichen.[1026] Wie Lebensmittelkennzeichnungen enthält der kurze Datenschutzhinweis auf das Wesentliche reduzierte Informationen.

Der kurze Datenschutzhinweis besteht aus zwei Listen:
1. die Kategorien der erhobenen persönlichen Informationen.[1027] Die Kategorienbegriffe sind dabei vorgegeben durch die 137 Regelbeispiele in der Legaldefinition persönlicher Informationen.[1028]

[1021] Siehe Kapitel 2:B.I.3 (ab S. 24).

[1022] Proposition 24 (Cal. 2020), Sec. 2(E) a.E.

[1023] Einen ähnlichen, gut durchdachten Vorschlag enthält: *American Law Institute*, Principles of the law, data privacy, §§ 3, 4.

[1024] Zu der Informationspflicht über das Widerspruchsrecht gegen Datenhandel siehe Kapitel 3:C.I.2.b)bb) (ab S. 87). Zu der Informationspflicht bei finanziellen Anreizen siehe Kapitel 3:C.I.4.b)aa) (ab S. 101).

[1025] Cal. Civ. Code § 1798.100(a), 11 C.C.R. § 7012(b)(3).

[1026] Proposition 24 (Cal. 2020), Sec. 2(G).

[1027] Cal. Civ. Code § 1798.100(a)(1), 11 C.C.R. § 7012(b)(1).

[1028] Cal. Civ. Code §§ 1798.130(c), 1798.140(v)(1). Zur Definition siehe Kapitel 3:B.I.1.a) (ab S. 43). Die Durchführungsverordnung enthält insoweit die noch auf dem CCPA-2018 basierende Anforderung, dass die Kategorien »meaningful« sein sollen, 11 C.C.R. § 7012(b)

2. die Kategorien der gesammelten sensiblen Informationen,[1029] welche ebenso den 23 Kategorien der Legaldefinition sensibler Informationen folgen müssen.[1030]

Separat für jede Kategorie persönlicher oder sensibler Informationen enthält der kurze Datenschutzhinweis zudem:
- die Zwecke der Erhebung und späteren Nutzung.[1031]
- die Speicherfrist.[1032] Falls eine exakte Angabe nicht möglich ist, müssen Unternehmen zumindest die Kriterien für die Festlegung der Speicherfrist mitteilen.[1033]
- ob das Unternehmen mit den persönlichen Informationen handelt.[1034] Wenn dies für eine Kategorie der Fall ist, muss das Unternehmen auf das Widerspruchsrecht gegen Datenhandel hinweisen (online: mit einem Link »Do Not Sell or Share My Personal Information«).[1035]

Schließlich muss der kurze Datenschutzhinweis auf die umfassende Datenschutzerklärung hinweisen (online: mit einem Link).[1036] Dadurch sollen sich interessierte Verbraucher:innen detaillierter informieren können.[1037]

Unklar ist, wie spezifisch Unternehmen über den Zweck informieren müssen. Nach den Erwägungsgründen der Proposition 24 sollen Unternehmen zwar persönliche Informationen nur für »specific […] purposes« nutzen.[1038] Im Gesetzestext des CCPA findet sich dies aber nicht wieder. Erwägungsgründe kalifornischer Gesetze können zwar für die Auslegung berücksichtigt werden, haben aber wie im Europarecht keinen eigenständigen Regelungsgehalt.[1039] Daher muss der Zweck im kurzen Datenschutzhinweis nur abstrakt angegeben werden. Die verpflichtende Auflistung der erhobenen persönlichen Informationen kann Unternehmen motivieren, den Zweck verständlich zu erklären und sich so zu rechtfertigen. Allerdings bildet die Zweckbezeichnung zugleich Grundlage der Zweckbindung.[1040] Unternehmen haben dadurch einen Anreiz, den Zweck offen und schwammig

---

(1). Dies ist durch den von Proposition 24 eingefügten Cal. Civ. Code § 1798.130(c) allerdings wohl überholt.

[1029] Cal. Civ. Code § 1798.100(a)(2).

[1030] Cal. Civ. Code § 1798.130(c). Zur Definition sensibler Informationen siehe Kapitel 3:C.II.1.a) (ab S. 109).

[1031] Cal. Civ. Code § 1798.100(a)(1),(2), 11 C.C.R. § 7012(b)(2).

[1032] Cal. Civ. Code § 1798.100(a)(3).

[1033] Cal. Civ. Code § 1798.100(a)(3).

[1034] Cal. Civ. Code § 1798.100(a)(1),(2). Zur Datenhandelsdefinition siehe Kapitel 3:C.I.2.a) (ab S. 82).

[1035] 11 C.C.R. § 7012(b)(3).

[1036] 11 C.C.R. § 7012(b)(4).

[1037] *Cal. Attorney General*, Initial Statement of Reasons, S. 9.

[1038] Proposition 24 (Cal. 2020), Sec. 3(B)(2).

[1039] Cal. Supreme Court vom 06.05.2019, *FilmOn.com Inc. v. DoubleVerify Inc.*, 7 Cal. 5th 133, 151. Ebenso auf Bundesebene: U.S. Supreme Court vom 31.03.2009, *Hawaii v. Office of Hawaiian Affairs*, 556 U.S. 163, 175.

[1040] Cal. Civ. Code § 1798.100(a)(1),(2).

zu beschreiben, um sich für die Zukunft viele Handlungsoptionen offenzuhalten. Zukünftig könnte die California Privacy Protection Agency Unternehmen in der Durchführungsverordnung verpflichten, den Zweck exakt anzugeben.[1041]

Unternehmen müssen den kurzen Datenschutzhinweis vor oder bei der Erhebung persönlicher Informationen leicht zugänglich bereitstellen.[1042] Ohne einen solchen Hinweis dürfen sie keine persönlichen Informationen erheben.[1043] Auf seiner Webseite muss das Unternehmen den Datenschutzhinweis auf der Startseite prominent verlinken.[1044] Bei Smartphone-Apps soll der Datenschutzhinweis-Link sowohl auf der Download-Seite abrufbar als auch über die Smartphone-Apps selbst zugänglich sein.[1045] Falls die App persönliche Informationen erhebt, die nicht berechtigterweise zu erwarten sind, muss das Unternehmen auf die zusätzlich erhobenen persönlichen Informationen in einem Pop-Up hinweisen.[1046] Bei einer Erhebung persönlicher Informationen mittels eines Papierformulars soll das Unternehmen den Hinweis in das Formular aufnehmen und bei einer persönlichen Erhebung mündlich erteilen.[1047] Einzelhandelsunternehmen sind gehalten, ein Schild mit dem kurzen Datenschutzhinweis nahe der Kasse aufzustellen.[1048]

Wenn das Unternehmen als Dritter handelt, muss es den Datenschutzhinweis zumindest auf seiner Webseite verlinken.[1049] Unternehmen handeln als Dritte im Sinne des CCPA, wenn sie nicht im direkten Kontakt mit den jeweiligen Verbraucher:innen stehen.[1050] Bei einer Erhebung auf seinem Firmengelände ohne direkten Kontakt mit Verbraucher:innen (z. B. bei Videoüberwachung) muss das Unternehmen den kurzen Datenschutzhinweis vor Ort klar und deutlich bereitstellen.[1051] In diesem Fall enthält der kurze Datenschutzhinweis keine Speicherfristen und keine gesonderte Liste sensibler Informationen.[1052] Datenhändler, die ebenfalls typischerweise nicht im direkten Kontakt mit Verbraucher:innen stehen, müssen keinen kurzen Datenschutzhinweis bereitstellen, wenn die gleichen Informationen bereits aus dem kalifornischen Datenhändlerregister

---

[1041] Die Verordnungsermächtigung enthält eine Generalklausel zur Harmonisierung der Informationspflichten: Cal. Civ. Code § 1798.185(a)(22).

[1042] Cal. Civ. Code § 1798.100(a), 11 C.C.R. § 7012(a)(3).

[1043] 11 C.C.R. § 7012(a)(6).

[1044] 11 C.C.R. § 7012(a)(3)(A).

[1045] 11 C.C.R. § 7012(a)(3)(B).

[1046] 11 C.C.R. § 7012(a)(4). Vgl. *Artikel-29-Datenschutzgruppe*, WP 260 Transparenz, Rn. 15: Verantwortliche »sollten« die betroffene Personen auf unerwartete Verarbeitung gesondert hinweisen.

[1047] 11 C.C.R. § 7012(a)(3)(C),(d).

[1048] Cal. Attorney General, Initial Statement of Reasons, S. 6.

[1049] Cal. Civ. Code §§ 1798.100(b), 1798.140(ai)(1).

[1050] Zum Konzept eines Unternehmens als Dritten siehe Kapitel 3:B.II.4 (ab S. 71).

[1051] Cal. Civ. Code § 1798.100(b).

[1052] Cal. Civ. Code § 1798.100(b).

hervorgehen.[1053] Insoweit genüge die Transparenz, welche dieses öffentliche Register schaffe.[1054]

bb) Effektivität

Inwieweit hilft der kurze Datenschutzhinweis tatsächlich Verbraucher:innen? Transparenzvorschriften sind schwierig zu gestalten.[1055] Damit sie tatsächlich zu einer inhaltlichen Änderung führen, müssen sie einen komplexen Prozess in Gang setzen. Dies setzt voraus, dass die jeweiligen Adressat:innen die erhaltenen Informationen tatsächlich in ihre Entscheidungen einbeziehen. Zuerst müssen die Informationen für die Adressat:innen wertvoll sein. Wenn sich diese schlichtweg nicht für ein Thema interessieren, wird erhöhte Transparenz zu keiner Verhaltensänderung führen. Die gebotene Information muss zudem leicht zugänglich sein. Vor allem aber ist entscheidend, ob die Informationsnutzenden sie verstehen können. Wenn insbesondere Verbraucher:innen mit zu vielen Informationen überhäuft werden oder die Informationen für sie unverständlich sind, ist ein Ignorieren dieser Informationen rational.

Gemessen daran sind die im kurzen Datenschutzhinweis bereitgestellten Informationen für Verbraucher:innen hilfreich. Die Auswahl der mitzuteilenden Informationen ist am Prinzip der Datenminimierung ausgerichtet. Verbraucher:innen können auf einen Blick erkennen, ob das Unternehmen mehr oder sensiblere Informationen als nötig erhebt, diese länger als erforderlich speichert oder durch Datenhandel weiterverbreitet. Mit dem obligatorischen Widerspruchslink können sie von Anfang an verhindern, dass das Unternehmen ihre persönlichen Informationen kommerziell verwertet und weiterverbreitet.[1056] Die Zweckangabe ermöglicht es Verbraucher:innen zu prüfen, warum das Unternehmen die persönlichen Informationen benötigt.[1057]

Datenminimierung ist ein allgemein anerkanntes Prinzip, das für die Entscheidung über einen Vertragsschluss von Verbraucher:innen relevant ist. In einer repräsentativen Umfrage von *Hoofnagle et al.* haben 88 % der befragten Amerikaner:innen angegeben, dass sie bereits einen Vertragsschluss abgelehnt haben, weil der Anbieter offensichtlich unnötige persönliche Informationen abgefragt habe.[1058] Vor oder zum Zeitpunkt der ersten Erhebung persönlicher Informationen wird der Vertragsschluss häufig noch ausstehen.

[1053] 11 C.C.R. § 7012(e). Das Datenhändlerregister ist geregelt in: Cal. Civ. Code § 1798.99.80–88.

[1054] Cal. Attorney General, Initial Statement of Reasons, S. 12.

[1055] Die folgende Darstellung der Anforderungen an Transparenzvorschriften beruht auf: *Fung/Graham/Weil*, Full disclosure: the perils and promise of transparency, S. 54–65.

[1056] *Cal. Attorney General*, Initial Statement of Reasons, S. 9.

[1057] Vgl. allgemein zur Zweckangabe: *Hintze*, 76 Md. L. Rev. 1044, 1073.

[1058] *Hoofnagle et al.*, How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes & Policies?, S. 10.

Der kurze Datenschutzhinweis ist nur mittelmäßig zugänglich. Verbraucher:innen müssen erst nach diesem aktiv suchen (z. B. online auf einen Link klicken).[1059] Die Aufteilung bei Smartphone-Apps zwischen einer aktiven Ansprache für nicht überraschende Verarbeitungen persönlicher Informationen und einem bloßen Link für zu erwartende Verarbeitungen ist sinnvoll.[1060] Sie ist allerdings offen formuliert, da unklar ist, welche Verarbeitungen zu erwarten sind. Dies gibt Unternehmen einen erheblichen Spielraum, sie zu umgehen.

Die Verständlichkeit ist eher positiv zu bewerten. Datenminimierung ist ein leicht verständliches und allgemein bekanntes Prinzip. Auch reduziert der Datenschutzhinweis die Informationsmenge deutlich. Verbraucher:innen können schon allein an der Länge der Liste erhobener persönlicher Informationen erkennen, inwieweit ein Unternehmen Datenminimierung beherzigt. Die standardisierten Begriffe für Kategorien persönlicher Informationen verhindern, dass Unternehmen ihre Datenverarbeitung mit einer nichtssagenden Wortwahl verschleiern. Die Angabe der Zwecke ist nicht standardisiert – was allerdings wohl angesichts der Vielfalt der erfassten Verarbeitungssituationen nur schwer möglich ist. Schwerer wiegt, dass keine genaue Form des Datenschutzhinweises vorgegeben ist (z. B. als Tabelle). So können Verbraucher:innen verschiedene Unternehmen nur mit erheblichem Aufwand vergleichen.

b) Umfassende Datenschutzerklärung

aa) Inhalt für alle Unternehmen

Die umfassende Datenschutzerklärung (»privacy policy«) soll ein detailliertes Gesamtbild der Datenverarbeitung eines Unternehmens bieten.[1061] Sie enthält zwar auch weiterführende Informationen für besonders interessierte Verbraucher. Vor allem aber dient sie der Transparenz für die Öffentlichkeit als Ganzes.[1062] Die umfassende Datenschutzerklärung bezieht sich daher nicht auf eine konkrete Verarbeitungssituation, sondern auf das gesamte Unternehmen. Sie ist eine einheitliche Anlaufstelle für Informationen zur Datenverarbeitung online wie offline. Dabei informiert sie darüber, wie das Unternehmen persönliche Informationen nutzt und welche Verbraucherrechte bestehen.

Erstens muss jedes Unternehmen umfassende Informationen über seine Datenverarbeitung der letzten zwölf Monate mitteilen:

[1059] 11 C.C.R. § 7012(a)(3)(A).

[1060] 11 C.C.R. § 7012(a)(4).

[1061] Vgl. 11 C.C.R. § 7011(a)(1): »comprehensive description of a business's online and offline practices«.

[1062] Speziell zu der Verbraucherrechte-Statistik: Cal. Attorney General, Initial Statement of Reasons, S. 14.

– die erhobenen Kategorien persönlicher Informationen.[1063] Dabei muss das Unternehmen die Regelbeispiel-Begriffe aus der Legaldefinition persönlicher Informationen verwenden.[1064]
– die Kategorien der Quellen.[1065] Die Quellenangabe muss so genau sein, um den Quellentyp zu verstehen.[1066] Zulässig sind z. B. die Quellenangaben »advertising network«, »government entities« oder »the consumer directly« (wobei es hierfür keine abschließende Liste gibt).[1067]
– die Zwecke der Erhebung und späteren Nutzung[1068] in aussagekräftiger Weise.[1069]
– ob das Unternehmen mit persönlichen Informationen handelt.[1070] Wenn das Unternehmen keinen Datenhandel betreibt, muss es diese Tatsache mitteilen.[1071]
– ob es nach seiner Kenntnis mit persönlichen Informationen von Unter-16-Jährigen handelt.[1072]
– in zwei separaten Listen die Kategorien der an Dienstleister und an Dritte im Rahmen eines Datenhandels übermittelten persönlichen Informationen.[1073] Pro Kategorie persönlicher Informationen muss das Unternehmen auch die Kategorien der Dienstleister und Käufer angeben, welche die persönlichen Informationen erhalten haben.[1074]
– eine Kontaktmöglichkeit, die dem Weg entsprechen muss, wie das Unternehmen hauptsächlich mit Verbraucher:innen interagiert (beispielsweise bei einem Online-Shop eine E-Mail-Adresse).[1075]
– das Datum der letzten Aktualisierung, die mindestens alle zwölf Monate erfolgen muss.[1076]

Zweitens erklärt die umfassende Datenschutzerklärung die Verbraucherrechte. Ein Unternehmen muss darüber aufklären, dass ein Recht auf Löschung, auf Berichtigung, auf Auskunft, auf Nicht-Diskriminierung und ein Widerspruchsrecht

---

[1063] Cal. Civ. Code §§ 1798.110(c)(1), 1798.130(a)(5)(B)(i), 11 C.C.R. § 7011(c)(1)(D).
[1064] Cal. Civ. Code §§ 1798.130(a)(5)(B)(i),(c).
[1065] Cal. Civ. Code §§ 1798.110(c)(2), 1798.130(a)(5)(B)(ii), 11 C.C.R. § 7011(e).
[1066] 11 C.C.R. § 7001(d).
[1067] 11 C.C.R. § 7001(d).
[1068] Cal. Civ. Code §§ 1798.110(c)(3), 1798.130(a)(5)(B)(iii); 11 C.C.R. § 7011(c)(1)(F).
[1069] 11 C.C.R. § 7011(c)(1)(F). Die Anforderung an die Genauigkeit der Zweckangabe findet sich so nur bei der umfassenden Datenschutzerklärung, nicht in dem kurzen Datenschutzhinweis.
[1070] Cal. Civ. Code § 1798.115(c)(1), 11 C.C.R. § 7011(c)(3)(B). Zum Datenhandelsbegriff siehe Kapitel 3:C.I.2 (ab S. 82).
[1071] Cal. Civ. Code §§ 1798.115(c)(1), 1798.130(a)(5)(C)(i), 11 C.C.R. §§ 7011(c)(3)(B).
[1072] 11 C.C.R. § 7011(c)(1)(G)(3).
[1073] Cal. Civ. Code §§ 1798.110(c)(4), 1798.115(c), 1798.130(a)(5)(C), 11 C.C.R. § 7011(c)(1)(G)(1).
[1074] Cal. Civ. Code §§ 1798.110(c)(4), 1798.115(c), 1798.130(a)(5)(B)(iv),(C), 11 C.C.R. § 7011(c)(1)(G)(2).
[1075] 11 C.C.R. § 7011(c)(6)(A), (c)(7).
[1076] 11 C.C.R. § 7011(c)(7).

gegen Datenhandel besteht.[1077] Es ist verpflichtet zu erklären, wie Verbraucher:innen diese ausüben können und wie es Verbraucher:innen im Allgemeinen[1078] identifiziert (insbesondere welche Informationen zur Identifizierung nötig sind).[1079] Das Unternehmen muss auch über diese Rechte aufklären, wenn es sie für nicht einschlägig hält.[1080] Zudem weist die umfassende Datenschutzerklärung darauf hin, dass Verbraucher:innen auch Datenschutzagenturen bevollmächtigen können und wie diese die Verbraucherrechte ausüben können.[1081] Das Recht auf Beschränkung sensibler Informationen fehlt bisher, wobei die California Privacy Protection Agency eine Ergänzung in ihrer Durchführungsverordnung plant.[1082]

bb) Verbraucherrechte-Statistik für besonders große Unternehmen

Drittens müssen besonders große Unternehmen eine jährliche Verbraucherrechte-Statistik in ihrer umfassenden Datenschutzerklärung veröffentlichen.[1083] Besonders groß ist ein Unternehmen, wenn es persönliche Informationen von mehr als zehn Millionen Verbraucher:innen in einem Kalenderjahr entweder erhält oder an Dritte weitergibt.[1084] Dieser Schwellenwert entspricht einem Viertel der kalifornischen Bevölkerung, da Verbraucher:innen nur Personen mit Wohnsitz oder gewöhnlichen Aufenthalt in Kalifornien sind.[1085] Daher dürfte diese Pflicht nur die wenigsten Unternehmen betreffen, was den Fokus des CCPA auf große Unternehmen unterstreicht. Kleine Unternehmen sollen nicht durch die Umsetzungskosten übermäßig belastet werden.[1086] Bei großen Unternehmen fällt der Aufwand dagegen verhältnismäßig weniger ins Gewicht. Daher verstößt auch diese Verbraucherrechte-Statistik nicht gegen das *First Amendment*: sie

---

[1077] Cal. Civ. Code §§ 1798.110(c)(5), 1798.130(a)(5)(A), 11 C.C.R. § 7011(c)(1)(A),(2)(A),(3)(A),(4)(A).

[1078] Die Einschränkung auf eine allgemeine Beschreibung des Identifizierungsverfahren soll das böswillige Ausnutzen von dessen Schwächen verhindern: Cal. Attorney General, Initial Statement of Reasons, S. 19.

[1079] Cal. Civ. Code § 1798.130(a)(5)(A), 11 C.C.R. § 7011(c)(1)(B),(c)(1)(C),(c)(2)(B),(c)(2)(C).

[1080] *Cal. Attorney General*, Summary and Response to Comments Submitted During 45-Day Period, S. 92.

[1081] 11 C.C.R. § 7011(c)(5)(A).

[1082] Cal. Privacy Protection Agency, Proposed Regulations, § 7011(e)(2)(E).

[1083] 11 C.C.R. § 7102(a).

[1084] 11 C.C.R. § 7102(a) a.A.

[1085] Cal. Civ. Code § 1798.140(i). Zu dieser Definition siehe Kapitel 3:B.II.1 (ab S. 56). Kalifornien hatte zum Stichtag der letzten Volkszählung (01.04.2020) 39.538.223 Einwohner:innen: *U. S. Census Bureau*, 2020 Census Apportionment Results.

[1086] *Cal. Attorney General*, Summary and Response to Comments Submitted During 45-Day Period, S. 226.

ist zwar *compelled speech,* wird allerdings von einem gewichtigen öffentlichen Interesse getragen und ist auch nicht übermäßig belastend.[1087]

In der Verbraucherrechte-Statistik müssen Unternehmen angeben, wie viele Anträge auf Löschung und Auskunft sowie Widerspruchserklärungen gegen Datenhandel sie erhalten haben.[1088] Für jede dieser drei Kategorien sind sie verpflichtet, anzugeben, wie lange sie für die Antwort benötigt haben (nach ihrer Wahl als Durchschnitt oder Median) und in wie vielen Fällen die Antwort positiv, teilweise positiv oder negativ ausgefallen ist.[1089] Sie können freiwillig zusätzlich Ablehnungsgrund-Kategorien angeben.[1090] Ebenso dürfen sie die Zahlen hinsichtlich aller Individuen ausweisen[1091] – dies dürfte vor allem für Unternehmen sinnvoll sein, welche die Verbraucherrechte des CCPA zur Vereinfachung auch auf Nicht-Verbraucher:innen erstrecken. Auf Anfrage des kalifornischen Attorney General müssen sie dennoch die Zahlen für Verbraucher:innen im Sinne des CCPA mitteilen.[1092] Die Anforderungen an die Verbraucherrechte-Statistik sind noch nicht an Proposition 24 angepasst, da noch die neu eingeführten Rechte auf Berichtigung und auf Beschränkung sensibler Informationen fehlen.[1093] Es ist zu erwarten, dass die California Privacy Protection Agency in der neuen Durchführungsverordnung die Verbraucherrechte-Statistik auf diese beiden Rechte erstreckt.[1094] Die Verbraucherrechte-Statistik müssen Unternehmen jeweils zum 1. Juli jedes Jahres aktualisieren.[1095]

Die ersten Mitte 2021 veröffentlichten Verbraucherrechte-Statistiken zeigten weitgehend für Verbraucher:innen positive Zahlen. Die großen Technologieunternehmen Google, Facebook und Apple haben jeweils mehr als 95 % der erhaltenen Lösch- und Auskunftsanträge erfüllt.[1096] Weniger positiv fällt die Bilanz bei dem Datenhändler Axicom und dem Fernsehsender Fox News aus, die jeweils weniger als die Hälfte der Lösch- und Auskunftsanträge akzeptiert haben.[1097] Beide geben an, dass die hohen Anforderungen an die Identifizierung des CCPA hierfür ursächlich seien.[1098] Die Summe der jeweils gestellten Anträge

---

[1087] *Cal. Attorney General*, Summary and Response to Comments Submitted During 45-Day Period, S. 232. Zur *compelled speech* siehe Kapitel 2:A.I.2.a) (ab S. 10).

[1088] 11 C.C.R. § 7102(a)(1)(A)–(C).

[1089] 11 C.C.R. § 7102(a)(1)(A)–(C).

[1090] 11 C.C.R. § 7102(a)(2)(A).

[1091] 11 C.C.R. § 7102(b).

[1092] 11 C.C.R. § 7102(b).

[1093] Cal. Civ. Code §§ 1798.106, 121. Zu dem Recht auf Beschränkung sensibler Informationen siehe Kapitel 3:C.II (ab S. 109) und zu dem Recht auf Berichtigung siehe Kapitel 3:C.V (ab S. 145).

[1094] Die Verordnungsermächtigung enthält eine Generalklausel zur Harmonisierung der Informationspflichten: Cal. Civ. Code § 1798.185(a)(22).

[1095] 11 C.C.R. § 7102(a)(2).

[1096] *Apple.*, Your California Privacy Disclosures; *Facebook*, California Privacy Rights Report; *Google*, CCPA Transparency Report.

[1097] *Axicom*, US Products Privacy Policy; *Fox News Network*, CCPA Recordkeeping.

[1098] *Ebd.*

ist weniger ergiebig, da manche Unternehmen nur explizit auf den CCPA bezogene Anträge zählen, während andere Unternehmen jeden Antrag berücksichtigen.[1099] Insoweit kann und sollte die California Privacy Protection Agency diese Frage noch in der Durchführungsverordnung spezifizieren.

cc) Zugänglichkeit

Das Unternehmen muss die umfassende Datenschutzerklärung auf seiner Webseite veröffentlichen.[1100] Auf dessen Startseite muss ein auffälliger Link, der das Wort »Privacy« enthält, auf die Datenschutzerklärung verweisen.[1101] Bei einer Smartphone-App soll das Unternehmen die Datenschutzerklärung zudem auf der Download-Seite der Smartphone-App verlinken.[1102] Ein Unternehmen, das über keine Webseite verfügt, muss die Datenschutzerklärung auf andere, auffällige Weise bereitstellen (wobei nur wenige Unternehmen über keine Webseite verfügen dürften, welche die Schwellenwerte des CCPA für die Unternehmensdefinition erfüllen).[1103] Die Informationen müssen sich zusammenhängend in einem Dokument befinden, das zudem auch ausdruckbar sein muss.[1104] Die Verbraucherrechte-Statistik kann das Unternehmen in die umfassende Datenschutzerklärung entweder integrieren oder einen Link auf diese aufnehmen.[1105]

dd) Effektivität

Zielpublikum der umfassenden Datenschutzerklärung ist die Öffentlichkeit als Ganzes: Aufsichtsbehörden, Forschung, Medien, Politik und Verbraucherschutzorganisationen. So soll die umfassende Datenschutzerklärung, losgelöst vom konkreten Fall, die gesamte Verarbeitung persönlicher Informationen eines Unternehmens darstellen. Zudem muss das Unternehmen sie ähnlich wie ein Jahresbericht nur alle zwölf Monate aktualisieren und Informationen aufnehmen, die für Verbraucher:innen irrelevant sind (beispielsweise ob das Unternehmen persönliche Informationen von Unter-16-Jährigen speichert).[1106]

Ist die umfassende Datenschutzerklärung für diese Zielgruppen hilfreich? Das Konzept einer zentralen Sammlung aller Informationen über die Datenverarbeitung eines Unternehmens ist in jedem Fall wertvoll. Für Aufsichtsbehörden erleichtert sie die Rechtsdurchsetzung, da diese nicht erst Informationen vom Unternehmen anfordern müssen, sondern diese direkt abrufen können. Dies ermöglicht es Aufsichtsbehörden, ihre Ressourcen zielgerichtet einzusetzen.

[1099] *Luthi*, Politico PRO, »Functionally useless«: California privacy law's big reveal falls short: mit weiteren Statistiken.

[1100] Cal. Civ. Code § 1798.130(a)(5) a.A.; 11 C.C.R. § 7011(b).

[1101] 11 C.C.R. § 7011(b).

[1102] 11 C.C.R. § 7011(b).

[1103] 11 C.C.R. § 7011(b). Zur Unternehmensdefinition siehe Kapitel 3:B.II.2 (ab S. 56).

[1104] 11 C.C.R. § 7011(a)(2)(E).

[1105] 11 C.C.R. § 7011(c)(8).

[1106] 11 C.C.R. § 7011(c)(1)(G)(3).

Akademische Forschung, Medien, Politik und Bürgerrechtsorganisationen sind dagegen Intermediäre. Sie können die in der umfassenden Datenschutzerklärung enthaltenen Informationen aufbereiten und in den öffentlichen Diskurs einbringen. Dafür ist eine öffentlich frei zugängliche Quelle effektiver als ein bloßer Auskunftsanspruch, da sie den Aufwand für die Intermediäre erheblich senkt.[1107]

Die Umsetzung ist aber nicht durchdacht. Negativ ist, dass Unternehmen durchgängig nur Kategorien angeben müssen. Bei persönlichen Informationen ist dies verständlich, da sich diese naturgemäß von Person zu Person unterscheiden und die Kategorisierung mit 137 Regelbeispielen[1108] ohnehin fein granular ist. Die Kategorien der Quellen sind weniger hilfreich. So sind selbst die in der Durchführungsverordnung vorgeschlagenen Kategorien für Quellen unscharf: beispielsweise kann die genannte Kategorie »government entities«[1109] Behörden des Bundes, eines Bundesstaats oder gar ausländische Behörden bedeuten. Dies erschwert es z. B. Journalist:innen, die übermäßige Weiterübermittlung persönlicher Informationen durch eine bestimmte Behörde als Quelle aufzudecken. Auch bleibt die genaue Kategorisierung der Quellen und Empfänger dem Unternehmen überlassen, das so verschleiernde Begriffe wählen kann. Zudem müssen Unternehmen weder Quellen noch Zwecke den Kategorien persönlicher Informationen zuordnen und keine Speicherfristen angeben. Insoweit enthält die umfassende Datenschutzerklärung sogar systemwidrig weniger Informationen als der kurze Datenschutzhinweis.

c) Vergleich mit Art. 13, 14 DSGVO

Der Verantwortliche muss nach Art. 13, 14 DSGVO ähnliche Informationen wie unter dem CCPA mitteilen. Dabei unterscheidet die DSGVO jedoch nicht zwischen Informationen für die betroffene Person selbst und Informationen für die Öffentlichkeit als Ganzes.

Nominelle Adressat:in der Informationen nach Art. 13, 14 DSGVO ist die betroffene Person.[1110] Damit ist aber kaum vereinbar, welche Fülle an schwer verständlichen und für die betroffene Person irrelevanten Fakten der Verantwortliche mitteilen muss. So führen Art. 13 Abs. 1, 2 DSGVO bei Direkterhebung und Art. 14 Abs. 1, 2 DSGVO bei Dritterhebung jeweils 27 verschiedene Informationsarten auf, welche die betroffene Person in der Regel erhalten muss.[1111] Die mitzuteilenden Informationen vervielfachen sich zudem

---

[1107] So zur Verbraucherrechte-Statistik: *Cal. Attorney General*, Summary and Response to Comments Submitted During 45-Day Period, S. 223.

[1108] Siehe Kapitel 3:B.I.1.a) (ab S. 43).

[1109] 11 C. C. R. § 7001(d).

[1110] So einhellig die Literatur: *Bäcker* in: Kühling/Buchner, DS-GVO Art. 13 Rn. 8; *Ingold* in: Sydow, DSGVO Art. 13 Rn. 1; *Schmidt-Wudy* in: BeckOK DatenschutzR, DS-GVO Art. 13 Rn. 2.

[1111] Bei Direkterhebung nach Art. 13 DSGVO muss der Verantwortliche nicht über die Kategorien der erhobenen personenbezogenen Daten und deren Quellen informieren, vgl. Art. 14 Abs. 1 lit. d, Abs. 2 lit. f DSGVO e contrario. Bei Dritterhebung nach Art. 14 DSGVO

dadurch, dass Verantwortliche in der Praxis ähnliche Verarbeitungsschritte in einer Datenschutzerklärung zusammenfassen.[1112]

Die nach Art. 13, 14 DSGVO mitzuteilenden Informationen sind zudem nicht allgemein verständlich, sondern setzen teils deutliches Vorwissen voraus. So muss der Verantwortliche auch die Rechtsgrundlage nennen (Art. 13 Abs. 1 lit. c Alt. 2, Art. 14 Abs. 1 lit. c Alt. 2 DSGVO) – und zwar nicht mit einem Schlagwort umschrieben, sondern nach §, Abs., S. und lit.[1113] Laien werden wohl kaum jede einzelne Rechtsgrundlage kennen.[1114] Ebenso können Laien kaum beurteilen, welche Auswirkungen die Übermittlung in ein Drittland für einen Betroffenen hat und ob diese durch angemessene Garantien wirksam abgemildert werden (Art. 13 Abs. 1 lit. f, 14 Abs. 1 lit. f DSGVO). Dies ist selbst für Datenschutzexpert:innen und Aufsichtsbehörden nur schwer zu beantworten, wie die Kontroverse nach dem *Schrems-II*-Urteil[1115] zeigt. Insoweit ist zu befürchten, dass solch schwer greifbaren Informationen für Laien nicht nur wertlos sind, sondern dazu führen, dass sie die für sie relevanten Informationen nicht mehr herausfiltern können.

Gleichzeitig sind diese Informationen für die Öffentlichkeit als Ganzes nur schwer zugänglich. Forschung, Medien, Politik und Bürgerrechtsorganisationen können nicht an einer zentralen Stelle alle Informationen über einen Verantwortlichen abrufen, sondern müssen diese mühsam aus zahlreichen spezifischen Datenschutzerklärungen sammeln. Bei Erhebungen außerhalb des Internets werden diese häufig nur in Papierform den jeweiligen Betroffenen ausgehändigt,[1116] was ein Sammeln dieser Informationen für Intermediäre weiter erschwert.

Zweistufige Datenschutzinformationen wurden zwar oft diskutiert,[1117] haben sich jedoch bisher nur in Randbereichen durchgesetzt. Die Aufsichtsbehörden stehen einer Aufteilung der Informationen auf mehrere Ebenen skeptisch gegenüber: schon auf der ersten Ebene müsse ersichtlich sein, welche Informationen

---

muss der Verantwortliche dagegen nicht über eine Pflicht zur Bereitstellung und die Folgen einer Nichtbereitstellung informieren, vgl. Art. 13 Abs. 2 lit. e DSGVO.

[1112] Vgl. als Extrembeispiel: *Finanzbehörden des Bundes und der Länder*, Informationen zur Umsetzung der datenschutzrechtlichen Vorgaben: eine Datenschutzerklärung für alle deutschen Finanzbehörden und für sämtliche Verarbeitungen personenbezogener Daten für Steuerzwecke.

[1113] *Nink* in: Spindler/Schuster, DS-GVO Art. 13 Rn. 13; *Paal/Hennemann* in: Paal/Pauly, DS-GVO Art. 13 Rn. 16; *Veil* in: Gierschmann, DSGVO Kap. III Rn. 65.

[1114] Deswegen eine Erläuterung komplexer Rechtsgrundlagen fordernd: *Bäcker* in: Kühling/Buchner, DS-GVO Art. 13 Rn. 26; *Mester* in: Taeger/Gabel, DS-GVO Art. 13 Rn. 11; a. A. *Knyrim* in: Ehmann/Selmayr, DS-GVO Art. 13 Rn. 38; *Schmidt-Wudy* in: BeckOK DatenschutzR, DS-GVO Art. 14 Rn. 46.

[1115] EuGH vom 16.07.2020 – C311/18, *Schrems II*, ECLI:EU:C:2020:559.

[1116] Ein solcher Medienbruch ist nämlich unzulässig, wenn sich die Datenschutzinformation nicht anders realisieren lässt: *Mester* in: Taeger/Gabel, DS-GVO Art. 13 Rn. 36.

[1117] *Bundesministerium der Justiz und für Verbraucherschutz*, One-Pager – Muster für transparente Datenschutzhinweise; *Hacker*, Verhaltensökonomik und Normativität, S. 454–457 m. w. N. zu Reformvorschlägen; *ders.*, Datenprivatrecht, S. 580–583; *Kettner/Thorun/Vetter*, Wege zur besseren Informiertheit, passim.

auf den weiteren Ebenen zur Verfügung stehen.[1118] Diese Skepsis ist auch nicht unberechtigt – Verantwortliche haben kein Interesse daran, die für die betroffene Person wichtigen, für sie potenziell ungünstigen Informationen prominent herauszustellen. Vielmehr haben sie Anreize, ungünstige Informationen auf den weiteren Ebenen zu »verstecken«. Es bestehen keine festen Regeln, welche Informationen auf einer ersten Ebene zu präsentieren sind. Zwar teilen Art. 13 DSGVO und Art. 14 DSGVO die bereitzustellenden Informationen in zwei Gruppen ein (Abs. 1 und Abs. 2). Diese Unterteilung ist aber nur redaktionell, während rechtlich kein Unterschied zwischen beiden Gruppen besteht.[1119] Der Europäische Datenschutzausschuss schlägt vor, dass der Verantwortliche auf einer ersten Ebene zumindest seine Identität, die Verarbeitungszwecke, die Datenschutzrechte und »Angaben über die Verarbeitung, welche sich am stärksten auf die betroffene Person auswirkt [sic], und die Verarbeitungsvorgänge, mit denen Letztere ggfs. nicht gerechnet hat« mitteilen soll.[1120] Diese schwammige Formulierung führt mit dazu, dass Verantwortliche regelmäßig die gesamten Informationen auf der ersten Ebene mitteilen, um Rechtssicherheit zu erlangen. In der Praxis sind mehrstufige Informationen daher eher unüblich (abgesehen von Situationen, in denen eine vollständige Information auf der ersten Ebene an Platzgründen scheitert).[1121]

Insgesamt ist das mehrstufige Informationsmodell des CCPA besser geeignet, die Entscheidungen von Verbraucher:innen zu beeinflussen und gleichzeitig Transparenz für die Öffentlichkeit als Ganzes zu schaffen. Verbraucher:innen erhalten mit dem kurzen Datenschutzhinweis die für sie relevantesten Informationen. Aufsichtsbehörden, Forschung, Medien, Politik und Verbraucherschutzorganisationen können dagegen über die umfassende Datenschutzerklärung an einem zentralen Ort umfangreiche Informationen abrufen. Damit wird der CCPA beiden Zielgruppen besser gerecht als die DSGVO. Als Vorbild für die DSGVO eignet sich das Modell des CCPA jedoch nicht, weil die Umsetzung des CCPA nicht ausreichend konsequent durchdacht ist.

[1118] *Artikel-29-Datenschutzgruppe*, WP 260 Transparenz, Rn. 35; später bestätigt durch: *EDSA*, Endorsement 1/2018.

[1119] *Artikel-29-Datenschutzgruppe*, WP 260 Transparenz, Rn. 23; *Bäcker* in: Kühling/Buchner, DS-GVO Art. 13 Rn. 20; *Dix* in: NK-DatenschutzR, DS-GVO Art. 13 Rn. 13; *Mester* in: Taeger/Gabel, DS-GVO Art. 13 Rn. 17; *Schmidt-Wudy* in: BeckOK DatenschutzR, DS-GVO Art. 13 Rn. 58, 59 a. A. *Paal/Hennemann* in: Paal/Pauly, DS-GVO Art. 13 Rn. 22, 23: in der Regel Informationen nach Art. 13 Abs. 2, 14 Abs. 2 DSGVO mitzuteilen.

[1120] *Artikel-29-Datenschutzgruppe*, WP 260 Transparenz, Rn. 38.

[1121] Bei Videoüberwachung typischerweise ein Schild mit den aus Sicht des Verantwortlichen wesentlichsten Informationen, vgl. z. B. das Muster der Aufsichtsbehörden: *EDSA*, Leitlinien 3/2019 Videogeräte Rn. 116. Daneben ist ein kurzer mündlicher Hinweis auch bei Callcentern ausreichend, *Artikel-29-Datenschutzgruppe*, WP 260 Transparenz, Rn. 38; *Franck* in: Gola, DS-GVO Art. 13 Rn. 40.

3. Form und Sprache

a) Darstellung

Für sämtliche Informationspflichten des CCPA gelten einheitliche Anforderungen an Form und Sprache. Dies gilt auch für die Mitteilung über das Widerspruchsrecht gegen Datenhandel und bei dem Angebot finanzieller Anreize.[1122] Der CCPA gibt das Format nicht exakt vor, um Unternehmen nicht zu sehr einzuengen.[1123] Dem liegt der Gedanke zugrunde, dass ein starres Format nicht in den zahlreichen Verarbeitungskontexten funktioniere, in denen Unternehmen Verbraucher:innen informieren.[1124] Die verwendete Sprache muss einfach und klar sein.[1125] Juristische und technische Fachbegriffe sind zu vermeiden.[1126] Das Format muss zudem leicht lesbar sein.[1127]

Die Informationen sind in derjenigen Sprache zu verfassen, in der das Unternehmen in Kalifornien hauptsächlich mit Verbraucher:innen kommuniziert.[1128] Dies kann auch dazu führen, dass die Datenschutzinformationen nicht in Englisch verfasst sein müssen, da viele kalifornische Unternehmen in anderen Sprachen kommunizieren. Kalifornien ist ein vielsprachiger Staat. So sprechen 45,6 % der kalifornischen Haushalte überwiegend eine andere Sprache als Englisch.[1129] Auch wenn ein verfassungsändernder Volksentscheid 1986 Englisch zur einzigen Amtssprache erklärt hatte,[1130] war dies nahezu ausschließlich Symbolpolitik.[1131] Die einfachgesetzliche Rechtslage ist weiterhin mehrsprachig. So müssen kalifornische Behörden ihre Materialien in allen Sprachen anbieten, die mindestens 5 % der von ihr betreuten Personen als Muttersprache sprechen, und für diese ausreichend zweisprachige Beschäftige anstellen.[1132] Damit ist Spanisch, das in 25,8 % der Haushalte gesprochen

---

[1122] Zu der Informationspflicht über das Widerspruchsrecht gegen Datenhandel siehe Kapitel 3:C.I.2.b)bb) (ab S. 87). Zu der Informationspflicht bei finanziellen Anreizen siehe Kapitel 3:C.I.4.b)aa) (ab S. 101).

[1123] *Cal. Attorney General*, Initial Statement of Reasons, S. 8, 10, 12 f.

[1124] *Cal. Attorney General*, Initial Statement of Reasons, S. 8, 42 f.

[1125] 11 C.C.R. §§ 7012(a)(2)(A), 7013(a)(2)(A), 7016(a)(2)(A), 7011(a)(2)(A).

[1126] 11 C.C.R. §§ 7012(a)(2)(A), 7013(a)(2)(A), 7016(a)(2)(A), 7011(a)(2)(A).

[1127] 11 C.C.R. §§ 7012(a)(2)(B), 7013(a)(2)(B), 7016(a)(2)(B), 7011(a)(2)(B).

[1128] 11 C.C.R. §§ 7012(a)(2)(C), 7013(a)(2)(C), 7016(a)(2)(C), 7011(a)(2)(C).

[1129] *U. S. Census Bureau*, 2020 American Community Survey Household Language Table: 7.279.814 Haushalte primär Englisch, 3.393.655 Haushalte primär Spanisch, 2.461.919 Haushalte primär sonstige Sprachen.

[1130] Proposition 63 (Cal. 1986), kodifiziert in Cal. Const. Art. III § 6.

[1131] Vgl. U. S. Court of Appeals 9th Circuit vom 27.01.1988, *Gutierrez v. Municipal Court of Southeast Judicial Dist.*, 838 F.2d 103, 1045: »symbolic statement«.

[1132] Cal. Gov. Code §§ 7292–7296.2. Weitere Pflichten zu mehrsprachigen Materialien: Cal. Bus. & Prof. Code §§ 7312(a)(6), 7353.4, 25681(a); Cal. Civ. Proc. Code § 412.20(a)(6); Cal. Gov. Code §§ 7284.10(a)(1), 11435.40(a), 12950(d), 13952(d)(4), 68511.1, Cal. Pen. Code §§ 646.91(c)(4), 31640(a).

wird,[1133] faktisch zweite Amtssprache. In der Praxis kommunizieren viele Behörden noch in zahlreichen weiteren Sprachen. Die kalifornische Wahlinformationsbroschüre mit Informationen über Proposition 24 war beispielsweise neben Englisch in der American Sign Language, Chinesisch, Hindi, Japanisch, Kambodschanisch, Koreanisch, Spanisch, Tagalog, Thailändisch und Vietnamesisch verfügbar.[1134]

Überdies müssen die Informationen unter dem CCPA barrierefrei für Menschen mit Behinderung zugänglich sein.[1135] Unternehmen sollen für die Barrierefreiheit auf ihrer Webseite den Web Content Accessibility Guidelines des World Wide Web Consortiums folgen,[1136] der sowohl in den Vereinigten Staaten[1137] als auch in der EU[1138] der wichtigste Standard für Barrierefreiheit ist.

Kein bestimmtes Format vorzugeben, ist zwar flexibel. Allerdings ist zu befürchten, dass Unternehmen die dadurch eingeräumte Flexibilität zu ihren eigenen Gunsten ausnutzen. Es ist aber durchaus möglich, dass die California Privacy Protection Agency die Regeln für einfache Sprache zukünftig präzisiert.[1139]

b) Vergleich mit Art. 12 DSGVO

Hinsichtlich der Anforderungen an Form und Sprache unterscheiden sich DSGVO und CCPA nur gering. Art. 12 Abs. 1 S. 1 HS 1 DSGVO verpflichtet Verantwortliche ebenso zu einer klaren und einfachen Sprache. Die Form soll nach dieser Norm zudem leicht zugänglich sein. Die konkretisierende Leitlinie des Europäischen Datenschutzausschusses erwähnt ähnliche Kriterien für einfache und klare Sprache wie die Durchführungsverordnung des CCPA. So sollen Verantwortliche ebenfalls juristische Fachbegriffe vermeiden[1140] und die Informationen barrierefrei bereitstellen.[1141] Darüber hinaus überlässt die

---

[1133] *U. S. Census Bureau*, 2020 American Community Survey Household Language Table: 3.393.655 primär spanisch sprechende Haushalte von insgesamt 13.135.388 Haushalten.

[1134] *Cal. Secretary of State*, Voter Guide 2020, S. 84.

[1135] 11 C. C. R. §§ 7012(a)(2)(D), 7013(a)(2)(D), 7016(a)(2)(D), 7011(a)(2)(D).

[1136] 11 C. C. R. §§ 7012(a)(2)(D), 7013(a)(2)(D), 7016(a)(2)(D), 7011(a)(2)(D).

[1137] Cal. Attorney General, Initial Statement of Reasons, S. 7. Vgl. U. S. District Court N. D. N. Y. vom 22. November 2017, *Andrews v. Blick Art Materials, LLC*, 286 F. Supp. 3d 365, 386: »nearly universally accepted«.

[1138] Wenn deutsche Behörden diesen Standard beachten, wird vermutet, dass sie den Barrierefreiheit-Pflichten auf ihrer Webseite nachgekommen sind, § 3 Abs. 2 Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz i. V. m. Art. 1 Durchführungsbeschluss (EU) 2018/2048 der Kommission vom 20. Dezember 2018 über die harmonisierte Norm für Websites und mobile Anwendungen zur Unterstützung der Richtlinie (EU) 2016/2102 des Europäischen Parlaments und des Rates, Anhang, S. 40.

[1139] Zulässig nach Cal. Civ. Code § 1798.185(a)(6).

[1140] *Artikel-29-Datenschutzgruppe*, WP 260 Transparenz Rn. 13; später bestätigt durch: *EDSA*, Endorsement 1/2018.

[1141] *Artikel-29-Datenschutzgruppe*, WP 260 Transparenz Rn. 16, 21.

DSGVO dem Verantwortlichen einen vergleichbaren Gestaltungsspielraum wie der CCPA dem Unternehmen.[1142]

Ein interessanter Unterschied ist, dass Art. 12 Abs. S. 1 HS 2 DSGVO explizit kindgerechte Sprache fordert, wenn der Verantwortliche sein Angebot an Kinder richtet, während dies im CCPA fehlt. Der Europäische Datenschutzausschuss leitet dieses Erfordernis explizit aus Art. 13 Übereinkommen der Vereinten Nationen über die Rechte des Kindes her.[1143] Hiernach haben Kinder ein Recht auf Zugang auf Informationen und Gedankengut aller Art, was auch kindgerechte Sprache einschließt. Der CCPA verzichtet dagegen als Verbraucherschutzgesetz auf eine speziell kindgerechte Information, wohl da Kinder realistischerweise ohnehin nicht auf Basis dieser Informationen handeln können. Die DSGVO fordert bezeichnenderweise jedoch auch schon vor dem Alter der Einwilligungsfähigkeit[1144] eine kindgerechte Information. Darin kommt die Orientierung der DSGVO an Grundrechten zum Ausdruck.

Art. 12 DSGVO regelt hingegen nicht explizit, in welcher Sprache der Verantwortliche Informationen und Mitteilungen verfassen soll. Es wäre naheliegend, auf die Sprache der intendierten Zielgruppe abzustellen, da gemäß Art. 12 Abs. 1 S. 1 HS 1 DSGVO die Informationen der jeweiligen betroffenen Person leicht zugänglich sein sollen. So stellt die Artikel-29-Datenschutzgruppe (später bestätigt durch den Europäischen Datenschutzausschuss) vergleichbar mit dem CCPA auf das »Zielpublikum« ab, an das sich der Verantwortliche objektiv betrachtet richtet.[1145] Überraschenderweise ist dies in Deutschland absolute Mindermeinung.[1146] Die deutschen Aufsichtsbehörden und die ganz herrschende Meinung in der deutschen Literatur wollen dagegen allein auf die Landessprache des Ziellandes abstellen.[1147] Daher sei in Deutschland stets Deutsch ausreichend.[1148] Hintergrund ist, dass Deutschland sprachlich wesentlich homogener als Kalifornien ist. Selbst in Haushalten, in denen alle Haushaltsmitglieder Migrationshintergrund haben,

---

[1142] *Bäcker* in: Kühling/Buchner, DS-GVO Art. 12 Rn. 12.

[1143] *Artikel-29-Datenschutzgruppe*, WP 260 Transparenz Rn. 16.

[1144] *Artikel-29-Datenschutzgruppe*, WP 260 Transparenz Rn. 15.

[1145] *Artikel-29-Datenschutzgruppe*, WP 260 Transparenz Rn. 13.

[1146] Soweit ersichtlich allein: *Dix* in: NK-DatenschutzR, DS-GVO Art. 12 Rn. 15. Ähnlich (allerdings wohl veraltet): *BayLfD*, 17. Tätigkeitsbericht 1996, Nr. 10.1.

[1147] *BayLDA*, FAQ zur DSGVO: Informationspflicht bei ausländischen Kunden; *HBDI*, Häufig gestellte Fragen; wohl auch: *ULD*, Medizindatenschutz, Berufsgeheimnisträger, Folie 37: »Landessprache«.
Greve in: Sydow, DSGVO Art. 12 Rn. 15; *Heckmann/Scheurer* in: Heckmann/Paschke, JurisPraxisKommentar Internetrecht, Kap. 9 Rn. 414; *Paal/Hennemann* in: Paal/Pauly, DS-GVO Art. 12 Rn. 35; *Pohle/Spittka* in: Taeger/Gabel, DS-GVO Art. 12 Rn. 10; *Schwartmann/Schneider* in: *Schwartmann et al.*, DS-GVO Art. 12 Rn. 30; *Quaas* in: BeckOK DatenschutzR, DS-GVO Art. 12 Rn. 20; *Taeger* in: Taeger/Gabel, DS-GVO Art. 7 Rn. 61: Amtssprache sei maßgeblich.

[1148] *HBDI*, Häufig gestellte Fragen: »[Für Behörden] ist die Information in Deutschland auf Deutsch ausreichend«; *Pohle/Spittka* in: Taeger/Gabel, DS-GVO Art. 12 Rn. 10; wohl auch: *Nink* in: Spindler/Schuster, DS-GVO Art. 12 Rn. 8: »in deutscher Sprache«.

wird mehrheitlich deutsch gesprochen.[1149] Die in Deutschland noch am stärksten verbreitete Sprache ist Türkisch, das in 1,3 % der Haushalte gesprochen wird[1150] – eine geringe Anzahl verglichen mit den 25,8 % der kalifornischen Haushalte, in denen überwiegend Spanisch gesprochen wird.[1151] Dementsprechend richten sich in Deutschland nur einzelne Verantwortliche ausschließlich an nicht-deutschsprachige Minderheiten. Dies scheint auch die deutsche rechtswissenschaftliche Debatte zu beeinflussen, die Staat und »Landessprache« gleichsetzt.

Stärker mehrsprachig geprägte Mitgliedsstaaten interpretieren das europäische Datenschutzrecht anders. So spricht sich beispielsweise die belgische Aufsichtsbehörde dafür aus, die Datenschutzinformationen je nach Zielgruppe in französisch oder niederländisch zu verfassen.[1152] Die insoweit offen formulierte DSGVO ist somit stärker von der jeweiligen nationalen Rechtskultur abhängig (selbst wenn bereits eine Leitlinie des Europäischen Datenschutzausschusses existiert), als der auf Kalifornien zugeschnittene, sehr spezifisch formulierte CCPA.

II. Zweckbindung

1. Darstellung

Im engen Zusammenhang mit den Informationspflichten steht die Zweckbindung. So können sich Verbraucher:innen nicht informiert entscheiden, wenn Unternehmen anschließend entgegen ihrer Ankündigungen handeln.

Dieser Gedanke ist schon lange im amerikanischen Datenschutzrecht verankert. So war die Zweckbindung schon 1973 in den einflussreichen[1153] »Fair Information Practices« des U. S. Department of Health, Education, and Welfare enthalten.[1154] Auch hat der kalifornische Supreme Court 1975 das Prinzip der Zweckbindung aus dem Recht auf Privatsphäre der kalifornischen Verfassung hergeleitet.[1155] Die FTC hat seit dem Ende der 1990er-Jahre zahlreiche Verfahren eingeleitet, weil Unternehmen ihre Versprechen zur Nutzung von Kundendaten gebrochen haben.[1156] Dabei folgt die FTC folgendem System: bei einer einfachen Änderung muss das Unternehmen die von der Änderung betroffenen

---

[1149] *Statistisches Bundesamt*, Mikrozensus 2020 Migrationshintergrund, S. 496: 4.051.000 (52,0 %) der 7.788.000 Haushalte, in denen alle Haushaltsmitglieder Migrationshintergrund haben.

[1150] *Statistisches Bundesamt*, Mikrozensus 2020 Migrationshintergrund, S. 496–498: 538.000 der insgesamt 40.545.000 Haushalte.

[1151] *U. S. Census Bureau*, 2020 American Community Survey Household Language Table: 3.393.655 primär spanisch sprechende Haushalte von insgesamt 13.135.388 Haushalten.

[1152] *Autorité de protection des données* (Belgien), Cookies et autres traceurs.

[1153] *Hoofnagle*, FTC, S. 152f; *Rothchild*, 66 Clev. St. L. Rev. 559, 585 f.

[1154] *U. S. Department of Health, Education, and Welfare*, Records, Computers and the Rights of Citizens, S. 61 f.

[1155] Cal. Supreme Court vom 24.03.1975, *White v. Davis*, 13 Cal. 3d 757, 775. Zu diesem Recht siehe Kapitel 2:A.II (ab S. 15).

[1156] FTC vom 13.08.1998, *GeoCities*, 127 F.T.C. 94, 97 f.; vom 10.09.2004, *Gateway*

Personen benachrichtigen und ihnen einen Widerspruch ermöglichen.[1157] Eine wesentliche Änderung ist ausschließlich dann zulässig, wenn die jeweilige Person informiert und aktiv einwilligt.[1158] Eine solche wesentliche Änderung ist insbesondere eine Weiterübermittlung an Dritte.[1159] Zusätzlich enthalten einzelne branchenspezifische Datenschutzgesetze ähnliche Konzepte: so regeln sie die zulässigen Nebenzwecke abschließend[1160] oder verpflichten zur Löschung bei Zweckfortfall.[1161]

Unter dem CCPA ist eine Verarbeitung persönlicher Informationen nur zulässig, wenn sie mit dem bei der Erhebung offengelegten Zweck vereinbar ist.[1162] Wenn das Unternehmen persönliche Informationen zu einem anderen Zweck nutzen will, muss es dies den jeweiligen Verbraucher:innen zuerst mitteilen.[1163] Die Zweckbindung gilt explizit auch nach Unternehmenstransaktionen.[1164] Für einen Datenhandel, über den das Unternehmen ursprünglich nicht informiert hatte, muss es die ausdrückliche und aktive Einwilligung des Verbrauchers einholen.[1165] Dies ähnelt dem Einwilligungserfordernis der FTC bei einer nicht angekündigten Weiterübermittlung an Dritte, da diese in der Regel auch einen Datenhandel im Sinne des CCPA darstellt.[1166] Zudem dürfen Dienstleister persönliche Informationen nur für die vertraglich festgelegten Zwecke nutzen.[1167] Als Ausnahme von der Zweckbindung erlauben die Bereichsausnahmen des CCPA zweckändernde Verarbeitungen – unter anderem, wenn das Unternehmen zu

---

Learning Corp., 138 F.T.C. 443, 449. Vgl. *FTC*, Protecting Consumer Privacy in an Era of Rapid Change, S. 57 f.; *Hoofnagle*, FTC, S. 160 f.; *Solove/Hartzog*, 114 Colum. L. Rev. 583, 640 f.

[1157] *FTC*, Comment: Privacy of Customers of Broadband and Other Telecommunications Services, S. 14 Fn. 60.

[1158] *FTC*, Protecting Consumer Privacy in an Era of Rapid Change, S. 57 f.; *Solove/Hartzog*, 114 Colum. L. Rev. 583, 640 f.

[1159] *FTC*, Protecting Consumer Privacy in an Era of Rapid Change, S. 57 f.

[1160] Cable Communications Act, 47 U. S. C. § 551(b),(c); Driver's Privacy Protection Act, 18 U. S. C. §§ 2721(b); FCRA, 15 U. S. C. § 1681b; HIPAA, 45 C. F. R. § 164.508(a); Privacy Act, § 552a(b). Dies zu einem umfassenden Prinzip erweiternd: *Solove*, 154 U. Pa. L. Rev. 477, 520–522.

[1161] Cable Communications Act, 47 U. S. C. § 551(e); Video Privacy Protection Act, 18 U. S. C. § 2710(e).

[1162] Cal. Civ. Code § 1798.100(a)(1),(2),(c).

[1163] Cal. Civ. Code § 1798.100(a)(1),(2).

[1164] Cal. Civ. Code § 1798.140(ad)(2)(C),(ah)(2)(C).

[1165] 11 C. C. R. § 7013(e). Die Durchführungsverordnung verwendet hier in Anlehnung an das Einwilligungserfordernis den Begriff »affirmative authorization«,.

[1166] Z. B. FTC vom 13.08.1998, *GeoCities*, 127 F.T.C. 94, 97 f.; vom 10.09.2004, *Gateway Learning Corp.*, 138 F.T.C. 443, 449: Gateway »vermietete« seine Kundendaten, obwohl es dies in seiner Datenschutzerklärung ursprünglich ausgeschlossen hatte. Zur Datenhandelsdefinition siehe Kapitel 3:C.I.2 (ab S. 82).

[1167] Cal. Civ. Code § 1798.140(j)(1)(A)(ii),(ag)(1)(B).

der jeweiligen Verarbeitung gesetzlich verpflichtet ist oder sie zur Verteidigung gegen Rechtsansprüche notwendig ist.[1168]

Zusätzlich greift das kalifornische Unfair Competition Law, das neben dem CCPA anwendbar ist. Dieses verbietet irreführende oder unangemessen benachteiligende Handlungen gegenüber Verbraucher:innen.[1169] Dieser ist das kalifornische Äquivalent zum FTC Act,[1170] zu dem die FTC die eben dargestellten umfangreichen Anforderungen an Zweckänderungen entwickelt hat. Damit verpflichtet das Unfair Competition Law bei wesentlichen Änderungen dazu, eine Einwilligung einzuholen.[1171]

2. Vergleich mit Art. 5 DSGVO

Art. 5 Abs. 1 lit. b DSGVO statuiert einen vergleichbaren Zweckbindungsgrundsatz. Anders als unter dem CCPA müssen Verantwortliche der betroffenen Person jede Zweckänderung mitteilen, nicht nur mit dem ursprünglichen Zweck unvereinbare Änderungen (Art. 13 Abs. 3 DSGVO). Die Zweckänderungen regelt die DSGVO ausführlich durch den Kompatibilitätstest des Art. 6 Abs. 4 DSGVO. Mit dem ursprünglichen Zweck unvereinbare Verarbeitungen sind nur zulässig, wenn die betroffene Person einwilligt oder die Zweckänderung gesetzlich gestattet ist (Art. 6 Abs. 4 DSGVO a. A., Erwägungsgrund 50 S. 7 der DSGVO). Insbesondere ist eine Zweckänderung entsprechend der Bereichsausnahmen des CCPA zur Verfolgung von Straftaten oder zur Verteidigung gegen Rechtsansprüche zulässig (§§ 23 Abs. 1 Nr. 4, 24 BDSG).

Verglichen mit dem Zweckbindungsprinzip des CCPA ist die Regelung der DSGVO differenzierter. Dem detaillierten Kompatibilitätstest des Art. 6 Abs. 4 DSGVO steht auf Seiten des CCPA nur das nicht näher bestimmte Vereinbarkeitskriterium gegenüber. Zudem muss das Unternehmen eine inkompatible Nutzung den Verbraucher:innen nur mitteilen, während diese unter der DSGVO unzulässig ist. Allerdings wird die für 2023 zu erwartende Novelle der Durchführungsverordnung den Zweckbindungsgrundsatz voraussichtlich differenzierter regeln und voraussichtlich an die berechtigten Erwartungen der Verbraucher:innen anknüpfen sowie Regelbeispiele enthalten.[1172]

[1168] Cal. Civ. Code § 1798.145(a). Siehe Kapitel 3:B.IV.1 (ab S. 74).

[1169] Cal. Bus. & Prof. Code §§ 17200, 17203, 17206(a).

[1170] So erfasst z. B. unangemessene Benachteiligung (»unfair«) jedes Handeln im Rechtsverkehr, das eine andere Partei unbillig benachteiligt: Cal. Court of Appeal 3rd District vom 31. Juli 1996, *Olsen v. Breeze, Inc.*, 48 Cal. App. 4th 608, 646 f.

[1171] Davon gehen Cal. Civ. Code §§ 1798.140(ad)(2)(C),(ah)(2)(C) aus. Rechtsprechung hierzu existiert ersichtlich nicht.

[1172] Cal. Privacy Protection Agency, Proposed Regulations, § 7002.

III. Datenminimierung und Speicherfristbegrenzung

1. Darstellung

Verfassungsrechtlich ist Datenminimierung in Kalifornien bereits seit 1975 garantiert.[1173] Einfachgesetzlich und in der amerikanischen Rechtspraxis spielte sie vor dem CCPA allerdings nur eine minimale Rolle.[1174] Allenfalls war Datenminimierung im Rahmen der Datensicherheit relevant, da die Risiken für Betroffene bei einer größeren Datenmenge steigen.[1175] So ist eine größere Datenmenge gefährlicher für Verbraucher:innen, weil sie leichter identifiziert und charakterisiert werden können.[1176] Zudem zieht eine große Datenmenge auch Kriminelle an, da sie sich leichter vermarkten lässt.[1177] Daher hat die FTC wiederholt die Datensicherheit von Unternehmen als unzureichend beurteilt, wenn diese keine Speicherfristen festgelegt hatten.[1178] Ansonsten kennen nur zwei branchenspezifische Gesetze mit Datenminimierung verwandte Konzepte. Der Cable Communications Act verpflichtet Kabelanbieter, nicht mehr erforderliche personenbezogene Informationen zu löschen.[1179] Der Video Privacy Protection Act enthält eine ähnliche Löschpflicht für Videoverleihe.[1180] Keine Löschpflicht, aber ein Verwendungsverbot nach Zeitablauf enthält der Fair Credit Reporting Act: Wirtschaftsauskunfteien dürfen näher aufgezählte negative Tatsachen nach Ablauf bestimmter Fristen nicht mehr mitteilen (ausgenommen sind Transaktionen mit einer Gesamtsumme von mehr als 150.000 $).[1181]

Der CCPA erhebt Datenminimierung hingegen zu einem allgemeinen Prinzip. Unternehmen dürfen nur diejenigen Daten erheben, die für den mitgeteilten Zweck erforderlich und angemessen sind (»reasonably necessary and proportionate«).[1182] Darüber hinaus müssen Unternehmen Speicherfristen festlegen, die sich daran orientieren, wann die persönlichen Informationen nicht mehr für den mitgeteilten Zweck erforderlich sind.[1183]

[1173] Cal. Supreme Court vom 24.03.1975, *White v. Davis*, 13 Cal. 3d 757, 775. Zu dem auch Private verpflichtendem Recht auf Privatsphäre siehe Kapitel 2:A.II (ab S. 15).

[1174] *Determann*, 6 International Data Privacy Law 244, 247; *Solove/Hartzog*, 114 Colum. L. Rev. 583, 653.

[1175] *FTC*, Internet of Things: Privacy & Security in a Connected World, S. 34.

[1176] *FTC*, Internet of Things: Privacy & Security in a Connected World, S. 34.

[1177] *FTC*, Internet of Things: Privacy & Security in a Connected World, S. 34 f.

[1178] FTC vom 20.09.2005, *BJ's Wholesale Club, Inc.*, 140 F.T.C. 465, 467; vom 07.03.2006, *DSW Inc.*, 141 F.T.C. 117, 119; vom 16.04.2008, *Life is good, Inc. and Life is good Retail, Inc.*, 145 F.T.C. 192, 194; vom 08.06.2011, *Ceridian Corporation*, 151 F.T.C. 514, 516; vom 29.04.2013, *CBR Systems, Inc.*, 155 F.T.C. 841, 844.

[1179] 47 U.S.C. § 551(e).

[1180] 18 U.S.C. § 2710(e).

[1181] 15 U.S.C. § 1681c(a).

[1182] Cal. Civ. Code § 1798.100(c).

[1183] Cal. Civ. Code § 1798.100(a)(3).

Weiterhin begrenzt die Datenminimierung auch die zulässigen Zwecke.[1184] Der CCPA spricht etwas unklar davon, dass Unternehmen persönliche Informationen entweder für den mitgeteilten Zweck nutzen können (»purposes for which the personal information was collected or processed«) oder für einen weiteren Zweck, der mit dem Kontext kompatibel ist, in dem die persönlichen Informationen erhoben wurden (»another disclosed purpose that is compatible with the context in which the personal information was collected«).[1185] Nebenzwecke sind daher nur zulässig, wenn sie mit dem Kontext der Erhebung vereinbar sind. Die genauen Konturen dieser Einschränkung für Nebenzwecke sind noch unklar.

Schließlich finden sich spezielle Ausprägungen der Datenminimierung in den Vorschriften für die Ausübung der Verbraucherrechte. So dürfen Unternehmen für die Ausübung der Verbraucherrechte nicht mehr als die nötigen persönlichen Informationen erheben.[1186] Das gleiche gilt für die Identifizierung des Verbrauchers bei der Ausübung seiner Verbraucherrechte.[1187]

Proposition 24 hat dieses allgemeine Datenminimierungsprinzip wohl nach europäischem Vorbild eingeführt, um die Bedingungen für einen Angemessenheitsbeschluss zu erfüllen.[1188] Ein Angemessenheitsbeschluss war sekundäres Motiv für die Proposition 24.[1189] So betont *Alastair Mactaggart,* der Vorsitzende der Bürgeriniative Californians for Consumer Privacy, die das Volksbegehren initiiert hat, er habe die zwingend erforderlichen Elemente der europäischen Aufsichtsbehörden in den Text des Volksbegehrens aufgenommen.[1190] Damit nimmt er anscheinend Bezug auf die »Referenzgrundlage für Angemessenheit« des Europäischen Datenschutzausschusses, welches Datenminimierung und Speicherfristbegrenzung als zentralen Grundsätze für ein angemessenes Datenschutzniveau nennt.[1191] Daher liegt nahe, dass Art. 5 Abs. 1 lit. c, e DSGVO Vorbild für die Datenminimierung und Speicherfristbegrenzung des CCPA waren.

[1184] Cal. Civ. Code § 1798.100(c).

[1185] Cal. Civ. Code § 1798.100(c).

[1186] Cal. Civ. Code § 1798.135(c)(1), 11 C.C.R. § 7026(h)(4). Die Begründung des kalifornischen Attorney General nennt als Begründung explizit Datenminimierung: *Cal. Attorney General*, Second Addendum to Final Statement of Reasons, S. 4.

[1187] 11 C.C.R. § 7060(b)(2),(c).

[1188] Vgl. *Californians for Consumer Privacy*, Prop 24 Webinar, 13m:00s; *dies.*, Annotated Text of the CPRA, § 1798.100(c). Zu dem von Californians for Consumer Privacy initiierten Volksbegehren siehe Kapitel 2:C.IV (ab S. 35).

[1189] *Angwin*, The Markup, Tech on the Ballot: Interview with Ashkan Soltani; *Bracy*, Alastair Mactaggart on California's Prop 24, 43m:00s; *Californians for Consumer Privacy*, Prop 24 Webinar, 13m:00s; *Kohne/Reed/Kurzweil*, Law360, Calif. Privacy Law Resembles, Transcends EU Data Regulation.

[1190] *Bracy*, Podcast: Alastair Mactaggart on California's Prop 24, 41m:40s.

[1191] *Artikel-29-Datenschutzgruppe*, WP 254 Angemessenheit, S. 5, später bestätigt durch: *EDSA*, Endorsement 1/2018.

2. Vergleich mit Art. 5 DSGVO

Art. 5 Abs. 1 lit. c, e DSGVO regeln mit einem ähnlichen Wortlaut Datenminimierung und Speicherfristbegrenzung. Ähnlich wie beim CCPA muss die Verarbeitung personenbezogener Daten auf das für die verfolgten Zwecke nötige Maß beschränkt und dafür angemessen sein (Art. 5 Abs. 1 lit. c DSGVO). Die Datenminimierung knüpft anders als unter dem CCPA nur an die verfolgten Zwecke an und umfasst damit auch sämtliche Nebenzwecke,[1192] die allerdings durch Art. 6 Abs. 1 DSGVO beschränkt sind. Die konkreten Ausprägungen der Datenminimierung wie die Erforderlichkeit (Art. 6 Abs. 1 S. 1 lit. b–e DSGVO) und Datenschutz durch Technikgestaltung (Art. 25 Abs. 1, 2 S. 1 DSGVO)[1193] haben dagegen kein Äquivalent im CCPA.

IV. Datensicherheit

Unternehmen sind nach dem CCPA verpflichtet, die von ihnen gespeicherten persönlichen Informationen durch angemessene Sicherheitsmaßnahmen vor unbefugtem Zugriff, Änderung, Löschung oder Weiterübermittlung zu schützen.[1194] Dienstleister müssen ebenfalls angemessene Sicherheitsmaßnahmen ergreifen.[1195] Die Anforderungen für Unternehmen und Dienstleister entsprechen dem seit 2004 bestehenden kalifornischen Datensicherheitsgesetz,[1196] auf das sich der CCPA ausdrücklich bezieht.[1197] Weder der CCPA noch das frühere Gesetz schreiben konkrete Sicherheitsmaßnahmen vor. Vielmehr stellen sie nur darauf ab, ob die Sicherheitsmaßnahmen angemessen (»reasonable«) sind.[1198] *Reasonableness* ist ein objektiver Maßstab, der auf eine verständige Person in der jeweiligen Situation abstellt.[1199] Der kalifornische Attorney General stellte zu dem früheren kalifornischen Datensicherheitsgesetz darauf ab, dass der in den Vereinigten Staaten weit verbreitete IT-Sicherheits-Standard »CIS Critical Security Controls«[1200] das

[1192] *Schantz* in: BeckOK DatenschutzR, DS-GVO Art. 5 Rn. 25.

[1193] Dafür, dass Art. 25 DSGVO eine Ausprägung der Datenminimierung ist: *Heberlein* in: Ehmann/Selmayr, DS-GVO Art. 5 Rn. 23.

[1194] Cal. Civ. Code § 1798.100(e).

[1195] Cal. Civ. Code § 1798.130(a)(3)(A) a.E.

[1196] A. B. 1950, 2003–04 Leg., Reg. Sess. (Cal. 2004), Cal. Stats. 2004 ch. 877, kodifiziert in Cal. Civ. Code § 1798.81.5. Mehrere andere Bundesstaaten haben ähnliche Gesetze erlassen: Ark. Code. Ann. § 4-110-4(b); Fla. Stat. § 501.171(2); Md. Code Ann., Com. Law § 14-3503(a); 201 Mass. Code Regs. 17.03(1); N.Y. Gen. Bus. § 899-bb.

[1197] Cal. Civ. Code § 1798.100(e). Der verwendete Begriff »in accordance with« bedeutet keine vollständige Übereinstimmung, aber zumindest ein sehr enges Orientieren an diesem Gesetz, vgl. Cal. Supreme Court vom 10.08.1943, *San Francisco v. Boyd*, 22 Cal. 2d 685, 689 f.

[1198] Cal. Civ. Code §§ 1798.81.5(a), 1798.100(e).

[1199] Cal. Supreme Court vom 29.11.2007, *People v. Mendoza*, 42 Cal. 4th 686, 703; *Bertenthal*, 2020 Wis. L. Rev. 85, 98–108: statistische Auswertung von Gerichtsentscheidungen zum Verständnis von »reasonable«; *Zipursky*, 163 U. Pa. L. Rev. 2131, 2132–2153: Überblick über *Reasonableness* in verschiedenen Rechtsgebieten.

[1200] *Center for Internet Security*, CIS Controls Version 8.

Minimum an Datensicherheit bildet.[1201] Es liegt nahe, dass die California Privacy Protection Agency und der Attorney General diesen Maßstab auch für den CCPA anlegen werden.[1202] Eine wesentliche Änderung des CCPA gegenüber dem früheren Datensicherheitsgesetz ist, dass auch die California Privacy Protection Agency gegen unzureichende Datensicherheit vorgehen kann und die weitere Definition persönlicher Informationen gilt.[1203] Zudem unterstreicht diese Pflicht den Anspruch des CCPA als umfassendes Datenschutzgesetz.

Das frühere kalifornische Datensicherheitsgesetz galt bereits bei seiner Einführung 2004 als »gap filler«,[1204] falls kein branchenspezifisches Datenschutzgesetz Datensicherheit regelte. Dementsprechend verpflichten zahlreiche branchenspezifische Datenschutzgesetze zu Datensicherheit.[1205] Diese Datensicherheitspflichten sind wie der CCPA eher abstrakt.[1206] Am konkretesten ist noch die Verwaltungspraxis der FTC zur »reasonable security«.[1207] Es ist zu erwarten, dass sich die California Privacy Protection Agency und der kalifornische Attorney General auch an dieser orientieren.

Die Datensicherheitspflicht des CCPA entspricht dem Grundsatz der Integrität und Vertraulichkeit des Art. 5 Abs. 1 lit. f, Art. 32 DSGVO. Dabei nennt die DSGVO explizit bestimmte Sicherheitsmaßnahmen wie Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO), während der CCPA nur abstrakt angemessene Sicherheitsmaßnahmen fordert. In der Praxis ist der Unterschied zwischen beiden Regelungen allerdings gering, da beide Maßstäbe als abstrakte Regelungen für eine Vielzahl von Branchen und Verarbeitungssituationen notwendigerweise allgemein bleiben müssen. Vergleichbar mit dem Abstellen des kalifornischen Attorney

---

[1201] *Cal. Attorney General*, California Data Breach Report 2016, S. 20.

[1202] *Cohen et al.*, HL Chronicle of Data Protection, California Consumer Privacy Act: The Challenge Ahead – The CCPA's »Reasonable« Security Requirement; *Hammel*, Alliant Cybersecurity, Cybersecurity Risk; *Pink*, California Consumer Privacy Act Annotated, § 9:2. Vgl. Hyman/Walser-Jolly/Farrell, 73 Quarterly Report 173, 181–203: allein Einzelfall entscheidend, kein Abstellen auf IT-Sicherheits-Standards.

[1203] *Vibbert et al.*, Arnold & Porter, Voters Overhaul CCPA. Personenbezogene Informationen i.S.d. früheren Datensicherheitsgesetzes sind nur Name des Betroffenen in Kombination mit bestimmten abschließend geregelten Informationen, Cal. Civ. Code § 1798.81.5(d)(1). Zur Definition persönlicher Informationen siehe Kapitel 3:B.I.1.a) (ab S. 43).

[1204] *Cal. Senate Judiciary Comm.*, AB 1950 Bill Analysis, S. 30.

[1205] Bund: COPPA, 15 U.S.C. § 6502(b)(1)(D), 16 C.F.R. § 312.8; Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2); GLBA, 15 U.S.C. § 6801(b), 16 C.F.R. §§ 314.1–314.5; HIPAA, 42 U.S.C. § 1320d-2(d)(2), 45 C.F.R. §§ 164.302–164.318; Privacy Act, 5 U.S.C. § 552a(e)(10); Cal. Civ. Code §§ 56.20(a),1798.90.51(a). Andeutend, dass eine solche Pflicht schon aus dem Vierzehnten Verfassungszusatz folgen könne: U.S. Supreme Court vom 22.07.1977, *Whalen v. Roe*, 429 U.S. 589, 605.

[1206] Ebd. Zwei Ausnahmen: HIPAA (45 C.F.R. § 164.302–164.318) und GLBA (16 C.F.R. § 314) regeln umfangreiche Anforderungen an die Organisation der Datensicherheit.

[1207] Zu dieser: *Cooper/Kobayashi*, Rethinking the FTC's Current Approach to Data Security S. 7 f.; *Solove/Hartzog*, 114 Colum. L. Rev. 583, 650–658.

General auf die CIS Critical Security Controls wird auch Art. 32 DSGVO vielfach anhand IT-Standards und Zertifizierungen geprüft.[1208]

V. Weiterübermittlungs- und Dienstleistervertrag

Ein Unternehmen muss mit Dritten oder Dienstleistern einen Weiterübermittlungsvertrag abschließen, wenn es an diese in seinem Geschäftsbetrieb persönliche Informationen übermittelt.[1209] Weiterübermittlungsverträge dienen dazu, die persönlichen Informationen bei einer Weitergabe an Dienstleister oder Dritte genauso zu schützen, wie sie es bei dem Unternehmen selbst wären. Eine solche *chain of custody* ist beim CCPA besonders relevant, weil sowohl der persönliche als auch räumliche Anwendungsbereich des CCPA wesentlich enger als derjenige der DSGVO ist.[1210]

Den Weiterübermittlungsvertrag muss das Unternehmen mit jedem Empfänger abschließen, der die persönlichen Informationen entweder als Dienstleister oder aus einem Datenhandel erhält.[1211] Die Definition des Dienstleisters deckt die operativen Verarbeitungen ab, die das Unternehmen in seinem Geschäftsbetrieb sonst selbst vornehmen müsste.[1212] Die Definition des Datenhandels erfasst alle Übermittlungen, bei denen das Unternehmen persönliche Informationen als Wirtschaftsgut kommerziell verwertet.[1213] Beide Definitionen zusammengenommen umfassen den gesamten Geschäftsbetrieb eines Unternehmens.

Die Weiterübermittlungsverträge müssen den Übermittlungszweck genau festlegen.[1214] Zudem müssen sie den Dienstleister oder Dritten verpflichten, das Datenschutzniveau des CCPA aufrechtzuerhalten und alle auf ihn anwendbaren Pflichten aus dem CCPA nachzukommen.[1215] Für den Fall, dass er dies nicht mehr kann, ist eine Klausel aufzunehmen, dass er dem Unternehmen mitzuteilen hat.[1216] Der Vertrag muss zudem Kontroll- und Abhilferechte des Unternehmens regeln, wobei deren konkrete Details nicht vorgegeben sind.[1217]

[1208] Insbesondere die ISO/IEC 27001:2013: BKartA vom 19.07.2019 – VK 1-39/19, ZD 2020, 115, Rn. 41; *EDSA*, Guidelines 07/2020 Controller Processor Rn. 95; *LfDI Baden-Württemberg*, Tätigkeitsbericht Datenschutz 2019, S. 34; *Bitkom*, Mustervertragsanlage Auftragsverarbeitung, § 6 Abs. 1 Variante 3; *Schmieder* in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz: Rechtshandbuch, Teil XII Kapitel 2 Rn. 80.

[1209] Cal. Civ. Code § 1798.100(d).

[1210] *Californians for Consumer Privacy*, How Prop 24 Adds Even More Privacy Rights Compared to the CCPA. Zum persönlichen Anwendungsbereich siehe Kapitel 3:B.II (ab S. 56). Zum räumlichen Anwendungsbereich siehe Kapitel 3:B.III (ab S. 71).

[1211] Cal. Civ. Code § 1798.100(d).

[1212] Cal. Civ. Code § 1798.140(ad),(ah). Siehe Kapitel 3:B.II.3 (ab S. 65).

[1213] Cal. Civ. Code § 1798.140(j),(ag). Siehe Kapitel 3:C.I.2.a) (ab S. 82).

[1214] Cal. Civ. Code § 1798.100.100(d)(1).

[1215] Cal. Civ. Code § 1798.100(d)(2).

[1216] Cal. Civ. Code § 1798.100(d)(4).

[1217] Cal. Civ. Code § 1798.100(d)(3),(5).

Mit Dienstleistern muss das Unternehmen zusätzlich einen Dienstleistervertrag abschließen.[1218] Dienstleister ist dabei der Oberbegriff dieser Arbeit für *service provider* (die in etwa Auftragsverarbeitern entsprechen) und *contractor* (welche keinen Weisungen unterliegen, wie Rechtsanwaltskanzleien).[1219] Der Dienstleistervertrag muss den Dienstleister darauf verpflichten, nicht mit den erhaltenen persönlichen Informationen zu handeln,[1220] sie nicht außerhalb der Geschäftsbeziehung mit dem Unternehmen zu nutzen,[1221] nicht mit Daten aus anderen Geschäftsbeziehungen zu kombinieren[1222] und nach Ende der Geschäftsbeziehung zu löschen.[1223] Weiterer verpflichtender Vertragsinhalt sind zudem Kontrollrechte des Unternehmens – insbesondere, dass das Unternehmen den Dienstleister mindestens alle zwölf Monate kontrolliert.[1224] Ein *contractor* muss zusätzlich bekräftigen, dass er seine Verpflichtungen verstanden hat.[1225] Solche Bekräftigungen sind im amerikanischen Vertragsrecht üblich, haben aber nur deklaratorischen Charakter.[1226] Es ist wohl nur ein Redaktionsversehen, dass diese Bekräftigung nicht für *service provider* vorgesehen ist.

Eine ähnliche Pflicht existierte bereits im Privacy Act und HIPAA, unter denen mit Auftragnehmern die Einhaltung der jeweiligen Datenschutzverpflichtungen vertraglich vereinbart werden müssen.[1227] Unter anderen amerikanischen Datenschutzgesetzen müssen Vertragspartner zumindest auf Datensicherheit verpflichtet werden.[1228]

Die DSGVO kennt keine Pflicht, Verträge mit jedem Empfänger personenbezogener Daten abzuschließen.[1229] Vielmehr ist auf jeden in der EU niedergelassenen Empfänger die DSGVO ohnehin anwendbar (Art. 2 Abs. 1 DSGVO). Innerhalb des Binnenmarkts der EU als *level-playing-field* soll freier Datenverkehr herrschen (Art. 1 Abs. 1 S. 1 DSGVO).[1230] Wenn die personenbezogenen Daten diesen Schutz des Binnenmarkts verlassen, muss der Verantwortliche gem. Art. 44 S. 1 DSGVO das angemessene Datenschutzniveau sicherstellen. Dabei soll das durch die geeigneten Garantien, durchsetzbaren Rechte und wirksamen

---

[1218] Cal. Civ. Code § 1798.140(j)(1),(ag)(1).

[1219] Cal. Civ. Code § 1798.140(ad),(ah). Siehe Kapitel 3:B.II.3 (ab S. 65).

[1220] Cal. Civ. Code §§ 1798.140(j)(1)(A)(i),(ag)(1)(A).

[1221] Cal. Civ. Code §§ 1798.140(j)(1)(A)(iii),(ag)(1)(C).

[1222] Cal. Civ. Code §§ 1798.140(j)(1)(A)(iv),(ag)(1)(D).

[1223] Cal. Civ. Code §§ 1798.140(j)(1)(A)(iii),(ag)(1)(C).

[1224] Cal. Civ. Code § 1798.140(j)(1)(C),(ag)(1)(D).

[1225] Cal. Civ. Code § 1798.140(j)(1)(B).

[1226] So für eine solche Bekräftigung im Arbeitsrecht: Cal. Court of Appeals vom 08.07.2020, *Martinez v. BaronHR, Inc.*, 51 Cal. App. 5th 962, 965, 967.

[1227] Privacy Act, 5 U. S. C. § 552a(m)(1); HIPPA, 45 C. F. R. §§ 164.502(e)(2), 164.504(e). Der Inhalt ist jeweils vergleichbar.

[1228] GLBA, 16 C. F. R. § 314.4(b); Cal. Civ. Code § 1798.81.5(c); Md. Code Ann. Com. Law § 14-3503(b)(1).

[1229] Anders das Sozialdatenschutzrecht, das eine »Insel« im sonst europaweit vereinheitlichten Datenschutzrecht bildet: § 78 Abs. 1 S. 2 SGB X.

[1230] *Hornung/Spiecker gen. Döhmann* in: NK-DatenschutzR, DS-GVO Art. 1 Rn. 41–49.

Rechtsbehelfe hergestellte Schutzniveau im Wesentlichen gleichwertig sein.[1231] Die in der Praxis mit großem Abstand am weitesten verbreiteten Garantien für Übermittlungen in Drittländer sind die Standarddatenschutzklauseln des Art. 46 Abs. 2 lit. c DSGVO.[1232] Diese haben einen ähnlichen Inhalt und Funktion wie die Weiterübermittlungsverträge des CCPA. Sie sollen gerade eine flexible Weiterübermittlung von Datenschutzpflichten ermöglichen.[1233] Ähnlich wie die Weiterübermittlungsverträge des CCPA verpflichten sie den Datenimporteur dazu, das Datenschutzniveau des Exportlandes aufrechtzuerhalten.[1234] In der Praxis werden die allermeisten Übermittlungen in Drittländer durch Standardvertragsklauseln abgesichert und allenfalls durch einen kurzen Fragebogen für den Datenimporteur über das Rechtssystems des Drittstaats oder durch zusätzliche Vertragsklauseln ergänzt.[1235] Es bleibt abzuwarten, ob sich diese faktische Vertragslösung durch die *Schrems-II*-Entscheidung[1236] des EuGH zu einer stärkeren Datenlokalisierung in der EU verändern wird.

Proposition 24, das die Weiterübermittlungsverträge eingeführt hat, wollte damit ersichtlich den Punkt »Einschränkungen bei der Weiterleitung von Daten« der Referenzgrundlage Angemessenheit des Europäischen Datenschutzausschuss erfüllen.[1237] Diese Referenzgrundlage war Vorbild für die Erweiterung der Unternehmenspflichten.[1238] Eine umfassendere Lösung wäre wohl nicht mit der *dormant Commerce Clause* vereinbar gewesen, da sie den Handel zwischen den Bundesstaaten deutlich eingeschränkt hätte.[1239] Die Weitergabeverträge des CCPA sind deutlich weniger spezifisch als die Standarddatenschutzklauseln der DSGVO, da sie nur die oben dargestellten kurzen Inhalte enthalten müssen und keine konkreten Vertragsklauseln vorgegeben sind. Im praktischen Ergebnis erreicht der CCPA dennoch ein ähnliches Schutzniveau bei Übermittlungen,

---

[1231] EuGH vom 16.07.2020, *Schrems II*, ECLI:EU:C:2020:559 Rn. 105.

[1232] *Europäische Kommission*, Commission Staff Working Document: two years of application of GDPR, SWD/2020/115 final, Nr. 7.2: »by far the most widely used data transfer mechanism«; *IAPP/EY*, IAPP-EY Annual Privacy Governance Report 2021, S. 4.

[1233] *Schantz* in: NK-DatenschutzR, DS-GVO Art. 46 Rn. 30. Immer noch relevant zu den Vor- und Nachteilen der Vertragslösung für Übermittlungen in Drittländer: *Ellger*, 60 RabelsZ 60 (1996), 738, 760–767.

[1234] Erwägungsgrund 1 des Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, ABl. 2021 L 199, 31.

[1235] Vgl. *IAPP/EY*, IAPP-EY Annual Privacy Governance Report 2021, S. 4f: nur 38 % nutzen zusätzliche technische Sicherheitsmaßnahmen, und nur 4 % haben sich dazu entschieden einzelne Übermittlungen in Drittländer zu unterlassen.

[1236] EuGH vom 16.07.2020, *Schrems II*, ECLI:EU:C:2020:559.

[1237] *Artikel-29-Datenschutzgruppe*, WP 254 Angemessenheit, S. 6; später bestätigt durch *EDSA*, Endorsement 1/2018.

[1238] Siehe Kapitel 3:D.III.1 (ab S. 169).

[1239] Zu dieser siehe Kapitel 2:A.I.2.b) (ab S. 13).

da unter der DSGVO Standarddatenschutzklauseln häufig nur auf dem Papier Datentransfer absichern.

Der Dienstleistervertrag weicht nur in Details vom Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO ab. Der Auftragsverarbeitungsvertrag verpflichtet den Auftragsverarbeiter ebenso dazu, die personenbezogenen Daten nur im Rahmen der Geschäftsbeziehung mit dem Verantwortlichen auf dokumentierte Weisung einzusetzen (Art. 28 Abs. 3 S. 2 lit. a DSGVO), angemessene technische und organisatorische Maßnahmen zu ergreifen (Art. 28 Abs. 3 S. 2 lit. c) und zu Kontrollen durch den Verantwortlichen beizutragen (Art. 28 Abs. 3 S. 2 lit. h DSGVO). Über den Dienstleistervertrag hinausgehend verpflichtet der Auftragsverarbeitungsvertrag den Auftragsverarbeiter, seine unterstellten Personen auf das Datengeheimnis zu verpflichten (Art. 28 Abs. 3 S. 2 lit. b DSGVO) und den Verantwortlichen bei der Ausübung seiner Pflichten zu unterstützen (Art. 28 Abs. 3 S. 2 lit. e, f DSGVO). Letztere Unterstützungspflicht trifft den Dienstleister des CCPA jedoch schon *ipso iure*.[1240] Auch die Verpflichtung auf das Datengeheimnis ergibt sich zwar nicht direkt aus anderen Vorschriften des CCPA, ist aber wohl ein Teil der für Dienstleister verpflichtenden angemessener Sicherheitsmaßnahmen. So sieht der IT-Sicherheits-Standard »CIS Controls«, der als Maßstab für die angemessene Sicherheit gilt, eine solche Verpflichtung vor.[1241]

VI. Organisationspflichten

1. Trainings- und Dokumentationspflichten

Die Organisationspflichten des CCPA sind im Vergleich zur DSGVO nur sehr schwach ausgeprägt.[1242] So trifft Unternehmen nur die Pflicht, ihre Beschäftigten über die Verbraucherrechte zu informieren, die Ausübung der Verbraucherrechte zu dokumentieren und bei besonders riskanten Verarbeitungen persönlicher Informationen Risikoanalysen sowie Datensicherheits-Audits durchzuführen.

Jedes Unternehmen muss seine für Datenschutzanfragen zuständigen Beschäftigten so instruieren, dass diese die Verbraucherrechte des CCPA kennen und wissen, wie Verbraucher:innen diese ausüben können.[1243] Besonders große Unternehmen sind verpflichtet, ein umfassendes Ausbildungsprogramm über die Verbraucherrechte des CCPA aufzulegen.[1244] Unternehmen sind nur besonders groß, wenn sie in einem Kalenderjahr persönliche Informationen von mehr als zehn Millionen Verbraucher:innen verarbeiten (circa ein Viertel der kalifornischen Bevölkerung).[1245] Dieser hohe Schwellenwert liegt wohl darin begründet,

---

[1240] Cal. Civ. Code § 1798.130(a)(3)(A).

[1241] *Center for Internet Security*, CIS Controls Version 8, S. 45–47 vor. Dieser ist Maßstab für die angemessene Sicherheit, siehe Kapitel 3:D.IV (ab S. 171).

[1242] Ebenso zum CCPA-2018: *Chander/Kaminski/McGeveran*, 105 Minn. L. Rev. 1733, 1758.

[1243] Cal. Civ. Code §§ 1798.130(a)(6), 1798.135(c)(3), 11 C. C. R. § 7100(a).

[1244] 11 C. C. R. § 7100(b).

[1245] 11 C. C. R. § 7102(a) a. A. Kalifornien hatte zum Stichtag der letzten Volkszählung

dass die Durchführungsverordnung einen einheitlichen Schwellenwert für die Verbraucherrechte-Statistik und das Ausbildungsprogramm wählen wollte.

Unternehmen sind zudem verpflichtet, Verbraucherrechte-Anträge zu dokumentieren und die Dokumentation mindestens 24 Monate aufzubewahren.[1246] Sie können diese Dokumentationspflicht durch ein Protokoll erfüllen, welches mindestens das Antragsdatum, die Art des Antrags, das Antwortdatum und ob der Antrag erfüllt wurde, enthalten muss.[1247] Bei einer teilweise oder vollständigen Ablehnung muss das Protokoll auch den Ablehnungsgrund enthalten.[1248] Diese Dokumentation darf das Unternehmen nur nutzen, um die Umsetzung des CCPA zu überprüfen und gegebenenfalls zu modifizieren.[1249] Die Dokumentation hat das Unternehmen sicher aufzubewahren und darf sie außer zur Erfüllung einer Rechtspflicht nicht mit Dritten teilen.[1250] Der CCPA ermächtigt die California Privacy Protection Agency, weitere Dokumentationspflichten zu schaffen, was sie bisher noch nicht wahrgenommen hat.[1251] Insoweit regelt die DSGVO derzeit in Art. 5 Abs. 2, 24, 30 DSGVO umfassendere Dokumentationspflichten.

2. Risikoanalysen und Datensicherheit-Audits

Proposition 24 hat darüber hinaus eine Pflicht zur Durchführung regelmäßiger Risikoanalysen (»risk assessments«) und unabhängiger Datensicherheit-Audits (»cybersecurity audits«) eingeführt.[1252] Diese greift bei Verarbeitungen persönlicher Informationen, die ein hohes Risiko bergen.[1253] Die California Privacy Protection Agency muss in der Durchführungsverordnung festlegen, welche Verarbeitungen besonders risikoreich für Verbraucher:innen sind.[1254] Sie soll dabei die Größe und Komplexität der Unternehmen sowie die Art und den Umfang der Verarbeitung berücksichtigen.[1255]

Bei der Risikoanalyse muss das Unternehmen die Vorteile, die sich aus der Verarbeitung für das Unternehmen, andere Beteiligte und die Öffentlichkeit ergeben, abwägen mit den potenziellen Risiken für die Rechte der Verbraucher:innen, die

---

(01.04.2020) 39.538.223 Einwohner:innen: *U. S. Census Bureau*, 2020 Census Apportionment Results.

[1246] 11 C.C.R. § 7101(a).

[1247] 11 C.C.R. § 7101(b).

[1248] 11 C.C.R. § 7101(d).

[1249] 11 C.C.R. § 7101(d).

[1250] 11 C.C.R. § 7101(a),(e).

[1251] Cal. Civ. Code § 1798.199.40(b). Systemwidrig in der Vorschrift über Aufgaben der California Privacy Protection Agency und nicht in der Verordnungsermächtigung (Cal. Civ. Code § 1798.185) geregelt.

[1252] Cal. Civ. Code § 1798.185(a)(15).

[1253] Cal. Civ. Code § 1798.185(a)(15).

[1254] Cal. Civ. Code § 1798.185(a)(15)(A). Der bisherige Entwurf schweigt hierzu: Cal. Privacy Protection Agency, Proposed Regulations.

[1255] Cal. Civ. Code § 1798.185(a)(15)(A).

mit dieser Verarbeitung verbunden sind.[1256] Dabei hat es zu berücksichtigen, inwieweit es sensible Informationen verarbeitet.[1257] Falls die Risiken überwiegen, ist das Unternehmen verpflichtet, die Verarbeitung einzuschränken oder zu unterlassen.[1258] Die abgeschlossenen Risikoanalysen muss das Unternehmen der California Privacy Protection Agency vorlegen und regelmäßig aktualisieren.[1259] Die California Privacy Protection Agency veröffentlicht einen Jahresbericht, der die vorgelegten Risikoanalysen zusammenfasst.[1260]

Die Datensicherheits-Audits sollen unabhängig durchgeführt werden und eingehend sein.[1261] Die genaue Ausgestaltung der unabhängigen IT-Sicherheits-Prüfungen und Risikoanalysen obliegt der California Privacy Protection Agency in der zukünftigen Durchführungsverordnung.[1262]

Die Risikoanalysen waren schon lange in der amerikanischen Datenschutzpraxis als *privacy impact assessments* verbreitet.[1263] Schon der E-Government-Act of 2002 verpflichtete Bundesbehörden, *privacy impact assessments* durchzuführen, wenn diese neue personenbezogene Informationen erheben.[1264] Ähnlich dazu ordnen andere amerikanische Datenschutzgesetze Risikoanalysen für Datensicherheit an.[1265] Solche regelmäßigen Risikoanalysen waren zudem häufig Teil der Abhilfemaßnahmen der FTC[1266] und des kalifornischen Attorney General.[1267]

Die von der Europäischen Kommission zur Vorbereitung der DSGVO in Auftrag gegebene rechtsvergleichende Studie diskutierte die amerikanischen *privacy impact assessments* ausführlich.[1268] Die Datenschutz-Folgenabschätzung des Art. 35 DSGVO kombiniert diese mit weiteren Einflüssen, vor allem aus

---

[1256] Cal. Civ. Code § 1798.185(a)(15)(B).

[1257] Cal. Civ. Code § 1798.185(a)(15)(B).

[1258] Cal. Civ. Code § 1798.185(a)(15)(B).

[1259] Cal. Civ. Code § 1798.185(a)(15)(B).

[1260] Cal. Civ. Code § 1798.199.40(d). Der Bericht soll die Datensicherheit nicht kompromittieren. Die Publikationshäufigkeit ist nicht festgelegt.

[1261] Cal. Civ. Code § 1798.185(a)(15)(A).

[1262] Cal. Civ. Code § 1798.185(a)(15). Der bisherige Entwurf schweigt hierzu: Cal. Privacy Protection Agency, Proposed Regulations.

[1263] *Waldman*, Privacy, Practice, and Performance, S. 24 f.; *ders.*, 97 Wash. U. L. Rev. 773, 779 f.

[1264] 44 U. S. C. § 3501 note, Federal Management and Promotion of Electronic Government Services, Sec. 208(b)(1).

[1265] GLBA, 16 C. F. R. § 314.4(b); HIPAA, 45 C. F. R. § 164.308; 201 Mass. Code Regs. § 17.03(2)(B).

[1266] FTC vom 02.03.2011, *Twitter, Inc.*, 151 F.T.C. 162, 173; vom 13.08.2014, *Fandango, LLC*, 158 F.T.C. 50, 59 f.; vom 06.09.2018, *Blu Products, Inc. and Samuel Ohev-Zion*, 166 F.T.C. 143, 153; kritisch zu deren oft oberflächlichen Inhalt: *Waldman*, 97 Wash. U. L. Rev. 773, 806.

[1267] *Citron*, 92 Notre Dame L. Rev. 747, 785 m. w. N. auch zu durch andere Attorneys General der Bundesstaaten angeordnete Risikoanalysen.

[1268] *LRDP Kantor/Centre for Public Reform*, Vergleichende Studie Schutz der Privatsphäre für Europäische Kommission, Rn. 132.

dem angelsächsischen Raum.[1269] Sie ist allerdings nur bei einem hohen Risiko für betroffene Personen durchzuführen (Art. 35 Abs. 1 DSGVO), was wiederum der CCPA übernimmt.[1270]

Der Verantwortliche muss die Datenschutz-Folgenabschätzung jedoch anders als die Risikoanalyse des CCPA grundsätzlich nicht der zuständigen Aufsichtsbehörde vorlegen. Eine solche Vorlagepflicht besteht nur im Ausnahmefall des Art. 36 Abs. 1 DSGVO, wenn der Verantwortliche das hohe Risiko nicht durch technische oder organisatorische Maßnahmen eindämmen kann. Art. 36 DSGVO spielt ersichtlich in der Praxis keine Rolle: selbst größere Aufsichtsbehörden berichten maximal von einer Konsultation nach Art. 36 DSGVO im Jahr.[1271] Bei Kontrollen fordern die europäischen Aufsichtsbehörden die Datenschutz-Folgenabschätzung im Einzelfall an.[1272] Die weitergehende Vorlagepflicht des CCPA für jede Risikoanalyse sorgt hingegen für Qualitätssicherung: Selbst wenn die California Privacy Protection Agency wegen fehlender Ressourcen nicht jede Risikoanalyse im Detail prüft, wird ein Unternehmen sich wohl kaum die »Blöße geben«, eine auf den ersten Blick unzureichende Risikoanalyse vorzulegen. Die bloße Vorlage bei einer Beschwerde nach der DSGVO hat nicht dieselbe präventive Wirkung, weil sie typischerweise für den Verantwortlichen unerwartet ist. Gleichzeitig ist die Vorlagepflicht flexibel, da sie der California Privacy Protection Agency zwar eine Prüfung der riskanten Verarbeitung ermöglicht, das Unternehmen aber nicht auf eine Genehmigung warten muss.[1273]

Eine unabhängigen Audit der IT-Sicherheit sieht die DSGVO nicht vor.[1274] Zwar wird eine Datenschutz-Folgenabschätzung typischerweise auch technische Aspekte beinhalten, da sich nur so die Risiken für Betroffene sachgerecht beurteilen lassen. Eine reine Bewertung technischer Risiken durch den Verantwortlichen selbst ist jedoch nicht mit einer unabhängigen Prüfung vergleichbar, die konkreten (noch durch die California Privacy Protection Agency festzulegenden) Maßstäben folgt. Eine solche Prüfung durch unabhängige Dritte vermeidet

---

[1269] *Friedewald et al.*, White Paper Datenschutz-Folgenabschätzung, S. 9 f.; *Hansen* in: BeckOK DatenschutzR, DS-GVO Art. 35 Rn. 2.

[1270] Vgl. *Lejeune*, ITRB 2021, 13, Fn. 53: Riskoanalyse erinnere an Art. 35 DSGVO.

[1271] *BfDI*, Tätigkeitsbericht 2017 und 2018 zum Datenschutz, S. 21; *Datenschutzbehörde* (Österreich), Datenschutzbericht 2020, S. 46. Die Aufsichtsbehörden für Berlin, Brandenburg, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen-Anhalt, Schleswig-Holstein und Thüringen haben 2018 und 2019 keine solche Anfrage erhalten: *Braun*, ZD 2021, 297, 299.

[1272] *BfDI*, Tätigkeitsbericht 2020, S. 46; *LfDI Saarland*, 28. Tätigkeitsbericht Datenschutz 2019, S. 126: »in der Regel«.

[1273] Zu der nach Art. 20 DSRL noch vorgesehenen Vorabkontrolle: *Karg* in: NK-DatenschutzR, DS-GVO Art. 36 Rn. 2. Allgemein zu den Vor- und Nachteilen von Anmeldeverfahren vgl. Genehmigungsverfahren: *Ellger*, Der Datenschutz im grenzüberschreitenden Datenverkehr, S. 422–427.

[1274] Anders das IT-Sicherheits-Recht für kritische Infrastruktur, vgl. Art. § 8a Abs. 3 BSIG.

Betriebsblindheit.[1275] Sie lässt sich gut mit dem Fokus des amerikanischen Datenschutzrechts auf Datensicherheit vereinbaren.

3. Keine weiteren Organisationspflichten

Weitergehende Vorgaben für die Datenschutzorganisation enthält der CCPA nicht. So muss das Unternehmen nicht ab einer bestimmten Größe einen Datenschutzbeauftragten ernennen (Art. 37 DSGVO, § 38 BDSG), einen Vertreter innerhalb Kaliforniens ernennen (Art. 27 DSGVO), ein Verzeichnis der Verarbeitungstätigkeiten anlegen (Art. 30 DSGVO), Datenschutz durch Technikgestaltung oder datenschutzfreundliche Voreinstellungen wahren (Art. 25 DSGVO). Insoweit zeigt sich der CCPA als pragmatisch und liberal. Umfassende Transparenz soll eine Umsetzung des Datenschutzes sicherstellen – statt detaillierter Vorgaben für einen bestimmte Art der Datenschutzorganisation.[1276] In der Praxis sollten diese Unterschiede auch nicht überbewertet werden: um den CCPA zu erfüllen, ist eine mit den Vorgaben der DSGVO vergleichbare Datenschutzorganisation erforderlich. So empfiehlt amerikanische Praxisliteratur zur Umsetzung des CCPA z. B., ein zentrales Register aller Verarbeitungen anzulegen *(data mapping)*[1277] und einen *privacy officer* zu benennen.[1278]

4. Ergebnis

Die Unternehmenspflichten des CCPA haben eine geringere Reichweite als die Pflichten für Verantwortliche der DSGVO. Weitergehend als die DSGVO sind allerdings die eingehend geregelten Informationspflichten.[1279] Die Aufteilung in einen kurzen Datenschutzhinweis und eine umfassende Datenschutzerklärung sorgt für eine zielgruppengerechte Kommunikation. Insoweit ist die spezifische Regelungstechnik des CCPA besser für Informationspflichten geeignet als die offene, technologieneutrale Regelungstechnik der DSGVO.

[1275] *Bundesamt für Sicherheit in der Informationstechnik*, BSI-Standard 200-1: Managementsysteme für Informationssicherheit, S. 31.

[1276] Dieses Problem stellt sich bei der DSGVO vor allem bei der Frage, ob dem Datenschutzbeauftragten ein Weisungsrecht gegenüber anderen Fachabteilungen eingeräumt werden kann. Dazu: *Koglin* in: Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, A.III.2 Anmerkung 5.

[1277] *Bukaty*, CCPA Implementation Guide, S. 66; *Diamond*, 22 Journal of Internet Law 1, 17; R*yle et al.*, 21 Journal of Accounting, Ethics & Public Policy 247, 258; *Pink*, California Consumer Privacy Act Annotated, § 11:4; *Shelton Leipzig*, Implementing the CCPA: A Guide for Global Business, S. 45.

[1278] *Bukaty*, CCPA Implementation Guide, S. 68; *Diamond*, 22 Journal of Internet Law 1, 21; *Ryle et al.*, 21 Journal of Accounting, Ethics & Public Policy 247, 261; *Shelton Leipzig*, Implementing the CCPA: A Guide for Global Business, S. 45.

[1279] Cal. Civ. Code §§ 1798.100(a), 1798.110(c), 1798.115(c),1798.120(b), 1798.130(a), 1798.135(a), 11 C.C.R. §§ 7010–7011.

Diese spezifische Regelungstechnik verwendet der CCPA jedoch nicht für die Zweckbindung, Datenminimierung und Speicherfristbegrenzung.[1280] Proposition 24 wollte ersichtlich mit der Einführung dieser nur knapp geregelten Unternehmenspflichten vor allem die Bedingungen für einen Angemessenheitsbeschluss erfüllen.

Die Datensicherheitspflicht[1281] sowie Weiterübermittlungs- und Dienstleisterverträge[1282] sind dagegen detaillierter ausgestaltet und beruhen auf exponierten Vorläufern im amerikanischen Recht. Die Datensicherheitspflicht inkorporiert sogar nur ein früheres kalifornisches Datensicherheitsgesetz in den CCPA, der damit seinen Anspruch als umfassendes Datenschutzgesetz unterstreicht. Die Weiterübermittlungs- und Dienstverträge sollen für Rechenschaft in Übermittlungsketten sorgen und so die Reichweite des CCPA faktisch auch über Kalifornien hinaus erstrecken.

E. Rechtsdurchsetzung

I. Aufsichtsbehörden

1. Gewaltenteilung als typisches Element des amerikanischen Verwaltungsaufbaus

Gewaltenteilung ist ein tragendes Prinzip des amerikanischen Rechts. Die U. S. Constitution trennt Legislative, Judikative und Exekutive stärker als das Grundgesetz.[1283] So wollten die Verfassungsväter verhindern, dass zu viel Macht in Händen einer einzelnen Person liegt.[1284] Deswegen sollen sich die drei Gewalten durch *checks and balances* gegenseitig kontrollieren.[1285] Diese Grundentscheidung prägt auch den Verwaltungsaufbau.[1286] Die Verwaltung ist stark zersplittert. So wählt in Kalifornien das Volk nicht nur den Gouverneur und die Vize-Gouverneurin direkt, sondern auch Secretary of State, Attorney General, Treasurer, Controller,[1287] Superintendent[1288] und Insurance Commissioner.[1289]

[1280] Cal. Civ. Code § 1798.100(a),(c).

[1281] Cal. Civ. Code § 1798.100(e).

[1282] Cal. Civ. Code §§ 1798.100(d), 1798.140(j),(ag).

[1283] *Kischel*, 46 Admin. L. Rev. 213, 251 f.; *Michel*, Gerichtsverwaltung und Court Management in Deutschland und in den USA, S. 184 f.; *Möllers*, Gewaltengliederung, S. 72. Vgl. allgemein zur Bedeutung der Gewaltenteilung in amerikanischer Verfassung und im Verwaltungsaufbau: *Jacobs*, 129 Yale L. J. 378, 386 f.

[1284] Vgl. die ausführliche Begründung der Gewaltenteilung in: *Madison*, Federalist No. 47.

[1285] *Madison*, Federalist No. 48.

[1286] *Jacobs*, 129 Yale L. J. 378, 386–405.

[1287] Treasurer und Controller übernehmen ähnliche Aufgaben wie die Finanzministerien und Rechnungshöfe in Deutschland, vgl. Cal. Gov. Code §§ 12320–12333, 12410–12431.

[1288] Zuständig für das Bildungsministerium, vgl. Cal. Educ. Code §§ 33302, 33303.

[1289] Cal. Const. Art. V § 2, 11, IX § 2; Cal. Ins. Code § 12900(a).

Diese leiten ihre jeweiligen Ministerien voneinander unabhängig. Viele Gesetze räumen zudem mehreren Behörden gleichzeitig Befugnisse ein, um staatliche Macht weiter aufzuteilen.[1290] So vollziehen beispielsweise sowohl die FTC als auch das U. S. Department of Justice das Kartellrecht auf Bundesebene.[1291]

Dementsprechend teilt auch der CCPA die Rechtsdurchsetzung auf mehrere voneinander unabhängige Behörden auf. Die California Privacy Protection Agency entwickelt das Datenschutzrecht fort, ist beratend tätig und verhängt Bußgelder (2). Der direkt gewählte Attorney General sanktioniert dagegen die bedeutenden, öffentlichkeitswirksamen Fälle (3). Die ebenfalls zumeist direkt gewählten District und City Attorneys komplementieren diese beiden Aufsichtsbehörden, indem sie lokale Fälle übernehmen (4). Damit ist der Vollzug des CCPA wesentlich stärker zersplittert als die auf einheitliche Entscheidungen ausgerichteten europäischen Aufsichtsbehörden (5).

2. Calilfornia Privacy Protection Agency

a) Aufbau als unabhängige Kommission

Die wichtigste Aufsichtsbehörde ist die unabhängige California Privacy Protection Agency, die Proposition 24 geschaffen hat und die sich derzeit noch im Aufbau befindet. Sie hat nur weniger bedeutsame Vorläufer im amerikanischen Recht. In Kalifornien bestand zwar von 2000 bis 2012 ein Office of Privacy Protection; dieses sollte aber nur die Öffentlichkeit über Datenschutz informieren und hatte im Gegensatz zur California Privacy Protection Agency keine Sanktions- oder Regelungsbefugnis.[1292] Vielmehr orientiert sich die Ausgestaltung der California Privacy Protection Agency an den unabhängigen Aufsichtsbehörden der DSGVO.[1293]

Diese Ausgestaltung als unabhängige Behörde ist mit der amerikanischen Rechtskultur gut vereinbar, in dem auch sonst viele unabhängige Behörden bestehen, wie beispielsweise die FTC.[1294] Diese sollen isoliert von kurzfristiger Parteipolitik aufgrund eigenen Fachwissens rationale Entscheidungen treffen.[1295] Zudem kann eine unabhängige Behörde – losgelöst von kurzlebiger Parteipolitik – langfristig denken und so Stabilität erreichen. Auch den Einfluss der

---

[1290] *Gersen*, 2006 Sup. Ct. Rev. 201, 207–216.

[1291] Die wichtigsten Zuständigkeiten des Bundesjustizministeriums sind: Sherman Antitrust Act, 15 U. S. C. § 4; Wilson Tariff Act, 15 U. S. C. § 9, Clayton Act: 15 U. S. C. §§ 15f, 18a. Zuständigkeiten der FTC: Clayton Act, 15 U. S. C. 18a, 21(a); FTC Act, 15 U. S. C. § 45.

[1292] S.B. 129., 1999–2000 Leg., Reg. Sess (Cal. 2000), Cal. Stats. 2000 ch. 984 § 1. Später aufgehoben durch A. B. 2408, 2009–10 Leg., Reg. Sess (Cal. 2010), Cal. Stats. 2010 ch. 404.

[1293] Vgl. *Bracy*, Alastair Mactaggart on California's Prop 24, 31m:58s: Unabhängige Datenschutzbehörde sei weltweit bewährtes Modell. *Mactaggart* ist Vorsitzender der Bürgerinitiative, die Proposition 24 initiiert hat, siehe Kapitel 2:C.IV (ab S. 35).

[1294] *Jacobs*, 129 Yale L. J. 378, 395–399.

[1295] Die folgende Darstellung der Vorteile von unabhängigen Behörden beruht auf: *Barkow*, 89 Tex. L. Rev. 15, 19–25.

regulierten Unternehmen soll Unabhängigkeit lindern. Interessen der regulierten Wirtschaft sind typischerweise gut finanziert und organisiert vertreten, während die Kollektivinteressen weit verstreut sind. Dieser Effekt kann so stark werden, dass die Behörde effektiv als Interessenvertreterin der regulierten Unternehmen auftritt. Einen solchen *regulatory capture* verhindert die Unabhängigkeit bis zu einem gewissen Grad.

Anders als bei den meisten[1296] europäischen Aufsichtsbehörden wird die Unabhängigkeit der California Privacy Protection Agency zudem dadurch gestärkt, dass sie eine fünfköpfige Kommission leitet.[1297] Eine Kommission fördert die Unabhängigkeit, da Interessengruppen nicht nur eine Person, sondern die Mehrheit der Mitglieder umstimmen müssten.[1298] Solche Kommissionen sind für den amerikanischen Verwaltungsaufbau typisch.[1299] Die California Privacy Protection Agency ist dabei zwei ebenfalls fünfköpfigen Kommissionen nachgebildet: der FTC[1300] des Bundes und der Fair Political Practices Commission Kaliforniens.[1301] Verschiedene Amtsinhaber:innen ernennen die fünf Kommissionsmitglieder der California Privacy Protection Agency, um eine Einflussnahme von außen zu verhindern. Der Gouverneur benennt den Vorsitz und ein weiteres Mitglied,[1302] während der Attorney General, der Ältestenrat des kalifornischen Senats und der Sprecher der kalifornischen Assembly[1303] je eines der drei anderen Mitglieder bestimmen.[1304] Die Mitglieder müssen Kalifornier:innen sein, die über Expertise für Datenschutz, Technik und Verbraucherschutz verfügen.[1305] Sie sollen frei entscheiden, keine Absprachen vor Sitzungen treffen und alle Informationen an die anderen Mitglieder weitergeben.[1306] Die Kommissionsmitglieder sind zudem verpflichtet, die Vertraulichkeit der ihnen anvertrauten Informationen zu wahren.[1307]

[1296] Eine Kommission existiert nur in Belgien und Luxemburg: Art. 7, 9 wet tot oprichting van de Gegevensbeschermingsautoriteit [Gesetz über die Einrichtung der Datenschutzbehörde], Art. 16 Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données [Gesetz vom 01.08.2018 über die nationale Datenschutzkommission]. Das irische Datenschutzgesetz sieht eine Kommission vor (§ 15(1) Data Protection Act). Bisher wurde nur ein Kommissionsmitglied ernannt, wobei die Ernennung zusätzlicher Mitglieder geplant ist, vgl. *Weckler*, Independent, Will the appointment of more Data Protection Commissioners be enough to silence Ireland's critics?

[1297] Cal. Civ. Code § 1798.199.10(a).

[1298] *Jacobs*, 129 Yale L.J. 378, 433 f.

[1299] *Barkow*, 89 Tex. L. Rev. 15, 37–41.

[1300] *Bracy*, Alastair Mactaggart on California's Prop 24, 31m:58s: FTC sei primäres Vorbild für Aufbau.

[1301] *de la Torre*, Golden Data, What is the California Privacy Protection Agency? Zu dieser Kommission: Cal. Gov. Code §§ 81001, 83100–83124.

[1302] Cal. Civ. Code § 1798.199.10(a).

[1303] Die Assembly ist das kalifornische Unterhaus, Cal. Const Art. IV § 1, 2.

[1304] Cal. Civ. Code § 1798.199.10(a).

[1305] Cal. Civ. Code § 1798.199.10(a).

[1306] Cal. Civ. Code § 1798.199.15(c),(e).

[1307] Cal. Civ. Code § 1798.199.15(b).

Während ihrer Amtszeit dürfen die Kommissionsmitglieder keine entgeltliche oder unentgeltliche Tätigkeit ausüben, die Interessenskonflikte begründen könnte.[1308] Die verbotenen Tätigkeiten werden durch einen Conflict of Interests Code näher bestimmt.[1309] Zudem dürfen Mitglieder bis zu einem Jahr nach Ende der Amtszeit nicht für Unternehmen arbeiten, welche die Aufsichtsbehörden wegen eines Verstoßes gegen den CCPA während oder bis zu fünf Jahre vor Beginn der Amtszeit sanktioniert haben.[1310] Ausweislich des klaren Wortlauts (»enforcement action or civil action«) genügt dafür neben Bußgeldern der California Privacy Protection Agency auch eine *civil penalty* des Attorney General oder eines der District oder City Attorneys.[1311] Für zwei Jahre nach Ende der Amtszeit darf das ehemalige Mitglied zudem nicht als Vertreter:in in Verfahren vor der California Privacy Protection Agency auftreten.[1312] Diese beiden Regelungen sollen dem »Drehtür-Effekt« zwischen Behörde und regulierten Unternehmen nach Ende der Amtszeit vorbeugen.[1313]

Die Amtszeit beträgt acht Jahre, wobei die Ernennung jederzeit – auch ohne Angabe eines Grundes – widerrufen werden kann.[1314] Dies dient der demokratischen Legitimation: die mit einer weit gefassten Verordnungsermächtigung ausgestattete California Privacy Protection Agency soll nicht willkürlich und unkontrolliert Regeln erlassen können, sondern zumindest bei einem klaren Missbrauch von gewählten Politiker:innen beaufsichtigt werden können.[1315] Allerdings müssten mehrere unabhängig gewählte Organe übereinstimmend handeln, um eine Mehrheit der Mitglieder abzuberufen. Zudem erfordert eine Entlassung von Kommissionsmitgliedern erhebliches politisches Kapital, sodass sie auch ohne Pflicht zur Angabe eines Grundes selten vorkommen wird.[1316]

Die Kommissionsmitglieder sollen ähnlich zu einem Aufsichtsrat die strategische Richtung der California Privacy Protection Agency vorgeben, während die Angestellten das Tagesgeschäft erledigen sollen. Die Mitglieder sind dabei ehrenamtlich tätig (abgesehen von einer Aufwandsentschädigung von 100 $ pro Arbeitstag).[1317] Die Kommission bestellt für das Tagesgeschäft einen Executive

---

[1308] Cal. Civ. Code § 1798.199.15(d).

[1309] *Cal. Privacy Protection Agency*, Conflict of Interest Code. Angenommen in der Sitzung vom 18.10.2021: *Cal. Privacy Protection Agency*, Board Meeting October 18, 2021 Minutes, S. 10.

[1310] Cal. Civ. Code § 1798.199.15(f).

[1311] Cal. Civ. Code § 1798.199.15(f).

[1312] Cal. Civ. Code § 1798.199.15(g).

[1313] Vgl. allgemein *Barkow*, 89 Tex. L. Rev. 15, 46–49.

[1314] Cal. Civ. Code § 1798.199.20.

[1315] *Californians for Consumer Privacy*, Annotated Text of the CPRA, § 1798.199.20. Dies wegen des Missbrauchspotenziales kritisierend: *Monticollo/Reckell/Cividanes*, 35 Antitrust ABA 32, 34.

[1316] Vgl. allgemein: *Barkow*, 89 Tex. L. Rev. 15, 30.

[1317] Cal. Civ. Code § 1798.199.25. Die Aufwandsentschädigung ist indexiert und entspricht der Aufwandsentschädigung von einfachen Mitgliedern der Fair Political Practices Commission,

Director,[1318] an den sie laufende Angelegenheiten delegiert.[1319] Die Kommission muss aber die endgültige Entscheidung über Bußgeldverfahren und den Erlass von Verordnungen selbst treffen.[1320]

Den hohen Stellenwert der Transparenz unterstreicht, dass die Kommission öffentlich tagt.[1321] Jeder Bürger und jede Bürgerin darf sich zudem zu allen Tagesordnungspunkten in der öffentlichen Sitzung äußern.[1322] Eine Mehrheit der Kommissionsmitglieder dürfen auch nicht außerhalb der öffentlichen Sitzungen über Themen der California Privacy Protection Agency sprechen,[1323] damit nicht eine Mehrheit der Kommissionsmitglieder voreingenommen ist. Eine bloße Minderheit von zwei Mitgliedern darf allerdings auch außerhalb der Sitzungen miteinander kommunizieren, was die Kommission zur Bildung von zweiköpfigen Unterkomitees ausgenutzt hat.[1324]

Die im März 2021 ernannten Kommissionsmitglieder stammen aus der akademischen Forschung, Verwaltung und der schwarzen Bürgerrechtsbewegung.[1325] Die Vorsitzende *Jennifer Urban* ist eine Universitätsprofessorin, die sich auf Datenschutz spezialisiert hat. Ebenfalls Universitätsprofessorin ist das Kommissionsmitglied *Lydia de la Torre,* die früher in Spanien als Rechtsanwältin zum europäischen Datenschutz beraten und vielfach zum CCPA publiziert hat. Weiterhin ist die pensionierte Leiterin der Verbraucherschutzabteilung des Attorney General *Angela Sierra* Kommissionsmitglied, sodass auch auf Leitungsebene eine personelle Verflechtung zwischen den beiden wichtigsten Aufsichtsbehörden des CCPA entsteht.

Weitere Kommissionsmitglieder sind *John Thompson* (hochrangiger Verwaltungsangestellter für Olympischen Spiele 2028 in Los Angeles) und *Vinhcent Le* (Syndikusanwalt für eine Bürgerrechtsorganisation gegen Rassismus im Internet). Insgesamt fällt auf, dass alle Kommissionsmitglieder Jurist:innen sind und keine Informatiker:innen ausgewählt wurden. Ansonsten scheint die Zusammensetzung ausgewogen zu sein und weder zu stark in Richtung des Verbraucherschutzes noch die von Unternehmensinteressen zu gehen.

Die leichte Schwäche der Kommission im technischen Bereich gleicht der Executive Director *Ashkan Soltani* seit Oktober 2021 aus, der Informatiker,

---

vgl. Cal. Gov. Code § 83106. Sie fällt bereits ab einer Stunde Arbeit an, *Cal. Privacy Protection Agency*, »Per Diem« Policy as Approved in September 7, 2021 Board Meeting, S. 1.

[1318] Cal. Civ. Code § 1798.199.30.

[1319] *Cal. Privacy Protection Agency*, Board Meeting October 18, 2021 Minutes, S. 11, 15. Ermächtigung in Cal. Civ. Code § 1798.99.35.

[1320] Cal. Civ. Code § 1798.99.35.

[1321] Cal. Gov. Code §§ 11123(a), 11125.7(a).

[1322] Cal. Gov. Code §§ 11125.7(a).

[1323] Cal. Gov. Code §§ 11122.5(b).

[1324] *Cal. Privacy Protection Agency*, Board Meeting June 14, 2021 Minutes, S. 13–15.

[1325] Zu deren jeweiligem Lebenslauf: *Cal. Attorney General*, California Officials Announce California Privacy Protection Agency Board Appointments; *Duball*, The Privacy Advisor, What the CPPA's appointments say about enforcement priorities, strategy.

früherer Chief Technologist der FTC und langjähriger Datenschutzaktivist ist.[1326] Er war zudem an der Ausarbeitung beider Volksbegehren maßgeblich beteiligt.[1327] Bisher ist die California Privacy Protection Agency noch im Aufbau und verfügt neben dem Executive Director über keine Beschäftigten.[1328]

b) Budget und Consumer Privacy Fund

Die California Privacy Protection Agency verfügt über ein Jahresbudget von mindestens 10 Millionen Dollar.[1329] Die Zusicherung dieses Mindestbudgets durch Proposition 24 stärkt ihre Unabhängigkeit, da ihr nicht durch Budgetkürzungen die Arbeitsgrundlage entzogen werden kann. Diese Summe passt das kalifornische Department of Finance jährlich der Inflation an.[1330]

Daneben hat der CCPA den Consumer Privacy Fund eingerichtet.[1331] In diesen fließen die Bußgelder der California Privacy Protection Agency und die *civil penalties* des Attorney General ein.[1332] Zuerst soll der Consumer Privacy Fund die Kosten des Attorney General und kalifornischer Gerichte aus dem Vollzug des CCPA ausgleichen.[1333] Unklar ist, ob dies auch für Kosten der California Privacy Protection Agency gilt. Cal. Civ. Code § 1798.155(b) spricht insoweit davon, dass die Bußgelder einzuzahlen sind »with the intent to fully offset any costs incurred by the state courts, the Attorney General *and the California Privacy Protection Agency*[1334] in connection with this title«. Cal. Civ. Code § 1798.160(a) regelt die Kostenerstattung aus dem Consumer Privacy Fund, wobei nur die kalifornischen Gerichte und der Attorney General aufgeführt sind, während die California Privacy Protection Agency fehlt. Cal. Civ. Code § 1798.160(b)(1) wiederum wiederholt die Kostenerstattungsregelung aus Cal. Civ. Code § 1798.160(a) wortlautgleich ohne die California Privacy Protection Agency. Hier zeigt sich die oft geringe handwerkliche Qualität des CCPA. Streng am Wortlaut orientiert,[1335] ist eine Kostenerstattung der California Privacy Protection Agency wohl abzulehnen, da Cal. Civ. Code § 1798.155(b) nur das Ziel festlegt, während Cal. Civ. Code § 1798.160(a),(b)(1) die tatsächliche Kostenerstattung regeln.

Die nach der Kostenerstattung verbleibenden Beträge legt die State Treasurer zu 91 % langfristig an, wobei die Erträge in den allgemeinen Haushalt

---

[1326] *Cal. Privacy Protection Agency*, Ashkan Soltani Selected as California Privacy Protection Agency Executive Director.

[1327] Zu den Volksbegehren und *Soltanis* Rolle siehe Kapitel 2:C (ab S. 30).

[1328] *Cal. Privacy Protection Agency*, Board Meeting October 18, 2021 Minutes, S. 4.

[1329] Cal. Civ. Code § 1798.199.95(a).

[1330] Cal. Civ. Code § 1798.199.95(b). Das Department of Finance übernimmt die Haushaltsplanung, vgl. Cal. Gov Code §§ 13000–13012.

[1331] Cal. Civ. Code § 1798.160.

[1332] Cal. Civ. Code §§ 1798.155(b), 1798.199.90(b).

[1333] Cal. Civ. Code §§ 1798.155(b), 1798.160(a),(b)(1).

[1334] Hervorhebung durch Verfasser.

[1335] Zur wortlautorientierten amerikanischen Auslegung siehe Kapitel 3:B.I.1.a) (ab S. 43).

Kaliforniens fließen.[1336] Aus den anderen 9 % der Beträge soll die California Privacy Protection Agency Zuschüsse gewähren.[1337] Drei Prozentpunkte sollen gemeinnützige Vereinigungen erhalten, um Datenschutz zu fördern.[1338] Weitere drei Prozentpunkte sollen wohltätigen Organisationen oder öffentliche Einrichtungen zufließen, um Kinder über Datenschutz im Internet aufzuklären.[1339] Schließlich erhalten drei Prozentpunkte kommunale und staatliche Strafverfolgungsbehörden, um Datenpannen aufzuklären, insbesondere für internationale Kooperationen.[1340]

c) Verordnungsermächtigung

Der CCPA ermächtigt die California Privacy Protection Agency, eine Durchführungsverordnung zu erlassen.[1341] Der CCPA-2018 hatte diese Kompetenz ursprünglich dem Attorney General zugewiesen.[1342] Durch Proposition 24 ist die Regelungskompetenz am 21.04.2022 auf die neu geschaffene California Privacy Protection Agency übergegangen.[1343] Diese ist als unabhängige Behörde mit fachspezifischer Expertise als Normgeberin eher geeignet als der Attorney General, der trotz Leitung des Justizministeriums in der Regel keine Verordnungen oder andere Regelungen erlässt.[1344] Die Verordnungsermächtigung in die Hände einer Aufsichtsbehörde zu geben, ermöglicht eine enge Abstimmung der Normgebung und deren Vollzug.

Die Regelungskompetenz ist weit gefasst. Die California Privacy Protection Agency kann sich zunächst auf eine Generalklausel stützen, nach der alle Regelungen zulässig sind, welche den CCPA konkretisieren oder fortbilden (»to further the purposes of this title«).[1345] Daneben hat der CCPA-2018 sieben konkrete Ermächtigungen geschaffen, die Proposition 24 noch um 14 weitere Ermächtigungen ergänzt hat. Diese Ermächtigungen sind teilweise sehr konkret und lassen der California Privacy Protection Agency kaum Spielraum. Beispielsweise gibt die Ermächtigung für das Identifizierungsverfahren bei Auskunftsanträgen explizit vor, dass ein über ein passwortgeschütztes Benutzerkonto gestellter Auskunftsantrag ausreichen soll.[1346] Andere Ermächtigungen sind hingegen offener. So soll die California Privacy Protection Agency Widerspruchsrechte für automatisierte Entscheidungsfindung, insbesondere Profiling regeln, ohne das spezifiziert wäre,

[1336] Cal. Civ. Code § 1798.160(b)(2)(A).
[1337] Cal. Civ. Code § 1798.160(b)(2)(B).
[1338] Cal. Civ. Code § 1798.160(b)(2)(B)(i).
[1339] Cal. Civ. Code § 1798.160(b)(2)(B)(ii).
[1340] Cal. Civ. Code § 1798.160(b)(2)(B)(iii).
[1341] Cal. Civ. Code § 1798.185.
[1342] Cal. Civ. Code § 1798.185(d),(a) a. A.
[1343] Siehe Kapitel 2:C.V (ab S. 38).
[1344] *Cal. Attorney General*, California Consumer Privacy Act of 2018, S. 2.
[1345] Cal. Civ. Code § 1798.185(b).
[1346] Cal. Civ. Code § 1798.185(a)(7).

ob nur bestehende Rechte mit Profiling abgestimmt werden sollen oder ob ein neues Recht geschaffen werden soll (»opt-out rights with respect to businesses' use of automated decision-making technology, including profiling«).[1347]

Die Durchführungsverordnung entsteht in einem transparenten und stark formalisierten Verfahren. Die im amerikanischen Recht typische Formalisierung des Verordnungsgebungsverfahrens soll zu gut durchdachten und bestimmten Regeln führen sowie überflüssige Normen vermeiden.[1348] Die Transparenz solcher soll unangemessenen Einfluss von Wirtschaftsinteressen verhindern.[1349]

Zuerst muss die Behörde einen Entwurf veröffentlichen[1350] und jede Vorschrift dieses Entwurfs detailliert begründen sowie erklären, welche Alternativen sie verworfen sowie welche Materialien sie für den Entwurf verwendet hat.[1351]

Bei Verordnungsgebungsverfahren, die nach Einschätzung der Behörde zu wirtschaftlichen Folgen von mindestens 50 Millionen Dollar führen, muss die Behörde zudem ein externes Gutachten zu diesen Folgen einholen.[1352] Das externe Gutachten zur ersten Durchführungsverordnung schätzte die initialen Umsetzungskosten des CCPA für Unternehmen auf 55 Milliarden Dollar und damit sehr hoch ein.[1353] Diese Schätzung war explizit als grobe Überschlagsrechnung (»back of the envelope calculation«) deklariert[1354] und auch vom Attorney General als bloß theoretischer Maximalbetrag eingeordnet.[1355] Dennoch wurde sie weithin unkritisch als quasi-amtliche Zahl des Attorney General rezipiert.[1356] Tatsächlich sind wohl wesentlich geringere Umsetzungskosten angefallen.[1357] Dies zeigt die Schwäche der Pflicht zu einem solchen Gutachten:

[1347] Cal. Civ. Code § 1798.185(a)(16).

[1348] So explizit diesbezüglichen Erwägungsgründe in Cal. Gov. Code §§ 11340, 11340.1(a).

[1349] *Kagan*, Adversarial legalism: the American way of law, S. 188–190.

[1350] Cal. Gov. Code § 11346.2(a).

[1351] Cal. Gov. Code § 11346.2(b)(1),(3),(4).

[1352] Cal. Gov. Code §§ 11346.2(b)(2)(B), 11346.3(c).

[1353] *Roland-Holst et al.*, Standardized Regulatory Impact Assessment: CCPA, S. 11. Zu recht kritisch: Californians for Consumer Privacy, Comment in: *Cal. Attorney General*, Written Comments 45-Day Period, S. 45.

[1354] *Roland-Holst et al.*, Standardized Regulatory Impact Assessment: CCPA, S. 11.

[1355] *Cal. Attorney General*, Summary and Response to Comments Submitted During 45-Day Period, S. 282.

[1356] *Determann*, 26 Mich. Tech. L. Rev. 229, 229; *Janofsky*, Walt Street Journal, Compliance Costs for California Privacy Law Pegged at $55 Billion; *Kessler*, 93 S. Cal. L. Rev. 99, 120. Ebenfalls unkritisch die Zahl übernehmend, aber zumindest nicht den Attorney General als Quelle nennend: *Deb*, 31 DePaul J. Art Tech. & Intell. Prop. L. 115, 142; *Jeevanjee*, 70 Am. U. L. Rev. 75, 122; *McGruer*, 15 Wash. J. L. Tech. & Arts 120, 140; *Read*, 25 Ill. Bus. L. J. 19, 23; *Li*, 32 Loy. Consumer L. Rev. 177, 190; *Pink*, California Consumer Privacy Act Annotated, Introduction (nicht zutreffend das Cal. Deptartment of Finance als Autor nennend); *Yallen*, 53 Loy. L. A. L. Rev. 787, 818.

[1357] *Rix*, How Data Privacy Regulations Affect Public Corporations That Profit From Consumers' Data During an Ongoing Pandemic, S. 14–18.

der Zwang, eine Zahl zu nennen, obwohl sich die komplexen Auswirkungen eines umfassenden Datenschutzgesetzes kaum quantifizieren lassen.

Nach Veröffentlichung des Entwurfs läuft eine 45-tägige öffentliche Stellungnahmefrist.[1358] Bei anschließenden, substanziellen Änderungen muss die Behörde eine weitere 15-tägige Stellungnahmefrist gewähren.[1359] Die Behörde ist verpflichtet, auf jede Stellungnahme öffentlich zu antworten.[1360] Der Attorney General hat hierbei über 300 Stellungnahmen erhalten und beantwortet.[1361]

Nach diesem Konsultationsprozess legt die Behörde den fertigen Entwurf samt einer Begründung eventueller Änderungen zum Erstentwurf dem Office of Administrative Law vor, das zur Qualitätssicherung und Kontrolle der Rechtmäßigkeit eine Schlussredaktion vornimmt.[1362] Dieses hat die erste Durchführungsverordnung weitgehend genehmigt.[1363] Neben redaktionellen Änderungen hat der Attorney General nur in Absprache mit diesem Office die Vorschriften zur Zweckbindung zurückgezogen,[1364] wohl da das Office of Administrative Law davon ausging, dass diese dem Gesetzestext des CCPA widersprechen. Nach dieser Schlussredaktion muss die Behörde die Verordnung veröffentlichen und jede Änderung zum ursprünglichen Entwurf in einer öffentlichen Stellungnahme begründen.[1365]

Dieser Prozess ist zwar aufwendig, resultiert aber in einer ausgewogenen und klaren Durchführungsverordnung. Dabei sind über 2000 Seiten Stellungnahmen und über 500 Seiten Begründung und Antworten des Attorney General entstanden.[1366] Natürlich bindet das erhebliche Ressourcen.[1367] Diese umfassende öffentliche Diskussion hat aber auch dazu geführt, dass die Durchführungsverordnung wesentlich besser durchdacht ist als der CCPA selbst.[1368] Auch stellen die Antworten des Attorney General eine wertvolle Auslegungshilfe dar.

Der Attorney General hatte sich angesichts des Zeitdrucks für die erste Durchführungsverordnung eng an den verpflichtenden Regelungsgehalt gehalten und nur sehr begrenzt offene Ermächtigungen oder die Generalklausel ausgefüllt.

[1358] Cal. Gov. Code § 11346.4(a).

[1359] Cal. Gov. Code § 11346.8(c).

[1360] Cal. Gov. Code § 11346(a)(10).

[1361] *Cal. Attorney General*, Cal. Attorney General Becerra Submits Proposed Regulations for Approval Under the California Consumer Privacy Act.

[1362] Cal. Gov. Code §§ 11346.9(a), 11349–11349.6.

[1363] *Cal. Attorney General*, Attorney General Becerra Announces Approval of Final Regulations Under the California Consumer Privacy Act.

[1364] *Cal. Attorney General*, Attorney General Becerra Announces Approval of Final Regulations Under the California Consumer Privacy Act.

[1365] Cal. Gov. Code § 11346.9(a).

[1366] *Cal. Attorney General*, Initial Statement of Reasons; *ders*, Summary and Response to Comments Submitted During 45-Day Period; *ders*, Summary and Response to Comments Submitted during 1st 15-Day Comment Period; *ders*, Summary and Response to Comments Submitted during 2nd 15-Day Comment Period; *ders.*, Final Statement of Reasons.

[1367] *Cal. Attorney General*, Budget Change Proposal, S. 8 veranschlagt fünf Vollzeitstellen für das Verordnungsgebungsverfahren.

[1368] Zur klareren Systematik siehe Kapitel 3:A (ab S. 41).

Insbesondere hat er weitreichende Vorschläge wie eine Ausnahme für Unternehmen, die bereits die DSGVO befolgen, abgelehnt.[1369] Die bisher einzige Vorschrift der Durchführungsverordnung, bei welcher der Attorney General die Generalklausel genutzt hat, zeigt das Zusammenspiel zwischen Regulierung und Vollzug. Er hat besonders große Unternehmen verpflichtet, in ihrer Datenschutzerklärung eine Verbraucherrechte-Statistik aufzunehmen, die ausweist, wie viele Anträge von Verbraucher:innen das Unternehmen erfüllt und abgelehnt hat.[1370] Anhand dieser Zahlen kann er gezielt gegen diejenigen Unternehmen vorgehen, die besonders viele Anträge ablehnen. Es ist zu erwarten, dass nach ersten Erfahrungen in der Vollstreckung die Privacy Protection Agency die Durchführungsverordnung an diese Erfahrungen anpasst.

Die California Privacy Protection Agency hat das formelle Verordnungsgebungsverfahren der zweiten Durchführungsverordnung am 08.07.2022 in Gang gesetzt, wobei der Entwurf allerdings weitgehend nur den durch Proposition 24 erweiterten Mindestinhalt der Durchführungsverordnung umsetzt.[1371]

d) Betriebsprüfungen und Ermittlungen

Die California Privacy Protection Agency soll regelmäßig Betriebsprüfungen durchführen.[1372] Die Betriebsprüfungs-Abteilung leitet ein »Chief Privacy Auditor«.[1373] Dabei wird die Durchführungsverordnung konkretisieren, wie die California Privacy Protection Agency die zu überprüfenden Unternehmen ausgewählt werden und wie eine solche Überprüfung abläuft.[1374]

Für Betriebsprüfungen und Ermittlungen kann die California Privacy Protection Agency Zeugen laden, vereidigen und befragen[1375] sowie die Vorlage von Dokumenten anordnen.[1376] Dabei soll sie auch mit anderen Datenschutzbehörden in den Vereinigten Staaten und ausdrücklich auch international zusammenarbeiten.[1377] Daher ist auch eine Zusammenarbeit mit den europäischen Aufsichtsbehörden möglich.

Ermittlungen kann die California Privacy Protection Agency auf eine Beschwerde oder von Amts wegen einleiten.[1378] Sie muss Beschwerdeführer:innen schriftlich mitteilen, welche Maßnahmen sie ergriffen hat und warum, wenn die Beschwerde mit einer eidesstattlichen Erklärung über den Sachverhalt verbunden

---

[1369] Cal. Attorney General, Initial Statement of Reasons, S. 44 f.
[1370] 11 C. C. R. § 7102(a). Siehe Kapitel 3:D.I.2.b)bb) (ab S. 157).
[1371] Siehe Kapitel 2:C.V (ab S. 38).
[1372] Cal. Civ. Code § 1798.199.40(f).
[1373] Cal. Civ. Code § 1798.199.40(f).
[1374] Cal. Civ. Code § 1798.185(a)(18).
[1375] Cal. Civ. Code § 1798.199.65.
[1376] Cal. Civ. Code § 1798.199.65.
[1377] Cal. Civ. Code § 1798.199.40(i).
[1378] Cal. Civ. Code § 1798.199.45(a) a. A.

ist.[1379] Sie kann nach eigenem Ermessen entscheiden, ob sie Ermittlungen einleitet,[1380] und ob sie dem Unternehmen eine Abhilfefrist vor Einleitung eines Bußgeldverfahrens gewährt.[1381] Dabei soll sie berücksichtigen, ob das Unternehmen, der Dienstleister oder der Dritte vorsätzlich gehandelt hat und ob das Unternehmen bereits vor der Kontaktaufnahme durch die California Privacy Protection Agency angefangen hatte den Verstoß zu beheben.[1382]

e) Bußgelder

Die California Privacy Protection Agency kann wegen jedes Verstoßes gegen den CCPA ein Bußgeld verhängen.[1383] Schuld ist dabei ausweislich des Wortlauts nicht erforderlich und ist bei Verwaltungsstrafen auch nicht in den Wortlaut hineinzulesen.[1384] Ein Bußgeld können Unternehmen, Dienstleister oder Dritte erhalten.[1385] Wie typisch für amerikanische Recht, geht der CCPA stillschweigend davon aus, dass jeder Verstoß durch Beschäftigte der Organisation zuzurechnen ist (*vicarious liability)*.[1386]

Das Bußgeldverfahren ist stark formalisiert. Zuerst muss die California Privacy Protection Agency die beschuldigte Person schriftlich anhören und ihr eine 30-tägige Stellungnahmefrist einräumen.[1387] Dabei teilt sie ihr den Vorwurf mit, fasst die bisherigen Beweismittel zusammen und weist auf das Recht hin, sich anwaltlich vertreten zu lassen.[1388] Die Stellungnahmefrist löst nur eine Zustellung oder ein Einschreiben mit Rückschein aus.[1389] Eine etwaige persönliche Anhörung ist nicht-öffentlich, außer wenn die beschuldigte Person eine öffentliche Anhörung schriftlich beantragt.[1390]

Nach der Anhörung muss die California Privacy Protection Agency entscheiden, ob *probable cause* (Anfangsverdacht) besteht.[1391] Wenn ja, kann sie ein Bußgeldverfahren einleiten.[1392] Dazu stellt sie der beschuldigten Person eine

---

[1379] Cal. Civ. Code § 1798.199.45.

[1380] Cal. Civ. Code § 1798.199.45(a).

[1381] Cal. Civ. Code § 1798.199.45(a).

[1382] Cal. Civ. Code § 1798.199.45(a)(1),(2).

[1383] Cal. Civ. Code §§ 1798.155(a), 1798.199.55(a)(2).

[1384] Zur sehr ähnlichen Regelung in 12 U.S.C. § 93(b): U.S. Supreme Court vom 10.12.1997, *Hudson v. United States*, 522 U.S. 93, 104. Das fehlende Verschuldenserfordernis ist typisch für amerikanische Verwaltungsstrafen: *Mann*, 101 Yale L.J. 1795, 1806 Fn. 36, 1823 f.

[1385] Cal. Civ. Code § 1798.155(a).

[1386] Vgl. allgemein: Cal. Supreme Court vom 23.06.2011, *Diaz v. Carcamo*, 51 Cal. 4th 1148, 1154. Dieser Grundsatz gilt auch für Verwaltungssanktionen: *Minzner*, 53 Wm. & Mary L. Rev. 853, 907.

[1387] Cal. Civ. Code § 1798.199.50.

[1388] Cal. Civ. Code § 1798.199.50.

[1389] Cal. Civ. Code § 1798.199.50.

[1390] Cal. Civ. Code § 1798.199.50.

[1391] Vgl. zu diesem Begriff: *Sheppard*, Bouvier Law Dictionary, Probable Cause.

[1392] Cal. Civ. Code § 1798.199.55(a).

Anklageschrift zu, die sowohl die verletzten Normen des CCPA als auch den Sachverhalt nennt.[1393] Binnen 15 Tagen ab Zustellung kann die beschuldigte Person eine Verteidigungsschrift einreichen und eine mündliche Verhandlung beantragen.[1394]

Diese mündliche Verhandlung leitet ein *administrative law judge*.[1395] Dieser hat keine direkte Entsprechung im deutschen Recht. Einerseits sitzt der oder die *administrative law judge* unabhängig in einem mit Gerichtsprozessen vergleichbaren formalisierten Verfahren vor. Zudem stellt das kalifornische Office of Administrative Hearings den oder die *administrative law judge*,[1396] und sorgt so für eine gewisse Unabhängigkeit. Andererseits ist die Entscheidung des *administrative law judge* Teil des Verwaltungsverfahrens. Insbesondere kann die California Privacy Protection Agency in der mündlichen Verhandlung selbst über das Bußgeld entscheiden, wobei sie allerdings die Entscheidung nach ihrem freien Ermessen auch dem oder der *administrative law judge* überlassen kann.[1397] Die Entscheidung des oder der *administrative law judge* ist dann aber nur ein Vorschlag, über den die Kommission endgültig entscheidet.[1398] Falls die Kommission diesen Vorschlag verwirft, begründet sie dies schriftlich.[1399]

Die Entscheidung muss die California Privacy Protection Agency sofort veröffentlichen, nachdem sie diese getroffen hat.[1400] Gegen die Entscheidung der California Privacy Protection Agency kann die beschuldigte Person binnen 30 Tagen vor dem jeweiligen Superior Court klagen,[1401] der auch Vollstreckungsgericht ist.[1402] Bei einer Klage gegen die Entscheidung prüft das Gericht die Entscheidung zwar vollständig nach, gibt der Gesetzesauslegung der Behörde aber auch bei unbestimmten Rechtsbegriffen größeres Gewicht als im deutschen Recht.[1403]

Meistens werden Unternehmen das Bußgeld aber wohl nicht im streitigen Verfahren verhandeln wollen, sondern schon früh einen Vergleich akzeptieren. Dies ist die übliche Praxis in amerikanischen Straf- und Bußgeldverfahren.[1404] Unternehmen haben kein Interesse, durch einen langen Prozess

---

[1393] Cal. Gov. Code §§ 11503(a), 11505(a)–(c) i. V. m. Cal. Civ. Code § 1798.199.55(a).

[1394] Cal. Gov. Code § 11506(a) i. V. m. Cal. Civ. Code § 1798.199.55(a).

[1395] Cal. Gov. Code § 11502(a) i. V. m. Cal. Civ. Code § 1798.199.55(a).

[1396] Cal. Gov. Code § 11502(a) i. V. m. Cal. Civ. Code § 1798.199.55(a).

[1397] Cal. Gov. Code § 11517(a) i. V. m. Cal. Civ. Code § 1798.199.55(a).

[1398] Cal. Gov. Code § 11517(c)(2) i. V. m. Cal. Civ. Code § 1798.199.55(a).

[1399] Cal. Civ. Code § 1798.199.60.

[1400] Cal. Gov. Code § 11517(d) i. V. m. Cal. Civ. Code § 1798.199.55(a).

[1401] Cal. Gov. Code § 11523 i. V. m. Cal. Civ. Code § 1798.199.55(a). Trotz des historisch bedingten Namens ist der Superior Court das allgemeine erstinstanzliche Gericht.

[1402] Cal. Civ. Code §§ 1798.199.75, 1798.199.80.

[1403] Zu dieser sog. *deference*: Cal. Supreme Court vom 27.08.1998, *Yamaha Corp. of America v. State Bd. of Equalization*, 19 Cal. 4th 1, 7. Vgl. zur Rechtsprechung des Bundes und anderer Bundesstaaten: *Bertenthal*, 2020 Wis. L. Rev. 85–139.

[1404] Zum Strafprozess: *Gramlich*, Pew Research Center, Only 2 % of federal criminal defendants go to trial. Dies ist auch die übliche Praxis der FTC, siehe Kapitel 2:B.I.3 (ab S. 24).

negative Aufmerksamkeit der Öffentlichkeit auf sich zu lenken.[1405] Gleichzeitig erlaubt ein schneller Vergleich der California Privacy Protection Agency, ihre Ressourcen für weitere Fälle einzusetzen.

Die Bußgeldhöhe beträgt bis zu 2.500 $ pro Verletzung (»for each violation«) und bei vorsätzlichen Verstößen oder solchen, die Unter-16-Jährige betreffen, bis zu 7.500 $ pro Verletzung.[1406] Bedeutet pro Verletzung für eine Verletzungshandlung oder für einen Verletzungserfolg? Beim Abstellen auf eine Verletzungshandlung wäre der Bußgeldrahmen sehr niedrig, da auch bei einer Vielzahl von betroffenen Verbraucher:innen nur eine einzige Verletzungshandlung vorliegen kann. So wäre beispielsweise bei einer Datenpanne wegen unzureichender Sicherung der Kundendatenbank nur eine Verletzungshandlung gegeben, selbst wenn persönliche Informationen tausender Verbraucher:innen abhanden gekommen sind. Allerdings haben die kalifornischen Gerichte die Formulierung »for each violation« bei der Sanktionsvorschrift des Unfair Competition Law als pro Verletzungserfolg ausgelegt.[1407] Das Unfair Competition Law steht im engen Zusammenhang mit dem CCPA, da District und City Attorney CCPA-Verletzungen mittelbar über das Unfair Competition Law sanktionieren. Fachbegriffe aus demselben Rechtsgebiet sind einheitlich auszulegen.[1408] Daher wird der Bußgeldrahmen auch beim CCPA pro Verletzungserfolg berechnet, d. h. multipliziert mit der Zahl der betroffenen Verbraucher:innen.[1409] So können erhebliche Summen entstehen, zumal es keine Höchstgrenze für das Gesamtbußgeld gibt.

Sonstige Abhilfemaßnahmen sind lediglich schwach ausgeprägt. Die California Privacy Protection Agency kann nur Unterlassensanordnungen erlassen.[1410] Diese ermöglichen es ihr im Einzelfall einem Missstand abzuhelfen, haben aber im Gegensatz zu Bußgeldern keine abschreckende Wirkung.[1411]

Verstöße verjähren fünf Jahre nach ihrer Begehung.[1412] Diese Frist beginnt nicht zu laufen, solange das Unternehmen den Verstoß arglistig verschweigt

---

[1405] So zur FTC: *Hoofnagle*, FTC, S. 111.

[1406] Cal. Civ. Code § 1798.155(a).

[1407] Zu Cal. Bus. Prof. Code § 17206: Cal. Court of Appeal 3rd District vom 16.05.1984, *People v. Toomey*, 157 Cal. App. 3d 1, 22 f.; Cal. Court of Appeal 6th District vom 11.08.2003, *People ex rel. Kennedy v. Beaumont Investment, Ltd.*, 111 Cal. App. 4th 102, 128.
Zu Cal. Bus. Prof. Code § 17536: Cal. Supreme Court vom 05.04.1973, *People v. Superior Court*, 9 Cal. 3d 283, 288 f.

[1408] U. S. Supreme Court vom 14.06.1990, *Sullivan v. Stroop*, 496 U. S. 478, 483.

[1409] *Buresh*, 38 Santa Clara High Tech. L. J. 39, 64 f.; *Chander/Kaminski/McGeveran*, 105 Minn. L. Rev. 1733, 1759; *Clark/Halpert*, 17 PDP 7, 7; *Diamond*, Journal of Internet Law, April 2019, 12, 13; *Determann*, ZD 2018, 443, 445; *Schmidt*, The Privacy Advisor, Penalties and enforcement mechanisms; offenlassend: *Ballon*, E-commerce & Internet law, S. 26-423 f.; *Pink*, California Consumer Privacy Act Annotated, § 10:3.3[B]; a. A. (o.Bgr.) *Lejeune*, PinG 2021, 25, 26.

[1410] Cal. Civ. Code § 1798.199.55(a)(1).

[1411] Vgl. allgemein zur Wirksamkeit von Unterlassensanordnungen: *Glicksman/Earnhart*, 26 Stan. Envtl. L. J. 317, 359–364.

[1412] Cal. Civ. Code § 1798.199.70 a. A.

oder auf eine Vorlageanordnung im Prüfungs- oder Bußgeldverfahren nicht vorlegt.[1413] Ein Unternehmen verschweigt wohl Informationen arglistig, wenn es diese nicht in die umfassende Datenschutzerklärung aufnimmt, obwohl es dies hätte tun müssen und den Umfang der Informationspflicht kannte.[1414] Die Verjährung wird durch Zustellung des Anhörungsschreibens unterbrochen.[1415]

f) Öffentlichkeitsarbeit und Beratung

Die California Privacy Protection Agency soll nicht nur den CCPA durchsetzen, sondern auch eine umfassende Öffentlichkeitsarbeit leisten, um der Öffentlichkeit Risiken, Regeln und Zuständigkeiten im Datenschutz nahezubringen.[1416] Dabei soll sie besonders auch Kinder ansprechen, wozu sie ein Drittel der Zuschüsse aus dem Consumer Privacy Funds gewährt.[1417] Auch wird sie Verbraucher:innen[1418] und Unternehmen[1419] über ihre Rechte und Pflichten nach dem CCPA aufklären. Sie fasst die bei ihr von Unternehmen eingereichten Risikoanalysen in einem öffentlichen Jahresbericht zusammen.[1420] Schließlich berät sie auf Anfrage auch das kalifornische Parlament in Datenschutzfragen.[1421]

3. Kalifornischer Attorney General

a) Rolle als Vollzugsbehörde

Die California Privacy Protection Agency ergänzt der kalifornische Attorney General. Die deutsche Literatur beschreibt den Attorney General gemeinhin als eine Mischung aus Justizminister und Generalstaatsanwalt.[1422] Dies trifft seine Rolle jedoch nicht vollständig. Der Attorney General leitet zwar das kalifornische Department of Justice, das jedoch gänzlich andere Aufgaben als deutsche Bundes- oder Landesjustizministerien innehat. Das Department of Justice spielt insbesondere keine Rolle im Gesetzgebungsverfahren und erlässt kaum eigene Verordnungen.[1423] Auch die Gerichtsorganisation obliegt der Justiz im Lichte der starken Gewaltenteilung selbst.[1424] Vielmehr ist Aufgabe des Attorney General,

---

[1413] Cal. Civ. Code § 1798.199.70(b),(c).

[1414] Cal. Civ. Code § 1798.199.70(b): »defrauding the public of information to which it is entitled under this title« i. V. m. Cal. Civ. Code § 1798.130(a)(5).

[1415] Cal. Civ. Code § 1798.199.70(a).

[1416] Cal. Civ. Code § 1798.199.40(d).

[1417] Cal. Civ. Code § 1798.199.40(d).

[1418] Cal. Civ. Code § 1798.199.40(e).

[1419] Cal. Civ. Code § 1798.199.40(f).

[1420] Cal. Civ. Code § 1798.199.40(d).

[1421] Cal. Civ. Code § 1798.199.40(g).

[1422] *Botta*, PinG 2019, 261, 264, Fn. 54; *Hoeren/Pinelli*, MMR 2018, 711, 712, Fn. 7; *Lejeune*, ITRB 2021, 13, 16.

[1423] Sämtliche Verordnungen des Attorney General sind in 11 C. C. R. § 1–999.506 enthalten.

[1424] Cal. Const. art. VI § 6, Cal. Gov. Code § 68070. Der Attorney General ist als Ausprägung der *checks and balances* neben zwei Richter:innen Mitglied der Commission on Judicial

kalifornische Gesetze durchzusetzen.[1425] Er leitet die kalifornienweite Polizei und Staatsanwaltschaft und beaufsichtigt die District Attorneys sowie Sheriffs.[1426] Diese Vollzugsbehörden-Rolle ähnelt tatsächlich der eines Generalstaatsanwalts. Anders als dieser ist er jedoch nicht auf Strafrecht beschränkt, sondern setzt eine große Bandbreite verschiedener Gesetze durch. Dazu zählen insbesondere Kartellrecht sowie zahlreiche Verbraucher- und Datenschutzgesetze.[1427] Zudem ist er anders als ein Generalstaatsanwalt nicht in eine starre Verwaltungshierarchie eingebunden, sondern direkt vom Volk gewählt.[1428] Damit ist er unabhängig, muss sich aber für jede seiner Handlungen in der Öffentlichkeit rechtfertigen. Dies begünstigt Klagen gegen große Technologieunternehmen, mit denen sich der Attorney General als »Anwalt des Volkes« profilieren kann.[1429] Diese Tendenz zu öffentlichkeitswirksamen Klagen wird noch dadurch bestärkt, dass Attorney General häufig ein Durchgangsamt ist. Seit der Einführung des modernen Amts des Attorney General im Jahre 1934[1430] haben nahezu alle Amtsinhaber:innen später für das Gouverneursamt oder ein Amt auf Bundesebene kandidiert.[1431]

Die damalige Attorney General *Kamala Harris* – die jetzige U. S. Vizepräsidentin – hat 2012 erstmals eine Datenschutzabteilung eingerichtet. Diese war mit einem Jahresbudget von zunächst circa 1,5 Millionen Dollar ausgestattet und damit eher klein.[1432] Die Abteilung hat besondere Expertise für die IT-Branche entwickelt und hat bei staatenübergreifenden Kooperationen mit anderen Attorneys General häufig Verfahren gegen große Technologieunternehmen übernommen.[1433] Solche Kooperationen mehrerer Attorneys General können einen erheblichen Umfang erreichen und ergänzen die FTC auf Staatenebene.[1434] Attorney General

---

Appointments, die dem Gouverneur Richterernennungen vorschlägt, Cal. Const. art. VI § 7. Rechtsvergleichend zur Gerichtsverwaltung: *Michel*, Gerichtsverwaltung und Court Management in Deutschland und in den USA, S. 383–452.

[1425] Cal. Const. art. V § 13.

[1426] Cal. Const. art. V § 13.

[1427] Zur Durchsetzung anderer Datenschutzgesetze durch den Attorney General siehe Kapitel 2:B.II (ab S. 27).

[1428] Cal. Const. art. V § 11.

[1429] *Citron*, 92 Notre Dame L. Rev. 747, 803 f.

[1430] Proposition 4 (Cal. 1934).

[1431] Kandidaten für Gouverneurswahl (chronologisch): Earl Warren (gewählt; später Chief Justice am U. S. Supreme Court); Robert W. Kenny (nicht gewählt); Pat Brown (gewählt); Evelle J. Younger (nicht gewählt); George Deukmejian (gewählt); Dan Lungren (nicht gewählt); Bill Lockyer (nicht gewählt); Kerry Brown (gewählt).
Kandidaten für Amt auf Bundesebene: Thomas C. Lynch (Präsident; nicht gewählt), Kamala Harris (Vizepräsidentin; gewählt); Xavier Becerra (Bundesgesundheitsminister; ernannt).
Ernannt zum Cal. Supreme Court: Stanley Mosk.
Abgewählt: Frederick N. Howser.
Quelle: *Cal. Attorney General*, History of the Office of the Attorney General.

[1432] *Kemp*, California Privacy Protection Agency.

[1433] *Citron*, 92 Notre Dame L. Rev. 747, 786 f.

[1434] *Citron*, 92 Notre Dame L. Rev. 747, 758–795.

Becerra hat die Datenschutzabteilungen 2019 deutlich ausgebaut, um seine neue Rolle als Regulierungsbehörde mit Verordnungsermächtigung unter dem CCPA-2018 ausfüllen zu können (Jahresbudget: fünf Millionen Dollar).[1435] Nach Übergehen der Verordnungsermächtigung auf California Privacy Protection Agency im April 2022 kann der Attorney General aber weiterhin auf Verhängung einer *civil penalty* klagen.[1436]

b) Verhängung von civil penalties

C*ivil penalties* sind die typischen Verwaltungssanktionen in den Vereinigten Staaten.[1437] Der Attorney General klagt dabei vor einem kalifornischen Superior Court auf Festsetzung einer *civil penalty*.[1438] Das Gericht setzt daraufhin die Strafe im eigenen Ermessen fest.[1439] Warum wird diese Strafe im Zivilprozess verhängt? Der amerikanische Zivilprozess hat auch Sanktionsfunktion, wie der eng verwandte Strafschadensersatz zeigt.[1440] Die Rechtsprechung überlässt die Entscheidung, ob Geldstrafen im Zivil- oder Strafprozess verhängt werden sollen, nahezu vollständig dem Gesetzgeber (Freiheitsstrafen sind nur im Strafprozess möglich).[1441] Der Gesetzgeber wählt für Geldstrafen gegen juristische Personen typischerweise den Zivilprozess, weil dieser weniger umständlich ist als der Strafprozess.[1442] Der Strafprozess ist im Gegensatz zum Zivilprozess stark formalisiert, um Angeklagte zu schützen und Legitimität herzustellen.[1443] Das amerikanische Strafprozessrecht kennt insoweit mit dem deutschen Recht vergleichbare rechtsstaatliche Garantien wie die Selbstbelastungsfreiheit[1444] und den Zweifelsgrundsatz *(beyond a reasonable doubt).*[1445] Zusätzlich spielen die aufwendigen Jurys im amerikanischen Strafprozess eine größere Rolle als im Zivilprozess. Jury-Prozesse sind sehr aufwendig, da Juries für jeden Prozess neu zusammengestellt werden und das anschließende Verfahren langwieriger ist.[1446] Im Strafprozess entscheiden Berufsrichter:innen nur selten, da die Anforderungen an einen Verzicht auf eine

---

[1435] *Cal. Attorney General*, Budget Change Proposal, S. 2–4.

[1436] Cal. Civ. Code § 1798.199.90(a).

[1437] *Mann*, 101 Yale L. J. 1795, 1844; *Minzner*, 53 Wm. & Mary L. Rev. 853, 859 f.

[1438] Cal. Civ. Code § 1798.199.90(a).

[1439] Cal. Civ. Code § 1798.199.90(a).

[1440] U. S. Supreme Court vom 26.06.1989, *Browning-Ferris Indus. v. Kelco Disposal* – ablehnendes Sondervotum *O'Connor*, 492 U. S. 257, 287; *Mann*, 101 Yale L. J. 1795, 1867–1869.

[1441] Cal. Supreme Court vom 02.03.2015, *People v. Mosley*, 60 Cal. 4th 1044, 1063. Vgl. zur gleichlaufenden Rechtsprechung auf Bundesebene: U. S. Supreme Court vom 05.03.2002, *Smith v. Doe*, 538 U. S. 84, 92; *Mann*, 101 Yale L. J. 1795, 1814–1843.

[1442] *Mann*, 101 Yale L. J. 1795, 1844–1861; *Minzner*, 53 Wm. & Mary L. Rev. 853, 908–910.

[1443] *Mann*, 101 Yale L. J. 1795, 1853–1861.

[1444] U. S. Const. amend. V: »No person […] shall be compelled in any criminal case to be a witness against himself«.

[1445] Hergeleitet aus U. S. Const. amend. XIV § 1 durch: U. S. Supreme Court vom 04.01.1895, *Coffin v. United States*, 156 U. S. 432, 433; vom 31.03.1970, *In re Winship*, 397 U. S. 358, 362.

[1446] Cal. Civ. Proc. Code §§ 222–232, Cal. Pen. Code § 1046.

Jury deutlich höher sind.[1447] So urteilen im kalifornischen Strafprozess Jurys über ca. 64 % der Verbrechen und Vergehen, während Jurys nur ca. 3 % der Zivilverfahren entscheiden.[1448]

Die im Zivilverfahren verhängte *civil penalty* des CCPA ähnelt sowohl in Tatbestand als auch Höhe den Bußgeldern der California Privacy Protection Agency. Das Gericht kann *civil penalties* wegen jedes Verstoßes gegen den CCPA auf Klage des Attorney General hin verhängen.[1449] Die Höhe beträgt bis zu 2.500 $ pro Verletzungserfolg und bei Vorsatz oder bei einem Unter-16-Jährige betreffenden Verstoß bis zu 7.500 $ pro Verletzungserfolg.[1450] Das Gericht kann eine gute Zusammenarbeit mit dem Attorney General berücksichtigen, wobei eine *civil penalty* aber auch schon bei einem erstmaligen Verstoß möglich ist.[1451] Die *civil penalty* geht in den Consumer Privacy Fund ein[1452] und dient so auch der Kostenerstattung für den Attorney General und das Gericht.

Verglichen mit den Bußgeldern der California Privacy Protection Agency ist ein solches Verfahren immer noch aufwendiger, da zwingend ein Gerichtsverfahren durchgeführt werden muss.[1453] Zudem sind auch amerikanische Zivilprozesse mit typischerweise höheren Verfahrenskosten verbunden als in Europa.[1454] Allerdings erzeugt eine Gerichtsentscheidung erhöhte Legitimität und Aufmerksamkeit der Öffentlichkeit.[1455] Daher eignen sich *civil penalties* vor allem für öffentlichkeitswirksame, größere Verfahren.

Dies wirkt sich auch auf die Pläne des Attorney General aus. Er beabsichtigt, nur drei Klagen pro Jahr zu erheben.[1456] Dabei zielt er ersichtlich auf große Unternehmen ab. So erwartet er komplexe Ermittlungen, bei denen auf der Gegenseite einige der größten und erfahrensten Kanzleien stehen.[1457] Bisher hat er zwar nur Verwarnungen ausgesprochen und sich dabei auf eindeutige Verstöße wie fehlende Angaben in der Datenschutzerklärung konzentriert.[1458] Dies ist allerdings wohl dadurch bedingt, dass er durch das aufwendige Verordnungsgebungsverfahren

---

[1447] Cal. Const. I § 16 cl. 1, Cal. Civ. Proc. Code § 631(f).

[1448] *Judicial Council of California*, 2021 Court Statistics Report, S. 51, 54 f. Für geringfügige Gesetzesübertretungen (v.a. Verkehrsverstöße) kennt das kalifornische Recht noch die Kategorie der *infractions*, über die ausschließlich Berufsrichter:innen entscheiden, Cal. Pen. Code § 1042.5.

[1449] Cal. Civ. Code § 1798.199.90(a). Zur Auslegung des Wortlauts »for each violation« als »pro Verletzungserfolg« siehe Kapitel 3:E.I.2.e) (ab S. 191).

[1450] Cal. Civ. Code § 1798.199.90(a).

[1451] Unter dem CCPA-2018 konnten Unternehmen eine Sanktionierung durch Abhilfe binnen einer 30-tägigen Frist vermeiden, vgl. CCPA-2018, Sec. 3, § 1798.155(a).

[1452] Cal. Civ. Code § 1798.199.90(b). Zu diesem Siehe Kapitel 3:E.I.2.b) (ab S. 186).

[1453] Vgl. allgemein *Glicksman/Earnhart*, 26 Stan. Envtl. L. J. 317, 350.

[1454] *Cross*, 89 Va. L. Rev. 189, 196f; *Kagan*, Adversarial legalism: the American way of law, S. 104–109.

[1455] *Glicksman/Earnhart*, 26 Stan. Envtl. L. J. 317, 357.

[1456] *Cal. Attorney General*, Budget Change Proposal, S. 7.

[1457] *Cal. Attorney General*, Budget Change Proposal, S. 6 f.

[1458] *Becerra*, Testimony of Xavier Becerra, California Attorney General, S. 6; *Cal. Attorney*

für die erste Durchführungsverordnung ausgelastet war. Bei den ersten *civil penalties* ist ebenfalls zu erwarten, dass er sich auf eindeutige, gravierende Verstöße konzentrieren wird.[1459]

Der Attorney General soll eng mit der California Privacy Protection Agency zusammenarbeiten. Er stellt zu Beginn des Aufbaus der California Privacy Protection Agency dieser Personal, bis diese ihr eigenes angestellt hat,[1460] sodass eine enge personelle Verflechtung entsteht. So hat er z. B. bei dem Aufbau eines Personalverwaltungssystems unterstützt, Protokollkräfte gestellt und juristische Hilfstätigkeiten übernommen.[1461]

Zudem kann er Verfahren der California Privacy Protection Agency nach freiem Ermessen an sich ziehen.[1462] Dies wird besonders dann relevant sein, wenn er auch aus anderen Gesetzen wie z. B. dem Kartellrecht gegen dasselbe Unternehmen vorgeht. Wenn die California Privacy Protection Agency bereits ein Bußgeld verhängt hat, kann er aber nicht erneut wegen des gleichen Verstoßes klagen.[1463]

4. District und City Attorneys

Eine kleinere Rolle spielen District und City Attorneys. Diese sind das Äquivalent zu dem kalifornischen Attorney General auf *county*- und Stadt-Ebene. Föderalismus endet in den Vereinigten Staaten nicht auf Staatenebene. Kalifornien ist in 58 *counties* unterteilt. Die kleinsten *counties* entsprechen in etwa deutschen Landkreisen. Die größten *counties* hingegen verfügen über einen vergleichbar große Verwaltung wie deutsche Bundesländer. Die Verwaltung des größten kalifornischen *county* Los Angeles hat z. B. ein Jahresbudget von 36 Milliarden Dollar und ca. 110.000 Stellen,[1464] was in etwa der Verwaltung Niedersachsens entspricht.[1465] Dabei können die jeweiligen Bürger:innen des *county* eine Verwaltungsleitung wählen, die – von einzelnen Ausnahmen abgesehen – nicht Weisungen Kaliforniens unterworfen ist.

Eines der in jedem *county* direkt gewählten Ämter ist der oder die District Attorney.[1466] District Attorneys leiten die lokale Staatsanwaltschaft und vertreten den jeweiligen *county* vor Gericht.[1467] Daneben verfügen zumindest District

---

General, CCPA Enforcement Case Examples; *Mork/Baig/Garavaglia*, Consumer Privacy World, CCPA – 2020 Year in Review.

[1459] Ebenso *Snow* und *Hughes* in: *Kaminski et al.*, 54 Loy. L.A. L. Rev. 157, 195.

[1460] Cal. Civ. Code § 1798.199.95(c). Der Attorney General wird dafür nach dieser Norm auch entschädigt.

[1461] *Cal. Privacy Protection Agency*, Board Meeting October 18, 2021 Minutes, S. 3.

[1462] Cal. Civ. Code § 1798.199.90(c).

[1463] Cal. Civ. Code § 1798.199.90(d).

[1464] *County of Los Angeles Chief Executive Office*, Fiscal Year 2021–22 Recommended County Budget, S. 3.

[1465] *Niedersächsisches Finanzministerium*, Vorbericht zum Haushaltsplan für die Haushaltsjahre 2022 und 2023, S. 9: Gesamtausgaben 2022 von 36.653.749.000 €, S. 134: 142.200 Stellen.

[1466] Cal. Const. Art. XI § 1(b).

[1467] Cal. Gov. Code §§ 26500, 26520.

Attorneys größerer *counties* über eine Verbraucherschutzabteilung.[1468] Einige District Attorneys haben bereits vor dem CCPA eine Unterabteilung für Datenschutz eingerichtet und gegen Datenschutzverstöße geklagt.[1469]

District Attorneys können auf Basis der Generalklausel des Unfair Competition Laws auf die Verhängung einer *civil penalty* für jede Geschäftshandlung klagen, die »unlawful, unfair or fraudulent« ist.[1470] Die Höhe der *civil penalty* beträgt bis zu 2.500 $ pro Verletzungserfolg.[1471] Damit haben District Attorneys erheblichen Spielraum gegen eine geschäftliche Handlung in ihrem jeweiligen County vorzugehen, die »unlawful, unfair or fraudulent« ist.[1472]

Die Alternative *unlawful* ist bei einem Verstoß gegen ein anderes Gesetz des Bundes oder Kaliforniens erfüllt, wenn dieses das Unfair Competition Law nicht sperrt.[1473] Ein solches Gesetz ist auch der CCPA. Der CCPA-2018 hatte das Unfair Competition Law noch gesperrt.[1474] Diese Sperrklausel hat Proposition 24 allerdings entfernt.[1475] Dies ging auf eine Initiative von Verbraucherrechtsorganisationen zurück, die sich aus einer breiteren Streuung der Vollzugszuständigkeit eine wirksamere Durchsetzung erhoffen.[1476]

Weiterhin können aufgrund des Unfair Competition Law City Attorneys von Städten vorgehen, in denen über 750.000 Personen wohnen (derzeit: Los Angeles, San Diego, San Jose und San Francisco).[1477] Diese verfolgen sonst Vergehen und beraten die Stadt in allen Rechtsfragen.[1478] Auch die Verbraucherschutzabteilungen dieser City Attorneys sind bereits gegen Datenschutzverstöße vorgegangen.[1479]

Welche Rolle werden District und City Attorneys nach Inkrafttreten von Proposition 24 am 01.01.2023[1480] tatsächlich spielen? Wahrscheinlich eher eine kleine.

[1468] Zur historischen Entwicklung: *Reinholtsen*, 4 U.C. Davis L. Rev. 35, 44–45.

[1469] Z. B. derzeit laufendes Verfahren des San Francisco District Attorney: Cal. Superior Court San Francisco, *People v. Uber Technologies, Inc*, Case No. CGC-18-570124.

[1470] Cal. Bus. & Prof. Code §§ 17200, 17206.

[1471] Cal. Bus. & Prof. Code §§ 17206 Zur Auslegung als »pro Verletzungserfolg« siehe Kapitel 3:E.I.2.e) (ab S. 191)

[1472] Cal. Gov. Code § 41803.

[1473] Cal. Supreme Court vom 08.02.2018, *Solus Industrial Innovations, LLC v. Superior Court*, 4 Cal. 5th 316, 341. Umfassende Zusammenstellung: *Stroock*, California's Unfair Competition Law and Consumers Legal Remedies Act 2021 Annual Overview, S. 22–26.

[1474] CCPA-2018, Sec. 3 § 1798.155(a).

[1475] Vgl. CCPA-2018, Sec. 3, § 1798.155(a): »The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.« Dieser Satz wurde gestrichen durch Proposition 24 (Cal. 2020), Sec. 17 Cal. Civ. Code § 1798.155.

[1476] *American Civil Liberties Union of California et al.*, California Privacy Rights and Enforcement Act – Privacy Coalition Comments, S. 17 f.

[1477] Cal. Bus. & Prof. Code § 17206(a).

[1478] Cal. Gov. Code §§ 41801, 41803.

[1479] Z. B. derzeit laufendes Verfahren der San Diego City Attorney: Cal. Superior Court Orange County, *People v. Experian Data Corp.*, Case No. 30-2019-01047183.

[1480] Proposition 24 (Cal. 2020), Sec. 31(a).

Zwar ist Datenschutz durchaus auch in den Vereinigten Staaten populär.[1481] Allerdings haben District und City Attorneys keinen Anreiz, das Datenschutzrecht weiterzuentwickeln, und verfügen nur über begrenzte Mittel. Damit ist zu erwarten, dass sie nur vereinzelte, eindeutige Fälle nutzen werden, um sich zu profilieren. Auch so können sie aber Lücken im Vollzug der California Privacy Protection Agency und des Attorney General schließen.

5. Europäische Aufsichtsbehörden im Vergleich: Rechtssicherheit vor Effektivität

In Europa ist die Datenschutzaufsicht weniger zersplittert, sondern obliegt unabhängigen, spezialisierten Aufsichtsbehörden, die der California Privacy Protection Agency stark ähneln. Ebenso wie die California Privacy Protection Agency können diese Bußgelder verhängen (Art. 58 Abs. 2 lit. i, 83 DSGVO), sollen Öffentlichkeitsarbeit leisten (Art. 57 Abs. 1 lit. b DSGVO) und sind weitgehend vergleichbar unabhängig (Art. 52 DSGVO). Die europäischen Aufsichtsbehörden sind zwar insoweit unabhängiger, als im Gegensatz zur California Privacy Protection Agency eine ordentliche Kündigung ihrer Leitung ausgeschlossen ist (Art. 53 Abs. 4 DSGVO). Dies sollte allerdings nicht überbewertet werden, da für einen Widerruf der Mehrheit der Kommission mehrere unabhängig voneinander direkt gewählte Amtsinhaber:innen zusammenwirken müssten.[1482] Die Unabhängigkeit der California Privacy Protection Agency wird zudem dadurch gestärkt, dass sie über ein garantiertes Mindestbudget verfügt.[1483] Die DSGVO garantiert demgegenüber kein spezifisches Budget (Art. 52 Abs. 4 DSGVO), was bereits wiederholt zu Konflikten geführt hat.[1484] Das Budget für die California Privacy Protection Agency und die Datenschutzabteilung des Attorney General ist allerdings mit 0,33€ pro Kalifornier:in statt 0,56€ pro Unionsbürger:in leicht niedriger als bei den europäischen Aufsichtsbehörden (wobei letztere zusätzlich für den öffentlichen Sektor zuständig sind).[1485]

[1481] *Pew Research Center*, Americans and Privacy, S. 20.

[1482] Cal. Civ. Code § 1798.199.20, 1798.199.10. Siehe Kapitel 3:E.I.2.a) (ab S. 182).

[1483] Cal. Civ. Code § 1798.199.95.

[1484] Commission Staff Working Document: Accompanying the Document Communication from the Commission to the European Parliament and the Council: Data protection rules as a pillar of citizens empowerment and EUs approach to digital transition – two years of application of the General Data Protection Regulation, SWD/2020/115 final, Nr. 2.4; *LfD Niedersachsen*, Beschwerden zu Datenschutzverstößen und Komplexität von Verarbeitungsprozessen nehmen weiter zu; *Taylor*, The Irish Times, Data Protection Commission 'disappointed' at budget allocation.

[1485] *Europäische Kommission*, Commission Staff Working Document: two years of application of GDPR, SWD/2020/115 final, Annex II: Jährliches Gesamtbudget von 249.127.139 € (447.320.000 Einwohner:innen im Jahr 2020). Kalifornien gibt, wie gerade dargestellt, derzeit 10.000.000 $ für die California Privacy Protection Agency und 5.000.000 $ für die Datenschutzabteilung des Attorney General aus (39.538.223 Einwohner:innen im Jahr 2020).

Der wesentliche Unterschied zu den europäischen Aufsichtsbehörden ist deren fehlende Regelungskompetenz. Sie können zwar Stellungnahmen veröffentlichen, die als *soft law* die rechtswissenschaftliche Diskussion beeinflussen.[1486] So veröffentlicht insbesondere der Europäische Datenschutzausschuss Leitlinien, Empfehlungen und bewährte Verfahren (Art. 60 Abs. 1 lit. e–m DSGVO). Europäische Aufsichtsbehörden können jedoch keine allgemein verbindlichen Rechtsnormen wie die Durchführungsverordnung des CCPA erlassen. Ihre Stellungnahmen mögen zwar einen gewissen Einfluss haben, binden jedoch Gerichte nicht. Diese treffen vielmehr die letztendliche, verbindliche Entscheidung. Selbst deutsche Bundesgerichte entscheiden teilweise Datenschutzfragen, ohne die einschlägigen Stellungnahmen der Aufsichtsbehörden zu rezipieren.[1487] Damit hat die California Privacy Protection Agency eine wesentlich stärkere Rolle bei der Rechtsfortbildung, ist andererseits aber auch an eine umfassendes Verfahren der Öffentlichkeitsbeteiligung gekoppelt.

Weiterhin ist die California Privacy Protection Agency stärker an den Transparenzgrundsatz gebunden. Die Aufsichtsbehörden der DSGVO sollen zwar auch transparent handeln. Verpflichtend ist aber gemäß Art. 59 DSGVO nur ein jährlicher Tätigkeitsbericht. Weder die einzelnen Aufsichtsbehörden noch der Europäische Datenschutzausschuss tagen im Gegensatz zur California Privacy Protection Agency öffentlich.[1488] Während die California Privacy Protection Agency jeden ihrer Bußgeldbescheide veröffentlichen muss, dürfen dies zumindest deutsche Aufsichtsbehörden nur sehr eingeschränkt. Eine vollständige Veröffentlichung mit Namensnennung bedarf einer Rechtsgrundlage, die typischerweise nicht vorhanden ist.[1489] Vor Abschluss des Einspruchsverfahrens, das sich unter Umständen über Jahre erstrecken kann, ist eine Veröffentlichung generell

---

[1486] *Kibler*, Datenschutzaufsicht im europäischen Verbund, S. 207 f.

[1487] Vgl. BAG vom 23.08.2018 – 2 AZR 133/18, NZA 2018, 1329, Rn. 33: mehrmonatige Speicherfrist sei zulässig im Gegensatz zu den bereits damals vertretenen, aber nicht diskutierten maximal 72 Stunden der Aufsichtsbehörden, vgl. *Düsseldorfer Kreis*, Orientierungshilfe »Videoüberwachung durch nicht-öffentliche Stellen«, S. 11 f.; *DSK*, Kurzpapier Nr. 15: Videoüberwachung nach der Datenschutz-Grundverordnung, S. 2.
BGH vom 15.06.2021 – VI ZR 576/19, BeckRS 16831, Rn. 34–38: zum Recht auf Kopie, ohne eine einzige der zahlreichen, diesbezüglichen Stellungnahmen der Aufsichtsbehörden zu zitieren, vgl. *BfDI*, Arbeitshilfe Artikel 15 Jobcenter, S. 7; *LDI NRW*, 25. Datenschutzbericht 2019, S. 87; *LfD Bayern*, Orientierungshilfe Auskunft, Rn. 54–58; *LfD Niedersachsen*, 25. Tätigkeitsbericht 2019, S. 89; *LfDI Baden-Württemberg*, Tätigkeitsbericht Datenschutz 2019, S. 27; *SächsDSB*, Tätigkeitsbericht 2020, S. 101–105 *BayLDA*, Auskunft; *HBDI*, Tätigkeitsbericht 2018, S. 78; *LfDI Rheinland-Pfalz*, Tätigkeitsbericht zum Datenschutz 2019, S. 46 f.; *LfD Sachsen-Anhalt*, Tätigkeitsbericht 2019, S. 68; *LfDI Saarland*, 28. Tätigkeitsbericht Datenschutz 2019, S. 51f; *TLfDI*, Tätigkeitsbericht 2019, S. 32 f.

[1488] Kritisch zur fehlenden Öffentlichkeit: *Kibler*, Datenschutzaufsicht im europäischen Verbund, S. 406 f.

[1489] LG Hamburg vom 28.10.2021 – 625 Qs 22/21 OWi, *H&M*, BeckRS 2021, 38385 Rn. 33; *Hoeren*, ZD 2021, 497, 499 f. Vgl. OVG Münster vom 17.05.2021 – 13 B 331/21, juris Rn. 13–35 zur parallelen Situation bei der Bundesnetzagentur.

ausgeschlossen (§ 353d Nr. 3 Alt. 3 StGB). Auch über das bisher höchste Bußgeld unter der DSGVO von 746 Millionen Euro gegen Amazon[1490] ist kaum etwas bekannt, weil die luxemburgische Behörde nicht in identifizierbarer Weise über Bußgelder berichten darf.[1491] Damit zeigt sich der deutlich höhere Stellenwert der Transparenz im amerikanischen Recht.

Die Bußgeldkompetenz der Aufsichtsbehörden aus Art. 58 Abs. 2 lit. i, 83 DSGVO ähnelt eher den Bußgeldern der California Privacy Protection Agency als den *civil penalties,* da sie im Verwaltungsverfahren festgesetzt werden. Bei Art. 83 DSGVO ist wohl Verschulden erforderlich[1492] und in Deutschland strittig, ob eine der in § 30 Abs. 1 OWiG genannten Personen schuldhaft gehandelt haben muss.[1493] Beide Fragen hat das KG dem EuGH vorgelegt.[1494] Der CCPA ist pragmatischer, indem er auf ein Verschuldenserfordernis verzichtet. Insoweit sind die Bußgelder des CCPA weiter vom Strafverfahren entfernt als das deutsche Bußgeldrecht, das noch eng am Strafprozessrecht orientiert ist.

Die Bußgeldobergrenze wird zwar gem. Art. 83 Abs. 4–6 DSGVO nach dem weltweiten Jahresumsatz bestimmt. Der Umsatz wird jedoch bei Bußgeldern der California Privacy Protection Agency auch eine gewisse Rolle spielen – genauso wie er bei den *civil penalties* der District und City Attorneys explizit als Kriterium für die Sanktionshöhe genannt ist.[1495] Umgekehrt ist die Bußgeldobergrenze des CCPA (die Zahl der Verstöße und betroffenen Personen) auch gemäß Art. 83 Abs. 2 S. 2 lit. a DSGVO ein Teil der Kriterien für die Bußgeldzumessung der europäischen Aufsichtsbehörden. Die europäischen Aufsichtsbehörden bemessen Bußgelder nach einem Mischmodell, das die Schwere des Verstoßes (wie das Kriterium der Zahl der betroffenen Verbraucher:innen des CCPA) und den Umsatz des Verantwortlichen (wie die Bußgeldobergrenze des Art. 83 Abs. 4–6 DSGVO) als maßgebliche, gleichwertige Faktoren berücksichtigt.[1496]

[1490] *Bodoni*, Bloomberg, Amazon Gets Record $888 Million EU Fine Over Data Violations.

[1491] Art. 42 Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données [Gesetz vom 01.08.2018 über die nationale Datenschutzkommission].

[1492] *Frenzel* in: Paal/Pauly, DS-GVO Art. 83 Rn. 14: *Holländer* in: BeckOK DatenschutzR, DS-GVO Art. 83 Rn. 18; *Nietsch/Osmanovic*, BB 2021, 1858, 1861; a. A. *Bergt*, DuD 2017, 555, 558; *Sommer* in: Däubler et al., EU-DSGVO Art. 83 Rn. 12.

[1493] Für Anwendbarkeit des § 30 OWiG: LG Berlin vom 18.02.2021 – 526 OWi LG 212 Js-OWi 1/20 (1/20), *Deutsche Wohnen*, ZD 2021, 270, Rn. 13–28; *Bundesministerium des Innern, für Bau und Heimat*, Evaluierung BDSG, S. 61 f.; *Nietsch/Osmanovic*, BB 2021, 1858, 1860–1863; *Wybitul/Zhou* in: Taeger/Gabel, BDSG § 41 Rn. 9.
Dagegen: LG Bonn vom 11.11.2020 – 29 OWi 1/20, *1&1*, BeckRS 2020, 35663, Rn. 30–35; *DSK*, Entschließung Unternehmenshaftung, S. 1; *Bergt*, DuD 2017, 555, 558 f.; *Brodowski/Nowak* in: BeckOK DatenschutzR, BDSG § 41 Rn. 11–11.2; *Ehmann* in: Gola, BDSG § 41 Rn. 20; *Schaffland/Holthaus* in: Schaffland/Wiltfang, BDSG § 41 Rn. 1; *Sommer* in: Däubler et al., EU-DSGVO Art. 83 Rn. 12.

[1494] KG vom 06.12.2021 – 3 Ws 250/21, *Deutsche Wohnen*,BeckRS 2021, 39748, Fragen 1 f.

[1495] Cal. Bus. Prof. Code § 17206: »the court shall consider […] the defendant's assets, liabilities, and net worth.«.

[1496] *EDSA*, Guidelines 04/2022 Calculation of fines, Rn. 47–70.

Ein wesentlicher Unterschied zu den Aufsichtsbehörden des CCPA ist dagegen der *One-Stop-Shop*-Mechanismus und das damit verbundene Kohärenzverfahren der DSGVO. Statt gleichzeitiger Zuständigkeit vieler Aufsichtsbehörden dient eine federführende Aufsichtsbehörde als zentraler Ansprechpartner des Verantwortlichen (Art. 56 Abs. 1 DSGVO). Dies soll zu einer einheitlichen Rechtsanwendung führen.[1497]

Die herausgehobene Stellung der federführenden Aufsichtsbehörde ist bei grenzüberschreitenden Verfahren durch ein in Art. 63–67 DSGVO detailliert geregeltes Kohärenzverfahren eingeschränkt. Dieses leitet der Europäische Datenschutzausschuss (Art. 64 DSGVO), der auf Basis eines Entscheidungsentwurfs gemäß Art. 65 Abs. 1 S. 1 DSGVO für die beteiligten Aufsichtsbehörden verbindliche Entscheidungen treffen kann. Allerdings darf er die federführende Aufsichtsbehörde nicht zu neuen Sachverhaltsermittlungen verpflichten und muss deren Ermessensspielraum berücksichtigen.[1498] Auch kann die federführende Aufsichtsbehörde ein Verfahren dadurch faktisch blockieren, dass sie »endlose« Ermittlungen anstellt, ohne einen Entscheidungsentwurf gemäß Art. 60 Abs. 3 S. 2 DSGVO zu übermitteln.[1499] Die federführende Aufsichtsbehörde unterliegt häufig Interessenkonflikten, da sie aufgrund des Sitzes der Hauptverwaltung bestimmt wird (Art. 56 Abs. 1 S. 1 DSGVO).[1500] Am Sitz der Hauptverwaltung entrichtet der Verantwortliche auch Steuern, schafft Arbeitsplätze und stärkt so die lokale Wirtschaft.[1501] Dies erzeugt einen mittelbaren Einfluss auf die jeweilige Aufsichtsbehörde, die ihr Budget steigern und politisches Kapital durch populäre Entscheidungen erwerben will.[1502] Bisher sind nur 24[1503] der insgesamt circa 2000 Bußgelder[1504] nach dem *One-Stop-Shop*-Verfahren ergangen. Damit herrscht gerade bei den besonders bedeutsamen grenzüberschreitenden Fällen ein erhebliches Vollzugsdefizit.[1505]

Dagegen zeigen der CCPA und seine Vorläufer, dass eine gleichzeitige Zuständigkeit keine besondere Rechtsunsicherheit bedeuten muss. So sind zwar der

---

[1497] Generalanwalt *Bobek*, Schlussanträge vom 13.06.2021 – C645/19, *Facebook Ireland ./. Gegevensbeschermingsautoriteit* Rn. 75–80; *Europäische Kommission*, Data Protection Day 2014: Full Speed on EU Data Protection Reform, 3; *Dix* in: Kühling/Buchner, DS-GVO Art. 56 Rn. 1; *Kibler*, Datenschutzaufsicht im europäischen Verbund, S. 193; *Selmayr* in: Ehmann/Selmayr, DS-GVO Art. 56 Rn. 2.

[1498] *EDSA*, Beschluss 01/2020 Twitter, Rn. 131–135; *Thiel*, ZD 2021, 467, 470; *Weber/Dehnert*, ZD 2021, 63, 65 f.

[1499] *Caspar*, vorgänge 231/232 (2020), 99, 107; *Dix*, vorgänge 231/232 (2020), 87, 92 f; *Thiel*, ZD 2021, 467, 469. Deswegen ein Vertragsverletzungsverfahren gegen Irland fordernd: *Europäisches Parlament*, Resolution of 20 May 2021 on Schrems II Rn. 4.

[1500] *Caspar*, vorgänge 231/232 (2020), 99, 109.

[1501] *Caspar*, vorgänge 231/232 (2020), 99, 109.

[1502] *Caspar*, vorgänge 231/232 (2020), 99, 109.

[1503] *EDSA*, Final One Stop Shop Decisions.

[1504] *DSGVO-Portal*, DSGVO Bußgeld Datenbank.

[1505] *Caspar*, vorgänge 231/232 (2020), 99, 109.

kalifornische Attorney General und die California Privacy Protection Agency gleichzeitig für alle kalifornischen Unternehmen zuständig, stimmen sich jedoch informell ab, sodass keine uneinheitliche Rechtsanwendung droht. Auch der Vollzug anderer Datenschutzgesetze durch verschiedene einzelstaatliche Attorneys General führt ersichtlich nicht zu erheblichen Widersprüchen. Vielmehr stimmen sich diese umfangreich ab, um ihre knappen Ressourcen zu schonen.[1506]

Bezeichnenderweise wird in Europa als Alternative zum ungenügenden *One-Stop-Shop*-Mechanismus gerade nicht dessen naheliegende Streichung diskutiert. Vielmehr wird eine weitere Vereinheitlichung vorgeschlagen: entweder durch Stärkung des Kohärenzverfahrens[1507] oder durch eine zentrale europäische Aufsichtsbehörde.[1508] Dabei ist die Gefahr unterschiedlicher materieller Anforderungen zwischen den Aufsichtsbehörden tatsächlich gering, da diese ein europaweit einheitliches Datenschutzrecht durchsetzen.[1509] Auch stimmen sich die Aufsichtsbehörden eingehend im Europäischen Datenschutzausschuss inhaltlich ab, der inzwischen über 80 Leitlinien und Empfehlungen verabschiedet hat.[1510] Auch ist angesichts der knappen Ressourcen der europäischen Aufsichtsbehörden kaum zu befürchten, dass willkürlich anhand minimaler Verstöße gegen Verantwortliche und Auftragsverarbeitern aus anderen Mitgliedstaaten vorgehen. Wahrscheinlicher ist vielmehr, dass sie sich ohne das *One-Stop-Shop*-Verfahren weiterhin informell abstimmen, wie dies auch die Attorneys General der U. S. Bundesstaaten selbst ohne einheitliches Datenschutzrecht höchst erfolgreich tun.[1511] Trotz der geringen Nachteile spielt die ersatzlose Streichung des *One-Stop-Shop*-Mechanismus in der europäischen Diskussion aber kaum eine Rolle. Damit priorisiert Europa Rechtssicherheit vor Rechtsdurchsetzung.

II. Begrenztes Privatklagerecht bei Datenpannen

1. Sammelklagen wegen Datenpannen vor dem CCPA

Sammelklagen ermöglichen es, sowohl geringe Schäden effizient zu kompensieren als auch das Recht wirkmächtig durchzusetzen. Potenzielle Kläger:innen müssen über eine Sammelklage vor Bundesgerichten nur informiert werden, was auch durch öffentliche Bekanntmachung erfolgen kann.[1512] Falls die potenziellen Kläger:innen nicht in der gesetzten Frist widersprechen, sind sie Prozessparteien

---

[1506] *Citron*, 92 Notre Dame L. Rev. 747, 790 f.

[1507] *Dix*, vorgänge 231/232 (2020), 87, 93f; *Weber/Dehnert*, ZD 2021, 63, 68.

[1508] *Caspar*, vorgänge 231/232 (2020), 99, 113; *Kelber* in: *Neuerer*, Handelsblatt, Datenschützer Ulrich Kelber bringt neue EU-Behörde ins Spiel; *Weichert*, Überlegungen Evaluation DSGVO, S. 8; *Wiewiórowski* in: *Manacourt*, Politico, EU privacy chief bashes lack of GDPR enforcement against Big Tech.

[1509] Zu den begrenzten Öffnungsklauseln siehe Kapitel 3:B.IV.2 (ab S. 76).

[1510] *EDSA*, DSGVO: Leitlinien, Empfehlungen, bewährte Verfahren.

[1511] Zur informellen Entwicklung unter der DSRL: *Dix* in: Kühling/Buchner, DS-GVO Art. 56 Rn. 2.

[1512] Fed. R. Civ. P. 23(c)(2) a. A.

und an das Urteil gebunden (*opt-out*).[1513] Erfolgshonorare bieten Klägerkanzleien zudem einen Anreiz, auch Fälle von finanzschwachen Parteien anzunehmen.[1514] Die *discovery* ermöglicht, durch umfangreiche Vorlagepflichten hinter den Schleier großer Organisationen zu blicken.[1515] Kläger:innen haben schließlich ein geringeres Kostenrisiko, da in der Regel jede Partei ihre eigene Kosten trägt.[1516] Bürger:innen können sich in diesem Umfeld gegen mächtige Unternehmen verbünden und mit einer Sammelklage erhebliche Summen erstreiten.[1517]

Dementsprechend gab es schon vor Inkrafttreten des CCPA zahlreiche Sammelklagen nach Datenpannen.[1518] Datenpannen verursachen typischerweise nur geringe individuelle Schäden, dies aber bei vielen Personen.[1519] Diese typischerweise gleichartigen[1520] Schäden können Sammelklagen bündeln, die teilweise höchst erfolgreich waren und Schadensersatz in dreistelliger Millionenhöhe erreicht haben.[1521] Dabei haben sich solche Sammelklagen bisher vor allem auf das Deliktsrecht gestützt und wurden in erster Linie vor Bundesgerichten verhandelt.[1522] Zwar erheben nur bei 4–6 % der Datenpannen Betroffene eine Sammelklage.[1523] Dies sind aber vor allem die »großen« Fälle, in denen besonders viele Individuen betroffen sind.[1524]

Häufig haben Gerichte jedoch einen Schaden abgelehnt, weil die Kläger:innen bereits kein *standing* (Klagebefugnis) hätten. Dieses *standing* ist eine verfassungsrechtlich vorgegebene Zulässigkeitsvoraussetzung für jede Klage vor Bundesgerichten.[1525] Kläger:innen müssen eine bereits eingetretene oder unmittelbar bevorstehende Rechtsgutsverletzung plausibel darlegen (*injury in fact),* welche die jeweiligen Beklagten verursachen und die das Gericht beseitigen

---

[1513] Fed. R. Civ. P. 23(c)(2)(B)(v),(c)(3).

[1514] *Hagan*, 2019 Colum. Bus. L. Rev. 735, 748; *Kagan*, Adversarial legalism: the American way of law, S. 101.

[1515] *Discovery* bedeutet das umfassende Suchen nach Beweisen bei der Gegenpartei. Vgl. zu funktionalen Äquivalenten im deutschen Recht: *Kischel*, Rechtsvergleichung, § 1 Rn. 15.

[1516] *Kagan*, Adversarial legalism: the American way of law, S. 101.

[1517] *Kagan*, Adversarial legalism: the American way of law, S. 101; *Robinson*, 26 Rich. J.L. & Tech. 1, 53–56.

[1518] Vgl. die statistischen Auswertungen in: *Romanosky/Hoffman/Acquisti*, 11 Empirical Legal Stud. 74–104; *Valdetero/Zetoony/Maciejewski*, Data Breach Litigation Report: 2019 Edition, passim.

[1519] Vgl. *Cal. Attorney General*, California Data Breach Report 2016, S. 10.

[1520] Bei zu großen Sachverhaltsunterschieden scheidet eine Sammelklage aus, Fed. R. Civ. P. 23(b)(3).

[1521] Die bisher höchste Schadensersatzsumme war 380.500.000 $: U. S. District Court N. D. Ga. vom 17.03.2020, *In re Equifax Customer Data Sec. Breach Litig.*, 2020 U. S. Dist. LEXIS 118209, 150.

[1522] *Valdetero/Zetoony/Maciejewski*, Data Breach Litigation Report: 2019 Edition, S. 11.

[1523] *Valdetero/Zetoony/Maciejewski*, Data Breach Litigation Report: 2019 Edition, S. 4 f.

[1524] *Romanosky/Hoffman/Acquisti*, 11 Empirical Legal Stud. 74, 86.

[1525] Hergeleitet aus U. S. Const. Art. III § 2 cl. 1, zuletzt: U. S. Supreme Court vom 25.06.2021, *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2197 f.

oder kompensieren kann.[1526] Gerichte waren bisher zurückhaltend, eine *injury in fact* für Datenpannen anzunehmen. Bezifferbare Schäden bei Datenpannen festzustellen, ist schwierig, da sich die Spur der persönlichen Informationen in der Regel nach der Datenpanne verliert.[1527] Einigkeit besteht nur insoweit, dass tatsächlicher Identitätsdiebstahl eine *injury in fact* darstellt.[1528] Ob das Identitätsdiebstahls-Risiko oder durch das Risiko ausgelöstes seelisches Leid ausreichen, ist dagegen hoch umstritten.[1529] So gehen der 2nd, 3rd, 4th und 11th Circuit U. S. Court Appeals davon aus, dass solche Beeinträchtigungen noch keine *injury in fact* darstellt;[1530] der 6th, 7th, 9th und der D.C. Circuit vertreten die Gegenansicht.[1531] Unterschiede in den zugrunde liegenden Fällen können die Divergenz nur in begrenztem Maß erklären: zwar nehmen Gerichte bei sensibleren Daten eher eine *injury in fact* an, befolgen dies aber auch nicht konsequent.[1532] Der U. S. Supreme Court hat sich bisher noch nicht abschließend dazu geäußert.[1533] Daher herrscht erhebliche Rechtsunsicherheit.[1534]

[1526] U. S. Supreme Court vom 26.03.2013, *Clapper v. Amnesty Int'l USA*, 568 U. S. 398, 409; vom 16.06.2015, *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548; vom 25.06.2021, *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2203.

[1527] *Marcus*, 68 Duke L. J. 555, 567.

[1528] U. S. Court of Appeals 3rd Circuit vom 12.12.2011, *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42; U. S. Court of Appeals D.C. Circuit vom 01.08.2017, *Attias v. CareFirst, Inc.*, 865 F.3d 620, 627: »Nobody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury«.

[1529] *Haley*, 95 Wash. L. Rev. 1193, 1199–1244 mit einer statistischen Auswertung der diesbezüglichen Rechtsprechung.

[1530] U. S. Court of Appeals 2nd Circuit vom 02.05.2017, *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 90; U. S. Court of Appeals 3rd Circuit vom 12. Dezember 2011, *Reilly v. Ceridian Corp.*, 664 F.3d 38, 45; U. S. Court of Appeals 4th Circuit vom 06.02.2017, *Beck v. McDonald*, 848 F.3d 262, 271–277; U. S. Court of Appeals 8th Circuit vom 30.08.2017, *In re SuperValu, Inc., Customer Data Sec. Breach Litig.*, 870 F.3d 763, 767–774; U. S. Court of Appeals 11th Circuit vom 28.10.2020, *Muransky v. Godiva Chocolatier, Inc.*, 2020 U. S. App. LEXIS 33995, 12–40.

[1531] U. S. Court of Appeals D.C. Circuit vom 01.08.2017, *Attias v. CareFirst, Inc.*, 865 F.3d 620, 625–629; vom 21.06.2019, *In re United States OPM Data Sec. Breach Litig.*, 928 F.3d 42, 54–61; U. S. Court of Appeals 6th Circuit vom 12.09.2016, *Galaria v. Nationwide Mut. Ins. Co.*, 663 Fed. Appx. 384, 387–391; U. S. Court of Appeals 7th Circuit vom 11.04.2018, *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828; U. S. Court of Appeals 9th Circuit vom 05.12.2017, *In re Zappos.com, Inc.*, 888 F.3d 1020, 1023–1030.

[1532] *Urness*, 73 Vand. L. Rev. 1517, 1532.

[1533] In *Spokeo* hat er nur festgestellt, dass immaterielle Schäden bei Datenpannen an sich *injury in fact* sein können, aber nicht eingegrenzt, welche: U. S. Supreme Court vom 16.06.2015, *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540.
In *Transunion* diskutiert er zwar ein datenschutzrechtliches Problem (Richtigkeit einer Kreditauskunft), aber keine Datenpannen: U. S. Supreme Court vom 25.06.2021, *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190.

[1534] *Haley*, 95 Wash. L. Rev. 1193, 1230; *Nastasi*, 38 Cardozo Arts & Ent. L. J. 257, 278; *Solove/Citron*, 96 Tex. L. Rev. 737, 743; *Urness*, 73 Vand. L. Rev. 1517, 1559. U. S. Court of Appeals 9th Circuit vom 15.08.2017, *Robins v. Spokeo, Inc.*, 867 F.3d 1108, 1112 nennt dies treffend eine »somewhat murky area«.

Die Kodifizierung eines Privatklagerechts für Datenpannen konkretisiert die Anforderungen an die *injury in fact*. Zwar kann auch der einfache Gesetzgeber nicht ein Popularklagerecht entgegen der U. S. Constitution schaffen.[1535] Auch können Kläger:innen nach dem U. S. Supreme Court ein gesetzlich geregeltes Privatklagerecht nicht zum Anlass nehmen, eine bloße Ordnungsvorschrift durchzusetzen, ohne selbst betroffen zu sein.[1536] Die Legislative dürfe nicht die Exekutive umgehen, indem sie beliebigen Dritten ein Privatklagerecht einräumt.[1537] Insoweit ist der heutige, konservative U. S. Supreme Court wesentlich skeptischer gegenüber privater Rechtsdurchsetzung, als es dem deutschen Bild grenzenlos zulässiger Sammelklagen in den Vereinigten Staaten entspricht.[1538] Die Entscheidung des Gesetzgebers, ein Privatklagerecht für ein tatsächlich existierendes Individualinteresse zu schaffen, respektiert der U. S. Supreme Court aber grundsätzlich.[1539] Das gesetzlich neu geschützte Interesse muss dabei in engem Zusammenhang mit den Individualinteressen stehen, die amerikanische und englische Gerichte traditionell als Klagegründe akzeptiert hatten.[1540] Eine exakte Entsprechung in der amerikanischen Rechtstradition ist nicht erforderlich, allerdings dürfen Untergerichte auch nicht nebulös abstellen auf moderne, sich entwickelnde Ansichten darüber, welche Arten von Klagen vor Bundesgerichten verhandelt werden sollten.[1541] Dieser konservative Maßstab mag aus deutscher Sicht unverständlich klingen, ist aber im Rahmen des *common laws* durchaus konsequent: auch der Gesetzgeber darf bei der ihm gestatteten Rechtsfortbildung nicht den Rahmen des über Jahrhunderte geschaffenen traditionellen Richterrechts verlassen.

Der Schutz vor Kontrollverlust der Datenpannen-Opfer hält sich aber durchaus im bisher entwickelten Rahmen rechtlich geschützter Individualinteressen.

[1535] U. S. Supreme Court vom 03.03.2009, *Summers v. Earth Island Institute*, 555 U. S. 488, 497; vom 16.06.2015, *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 f.

[1536] U. S. Supreme Court vom 12.06.1992, *Lujan v. Defenders of Wildlife*, 504 U. S. 555, 572 Fn. 7; vom 16.06.2015, *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549; vom 25.06.2021, *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204–2207; a. A. (faktisches Leerlaufen gesetzlicher Rechte): U. S. Supreme Court vom 25.06.2021, *TransUnion LLC v. Ramirez* – ablehnendes Sondervotum *Thomas*, 141 S. Ct. 2190, 2219–2221, ablehnendes Sondervotum *Kagan*, 141 S. Ct. 2190, 2225; *Solove/Citron*, 101 B. U. L. Rev. Online 62, 69–71.

[1537] U. S. Supreme Court vom 25.06.2021, *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2207: »the choice of how to prioritize and how aggressively to pursue legal actions against defendants who violate the law falls within the discretion of the Executive Branch, not within the purview of private plaintiffs«.

[1538] *Stadler*, ZHR 2018, 623, 638 f. Umfassend zur inzwischen sehr sammelklagenskeptischen Rechtsprechung des U. S. Supreme Court: *Burbank/Farhang*, 165 U. Pa. L. Rev. 1495, 1517–1530.

[1539] U. S. Supreme Court vom 16.06.2015, *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549; vom 25.06.2021, *Transunion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 f.

[1540] U. S. Supreme Court vom 16.06.2015, *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549; U. S. Supreme Court vom 25.06.2021, *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204.

[1541] U. S. Supreme Court vom 25.06.2021, *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204.

Es ähnelt den deliktsrechtlich anerkannten immateriellen Schäden wegen Privatsphäreverletzungen, die auch gerade die Veröffentlichung privater Informationen erfassen (*public disclosure of private facts*).[1542] Deshalb haben Kläger:innen wohl *standing,* soweit sie den Datenpannen–Schadensersatztatbestand des CCPA erfüllen.[1543]

2. Regelung

a) Tatbestand

Der Tatbestand setzt eine Datenpanne voraus, in der bestimmte, einen Identitätsdiebstahl ermöglichende persönliche Informationen abhanden gekommen sind, und die auf eine unzureichende Sicherheit des Unternehmens zurückzuführen ist.[1544]

Eine Datenpanne ist dabei jeder unberechtigte Zugriff auf persönliche Informationen, der mit einem Diebstahl, einer Exfiltration oder einer Offenlegung verbunden ist.[1545] Diebstahl, Exfiltration oder Offenlegung können dabei sowohl Folge als auch Auslöser des unberechtigten Zugriffs sein. Daher sind neben dem klassischen Cyberangriff auch Fälle erfasst, in denen Unternehmen die persönlichen Informationen versehentlich im Internet offenlegen, sodass Dritte danach unberechtigt zugreifen.[1546] Die Datenpanne muss nach Inkrafttreten des CCPA-2018 am 01.01.2020 geschehen sein, da der CCPA nicht rückwirkend anwendbar ist.[1547]

Der unberechtigte Zugriff muss sich zudem auf risikoreiche persönliche Informationen beziehen, die einen Identitätsdiebstahl ermöglichen.[1548] Diese persönlichen Informationen »sind dieselben, wegen der Unternehmen nach kalifornischem Recht eine Datenpanne melden müssen:[1549]

»(A) An individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

[1542] *Nastasi*, 38 Cardozo Arts & Ent. L. J. 257, 263, 270 f. Zum deliktsrechtlichen Schutz des Persönlichkeitsrechts siehe Kapitel 2:B.I.1 (ab S. 17).

[1543] U. S. District Court N.D. Cal. vom 25.07.2022, *Wynne v. Audi of Am.*, 2022 U. S. Dist. LEXIS 131625, 10–14; *Determann*, ZD 2018, 443, 446; *Harris*, 54 Loy. L.A. L. Rev. 197, 227; *Nastasi*, 38 Cardozo Arts & Ent. L. J. 257, 263; wohl auch: U. S. District Court S. D. Cal. vom 19.11.2020, *Stasi v. Inmediata Health Group Corp.*, 501 F. Supp. 3d 898, 904.

[1544] Cal. Civ. Code § 1798.150(a)(1).

[1545] Cal. Civ. Code § 1798.150(a)(1).

[1546] U. S. District Court S. D. Cal. vom 19.11.2020, *Stasi v. Inmediata Health Group Corp.*, 2020 U. S. Dist. LEXIS 217097, 47–49.

[1547] U. S. District Court N. D. Cal. vom 05.03.2021, *Gardiner v. Walmart Inc.*, 2021 U. S. Dist. LEXIS 75079, 4–6; U. S. District Court S. D. Cal vom 12.08.2021, *In re Blackbaud, Inc.*, 2021 U. S. Dist. LEXIS 151831, 13; *Yannella*, Cyber Litigation, § 9:11.

[1548] Cal. Civ. Code § 1798.150(a)(1).

[1549] Cal. Civ. Code § 1798.150(a)(1) i. V. m. Cal. Civ. Code § 1798.81.5(d)(1).

(i) Social security number.
(ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.
(iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
(iv) Medical information.[1550]
(v) Health insurance information.[1551]
(vi) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.
(vii) Genetic data.[1552]
(B) A username or email address in combination with a password or security question and answer that would permit access to an online account.«[1553]

Die Auswahl dieser Informationen orientiert sich vor allem daran, Identitätsdiebstahl zu verhindern. Die unter (A) aufgeführten Informationen ermöglichen Identitätsdiebstahl in der analogen Welt, die Informationen unter (B) in der digitalen Welt. Dies trifft nur auf die Kategorien »Medical information«, »Health insurance information« und »Genetic data« nicht zu, die aber eine begrenzte Bedeutung haben, da für die Medizinbranche der vorrangige HIPAA und der kalifornische Confidentiality of Medical Information Act den CCPA verdrängen.[1554] Identitätsdiebstahl ist das wesentliche Risiko, das in den Vereinigten Staaten aufgrund einer Datenpanne befürchtet wird.[1555] Die Einschränkung auf risikoreiche Informationen soll verhindern, dass die erheblichen Schadensersatzpauschalen des CCPA auch für »belanglose« persönliche Informationen verlangt werden können. Daher sind auch persönliche Informationen explizit ausgenommen, wenn sie wirksam verschlüsselt oder geschwärzt sind.[1556] Die Informationen ähneln denjenigem Teilbereich der Definition sensibler Informationen, die Identitätsdiebstahl ermöglichen.[1557] Allerdings fehlt der Teilbereich höchstpersönlicher Informationen weitgehend (unter anderem sexuelle Orientierung, ethnische Herkunft, Religion und Gewerkschaftsangehörigkeit), wohl weil das Privatklagerecht vor allem auf das Identitätsdiebstahl-Risiko abzielt.

[1550] Legaldefinition: Cal. Civ. Code § 1798.81.5(d)(2).

[1551] Legaldefinition: Cal. Civ. Code § 1798.81.5(d)(3).

[1552] Legaldefinition: Cal. Civ. Code § 1798.81.5(d)(5). Diese Kategorie wurde erst im Oktober 2021 hinzugefügt durch A. B. 825, 2021–22 Leg., Reg. Sess. (Cal. 2021), Cal. Stats. 2021 ch. 527, Sec. 2.

[1553] Deklaratorisch in Cal. Civ. Code § 1798.150(a)(1) wiederholt.

[1554] Cal. Civ. Code § 1798.145(c)(1)(A). Zum HIPAA selbst siehe Kapitel 2:B.I.2 (ab S. 19). und zu dessen vorrangiger Geltung siehe Kapitel 3:B.IV.2 (ab S. 76).

[1555] *Solove/Citron*, 96 Tex. L. Rev. 737, 756 f.

[1556] Cal. Civ. Code §§ 1798.150(a)(1), 1798.81.5(d)(1)(A).

[1557] Cal. Civ. Code §§ 1798.140(ae)(1)(A),(B). Siehe Kapitel 3:C.II.1.a) (ab S. 109).

Die Datenpanne muss zudem darauf zurückzuführen sein, dass das Unternehmen keine angemessene Sicherheit gewährleistet hat.[1558] Der Maßstab der angemessenen Sicherheit ist genauso wie in der Datensicherheitspflicht des CCPA formuliert und daher wohl einheitlich auszulegen.[1559] Er ist zwar etwas unscharf.[1560] Es lässt sich jedoch in der Rückschau auf einen konkreten unberechtigten Zugriff leichter feststellen, ob die Datensicherheit angemessen war. Auch haben Beklagte bei bisherigen Datenpannen-Sammelklagen selten bestritten, dass ihre Datensicherheit unzureichend war.[1561]

Schließlich müssen Kläger:innen vor einer Klage dem Unternehmen eine 30-tägige Abhilfefrist einräumen.[1562] Bloß nachträglich die Datensicherheit zu verbessern, genügt aber ausdrücklich nicht.[1563] Die Frist lösen Kläger:innen dadurch aus, dass sie das Unternehmen schriftlich auf die behauptete Datenpanne hinweisen und dabei die Schadensersatzvorschrift des CCPA (Cal. Civ. Code § 1798.150) nennen.[1564] Danach hat das Unternehmen 30 Tage Zeit, die Datenpanne zu beheben, den Verbraucher:innen die Behebung mitzuteilen und eine Unterlassungserklärung abzugeben.[1565] Nach einer solchen Behebung können die Verbraucher:innen nur noch ihre Auslagen verlangen, aber nicht mehr die Schadensersatzpauschale (außer wenn das Unternehmen gegen die Unterlassungserklärung verstößt).[1566]

Wann ist eine Datenpanne aber behoben? »Gestohlene« persönliche Informationen lassen sich wegen ihrer Flüchtigkeit nur selten nachverfolgen. Es mag Grenzfälle geben, in denen eine konkret bekannte Person persönliche Informationen unberechtigt erhalten hat (z. B. bei einem fehladressiertem Brief), aber die Löschung glaubwürdig versichert. Meist ist aber nicht einmal erkennbar, wer auf persönliche Informationen unberechtigt zugegriffen hat.[1567] Eine Naturalrestitution dürfte daher in den meisten Fällen ausscheiden.[1568] Unklar ist, ob in solchen Fällen eine Kompensation in Geld als Abhilfe genügt.

[1558] Cal. Civ. Code § 1798.150(a)(1).

[1559] Cal. Civ. Code § 1798.100(e). Zur einheitlichen Auslegung von Begriffen siehe Kapitel 3:B.II.2.b) (ab S. 58).

[1560] *Ballon*, E-commerce & Internet law. S. 26-426; *Kress/Trifon*, JD Supra, CCPA's Private Right of Action.

[1561] *Solove/Citron*, 96 Tex. L. Rev. 737, 739.

[1562] Cal. Civ. Code § 1798.150(b).

[1563] Cal. Civ. Code § 1798.150(b). Dieser durch Proposition 24 eingeführte Satz ist eine Reaktion auf eine entsprechende Auslegung des CCPA-2018, vgl. *Californians for Consumer Privacy*, Annotated Text of the CPRA, § 1798.150(b). Diese war aber ohnehin nur eine Mindermeinung, vgl. *Silvers et al.*, Reducing Risk of Litigation under the CCPA.

[1564] Cal. Civ. Code § 1798.150(b).

[1565] Cal. Civ. Code § 1798.150(b).

[1566] Cal. Civ. Code § 1798.150(b).

[1567] *Cal. Attorney General*, California Data Breach Report 2016, S. 11–13: die meisten Datenpannen seien Hackerangriffe.

[1568] *Ballon*, E-commerce & Internet law. S. 26-426; *Hyman/Walser-Jolly/Farrell*, 73 Quarterly Report 173, 181; *Kosseff*, Technology & Marketing Law Blog, Ten Reasons.

Aufschlussreich ist dazu die extensive Rechtsprechung zur Parallelnorm im kalifornischen Consumer Legal Remedies Act. Dieses Verbraucherschutzgesetz setzt vor einer Klage ebenfalls voraus, dass Verbraucher:innen eine 30-tägige Abhilfefrist einräumen.[1569] Hierzu ist anerkannt, dass eine Kompensation in Geld ausreichende Abhilfe schaffen kann, soweit sie in einer Gesamtbetrachtung aller Umstände angemessen ist.[1570] Ob sich das übertragen lässt, ist noch offen.[1571] Jedenfalls müsste sich die Kompensation in Geld an der Höhe der Schadensersatzpauschale orientieren.[1572]

b) Schadensersatzhöhe

Die Schadensersatzpauschale beträgt 100 bis 750 $ pro Verbraucher oder Verbraucherin sowie pro Datenpanne.[1573] Dies mag *prima facie* gering erscheinen, erreicht aber multipliziert mit den typischerweise zahlreichen Betroffenen bei Datenpannen erhebliche Gesamtsummen.[1574] Die Kriterien für die Höhe tragen deutliche Züge eines Strafschadensersatzes. Bei der Festlegung der Höhe soll das Gericht das Vermögen des Unternehmens berücksichtigen.[1575] Weitere Faktoren sind das Gewicht, Art, Verschulden und Dauer des Fehlverhaltens des Unternehmens.[1576] Aber auch alle anderen Umstände der Datenpanne kann das Gericht in einer Gesamtbetrachtung bei der Festlegung der Schadensersatzpauschale würdigen.[1577] Diese Kriterien sind den Strafzumessungsvorschriften des kalifornischen Unfair Competition Law entnommen.[1578]

[1569] Cal. Civ. Code § 1782(a). Der Wortlaut spricht dieser Norm spricht zwar von »correct, repair, replace, or otherwise rectify« statt »cure« wie der CCPA. Gerichte verwenden aber »cure« als Obergriff »correct, repair, replace, or otherwise rectify« i.S.d. Cal. Civ. Code § 1782(a): U. S. District Court C. D. Cal. vom 10.09.2018, *Arechiga v. Ford Motor Co.*, 2018 U. S. Dist. LEXIS 237329, 4–6.

[1570] Cal. Court of Appeal 4th District vom 27.08.2015, *Benson v. Southern California Auto Sales, Inc.*, 239 Cal. App. 4th 1198, 1209; Cal. Court of Appeal 2nd District vom 27.03.2019, *Valdez v. Seidner-Miller, Inc.*, 33 Cal. App. 5th 600, 614.

[1571] Offenlassend: *Ballon*, E-commerce & Internet law. S. 26-426; *Silvers et al.*, Steps You Can Take Now To Reduce The Risk Of Litigation Under The New California Consumer Privacy Act.

[1572] *Silvers et al.*, Steps You Can Take Now To Reduce The Risk Of Litigation Under The New California Consumer Privacy Act.

[1573] Cal. Civ. Code § 1798.150(a)(1)(A).

[1574] *Byun*, 32 Loy. Consumer L. Rev. 246, 260; *de la Lama/Markert*, Bryan Cave Leighton Paisner, The Expanded Private Right of Action under the CPRA.

[1575] Cal. Civ. Code § 1798.150(a)(2).

[1576] Cal. Civ. Code § 1798.150(a)(2).

[1577] Cal. Civ. Code § 1798.150(a)(2).

[1578] Vgl. Cal. Bus. Prof. Code § 17206(b). Der CCPA übernimmt den Wortlaut des Unfair Competition Law, ohne ihn an die Nomenklatur des CCPA anzupassen: z. B. »defendant« statt »business«.

Statt dieser Schadensersatzspauschale können die Verbraucher:innen auch den tatsächlichen Schaden verlangen.[1579] Dies ist vor allem bei einem durch die Datenpanne hervorgerufenen Identitätsdiebstahls relevant.[1580] Solche tatsächlichen Schäden waren bisher nur schwer nachzuweisen, da selbst, wenn beispielsweise ein Identitätsdiebstahl eingetreten ist, sich nur schwer beweisen lässt, dass dafür die konkrete Datenpanne ursächlich war.[1581] Daneben kann das Gericht auch Unterlassung, Feststellung oder eine bestimmte Leistung tenorieren[1582] – was vor allem bei Unternehmen relevant sein dürfte, die trotz Datenpanne nicht angemessene Sicherheitsmaßnahmen ergreifen.

c) Verfahren

Bisherige Verfahren waren vor allem Sammelklagen vor Bundesgerichten, welche die Schadensersatzpauschale geltend machten.[1583] Die kalifornischen Gerichte

---

[1579] Cal. Civ. Code § 1798.150(a)(1)(A).

[1580] Dementsprechend lag ein Identitätsdiebstahl dem bisher einzigen Fall zugrunde, bei tatsächlicher Schadensersatz unter dem CCPA geltend gemacht wurde: U. S. District Court C. D. Cal. vom 26.10.2020, *Fuentes v. Sunshine Behavioral Health Group*, 2020 U. S. Dist. LEXIS 198900. Der Musterkläger hat die Klage später zurückgenommen.

[1581] *Marcus*, 68 Duke L. J. 555; *Romanosky/Hoffman/Acquisti*, 11 Empirical Legal Stud. 74, 92; *Solove/Citron*, 96 Tex. L. Rev. 737, 750 f.

[1582] Cal. Civ. Code § 1798.150(a)(1)(B),(C).

[1583] Abgeschlossene Sammelklagen: U. S. District Court S. D. Cal. vom 19.11.2020, *Stasi v. Inmediata Health Group Corp.*, 2020 U. S. Dist. LEXIS 217097, 47–49; U. S. District Court N. D. Cal. *Barnes v. Hanna Andersson, LLC*, Vergleich abrufbar unter: https://www.dwt.com/-/media/files/blogs/privacy-and-security-blog/2020/12/hannah-andersson-salesforce-data-breach-settlement.pdf, [perma.cc/5VHH-D8LL]; U. S. District Court C. D. Cal. vom 21.01.2021, *Flores v. Saul*, 2021 U. S. Dist. LEXIS 11785: Klageabweisung ohne Erwähnung des CCPA; U. S. District Court C. D. Cal. vom 26.10.2020, *Fuentes v. Sunshine Behavioral Health Group*, 2020 U. S. Dist. LEXIS 198900, Klagerücknahme; U. S. District Court C. D. Cal. vom 12.01.2021, *Rahman, et al v. Marriott*, 2021 U. S. Dist. LEXIS 15155: Klageabweisung; U. S. District Court N. D. Cal. vom 02.02.2021, *McCoy v. Alphabet, Inc.*, 2021 U. S. Dist. LEXIS 24180, 28: Klageabweisung; U U. S. District Court S. D. Cal vom 12.08.2021, *In re Blackbaud, Inc.*, 2021 U. S. Dist. LEXIS 151831, 13: Klageabweisung; U. S. District Court W. D. Mo., *In Re T-Mobile Customer Data Security Breach Litigation*, 2022 U. S. DIST. CT. MOTIONS LEXIS 199933: Einigung über Vergleich. Noch laufende Sammelklagen: U. S. District Court N. D. Cal, *Atkinson v. Minted, Inc.*, Case No. 3:20-cv-03869, U. S. District Court N. D. Cal. *Conditi v. Instagram, LLC et al.*, Case No. 3:20-cv-06534; U. S. District Court N. D. Cal., *Wesch v. Yodlee, Inc. et al.*, Case No. 3:20-cv-05991; U. S. District Court C. D. Cal, Karter v. Equip, Case No. 8:20-CV-1385, U. S. District Court N. D. Cal., *Yick v. Bank of America, N.A.*, Case No. 3:21-cv-376; U. S. District Court S. D. Cal., *In re Blackbaud, Inc.*, *Customer Data Breach Litigation*, Case. No. 3:20-mn-02972-JMC; U. S. District Court C. D. Cal., *Calixte et al. v. Dave*, Inc., Case No. 2:20-cv-07704; U. S. District Court C. D. Cal., *Schaubach v. Hotels.Com, LP et al.*, No. 8:20-cv-2370; U. S. District Court N. D. Cal., *Glinoga v. Robinhood Markets, Inc. et al.*, Case No. 3:21-cv-09290; U. S. District Court C. D. Cal., *Ponce v. Smile Brands Inc. et al.*, Case No. 8:21-cv-2115; U. S. District Court N. D. Cal., *Hammerling et al. v. Google LLC*, Case No. 3:21-cv-9004.
Eine regelmäßig aktualisierte Übersicht bietet: *Perkins Coie*, CCPA Litigation Tracker.

sind zwar grundsätzlich für Klagen nach kalifornischem Recht zuständig.[1584] Allerdings können Kläger:innen auch die Bundesgerichte wählen, wenn der Streitwert mehr als 75.000 $ beträgt und Kläger:innen sowie Beklagte in verschiedenen Bundesstaaten ihren Sitz haben *(diversity jurisidiction)*.[1585] Bei Sammelklagen genügt es, wenn einer der Kläger:innen in einem anderen Bundesstaat als einer der Beklagten seinen Sitz hat, der Gesamtstreitwert über 5.000.000 $ liegt und mindestens 100 Kläger:innen beteiligt sind.[1586] Beklagte können in diesen Fällen auch beantragen, dass ein einzelstaatliches Gericht die ursprünglich vor ihm erhobene Klage an die Bundesgerichte verweist *(removal jurisdiction)*.[1587] Dies beantragen Beklagte in Kalifornien auch häufig,[1588] da die kalifornischen Gerichte als verbraucherfreundlich gelten.[1589] Zukünftig werden möglicherweise Datenschutzklagen eher vor einzelstaatlichen Gerichten verhandelt werden, wenn der von republikanischen Richter:innen dominierte U. S. Supreme Court seine Anforderungen an *standing* weiter verschärft.[1590] Die oben dargestellte *standing doctrine* ist nämlich für einzelstaatliche Gerichte nicht bindend,[1591] und Kalifornien folgt dieser auch nicht.[1592]

Die bisherigen Sammelklagen unter dem CCPA sind größtenteils noch rechtshängig.[1593] In den ersten drei Vergleichen haben die Kläger:innen gegen die Online-Versandhändlerin Hanna Andersson, LLC eine Schadensersatzsumme von 400.000 $,[1594] gegen die Kunsthändlerplattform Minted, Inc. eine Summe von 5.000.00 $[1595] und gegen den Mobilfunkanbieter T-Mobile einen Summe von

---

[1584] Im Umkehrschluss zu 28 U. S. C. § 1331.

[1585] U. S. Const. Art. III § 2 cl. 1; 28 U. S. C. § 1332(a).

[1586] 28 U. S. C. § 1332(d)(2).

[1587] 28 U. S. C. § 1453(b).

[1588] Beim CCPA z. B. im Verfahren: U. S. District Court C. D. Cal, *Karter v. Equip*, Case No. 8:20-CV-1385.

[1589] *U. S. Chamber Institute for Legal Reform*, 2019 Lawsuit Climate Survey, S. 2: Kalifornien auf Platz 48 von 50 bei einer Umfrage unter Rechtsanwält:innen, welche einzelstaatlichen Gerichte unternehmensfreundlich urteilen.

[1590] Eine solche Entwicklung selbst für Bundesgesetze vorhersagend: U. S. Supreme Court vom 25.06.2021, *TransUnion LLC v. Ramirez* – ablehnendes Sondervotum *Thomas*, 141 S. Ct. 2190, 2225 Fn. 9.

[1591] U. S. Supreme Court vom 27.02.1989, *ASARCO, Inc. v. Kadish*, 490 U. S. 605, 617; *Elliott*, 49 Seton Hall L. Rev. 233, 254.

[1592] Cal. Court of Appeal 6th District vom 29.12.2009, *Jasmine Networks, Inc. v. Superior Court*, 180 Cal. App. 4th. 980, 990.

[1593] *Perkins Coie*, CCPA Litigation Tracker.

[1594] U. S. District Court N. D. Cal. *Barnes v. Hanna Andersson, LLC*, Case No. 20-cv-00812, Vergleich abrufbar unter: https://www.dwt.com/-/media/files/blogs/privacy-and-security-blog/2020/12/hannah-andersson-salesforce-data-breach-settlement.pdf, [perma.cc/5VHH-D8LL].

[1595] U. S. District Court N.D. Cal. vom 17.12.2021, *Atkinson v. Minted, Inc.*, 2021 U. S. Dist. LEXIS 244257.

350.000.000 $ erzielt.[1596] Dies liegt deutlich über dem Durchschnitt bei Datenpannen-Sammelklagen vor dem CCPA.[1597]

d) Kein weitergehendes Privatklagerecht

Die Beschränkung des Privatklagerechts auf Datenpannen war das einzige signifikante Zugeständnis an Wirtschaftsverbände bei den Verhandlungen um den CCPA-2018.[1598] Wirtschaftsverbände sehen Sammelklagen nicht nur kritisch, weil sie Recht gegen Unternehmen effektiv durchsetzen, sondern auch wegen ihrer hohen Kosten und der durch sie erzeugten Rechtsunsicherheit. Aufwendige und lange Prozesse führen zu höheren Rechtsfindungskosten.[1599] Dass bei jeder Sammelklage eine andere Jury oder direkt gewählte[1600] Berufsrichter:innen entscheiden, führt zu erheblicher Rechtsunsicherheit.[1601] Dies gilt besonders bei Fällen mit technischem Bezug, wie sie für das Datenschutzrecht prägend sind, da Berufsrichter:innen und Juries kaum über technischen Sachverstand verfügen.[1602] Die Kosten sind durch die aufwendige *pre-trial discovery* hoch und werden im Regelfall auch bei Obsiegen nicht erstattet.[1603] Diese Unsicherheit übt auf Beklagte Druck aus, einem Vergleich zuzustimmen, selbst wenn sie im Recht sind.

Bei der Schadensersatzvorschrift des CCPA mag dieser Druck gerechtfertigt sein, da deren einziges offene Tatbestandsmerkmal ist, ob die Sicherheitsmaßnahmen ausreichend waren. Selbst ein Vergleich wegen einer Datenpanne trotz gerade noch angemessener Sicherheitsmaßnahmen gibt Unternehmen einen Anreiz, zukünftigen Datenpannen vorzubeugen.[1604] Bei einem Verstoß gegen andere Unternehmenspflichten oder Verbraucherrechte erzeugt ein Privatklagerecht aber

---

[1596] U. S. District Court W. D. Mo., *In Re T-Mobile Customer Data Security Breach Litigation*, 2022 U. S. DIST. CT. MOTIONS LEXIS 199933 (allerdings U. S. A-weite Sammelklage, die sich neben dem CCPA auch auf andere Ansprüche gestützt hat).

[1597] *Dyadkina/de la Torre/Bryan*, First CCPA Settlement Reached in Hanna Andersson Case.

[1598] Siehe Kapitel 2:C.II (ab S. 32).

[1599] *Kagan*, Adversarial legalism: the American way of law, S. 104–109. Dieser für Sammelklagen zutreffende Befund lässt sich hingegen nur schwer auf das gesamte amerikanische Rechtssystem übertragen, vgl. *Cross*, 89 Va. L. Rev. 189, 196–200.

[1600] In Kalifornien wählt das Volk die Richterschaft, wobei der Gouverneur sie i. d. R. zuvor vorläufig ernennt, Cal. Const. Art. VI § 16 (a),(b),(d)(2). Im Bund ernennt der Präsident im Einvernehmen mit dem Senat die Richter, U. S. Const Art. II § 2 cl. 2. Zur größeren Politisierung der amerikanischen Richterschaft rechtsvergleichend: *Michel*, Gerichtsverwaltung und Court Management in Deutschland und in den USA, S. 223 f.

[1601] *Kagan*, Adversarial legalism: the American way of law, S. 110–117.

[1602] *Jeong*, The Verge, How the judge on Oracle v. Google taught himself to code; *Rogers/Paul*, Vice, The Jury Doesn't Get the Internet.

[1603] Fed. R. Civ. P. 54(d).

[1604] Dementsprechend vertreten einige Literaturstimmen auch eine Garantiehaftung für Datenpannen: *Citron*, 80 Cal. L. Rev. 241, 261–268; *Meglio*, 61 B.C. L. Rev. 1223, 1258–1269; *Ormerod*, 60 B.C.L. Rev. 1893, 1914–1941.

deutlich stärkere Rechtsunsicherheit, da diese eine Vielzahl offener Tatbestandselemente enthalten und stärker von einer Auslegung durch politisch gewählte Berufsrichter:innen im Einzelfall abhängig sind.

Daher wurde aufgrund der Verhandlungen um den CCPA-2018 folgender Abschnitt in die Vorschrift zum Privatklagerecht aufgenommen:

»The cause of action established by this section shall apply only to violations as defined in subdivision (a) [data breaches] and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law.«[1605]

Der erste Satz stellt klar, dass das explizit geregelte Privatklagerecht nur für Datenpannen gilt. Der zweite Satz soll ausweislich der Gesetzesmaterialien verhindern, dass sich aus dem kalifornischen Unfair Competition Law ein mittelbares Privatklagerecht ergibt.[1606] Unter diesem Gesetz können kalifornische Bürger:innen auf Unterlassung jedes Rechtsverstoßes gegen ein anderes Gesetz klagen, wenn zumindest der Musterkläger oder die Musterklägerin geschädigt ist.[1607] Die Literatur und der kalifornische Attorney General gehen einhellig davon aus, dass der eindeutige Wortlaut des obigen Abschnitts das Unfair Competition Law sperrt.[1608] Trotzdem haben sich zahlreiche Sammelklagen wegen Verstößen gegen Unternehmenspflichten oder Verbraucherrechte des CCPA auf das Unfair Competition Law gestützt.[1609] Erfolg hatten sie damit bisher nicht.[1610]

[1605] Cal. Civ. Code § 1798.150(c).

[1606] *Cal. Senate Judiciary Comm.*, AB 375 Bill Analysis, S. 22.

[1607] Cal. Bus. Prof. Code §§ 17203, 17200. Andere Kläger:innen müssen nicht geschädigt sein, vgl. Cal. Supreme Court vom 18.05.2009, *In re Tobacco II Cases*, 46 Cal. 4th 298, 314–324.

[1608] *Ballon*, E-commerce & Internet law. S. 26-427; *Iliadis/Maddigan*, HL Chronicle of Data Protection, Consumer Litigation and the CCPA; *Michaud/Davis*, Privacy Perspectives, Will private litigants be able to enforce the CCPA compliance provisions; *Pink*, California Consumer Privacy Act Annotated, § 9:5.5; *Yannella*, Cyber Litigation, §§ 9:7, 9:10; ein umfassendes Privatklagerecht verneinend, ohne auf das UCL einzugehen: *Cal. Attorney General*, California Consumer Privacy Act of 2018, S. 2; *ders.*, CCPA FAQ, A.7; *Aubuchon*, 98 Wash. U. L. Rev. 1289, 1308; *Ashman*, 99 Or. L. Rev. 523, 543; *Goldman*, Internet Law, S. 377; *Flor*, 96 Notre Dame L. Rev. 2035, 2042; *Monticollo/Reckell/Cividanes*, 35 Antitrust ABA 32, 34, 36; *Ormerod*, 60 B.C.L. Rev. 1893, 1907f; *Pardau*, 23 J. Tech. L. & Pol'y 68, 105; *Resnick*, 46 Brook. J. Int'l L. 277, 292; *del Rosario*, 90 Fordham L. Rev. 1699, 1724; *Smith*, 93 St. John's L. Rev. 851; *Stuenkel*, 19 Colo. Tech. L. J. 429, 458.

[1609] U. S. District Court S. D. Cal., *Sean Burke et al. v. Clearview AI, Inc., et al.*, Case No. 20-CV-0370-BAS-MSB; U. S. District Court N. D. Cal., *Conditi v. Instagram, LLC et al*, Case No. 3:20-cv-6534; *Wesch v. Yodlee, Inc.*, Case No. 3:20-cv-05991.

[1610] Vgl. die Klageabweisung in: U. S. District Court N. D. Cal. vom 02.02.2021, *McCoy v. Alphabet, Inc.*, 2021 U. S. Dist. LEXIS 24180, 28; U. S. District Court S. D. N. Y. vom 24.02.2022, *In re Waste Mgmt. Data Breach Litig.*, 2022 U. S. Dist. LEXIS 3279824, 18–19.

3. Vergleich mit europäischem und deutschem Datenschutzrecht sowie Zivilprozessrecht

Die Privatklagerechte des Art. 79, 82 DSGVO sind *prima facie* die umfassenden Klagerechte, die das kalifornische Parlament abgelehnt hatte. Art. 82 Abs. 1 DSGVO regelt einen umfassenden Schadensersatzanspruch bei jedem Schaden aufgrund eines Verstoßes gegen die DSGVO. Zwar ist der Schadensbegriff unklar und Gegenstand von fünf Vorlageverfahren vor dem EuGH.[1611] Allerdings ist zumindest der Tatbestand des CCPA erfasst, da jedenfalls ein nachweisbarer unberechtigter Zugriff auf risikoreiche personenbezogene Daten ein Schaden ist.[1612]

Diese Privatklagerechte sind allerdings in ein prozessuales Umfeld eingebettet, in dem eine private Rechtsdurchsetzung bei Datenpannen kaum möglich ist.[1613] Bei Datenpannen gibt es typischerweise viele Geschädigte, die als gleichartigen Schaden einen Kontrollverlust über ihre personenbezogenen Daten erlitten haben. Eine individuelle Klage »lohnt« sich bei solch breit gestreuten, niedrigen Schäden nicht.[1614] Bereits die DSGVO zeigt sich in Art. 80 Abs. 1 DSGVO skeptisch gegenüber einer privaten Rechtsdurchsetzung. Eine Vertretung bei der Geltendmachung von Schadensersatzansprüchen ist hiernach nur durch bestimmte, gemeinnützige Organisationen möglich und dies auch nur, sofern dies im Recht der Mitgliedsstaaten vorgesehen ist. Insoweit ist im deutschen Prozessrecht zu betrachten: die gebündelte Geltendmachung abgetretener Ansprüche durch objektive Klagehäufung, die Musterfeststellungsklage und ob sich daran etwas durch die Verbandsklagen-RL ändern wird.

Eine Bündelung von Ansprüchen mittels Abtretung an einen Inkasso-Anbieter ist zwar an sich zulässig.[1615] Allerdings muss die betroffene Person nicht nur selbst aktiv werden, sondern sogar einen Vertrag mit dem Inkassodienstleister

---

[1611] OGH (Österreich) vom 15.04.2021 – 6Ob35/21x, Az. beim EuGH: C-300/21, *Österreichische Post*, ZD 2021, 631, Fragen 1–3; Varhoven administrativen sad (Bulgarien) vom 14.05.2021, *Natsionalna agentsia za prihodite*, Az. beim EuGH: C-340/21, InfoCuria, Frage 5, BAG vom 26.08.2021 – 8 AZR 253/20 (A), Az. beim EuGH: C-560/21, *KISA*, BeckRS 2021, 29622, Fragen 4 und 5; LG Saarbrücken vom 22.11.2021 – 5 O 151/19, Az. beim EuGH: C-741/21, *juris*, GRUR-RS 2021, 39544, Fragen 1–4; AG Hagen vom 16.11.2021, Az. beim EuGH: C-687/21, *Saturn Electro*, InfoCuria, Fragen 1–6; AG München vom 02.03.2022 – 132 C 737/22, AG München vom 03.03.2022 – 132 C 737/2, REWIS RS 2022, 905 Fragen 1–5; AG München vom 03.03.2022 – 132 C 1263/21, Az. beim EuGH: C-182/22, openJur 2022, 8185, Fragen 1–5 (gleich lautend mit AG München vom 03.03.2022 – 132 C 737/2).

[1612] Bei einem Kontrollverlust über sensible Daten einen Schaden bejahend: LAG Baden-Württemberg vom 25.02.2021, BeckRS 2021, 5529, Rn. 82; LAG Köln vom 14.09.2020, ZD 2021, 168, Rn. 26 f.; *Bergt* in: Kühling/Buchner, DS-GVO Art. 82 Rn. 18b. a. A. LG Frankfurt/M. vom 18.09.2020, ZD 2020, 639, Rn. 45: nur bei tatsächlicher, nachweisbarer Kenntnisnahme.

[1613] Im Ergebnis ähnlich für Europa: *Monticollo/Reckell/Cividanes*, 35 Antitrust ABA 32, 36: Kostenrisiko abschreckend wegen Kostenerstattung für obsiegende Partei.

[1614] Anders bei einem Fehlverhalten gegenüber einer bestimmten Person wie einer verspätetem Auskunftserteilung, wenn man insoweit einen Schaden bejaht.

[1615] BGH vom 13.07.2021 – II ZR 84/20, juris Rn. 16–44.

schließen.[1616] Dabei ist sie anders als bei den amerikanischen Sammelklagen nicht durch ein Gericht geschützt, sondern muss in der Regel ihre Forderung unwiderruflich abtreten.[1617] Daher sind solche Zessionsmodelle für betroffene Personen aufwendig und schwer zu beurteilen. Verantwortliche müssen die betroffene Person nach Art. 34 Abs. 1 DSGVO zudem nur bei einem hohen Risiko benachrichtigen. Dementsprechend erfahren betroffene Personen häufig nicht einmal von der Datenpanne. Zudem ist unklar, ob Art. 80 Abs. 1 DSGVO der Abtretung an gewinnorientierte Inkasso-Anbieter entgegensteht.[1618] Zessionsmodelle spielen daher nur eine geringe Rolle in der deutschen datenschutzrechtlichen Rechtspraxis.[1619]

Die Musterfeststellungsklage nach §§ 606–614 ZPO ist ebenfalls kaum für Streuschäden geeignet.[1620] Deren zweistufiges Konzept ist noch komplexer als die Inkasso-Sammelklage. Der Gesetzgeber hatte zwar gehofft, dass sich die Parteien bereits auf der Feststellungsklagen-Stufe vergleichen und dabei gemäß § 611 Abs. 2 Nr. 1 ZPO konkrete Leistungen vereinbaren.[1621] Warum Beklagte einen Vergleich annehmen sollten statt Verbraucher auf die für die Klageseite wesentlich aufwendigeren Leistungsklagen zu verweisen, ist jedoch unklar.[1622] Dementsprechend haben sich die Parteien seit Inkrafttreten der §§ 606–614 ZPO im Jahr 2018 nur in einem der 29 Musterfeststellungsklage-Verfahren (außergerichtlich) verglichen.[1623] Zudem regelt § 606 Abs. 1 S. 2 ZPO einen komplexen und von hohem Misstrauen gegenüber Sammelklagen geprägten Anforderungskatalog für die Klagebefugnis, den bisher erst ein einziger Kläger erfüllt hat.[1624] Alle sonstigen, nicht wegen fehlender Klagebefugnis abgewiesenen Musterfeststellungsklagen haben die Verbraucherschutzzentralen erhoben, deren Klagebefugnis unwiderleglich vermutet wird (§ 606 Abs. 1 S. 4 ZPO).[1625] Bisher gab es keine Musterfeststellungsklage wegen Datenschutzverstößen.

[1616] *Meller-Hannich*, Sammelklagen, Gruppenklagen, Verbandsklagen, S. A 58.

[1617] *Voit*, Sammelklagen, S. 192–194.

[1618] Zum Streitstand: *Heinzke/Storkenmaier*, CR 2021, 299 Rn. 26 f.; *Voit*, Sammelklagen, S. 175 f. Der BGH hat eine verwandte Frage zu Art. 80 Abs. 1 DSGVO vorgelegt: BGH vom 28.05.2020 – I ZR 186/17, Az. beim EuGH: C-319/20, *App-Zentrum*, GRUR 2020, 896.

[1619] *Heinzke/Storkenmaier*, CR 2021, 299, 305.

[1620] *Stadler* in: Musielak, ZPO vor §§ 606 ff. Rn. 1; *Heinzke/Storkenmaier*, CR 2021, 299 Rn. 37; *Voit*, Sammelklagen, S. 220; a. A. *Kremer/Conrady/Penners*, ZD 2021, 128, 132.

[1621] BT-Drs. 19/2439, 17.

[1622] *Heinzke/Storkenmaier*, CR 2021, 299 Rn. 37; *Meller-Hannich*, Sammelklagen, Gruppenklagen, Verbandsklagen, S. 54 f.; *Stadler* in: *Musielak*, ZPO vor §§ 606 ff. Rn. 1; *Voit*, Sammelklagen, S. 209–211.

[1623] *Bundesamt für Justiz*, Klageregister.

[1624] BGH vom 18.03.2021 – VIII ZR 305/19, NZM 2021, 463 Rn. 20–22.

[1625] *Bundesamt für Justiz*, Klageregister. Diese haben 21 der bisherigen 24 Musterfeststellungsklagen erhoben. Zwei der drei weiteren Musterfeststellungsklagen hat die Schutzgemeinschaft für Bankkunden e.V. erhoben, die allerdings nicht klagebefugt ist: BGH vom 17.11.2020 – XI ZR 171/19, *Mercedes*, NJW 2021, 1014 Rn. 14–32.

Ob sich daran etwas durch die bis zum 25.12.2022 umzusetzende Verbandsklagen-RL[1626] ändert, ist zweifelhaft. Unter dieser muss Deutschland auch eine einstufige Verbandsklage auf Abhilfe einführen (Art. 9 Abs. 7 Verbandsklagen-RL). Allerdings sind weiterhin nur bestimmte qualifizierte gemeinnützige Einrichtungen klagebefugt (Art. 4 Verbandsklagen-RL). Diesbezüglich will die »Ampelkoalition« für die Verbandsklage an den hohen Klagebefugnisanforderungen der Musterfeststellungsklage festhalten,[1627] sodass auch die Verbandsklage fast ausschließlich ein Instrument der Verbraucherzentralen sein wird. Zudem ist zwar eine Prozessfinanzierung grundsätzlich zulässig, der Prozessfinanzierer darf aber nicht mehr Einfluss als unbedingt nötig ausüben (Art. 10 Abs. 2 lit. a Verbandsklage-RL). Der Prozessfinanzierer müsste also praktisch die »Katze im Sack kaufen«, was wirtschaftlich kaum attraktiv ist.[1628] Diese Finanzierungsregelungen dürften dazu führen, dass die qualifizierte Einrichtung die Prozesskosten aus Eigenmitteln erbringen muss.[1629] Dieses Problem sieht auch der europäische Gesetzgeber und fordert die Mitgliedstaaten zu Maßnahmen auf, um qualifizierte Einrichtungen nicht von Verbandsklagen abzuhalten (Art. 20 Abs. 1 Verbandsklagen-RL). Diese können gemäß Art. 20 Abs. 2 Verbandklagen-RL beispielsweise öffentliche Finanzierung umfassen, wie sie die Verbraucherzentralen in Deutschland erhalten.[1630] Öffentlich finanzierte Verbandsklagen sind jedoch keine private Rechtsdurchsetzung, sondern nur staatlich determiniertes Handeln in anderem Gewand.

Die Angst vor einer »Klageindustrie«[1631] und »amerikanischen Verhältnissen«[1632] führt dazu, dass der Schadenersatzanspruch des Art. 82 DSGVO faktisch leerläuft.[1633] So beträgt die Schadensersatzsumme in sämtlichen veröffentlichten deutschen Urteilen zu Art. 82 DSGVO insgesamt nur 75.092 €[1634] – »Peanuts« im Vergleich zu den 355.400.000 $ allein in den ersten drei Vergleichen aufgrund von CCPA-Sammelklagen. Auch beim Abhandenkommen

---

[1626] Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher und zur Aufhebung der Richtlinie 2009/22/EG.

[1627] *SPD/Bündnis 90/Die Grünen/FDP*, Koalitionsvertrag 2021–2025, S. 106.

[1628] *Stadler*, ZHR 2018, 623, 652.

[1629] *Röthemeyer*, VuR 2021, 43, 52; *Stadler*, ZHR 2018, 623, 650–653.

[1630] Z. B. *Verbraucherzentrale Bundesverband*, Jahresbericht 2019, S. 74: ca. 98 % der Einnahmen im institutionellen Haushalt aus öffentlichen Mitteln.

[1631] So explizit die Gesetzesbegründung zu § 606 ZPO: BT-Drs. 19/2439, 23. Zu recht kritisch: *Röthemeyer*, VuR 2020, 130, 131–133.

[1632] *Schubert*, Deutscher AnwaltSpiegel, Drohen amerikanische Verhältnisse? Im Blickpunkt: Die EU-Verbandsklage kommt.

[1633] Anders wird dies enventuell zukünftig für den Unterlassenanspruch zu beurteilen sein, für den jetzt der EuGH festgestellt hat, dass zumindest Verbände ihn auf § 3 Abs. 1 Satz 1 Nr. 1 UKlaG gestützt durchsetzen können: EuGH vom 28.04.2022 – C-319/20, Meta Platforms Ireland, ECLI:EU:C:2022:322 Rn. 83.

[1634] *Leibold*, Übersicht über den Schadensersatzanspruch nach Art. 82 DS-GVO: nur Schadensersatz

umfangreicher, sensibler Daten sprechen deutsche Gerichte nur Schadensersatz in niedriger vierstelliger Höhe zu.[1635] Dass diese niedrigen Beträge unter Art. 82 DSGVO keinerlei generalpräventive Wirkung haben, liegt auf der Hand.[1636] Demgegenüber zeigt der CCPA, dass Sammelklagen ein sachgerechtes Mittel sind, um die massenhaften Schäden durch Datenpannen zu kompensieren.

III. Ergebnis

Primär obliegt die Rechtsdurchsetzung sowohl in Kalifornien als auch in Europa den Aufsichtsbehörden. Als Ausdruck der im amerikanischen Recht starken Gewaltenteilung sind allerdings California Privacy Protection Agency, kalifornischer Attorney General, District und City Attorneys gleichzeitig für die Sanktionierung von CCPA-Verstößen zuständig.

Die wichtigste kalifornische Aufsichtsbehörde ist die California Privacy Protection Agency. Diese ist eine unabhängige Datenschutzbehörde, die ein fünfköpfiges Gremium leitet.[1637] Sie hat ein garantiertes Mindestbudget von 10 Millionen Dollar.[1638]

Die California Privacy Protection Agency kann wegen Verstößen gegen den CCPA Ermittlungen einleiten und Betriebsprüfungen durchführen.[1639] Aufgrund dieser Prüfungen verhängt sie Bußgelder,[1640] die sie in einem Verwaltungsverfahren vor einem *administrative law judge* festsetzt.[1641] Der Bußgeldrahmen beträgt bis zu 2.500 $ pro Verletzungserfolg, bei vorsätzlichen Verstößen oder solchen, die Verbraucher:innen unter 16 Jahren betreffen, bis zu 7.500 $ pro Verletzungserfolg.[1642] Weiterhin soll die California Privacy Protection Agency durch eine umfassende Öffentlichkeitsarbeit Verstößen vorbeugen und Verbraucher:innen über ihre Rechte aufklären.[1643] Ein wesentlicher Unterschied zu den Aufsichtsbehörden der DSGVO ist, dass die California Privacy Protection Agency über eine umfassende Verordnungsermächtigung verfügt.[1644]

Den kalifornischen Attorney General ergänzt die California Privacy Protection Agency. Dieser direkt gewählte Minister[1645] leitet die wichtigste Vollzugs-

---

[1635] OLG Düsseldorf vom 28.10.2021 – 16 U 275/20, REWIS RS 2021, 1463: Schadensersatz i.H.v. 2.000 € bei einer Datenpanne, die eine 100-seitige Gesundheitsakte mit u. a. das Sexualleben der Klägerin offenlegenden Befunden betraf.

[1636] A. A. offenbar *Halim/Klee*, CCZ 2021, 300, 304 f.: Haftungshöchstgrenze pro Verbraucher:in resultiere in Rechtssicherheit, die unter der DSGVO fehle (allerdings ist eine Multiplikation mit der Zahl der Verbraucher:innen ohne Sammelklage kaum möglich).

[1637] Cal. Civ. Code § 1798.199.10(a).

[1638] Cal. Civ. Code § 1798.199.95(a).

[1639] Cal. Civ. Code §§ 1798.199.45, 1798.199.50.

[1640] Cal. Civ. Code § 1798.155.

[1641] Cal. Civ. Code § 1798.199.55(a) i. V. m. Cal. Gov. Code § 11502(a).

[1642] Cal. Civ. Code § 1798.155(a).

[1643] Cal. Civ. Code § 1798.199.40(d)–(g).

[1644] Cal. Civ. Code § 1798.185.

[1645] Cal. Const. Art. V § 11.

behörde Kaliforniens: das Department of Justice. Dieses hat bereits 2012 eine eigene Datenschutzabteilung eingerichtet, die seitdem zahlreiche Verfahren gegen große Technologieunternehmen durchgeführt hat. Der CCPA ermöglicht dem Attorney General auf Verhängung von *civil penalties* zu klagen.[1646] Diese sind gerichtlich festgesetzte Strafen, die ein Zivilgericht verhängt. Ein solches Gerichtsverfahren ist aufwendiger und kostspieliger als die Festsetzung von Geldbußen durch die California Privacy Protection Agency. Daher wird sich der Attorney General wahrscheinlich auf große, öffentlichkeitswirksame Verfahren konzentrieren, mit denen er sich als »Anwalt des Volkes« profilieren kann.

Eine ergänzende Rolle spielen in einzelnen Fällen District und City Attorneys. Diese können ebenfalls auf die Verhängung von *civil penalties* klagen.[1647] Sie haben allerdings nur begrenzte Mittel.

Die europäischen Aufsichtsbehörden sind im Vergleich dazu wesentlich eher auf einheitliche Entscheidungen ausgerichtet. Statt der gleichzeitigen Zuständigkeit vieler Aufsichtsbehörden wie unter dem CCPA soll eine federführende Aufsichtsbehörde als *One-Stop-Shop* fungieren (Art. 56 Abs. 1 DSGVO). Das Kohärenzverfahren der Art. 60–67 DSGVO soll dabei Einheitlichkeit und Rechtssicherheit herstellen, funktioniert aber in der Praxis nur schlecht. Der Vergleich mit dem CCPA zeigt, dass aus der gleichzeitigen Zuständigkeit mehrerer Aufsichtsbehörden nicht die befürchtete Rechtsunsicherheit resultieren muss.

Das Privatklagerecht des CCPA[1648] ist auf Datenpannen beschränkt. Es erlaubt Verbraucher:innen, auf Schadensersatz und Unterlassung zu klagen, wenn bestimmte, einen Identitätsdiebstahl ermöglichende Informationen bei Datenpannen abhanden gekommen sind. Entscheidend ist dabei, dass Verbraucher:innen auch ohne Nachweis eines konkreten Schadens eine Schadensersatzpauschale von 100 bis 750 $ verlangen können.[1649] Diese Schadensersatzpauschalen sind auf Sammelklagen zugeschnitten, welche bisher häufig wegen fehlendem Schadensnachweis gescheitert sind. In Vergleichen unter dem CCPA haben Kläger:innen bei Datenpannen-Sammelklagen deutlich höhere Summen erzielt als bisher.

Das Privatklagerecht des Art. 79, 82 DSGVO ist dagegen umfassend. Es ist allerdings in ein europäisches und deutsches prozessuales Umfeld eingebettet, in dem eine Durchsetzung der im Datenschutz typischen Streuschäden kaum möglich ist. So sind Sammelklagen anders als im amerikanischen Recht nur theoretisch möglich.

[1646] Cal. Civ. Code § 1798.199.90(a).
[1647] Cal. Bus. & Prof. Code §§ 17200, 17206.
[1648] Cal. Civ. Code § 1798.150.
[1649] Cal. Civ. Code § 1798.150(a)(1)(A).

F. Rechtsvergleichendes Fazit

I. Privatautonomie statt Paternalismus

1. Selbstermächtigung als Ziel des CCPA

Der primäre Unterschied zwischen CCPA und DSGVO liegt in der jeweiligen Regelungsphilosophie. Der CCPA will Verbraucher:innen ermächtigen, ihre persönlichen Informationen selbst zu schützen,[1650] während die DSGVO die staatliche Schutzpflicht der Art. 7, 8 GRCh mittels einer mittelbaren Drittwirkung von Grundrechten verwirklichen will.[1651]

Das liberale amerikanische Zivilrecht ist allgemein am Bild eines rationalen, selbstbestimmten Individuums ausgerichtet. Aufschlussreich ist vor allem das kaum ausgeprägte amerikanische AGB-Recht *(contracts of adhesision)*. Dieses orientiert sich vor allem daran, ob die schwächeren Vertragsparteien dem Vertrag als Ganzem freiwillig zustimmt.[1652] Die kalifornische Rechtsprechung hat zwar auch eine inhaltliche Angemessenheitskontrolle *(unconscionability)* entwickelt.[1653] Diese spielt allerdings nur bei Prozessverträgen eine nennenswerte Rolle. So bezieht sich nur eine einzige Entscheidung des kalifornischen Supreme Court zur *unconscionability* auf einen materiell-rechtlichen Vertrag.[1654] Selbst bei den besonders missbrauchsanfälligen Prozessverträgen sind die Anforderungen nicht besonders hoch: so sind Schiedsgerichtsklauseln unter Verzicht auf eine Sammelklage auch in *contracts of adhesision* möglich[1655] und üblich. Auch vorsorgende Rechtspflege ist dem amerikanischen Recht fremd.[1656] Darin zeigt sich, dass das an der Vertragsfreiheit orientierte amerikanische Zivilrecht strukturellen Ungleichgewichten kaum eine Bedeutung einräumt.[1657]

[1650] Den CCPA-2018 als Verbraucherschutzgesetz einordnend: *Chander/Kaminski/McGeveran*, 105 Minn. L. Rev. 1733, 1756–1757 wegen fehlender Datenminimierung und Zweckbindung im CCPA-2018, welche Proposition 24 allerdings eingefügt hat.

[1651] *Lewinski*, Die Matrix des Datenschutzes, S. 46–48: DSGVO-E regele »informationelle Fremdbestimmung«.

[1652] Cal. Supreme Court vom 17.10.2013, *Sonic-Calabasas A, Inc. v. Moreno*, 57 Cal. 4th 1109, 1145: »the core concern of the unconscionability doctrine is the absence of meaningful choice on the part of one of the parties«; vom 03.08.2015, *Sanchez v. Valencia Holding Co., LLC*, 61 Cal. 4th 899, 910. Kritisch zu diesem Fokus: *Tutt*, 30 Yale J. on Reg. 439, 444–446.

[1653] Cal. Supreme Court vom 05.02.1981, *Graham v. Scissor-Tail, Inc.*, 28 Cal. 3d 807, 820; vom 17.10.2013, *Sonic-Calabasas A, Inc. v. Moreno*, 57 Cal. 4th 1109, 1145; vom 03.08.2015, *Sanchez v. Valencia Holding Co., LLC*, 61 Cal. 4th 899, 910 f.; vom 29.08.2019, *OTO, L.L.C. v. Kho*, 8 Cal. 5th 111, 124.

[1654] Cal. Supreme Court vom 18.12.1982, *Steven v. Fidelity & Casualty Co.*, 58 Cal. 2d 862, 879.

[1655] U. S. Supreme Court vom 27.04.2011, *AT&T Mobility LLC v. Concepcion*, 563 U. S. 333, 346 f.; vom 21.05.2018, *Epic Sys. Corp. v. Lewis*, 138 S. Ct. 1612, 1645 f.

[1656] *Stürner*, AcP 210 (2010), 105, 122–124.

[1657] Ebd., 105, 122.

Auch das amerikanische Datenschutzrecht orientiert sich stark an der Privatautonomie. So war schon die Einführung des Rechts auf Privatsphäre in die kalifornische Verfassung maßgeblich durch eine stärkere Kontrolle über die eigenen Daten motiviert.[1658] Auch der U. S. Supreme Court hat Kontrolle über die eigenen Daten in *United States DOJ v. Reporters Comm. for Freedom of Press* (1989) als traditionelles Prinzip des amerikanischen Privatsphäreschutzes genannt.[1659] Vor allem nach dem *notice-and-choice*-Modell der FTC ist die autonome Entscheidung des Individuums zentral. So müssen Unternehmen nur Verbraucher:innen über diese informieren *(notice)* und ihnen eine *opt-out*-Möglichkeit einräumen *(choice).*[1660] Dieses *notice-and-choice*-Modell setzt sehr aktive Verbraucher:innen voraus, die in der Praxis häufig überfordert sind, ist aber unstrittig das entscheidende Paradigma des amerikanischen Datenschutzrechts.[1661]

Der CCPA betont dementsprechend schon in seinen ersten Erwägungsgründen das Ziel, dass Verbraucher:innen mehr Kontrolle über ihre persönlichen Informationen erlangen.[1662] Diesen Aspekt wiederholt der CCPA in sieben weiteren Erwägungsgründen und unterstreicht so seine zentrale Bedeutung.[1663] Verbraucher:innen sollen informierte Vertragsparteien in der Datenwirtschaft werden (»informed counterparties in the data economy«)[1664] und benötigten strengere Gesetze, um auf Augenhöhe mit Unternehmen verhandeln zu können (»Consumers need stronger laws to place on a more equal footing when negotiating with businesses«).[1665]

Der CCPA ist nach der Vorstellung des Gesetzgebers dieses strengere Gesetz. Auf der ersten Stufe ermöglichen die umfassenden Informationspflichten Verbraucher:innen, sich bewusst für oder gegen ein bestimmtes Unternehmen entscheiden zu können. Auf der zweiten Stufe können Verbraucher:innen frei wählen, ob das Unternehmen mit ihren persönlichen Informationen handeln darf und ob ihre sensiblen Informationen besonders geschützt sein sollen. Dies spiegelt das ebenfalls zweistufige *notice-and-choice*-Modell. Wenn sich Verbraucher:innen aufgrund ihrer Privatautonomie für eine kommerzielle Verwertung ihrer persönlichen Informationen entscheiden, sieht das der CCPA nicht kritisch. Vielmehr sollen sich Verbraucher:innen des Wertes ihrer persönlichen Informationen bewusst werden und sich informiert für oder gegen finanzielle

---

[1658] Siehe Kapitel 2:A.II (ab S. 15).

[1659] U. S. Supreme Court vom 22.03.1989, *United States DOJ v. Reporters Comm. for Freedom of Press*, 489 U. S. 749, 763: »both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person«.

[1660] Siehe Kapitel 2:B.I.3 (ab S. 24).

[1661] Siehe Kapitel 2:B.III (ab S. 29).

[1662] CCPA-2018, Sec. 2(a), Proposition 24 (Cal. 2020), Sec. 2(A), 3(A)(1).

[1663] CCPA-2018, Sec. 2(g)–(i), Proposition 24 (Cal. 2020), Sec. 2(G),(H),(J), 3(A)(2).

[1664] Proposition 24 (Cal. 2020), Sec. 2(G).

[1665] Proposition 24 (Cal. 2020), Sec. 2(H).

Anreize für die kommerzielle Verwertung ihrer persönlichen Informationen entscheiden können.[1666]

Der Charakter als ein Selbstdatenschutz-Gesetz, das Individuen in die Lage versetzen will, selbstbestimmt über ihre Daten zu verfügen, kommt in zahlreichen weiteren Vorschriften zum Ausdruck. So nennt der CCPA betroffene Personen durchgängig »consumer« (Verbraucher:innen),[1667] während der Verantwortliche »business« (Unternehmen) heißt, was den Fokus der Verantwortung anders als bei der DSGVO nicht auf den die wesentlichen Entscheidungen treffenden »Verantwortlichen«, sondern auf das Individuum Verbraucher:in legt.[1668] Durch Unternehmen vorzunehmende Interessenabwägungen finden sich nur in einem einzigen Auffangtatbestand.[1669] Unternehmen sind zudem nur gewinnorientierte Gesellschaften gewisser Größe, bei denen ein besonders großes Verhandlungsungleichgewicht zu Verbraucher:innen besteht.[1670] Diese Verhandlungsungleichgewicht sollen umfassende Informationspflichten ausgleichen.[1671]

2. Die DSGVO als Ausdruck der mittelbaren Drittwirkung von Grundrechten

Das europäische Datenschutzrecht ist dagegen primär grundrechtsgeprägt und will präventiv Gefahren für die betroffene Person abwehren.[1672] So hält die DSGVO schon zu Beginn in Art. 1 Abs. 2 DSGVO fest, dass ihr primäres Ziel der Schutz von Grundrechten und Grundfreiheiten natürlicher Personen ist. Dementsprechend ist das aus dem Polizeirecht stammende Verbot mit Erlaubnisvorbehalt[1673] gemäß Art. 6 Abs. 1 DSGVO ihr Grundprinzip. Jede Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage. Zentrale Rechtsgrundlage ist die durch den Verantwortlichen vorzunehmende Abwägung der berechtigten Interessen des Verantwortlichen mit den Grundrechten und Grundfreiheiten der betroffenen Person (Art. 6 Abs. 1 lit. f DSGVO). Auch sonst ziehen sich zahlreiche Abwägungen durch die gesamte DSGVO.[1674] Art. 9 Abs. 1, 3 DSGVO konstituiert sogar einen aus der Grundrechtsdogmatik stammenden weitgehenden Gesetzesvorbehalt für die Verarbeitung besonderer Kategorien personenbezogener Daten durch Private. Die Kontrolle über die eigenen Daten spielt hingegen keine große Rolle in

---

[1666] Siehe Kapitel 3:C.I.4.b)bb) (ab S. 104).

[1667] Cal. Civ. Code § 1798.140(i).

[1668] Cal. Civ. Code § 1798.140(b).

[1669] Cal. Civ. Code § 1798.145(k): Auffangtatbestand, wenn eine der zahlreichen pauschalen Ausnahmen beim Recht auf Auskunft nicht greift, siehe Kapitel 3:C.III.1.a) (ab S. 116).

[1670] Cal. Civ. Code § 1798.140(d). Siehe Kapitel 3:B.II.2 (ab S. 56).

[1671] Siehe Kapitel 3:D.I (ab S. 150).

[1672] *Bijok*, Kommerzialisierungsfester Datenschutz, S. 203f; *Haustein*, Möglichkeiten und Grenzen von Dateneigentum, S. 98 f.; *Sattler* in: Bakhoum et. al., Personal Data in Competition, Consumer Protection and Intellectual Property Law, 27, 36; *Schur*, Die Lizenzierung von Daten, S. 98; *Streinz, R./Michl*, EuZW 2011, 384, 385 f.; *Streinz T.* in: Craig/Búrca, The Evolution of EU Law, 902, 910–913; *Veil*, NVwZ 2018, 686, 689.

[1673] Kritisch zum Begriff: *Roßnagel*, NJW 2019, 1, 5.

[1674] *Veil*, NVwZ 2018, 686, 694.

der DSGVO. Die Erwägungsgründe erwähnen sie zwar beiläufig an vier Stellen, dabei betreffen zwei Stellen aber nicht die Ermöglichung eigener Kontrolle, sondern den Schutz der betroffenen Person vor einem Kontrollverlust durch den Verantwortlichen.[1675] Dagegen ist das Telemediendatenschutzrecht derzeit primär einwilligungsbasiert, entwickelt sich mit der ePrivacy-VO aber stärker in Richtung anderer Rechtsgrundlagen.[1676]

Hier wirkt sich aus, dass Datenschutz in der EU ein Grundrecht ist. Art. 7 GRCh schützt die Privatsphäre, während Art. 8 GRCh ein explizites Recht auf Datenschutz enthält. Art. 8 GRCh Abs. 2 legt sogar bereits bestimmte Inhalte der Datenschutzregulierung fest: Zweckbindung, das Verbot mit Erlaubnisvorbehalt, das Auskunftsrecht und das Berichtigungsrecht. Der EuGH und EGMR haben zahlreiche Urteile zu der grundrechtlichen Dimension des Datenschutzes erlassen.[1677] Zusätzlich hat der EuGH die Art. 7, 8 GRCh in nahezu jeder Entscheidung zur Auslegung der DSRL und DSGVO diskutiert.[1678] Auch nationale Verfassungsgerichte haben eine umfangreiche Datenschutz-Rechtsprechung entwickelt.[1679] So ist ein Wettbewerb zwischen den nationalen und europäischen Gerichten entstanden, der die Bedeutung der Grundrechte im europäischen Datenschutz weiter gestärkt hat.[1680] Art. 8 Abs. 1 GRCh ist schon nach seinem Wortlaut als staatliche Schutzpflicht gestaltet (Grundrecht auf »Schutz«), nicht als Ermöglichung eines Selbstdatenschutzes. Das deutsche Konzept der informationellen Selbstbestimmung, das gewisse Parallelen zum amerikanischen Verständnis einer Kontrolle über die eigenen Daten aufweist,[1681] spielt dagegen unter Art. 7, 8 GRCh

---

[1675] Ermöglichung eigener Kontrolle: Erwägungsgründe 7, 68 S. 2. Schutz vor einem Kontrollverlust: Erwägungsgründe 75, 85 S. 1.

[1676] Siehe Kapitel 3:C.I.2.d)cc) (ab S. 97).

[1677] EGMR vom 26.03.1998 – 23224/94, *Kopp v. Switzerland*, ECLI:CE:ECHR:1998:0325JUD002322494; vom 29.06.2006 – 54934/00, *Weber and Savaria v. Germany*, ECLI:CE:ECHR:2006:0629DEC005493400; vom 04.12.2015 – 47143/06, *Zakharov v. Russia*, ECLI:CE:ECHR:2015:1204JUD004714306; vom 12.01.2016 – 37138/14, *Szabó and Vissy v. Hungary*, ECLI:CE:ECHR:2016:0112JUD003713814; vom 30.01.2020 – 50001/12, *Breyer v. Germany*, ECLI:CE:ECHR:2020:0130JUD005000112. EuGH vom 08.04.2014, *Digital Rights Ireland Ltd*, ECLI:EU:C:2014:238; vom 26.07.2017 – Gutachten 1/15, *Fluggastdatensätze*, ECLI:EU:C:2017:592; vom 06.10.2020 – C511/18, *La Quadrature du Net u. a.*, ECLI:EU:C:2020:791; vom 02.03.2021 – C-746/18, *Prokuratuur*, ECLI:EU:C:2021:152.

[1678] Eine besonders ausführliche Diskussion der Art. 7, 8 GRCh enthalten: EuGH vom 13.05.2014 – C-131/12, *Google Spain*, ECLI:EU:C:2014:317 Rn. 69–81; vom 16.07.2020, *Schrems II*, ECLI:EU:C:2020:559 Rn. 137–149, 169–174.

[1679] Für das BVerfG: BVerfG vom 15.12.1983 – 1 BvR 209/83, *Volkszählung*, BVerfGE 65, 1; vom 27.02.2008 – 1 BvR 370/07, *Online-Durchsuchungen*, BVerfGE 120, 274; vom 06.11.2019 – 1 BvR 16/13, *Recht auf Vergessen I*, NJW 2020, 300; vom 06.11.2019 – 1 BvR 276/17, *Recht auf Vergessen II*, NJW 2020, 314.

[1680] *Streinz* in: Craig/Búrca, The Evolution of EU Law, 902, 911.

[1681] Rechtsvergleichend zwischen dem amerikanischen Verständnis von Datenschutz als Privatautonomie und informationeller Selbstbestimmung: *Mahieu*, 2021 TechReg 62, 64–69, 73 f.

kaum eine Rolle.[1682] So diskutiert die Rechtsprechung des EuGH das Konzept informationelle Selbstbestimmung nicht einmal (abgesehen von einer einmaligen Erwähnung in den Schlussanträgen des Generalanwalts *Cruz Villalon).*[1683]

3. Bewertung

Der liberale Ansatz des CCPA hat gegenüber dem grundrechtsorientierten, präventiven Ansatz der DSGVO sicherlich Vorteile. Er verschafft Verbraucher:innen Freiheiten, ohne sie einzuschränken. Damit wird er eher individuellen Datenschutzpräferenzen gerecht.[1684] Zudem führt dieser Fokus auf die Privatautonomie zu einer stärkeren demokratischen Legitimation als die präskriptiven Regeln der DSGVO, die im Austausch zwischen verhältnismäßig schwach demokratisch legitimierten Aufsichtsbehörden, Rechtsprechung und rechtswissenschaftlicher Literatur konkretisiert werden. Wenn ein Verbraucher oder eine Verbraucherin aktiv Datenhandel widersprochen hat, kann ein Unternehmen kaum das resultierende Datenhandelsverbot als staatliche Bevormundung[1685] oder als »Datenpaternalismus«[1686] kritisieren – beruht dieses Verbot doch auf dem bewussten Widerspruch der Verbraucher:innen.

Auf der anderen Seite überfordert die nötige Entscheidung Verbraucher:innen häufig. Diese können kaum jedes Unternehmen selbst prüfen. Es besteht schon deshalb eine erhebliche Informationsasymmetrie, weil ein Unternehmen »seine« Verarbeitungen gut kennt, während Verbraucher:innen mit vielen Unternehmen interagieren.[1687] Auch haben Unternehmen kein Interesse, Verbraucher:innen prägnant und präzise zu informieren, sondern nutzen Handlungsspielräume der Informationspflichten zu ihren Gunsten.[1688] Desinteresse von Verbraucher:innen ist angesichts der Informationsasymmetrie und der teilweise fehlenden Handlungsalternativen durchaus rational.[1689] Der CCPA geht auf dieses Problem bis zu einem gewissen Grad ein. So ist das automatische Widerspruchssignal per

---

[1682] *Bunnenberg*, Privates Datenschutzrecht Rn. 171–175; *Lewinski*, Die Matrix des Datenschutzes, S. 43f; *Marsch*, Das europäische Datenschutzgrundrecht, S. 74–79.

[1683] Generalanwalt *Cruz Villalón*, Schlussanträge vom 12.12.2013 – C293/12, *Digital Rights Ireland Ltd*, ECLI:EU:C:2013:845 Rn. 57.

[1684] Vgl. allgemein *Bunnenberg*, Privates Datenschutzrecht, S. 318; *Hacker*, Datenprivatrecht, S. 76 f.

[1685] *Härting*, Legal Tribune Online, Trilog erfolgreich, Einwilligung tot.

[1686] Vgl. den so betitelten Aufsatz *Krönke*, Der Staat 55 (2019), 319–351; ähnlich: *Schrader*, Datenschutz Minderjähriger, S. 201–204.

[1687] *McDonald/Cranor*, 4 ISJLP 543, 560–65 mit einer Kostenschätzung des hypothetischen Lesens aller Datenschutzerklärungen; *Solove*, 126 Harv. L. Rev. 1880, 1888 f.

[1688] *Fung/Graham/Weil*, Full disclosure: the perils and promise of transparency, S. 45; *Hartzog/Richards*, 61 B.C. L. Rev. 1687, 1734 f.; *Solove*, 126 Harv. L. Rev. 1880, 1883–1885; *Waldman*, Privacy, Practice, and Performance, S. 41.

[1689] *Hartzog/Richards*, 61 B.C. L. Rev. 1687, 1734 f.; *Lewinski*, Die Matrix des Datenschutzes, S. 75; *Solove*, 126 Harv. L. Rev. 1880, 1881; *ders.*, 89 Geo. Wash. L. Rev. 1, 45 f.; *Waldman*, Privacy, Practice, and Performance, S. 41.

Browser-Einstellung ein vielversprechender Weg, der in der Praxis bereits erste Verbreitung gefunden hat.[1690] Auch der kurze Datenschutzhinweis für Verbraucher:innen ist ein vielversprechender Ansatz.[1691]

Es ist aber zweifelhaft, ob diese Mittel wirklich das rationale Desinteresse nachhaltig beseitigen können. Datenschutz betrifft inhärent komplexe Risiken. Es ist schwierig, diese soweit zu vereinfachen, dass ein Verbraucher oder eine Verbraucherin sich im Alltag wirklich informiert entscheiden kann. Viele der Datenschutzprinzipien sind für Laien schwer verständlich und stehen in Konkurrenz zueinander. So ist beispielsweise Datenminimierung zwar im Ansatz gut verständlich, da das Prinzip »so wenig Daten wie möglich« leicht nachzuvollziehen ist.[1692] Dennoch wird Datenminimierung auch bei nur mäßig komplexen, praxisrelevanten Sachverhalten schwer vermittelbar.[1693] Ist die zusätzliche Speicherung von persönlichen Informationen in einem Back-up ein Verstoß gegen die Datenminimierung?[1694] Führt die Datenminimierung zu Informationslücken, die mit Unterstellungen gefüllt werden?[1695] Damit gerät Datenminimierung in Konflikt mit der Datensicherheit (1. Frage) und der Datenrichtigkeit (2. Frage). Solche Zielkonflikte sind kaum prägnant darstellbar. Damit ist die Gefahr der Überforderung real. Für ein abschließendes Urteil über den CCPA ist es – wie bei der DSGVO, die Unternehmen vielfach noch nicht umgesetzt haben –[1696] allerdings noch zu früh.

II. Transparenz und freier Informationsfluss

Eng verbunden mit der Privatautonomie ist der freie Informationsfluss, welcher ein weiteres Kernmotiv des CCPA und tragendes Prinzip des amerikanischen Rechts darstellt. Die U. S. Constitution schützt den freien Informationsaustausch auf dem *marketplace of ideas* nahezu absolut. Jeder Bürger und jede Bürgerin soll seine Ansichten im öffentlichen Diskurs frei verbreiten können, ohne dass der Staat entscheidet, was falsch, töricht, ungerecht oder schädlich ist, sodass die beste Idee gewinne.[1697] Die beste Lösung für anstößige Äußerungen sei nicht

---

[1690] Cal. Civ. Code § 1798.135(e). Siehe Kapitel 3:C.I.2.b)cc) (ab S. 89).

[1691] Cal. Civ. Code § 1798.100(a). Siehe Kapitel 3:D.I.2.a) (ab S. 151).

[1692] Siehe Kapitel 3:D.I.2.a)bb) (ab S. 154).

[1693] *Albers*, Informationelle Selbstbestimmung, S. 553–555; *Lewinski*, Die Matrix des Datenschutzes, S. 58.

[1694] *Albers*, Informationelle Selbstbestimmung, S. 554.

[1695] Ebd., S. 554.

[1696] *Bitkom*, DS-GVO und Corona – Datenschutzherausforderungen für die Wirtschaft, S. 2: nur 57 % der Unternehmen ab 20 Beschäftigen hätten DSGVO vollständig/größtenteils umgesetzt (Stand: 2020).

[1697] Grundlegend: U. S. Supreme Court vom 09.03.1964, *New York Times Co. v. Sullivan*, 376 U. S. 254, 298 f. Diese Rechtsprechungslinie ablehnend: U. S. Supreme Court vom 27.06.2022, *Coral Ridge Ministries Media, Inc. v. S. Poverty Law Ctr.* – ablehnendes Sondervotum *Thomas*, 2022 U. S. LEXIS 3099, 3–4.

Zensur, sondern engagierte Gegenrede.[1698] Transparenz ist dementsprechend ein Grundpfeiler des amerikanischen Rechts.[1699] Schon die Verfassungsväter der U. S. Constitution betonten den hohen Wert frei verfügbarer Informationen für den öffentlichen Diskurs. So fasst der primäre Autor der Bill of Rights[1700] *James Madison* diesen Gedanken wie folgt prägnant zusammen: »A popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or, perhaps both. Knowledge will forever govern ignorance: And a people who mean to be their own Governors, must arm themselves with the power which knowledge gives.«[1701]

Dementsprechend zieht sich das Grundprinzip Transparenz durch den gesamten CCPA. Die Informationspflichten sind umfangreich ausgeprägt und berücksichtigen explizit auch den Wert von Datenschutzinformationen für den öffentlichen Diskurs. Insbesondere die umfassende Datenschutzerklärung bietet einen zentralen Informationsfundus für Presse, Interessengruppen, akademische Forschung und Aufsichtsbehörden.[1702] Die bei besonders großen Unternehmen in ihr enthaltene Verbraucherrechte-Statistik ermöglicht eine öffentliche Kontrolle. Das Auskunftsrecht ist zudem sehr detailliert ausgestaltet und ermöglicht, zielgerichtet weitere Informationen über die Datenverarbeitung eines Unternehmens zu erlangen.[1703] Stärker als unter der DSGVO setzt sich die Transparenz auch bei den Aufsichtsbehörden fort. Die California Privacy Protection Agency veröffentlicht jeden ihrer Bußgeldbescheide[1704] und trifft ihre Beschlüsse in öffentlicher Sitzung.[1705] Ihre Durchführungsverordnung entsteht in einem transparenten Verfahren, in dem sie nicht nur der Öffentlichkeit Gelegenheit zur Stellungnahme geben, sondern auf jede Stellungnahme öffentlich antworten muss.[1706]

Andererseits schränkt die Bedeutung des freien Informationsflusses den CCPA wiederum ein. Dies ist zwar dem Gesetzgeber des CCPA an manchen Stellen ersichtlich unrecht. Die hohe Stellung der Meinungsfreiheit zwingt ihn aber zu entsprechenden Einschränkungen. So hatte die Bürgerinitiative Californians for Consumer Privacy im Rahmen des ersten Volksbegehrens anfangs einen *opt-in*-Mechanismus für Datenhandel geplant, sich wegen des Risikos der Verfassungswidrigkeit aber für einen *opt-out*-Mechanismus entschieden.[1707] Am stärksten zeigt sich der Einfluss der Meinungsfreiheit bei der pauschalen Ausnahme für Informationen

---

[1698] U. S. Supreme Court vom 16.05.1927, *Whitney v. Cal.* – ablehnendes Sondervotum *Brandeis*, 274 U. S. 357, 377; vom 28.06.2012, *United States v. Alvarez*, 567 U. S. 709, 727 f.

[1699] *Fung/Graham/Weil*, Full disclosure: the perils and promise of transparency, S. 19–34; *Kwoka*, 127 Yale L. J. 2204, 2211.

[1700] U. S. Const. amend. I–X (der Grundrechtsteil der U. S. Const.).

[1701] *Madison*, Letter to W. T. Barry. Mad. Mss., S. 1.

[1702] Siehe Kapitel 3:D.I.2.b) (ab S. 155).

[1703] Siehe Kapitel 3:C.III.1.a) (ab S. 116).

[1704] Cal. Civ. Code § 1798.155(a) i. V. m. Cal. Gov. Code § 11517(d).

[1705] Cal. Gov. Code § 11123(a).

[1706] Cal. Gov. Code § 11340–11361. Siehe Kapitel 3:E.I.2.c) (ab S. 187).

[1707] Siehe Kapitel 3:C.I.1 (ab S. 81).

von öffentlichem Interesse und für öffentliche frei verfügbare Informationen.[1708] Diese dem *marketplace of ideas* zu entziehen, ist mit dem amerikanischen Verständnis von Meinungsfreiheit unvereinbar. Daher kennt der CCPA auch kein Recht auf Vergessenwerden, sondern nur ein stark begrenztes Recht auf Löschung.[1709]

Die DSGVO enthält zwar einzelne Elemente von Transparenz wie die Informationspflichten der Art. 13, 14 DSGVO, den Auskunftsanspruch des Art. 15 DSGVO und die Tätigkeitsberichte der Aufsichtsbehörden (Art. 59 DSGVO). Diese sind aber nicht so umfassend wie die Transparenz unter dem CCPA.[1710] So sind die Informationspflichten des Art. 13, 14 DSGVO weniger ausdifferenziert als der kurze Datenschutzhinweis für Verbraucher:innen und die umfassende Datenschutzerklärung für die Öffentlichkeit als Ganzes.[1711] Auch ist ein jährlicher Tätigkeitsbericht nicht mit der Veröffentlichung sämtlicher Bußgeldbescheide und den öffentlichen Sitzungen der California Privacy Protection Agency vergleichbar.[1712] Ein freier Informationsfluss hat in europäischem Recht keine so herausragende Rolle wie im amerikanischen Rechtssystem. Dementsprechend nimmt die DSGVO zwar in einzelnen Vorschriften auf die Meinungsfreiheit Rücksicht, sieht diese aber durchaus als einer Abwägung zugänglich.[1713]

III. Exakte, aber fehlerreiche Regelungstechnik

Der CCPA übernimmt viele Formulierungen aus anderen Gesetzen wortwörtlich. Teilweise sind diese in den Gesetzestext des CCPA gut integriert, teilweise aber auch nicht. So lehnt sich beispielsweise die Vorschrift des CCPA zur Schadensersatzhöhe[1714] an die Zumessungsvorschrift für die *civil penalties* des kalifornischen Unfair Competition Laws[1715] an, passt diese jedoch nicht an die Nomenklatur des CCPA an.[1716] Auch die Vorschriften über den Aufbau der California Privacy Protection Agency lehnen sich eng an den entsprechenden Vorschriften über die California Fair Political Practices Commission und die europäischen Aufsichtsbehörden an.[1717] Diese Gesetzgebung nach dem »*copy-and-paste*-Verfahren« ist wohl auf die Herkunft des CCPA als Volksbegehren einer kleinen Bürgerinitiative zurückzuführen.

Der CCPA weist zudem viele widersprüchliche und unklare Passagen auf. Zum Beispiel regeln Cal. Civ. Code § 1798.155(b) und Cal. Civ. Code § 1798.160(a)

[1708] Cal. Civ. Code § 1798.140(v)(2). Siehe Kapitel 3:B.I.3 (ab S. 50).

[1709] Cal. Civ. Code § 1798.105. Siehe Kapitel 3:C.IV (ab S. 134).

[1710] A. A. wohl: *Chander/Kaminski/McGeveran*, 105 Minn. L. Rev. 1733, 1750–51: »Another similarity between the GDPR and the CCPA is the central role of transparency«.

[1711] Siehe Kapitel 3:D.I.2.c) (ab S. 160).

[1712] Siehe Kapitel 3:E.I.5 (ab S. 200).

[1713] Insbesondere zu Art. 17 DSGVO siehe Kapitel 3:C.IV.1.c) (ab S. 139).

[1714] Cal. Civ. Code § 1798.150(a)(2).

[1715] Cal. Bus. Prof. Code § 17206(b).

[1716] Siehe Kapitel 3:E.II.2.b) (ab S. 211).

[1717] Siehe Kapitel 3:E.I.2.a) (ab S. 182).

die Kostenerstattung aus dem Consumer Privacy Fund und folgen unmittelbar aufeinander. Dennoch widersprechen sie sich direkt, da nach Cal. Civ. Code § 1798.155(b) die Kosten der California Privacy Protection Agency, des Attorney General und der kalifornischen Gerichte zu erstatten sind, während Cal. Civ. Code § 1798.160(a) nur noch die Kosten des Attorney General und der kalifornischen Gerichte erwähnt.[1718] Auch die Legaldefinition von »sharing« als Weiterübermittlung an Dritte ausschließlich für bestimmte Werbezwecke ist nur schwer verständlich.[1719] Selbst der Gesetzgeber des CCPA wollte in der Unternehmensdefinition »sharing« offensichtlich in dem allgemein üblichen Sprachgebrauch »Weiterübermittlung für einen beliebigen Zweck« verwenden.[1720]

Auch viele amerikanische Rechtswissenschaftler:innen sehen die Vielzahl an Redaktionsfehlern und Unklarheiten kritisch.[1721] Diese handwerklichen Fehler sind wohl darauf zurückzuführen, dass der CCPA-2018 auf Basis eines Volksbegehrens in einem schnellen Gesetzgebungsverfahren und Proposition 24 ebenfalls als Volksbegehren in einer Verhandlung entstanden ist.[1722] Volksbegehren führen angesichts mangelnder Erfahrung in der Erstellung von Gesetzesentwürfen häufiger zu Redaktionsfehlern.[1723] Bezeichnenderweise gibt es ersichtlich keine Kritik an dem unsystematischen Aufbau des CCPA – was nahelegt, dass Systematik im amerikanischen Recht ein geringerer Wert eingeräumt wird.[1724]

Gleichzeitig ist der CCPA an vielen Stellen sehr exakt.[1725] Die Definition persönlicher Informationen beinhaltet 137 Regelbeispiele.[1726] Das Verfahren zur Identifizierung bei Auskunfts-, Löschungs- und Berichtigungsanträgen ist zudem in erschöpfender Detailtiefe geregelt.[1727] Selbst der Wortlaut des Widerspruchslinks ist als »Do not sell or share my personal information« exakt vorgegeben.[1728]

Diese spezifische Regelungstechnik ist eher typisch für das amerikanische Recht als die handwerklichen Unzulänglichkeiten des CCPA. Zwar sind amerikanische Gesetze tendenziell weniger systematisch aufgebaut als im deutschen oder europäischen Recht, zeichnen sich jedoch häufig durch präzise Regelungen aus, um

---

[1718] Siehe Kapitel 3:E.I.2.b) (ab S. 186).

[1719] Cal. Civ. Code § 1798.140(ah)(1). Siehe Kapitel 3:C.I.2.a) (ab S. 82).

[1720] Cal. Civ. Code § 1798.140(d)(2). Siehe Kapitel 3:B.II.2.c) (ab S. 62).

[1721] *Ballon*, E-commerce & Internet law, S. 26-423; *Brennan et al.*, HL Chronicle of Data Protection, California Consumer Privacy Act; *Gregg*, 60 Orange County Lawyer 32, 34; *Hess*, 47 Ecology L. Currents 233, 245–248; *Harris*, 54 Loy. L.A. L. Rev. 197; 219 f.; *Hintze*, 14 Wash. J.L. Tech. & Arts 103, 128; *Kress/Trifon*, JD Supra, CCPA's Private Right of Action; *Li*, 32 Loy. Consumer L. Rev. 177, 179; *Rose*, 15 Brook. J. Corp. Fin. & Com. L. 521, 524; *Yallen*, 53 Loy. L.A. L. Rev. 787, 819.

[1722] Siehe Kapitel 2:C (ab S. 30).

[1723] *Kelso*, 19 Pepp. L. Rev. 327, 339.

[1724] Zu dem Aufbau siehe Kapitel 3:A (ab S. 41).

[1725] Ebenso zum CCPA-2018: *Chander/Kaminski/McGeveran*, 105 Minn. L. Rev. 1733, 1760.

[1726] Cal. Civ. Code § 1798.140(v)(1)(A)–(L) mit den Verweisen auf andere Legaldefinitonen, siehe Kapitel 3:B.I.1.a) (ab S. 43).

[1727] Siehe Kapitel 3:C.III.2.a) (ab S. 125).

[1728] Cal. Civ. Code § 1798.135(a)(1).

keine Regelungslücken zu lassen.[1729] Hier wirkt sich die streng wortlautorientierte Auslegung aus, die das amerikanische Recht kennzeichnet. Der Wortlaut ist zugleich Ausgangs- und Endpunkt der Auslegung, wenn er hinreichend klar ist.[1730] Gesetzesauslegung prägt Gesetzgebung. Daher müssen amerikanische Gesetze sehr spezifisch sein, um ihre Ziele zu erreichen.

Der EuGH legt das Europarecht demgegenüber stark am *teleos* orientiert aus.[1731] Dementsprechend ist die DSGVO sehr offen und abstrakt formuliert (dies mag zum Teil auch darauf zurückzuführen sein, dass sie teilweise unverändert die DSRL übernimmt).[1732] Jedenfalls kann der EuGH und die europäische Rechtswissenschaft solche Unklarheiten durch teleologische Auslegung wohlwollend im Sinne des Gesetzgebers auflösen. Der kalifornische Gesetzgeber muss sich dagegen bereits im Wortlaut festlegen. Dementsprechend entwickeln amerikanische Rechtswissenschaftler:innen als Reaktion auf die Redaktionsfehler des CCPA nicht eine Lösung durch Auslegung, sondern fordern eine Korrektur durch das kalifornische Parlament.[1733]

IV. Oberflächlicher Einfluss der DSGVO

Auch die DSGVO benutzt der Gesetzgeber des CCPA als Fundus an Formulierungen. So übernimmt er in seiner Definition sensibler Informationen Teile der Definition besonderer Kategorien personenbezogener Daten des Art. 9 Abs. 1 DSGVO.[1734] Ebenso erinnert die Unternehmensdefinition an die Verantwortlichendefinition des Art. 4 Nr. 7 DSGVO, da sie ebenfalls auf das Bestimmen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten abstellt.[1735] In beiden Fällen übernimmt der CCPA die Definition aber nicht »eins zu eins«, sondern passt sie deutlich an. Sensible Informationen umfassen nicht die in den Vereinigten Staaten als unsensibel geltenden politischen Ansichten, während aber Identitätsdiebstahl ermöglichende Informationen erfasst sind.[1736] Der Begriff des Unternehmens ist deutlich enger als der des Verantwortlichen, da er nur profitorientierte Gesellschaften einer gewissen Größe erfasst.[1737]

Der CCPA übernimmt zudem punktuell einzelne Regelungen, soweit sie zu seiner Regelungsphilosophie passen. Die Erwägungsgründe der Proposition 24 sprechen davon, dass der CCPA soweit möglich mit Datenschutzgesetzen anderer Rechtsordnungen kompatibel sein soll, um Unternehmen die Umsetzung

---

[1729] Cal. Civ. Code § 1798.135(a)(1).

[1730] Siehe Kapitel 3:B.I.1.a) (ab S. 43).

[1731] *Gaitanides* in: Groeben/Schwarze/Hatje, Europäisches Unionsrecht, EUV Art. 19 Rn. 42–45.

[1732] *Hornung/Spiecker gen. Döhmann* in: NK-DatenschutzR, Einl. Rn. 250 f.

[1733] *Guzzetta*, 61 Orange County Lawyer 28, 33; *Hintze*, 14 Wash. J.L. Tech. & Arts 103, 128.

[1734] Cal. Civ. Code § 1798.140(ae).

[1735] Cal. Civ. Code § 1798.140(d)(1).

[1736] Cal. Civ. Code § 1798.140(ae). Siehe Kapitel 3:C.II.1.a) (ab S. 109).

[1737] Cal. Civ. Code § 1798.140(d)(1). Siehe Kapitel 3:B.II.2 (ab S. 56).

zu erleichtern.[1738] Viele große Unternehmen wollen möglichst ein einheitliches Datenschutzprogramm weltweit nutzen, um Kosten zu sparen.[1739] Daher übernehmen sie häufig die strenge Verbraucherschutzregulierung der EU weltweit. Dieser »Brüssel-Effekt« ist im Datenschutzrecht besonders ausgeprägt, weil die DSGVO und vor ihr die DSRL einen weiten räumlichen Anwendungsbereich haben und eine Trennung nach Regionen in der digitalen Welt schwieriger als in der analogen Welt ist.[1740] Dementsprechend geben 83 % der befragten internen Datenschutzbeauftragten für amerikanische Unternehmen in einer Umfrage der International Association of Privacy Professionals an, dass auch die Umsetzung der DSGVO zu ihren Aufgaben gehört.[1741] Manche Unternehmen lobbyieren sogar für eine weitgehende Übernahme der DSGVO in den Vereinigten Staaten.[1742]

Daher ist der CCPA auf der Umsetzungsebene weitgehend kompatibel mit der DSGVO. Diese Art des Einflusses der DSGVO zeigt sich besonders stark daran, dass die Durchführungsverordnung den geplanten zweistufigen Löschprozess für optional erklärt hatte. Grund hierfür war, dass Unternehmen sonst einen Verstoß gegen das Erleichterungsgebot des Art. 12 Abs. 2 DSGVO bei ihrem gemeinsamen Löschprozess befürchtet hatten.[1743] Zwar ist das Recht auf Löschung wesentlich schwächer ausgestaltet, weil öffentliche oder von Dritten erhaltene persönliche Informationen ausgenommen sind.[1744] Dies »stört« jedoch Unternehmen nicht, die den gleichen Prozess für Löschanfragen verwenden wollen, da sie im Zweifel dem umfassenderen Tatbestand des Recht auf Löschung der DSGVO folgen.

Weiterhin hat ein möglicher Angemessenheitsbeschluss die Unternehmenspflichten des CCPA beeinflusst. Einen solchen zu erreichen, war erklärtes Ziel der Proposition 24. Dabei hat dieses Volksbegehren offensichtlich die Referenzgrundlage Angemessenheit der Artikel-29-Datenschutzgruppe als »Checkliste« abgearbeitet. Dementsprechend sind die übernommenen Unternehmenspflichten Zweckbindung, Datenminimierung, Speicherfristbegrenzung und die Absicherung bei internationalen Weiterübermittlungen nur gering ausgeprägt.[1745] Wesentlich umfangreicher geregelt sind die Informationspflichten des CCPA, welche die Transparenz als wichtigen *topos* des amerikanischen Rechtes verwirklichen.[1746]

[1738] Proposition 24 (Cal. 2020), Sec. 3(C)(8).

[1739] *IAPP/EY*, IAPP-EY Annual Privacy Governance Report 2021, S. 3.

[1740] *Bradford*, 107 Nw. U. L. Rev. 1, 22–26; *Chander/Kaminski/McGeveran*, 105 Minn. L. Rev. 1733, 1765–1767; *Gunst/De Ville*, Eur. Foreign Aff. Rev. 26 (2021), 437, 447 f.; *Hennemann*, RabelsZ 84 (2020), 864, 875–877; *Humerick*, 27 Cath. U. J. L. & Tech. 77, 107 f.; *Schwartz*, 94 N. Y. U. L. Rev. 771, 809–818; *Streinz, T.* in: Craig/Búrca, The Evolution of EU Law, 902, 923–926.

[1741] *IAPP/EY*, IAPP-EY Annual Privacy Governance Report 2021, S. 48.

[1742] *Hamilton*, Business Insider, Microsoft CEO Satya Nadella Praises GDPR, Calls for Similar Laws Around the World.

[1743] Siehe Kapitel 3:C.IV.2 (ab S. 141).

[1744] Siehe Kapitel 3:C.IV.1 (ab S. 134).

[1745] Siehe Kapitel 3:D.VI.4 (ab S. 180).

[1746] Siehe Kapitel 3:D.I (ab S. 150).

Auch sonst übernimmt der CCPA Vorschriften der DSGVO nur, soweit sie mit amerikanischen Vorstellungen vereinbar sind. So ist die unabhängige Datenschutzbehörde California Privacy Protection Agency den Aufsichtsbehörden der DSGVO nachgebildet.[1747] Allerdings sind unabhängige Behörden auch in den Vereinigten Staaten weit verbreitet, und die Leitung der California Privacy Protection Agency durch eine Kommission ist typisch für das amerikanische Recht, während die Aufsichtsbehörden der DSGVO eher durch eine Einzelperson geleitet werden. Auch ist die California Privacy Protection Agency nicht wie die europäischen Aufsichtsbehörden alleinig zuständig *(One-Stop-Shop)*, sondern teilt ihre Zuständigkeit mit dem Attorney General und 58 District Attorneys sowie 4 City Attorneys.

Viele der an die DSGVO erinnernden Verbraucherrechte und Unternehmenspflichten haben zudem deutliche Vorläufer im amerikanischen Recht. Transparenz, Zweckbindung, Datensicherheit und Datenrichtigkeit waren schon 1973 Teil der einflussreichen »fair information practice principles« des U. S. Department of Health, Education & Welfare.[1748] Das Recht auf Auskunft ist zudem auf die starke amerikanische Tradition der Transparenz zurückzuführen und verallgemeinert bereits bestehende spezifische Auskunftsansprüche.[1749]

Dagegen ist der Einfluss der DSGVO eher oberflächlich und punktuell. Der CCPA ist tief in der Regelungsphilosophie des amerikanischen Rechts verwurzelt. Aus europäischer Sicht mögen viele Prinzipien, Rechte und Pflichten ähnlich klingen – allerdings ist dies häufig eher auf gemeinsame Vorläufer und parallele Entwicklungen zurückzuführen.[1750] Der CCPA will nicht ohne Grund inkompatibel mit der DSGVO sein, die auch viele amerikanische Unternehmen befolgen. Zudem ist ein potenzieller Angemessenheitsbeschluss ein Anlass, für den CCPA punktuell Unternehmenspflichten zu übernehmen. Viele Vorschriften sind allerdings nur deshalb ähnlich, weil der CCPA einzelne Formulierungen übernommen hat, ohne sich diesen inhaltlich vollends anzuschließen.

[1747] Siehe Kapitel 3:E.I.2.a) (ab S. 182).

[1748] *U. S. Department of Health, Education & Welfare*, Records, Computers and the Rights of Citizens, S. 41.

[1749] Siehe Kapitel 3:C.III.1.a) (ab S. 116).

[1750] Ebenso zum CCPA-2018: *Botta*, PinG 2019, 261, 265; *Chander/Kaminski/McGeveran*, 105 Minn. L. Rev. 1733, 1755.

Kapitel 4

Schlussfolgerungen aus der Analyse für das europäische Datenschutzrecht

A. Angemessenheitsbeschluss für Kalifornien?

I. Maßstab der Angemessenheit

Erklärtes Ziel von Proposition 24 war, einen Angemessenheitsbeschluss zu erreichen.[1] Auch der Referatsleiter für Internationale Datenströme der Europäischen Kommission Bruno Gencarelli hat informell bereits Interesse an einem Angemessenheits-Dialog mit Kalifornien bekundet.[2] Einen Angemessenheitsbeschluss für ein Gebiet in einem Drittstaat lässt Art. 45 Abs. 1 S. 1 DSGVO dabei explizit zu, wenn das Schutzniveau für personenbezogene Daten in diesem Gebiet angemessen ist.

Ein Schutzniveau ist angemessen, wenn es insgesamt »der Sache nach gleichwertig« mit dem Schutzniveau der DSGVO ist (Erwägungsgrund 104 S. 3 der DSGVO).[3] Dabei kann sich die Art und Weise der jeweiligen Datenschutzregeln unterscheiden, solange im Ergebnis Gleichwertigkeit erreicht wird.[4] Insofern gilt es, ein pragmatisches Gleichgewicht zwischen der Rücksicht auf fremde Rechtsordnungen und der notwendigen Bekräftigung der Grundrechte aus Art. 7, 8 GRCh zu finden.[5]

Art. 45 Abs. 2 DSGVO enthält hierfür nicht abschließende (»insbesondere«)[6] Kriterien. So sind gemäß Art. 45 Abs. 2 lit. a DSGVO rechtsstaatliche Grundsätze und das jeweilige Datenschutzrecht, auch in Bezug auf den Zugang von

---

[1] *Angwin*, The Markup, Tech on the Ballot: Interview with Ashkan Soltani; *Bracy*, Alastair Mactaggart on California's Prop 24, 43m:00s; *Californians for Consumer Privacy*, Prop 24 Webinar, 13m:00s; *Kohne/Reed/Kurzweil*, Law360, Calif. Privacy Law Resembles, Transcends EU Data Regulation.

[2] Vgl. die wiedergegebene Aussage in: *Manacourt*, Twitter-Beitrag vom 27.10.2020.

[3] EuGH vom 06.10.2015 – C-362/14, *Schrems I*, ECLI:EU:C:2015:650 Rn. 73; EuGH vom 16.07.2020, *Schrems II*, ECLI:EU:C:2020:559 Rn. 178.

[4] EuGH vom 06.10.2015 – C-362/14, *Schrems I*, ECLI:EU:C:2015:650 Rn. 74; Generalanwalt *Saugmandsgaard Øe*, Schlussanträge vom 19.12.2018, *Schrems II*, ECLI:EU:C:2019:1145 Rn. 118.

[5] Generalanwalt *Saugmandsgaard Øe*, Schlussanträge vom 19.12.2018, *Schrems II*, ECLI:EU:C:2019:1145 Rn. 5; *Hennemann*, RabelsZ 84 (2020), 864, 889.

[6] *Beck* in: BeckOK DatenschutzR, DS-GVO Art. 45 Rn. 20; *Bussche* in: Plath, DSGVO Art. 45 Rn. 5; *Pauly* in: Paal/Pauly, DS-GVO Art. 45 Rn. 4.

Behörden zu personenbezogenen Daten, und wirksame Rechtsbehelfe der betroffenen Personen zu berücksichtigen. Art. 45 Abs. 2 lit. b DSGVO nennt weiterhin die wirksame Funktionsweise unabhängiger Aufsichtsbehörden in dem jeweiligen Drittland. Außerdem sind gemäß Art. 45 Abs. 2 lit. c DSGVO die internationalen Verpflichtungen des jeweiligen Drittlandes relevant.

Die Rechtsprechung des EuGH konkretisiert den Gleichwertigkeitsmaßstab weiter. So genügt eine Selbstzertifizierung wie das Safe-Harbor- oder Privacy-Shield-System bei wirksamen Überwachungs- und Kontrollmechanismen grundsätzlich für ein angemessenes Schutzniveau.[7] Solche Selbstzertifizierungsprogramme erfassen allerdings nicht den Zugang von Sicherheitsbehörden zu personenbezogenen Daten, weshalb insoweit ein zusätzlicher Schutz erforderlich ist.[8] Ein formelles Gesetz muss den Umfang eines solchen Zugangs präzise festlegen, diesen auf das nötige Minimum reduzieren und ausreichend rechtsstaatliche Garantie vorsehen.[9] Eine zwingend erforderliche rechtsstaatliche Mindestgarantie ist dabei insbesondere die Möglichkeit für die betroffene Person, einen wirksamen Rechtsbehelf vor einem unabhängigen Gericht einzulegen.[10]

Die »Referenzgrundlage Angemessenheit« der Artikel-29-Datenschutzgruppe ist eine weitere wichtige Auslegungshilfe.[11] Sie enthält eine Art »Checkliste« von 20 Grundsätzen für ein angemessenes Datenschutzniveau und hilft die Anforderungen an Angemessenheit zu konkretisieren, ist allerdings zum Teil übermäßig präskriptiv formuliert.[12] So müssten nach der Referenzgrundlage selbst die verwendeten Begriffe und Rollen die DSGVO »widerspiegeln und mit dieser im Einklang stehen«.[13] Die explizit in der Referenzgrundlage genannten Begriffe »Verarbeitung« und »Auftragsverarbeiter« sind nicht das absolute Minimum für eine Datenschutzregulierung. Vielmehr ist genauso eine andere Nomenklatur oder Rollenverteilung denkbar. Einen solch strengen Maßstab könnten Drittstaaten faktisch nur durch eine vollständige und exakte Kopie der DSGVO erreichen, wobei allerdings auch die Artikel-29-Datenschutzgruppe ersichtlich keine so starre Prüfung intendiert.[14] Vielmehr ist die Referenzgrundlage ex-

[7] EuGH vom 06.10.2015 – C-362/14, *Schrems I*, ECLI:EU:C:2015:650 Rn. 81.

[8] EuGH vom 06.10.2015 – C-362/14, *Schrems I*, ECLI:EU:C:2015:650 Rn. 87; vom 16.07.2020, *Schrems II, ECLI:EU:C:2020:559* Rn. 176 f.

[9] EuGH vom 06.10.2015 – C-362/14, *Schrems I*, ECLI:EU:C:2015:650 Rn. 91; vom 16.07.2020, *Schrems II, ECLI:EU:C:2020:559* Rn. 176 f.; a. A. *Brauneck*, EuZW 2020, 933, 936 f.; *Lejeune*, CR 2020, 716, Rn. 4–13.

[10] EuGH vom 06.10.2015 – C-362/14, *Schrems I*, ECLI:EU:C:2015:650 Rn. 95; vom 16.07.2020, *Schrems II*, ECLI:EU:C:2020:559 Rn. 186, 187.

[11] *Artikel-29-Datenschutzgruppe*, WP 254 Angemessenheit; später bestätigt durch *EDSA*, Endorsement 1/2018.

[12] *Hennemann*, RabelsZ 84 (2020), 864, 888.

[13] *Artikel-29-Datenschutzgruppe*, WP 254 Angemessenheit, S. 5.

[14] A. A. wohl *Hennemann*, RabelsZ 84 (2020), 864, 888: Engführung intendiert.

plizit nur eine »Orientierungshilfe«,[15] welche die »Kernanforderungen«[16] des europäischen Datenschutzrechts abbilden soll. Der Drittstaat muss nur in der Praxis ein Ergebnis erzielen, das mit diesen Orientierungspunkten in der Praxis gleichwertig ist.[17]

Damit ist Art. 45 DSGVO ein Auftrag zur funktionalen Rechtsvergleichung.[18] Der Gleichwertigkeitsmaßstab soll dabei flexibel auch unterschiedlichen Rechtskulturen gerecht werden.[19] Zentral ist aber, dass das hohe Datenschutzniveau der EU gewahrt bleibt.[20]

Erreicht Kalifornien dieses hohe Datenschutzniveau? Bei der Beantwortung dieser Frage ist es sinnvoll, den drei Kategorien der Artikel-29-Datenschutzgruppe zu folgen:[21] die Angemessenheit des materiellen Datenschutzrechts (II), dessen Umsetzung durch Aufsichtsbehörden, private Klagen und Vorgaben für die Datenschutzorganisation (III) sowie der Zugang nationaler Sicherheitsbehörden zu personenbezogenen Daten (IV). Anschließend ist das kalifornische Datenschutzniveau in einer Gesamtbetrachtung zu bewerten (V).

II. Materielles Datenschutzrecht

Bereits der enge Anwendungsbereich des CCPA ist problematisch. Er verpflichtet nur gewinnorientierte Gesellschaften ab einer gewissen Größe (Unternehmen)[22] und schützt nur Personen mit Wohnsitz oder gewöhnlichen Aufenthalt in Kalifornien (Verbraucher:innen).[23] Die enge Unternehmensdefinition lässt sich noch durch eine entsprechende Einschränkung des Angemessenheitsbeschlusses auffangen. Einen solchen eingeschränkten Angemessenheitsbeschluss, der an den Anwendungsbereich bestimmter drittstaatlicher Rechtsnormen anknüpft, lässt Erwägungsgrund 104 S. 2 der DSGVO ausdrücklich zu. So erfassen auch die Angemessenheitsbeschlüsse für Kanada, die Färöer und Japan nur Datenimporteure, auf die das jeweilige Datenschutzgesetz anwendbar ist.[24] Hinsichtlich des Verbraucherbegriffs ist eine solche Einschränkung

---

[15] *Artikel-29-Datenschutzgruppe*, WP 254 Angemessenheit, S. 1.

[16] *Artikel-29-Datenschutzgruppe*, WP 254 Angemessenheit, S. 3.

[17] *Vgl. EDSA*, Opinion 14/2021 United Kingdom, Rn. 47: »the objective is not to mirror point by point the European legislation, but to establish the essential and core requirements of the legislation under examination«.

[18] *Botta*, CR 2020, 82 Rn. 14; *Hennemann*, RabelsZ 84 (2020), 864, 890–892.

[19] Generalanwalt *Saugmandsgaard Øe*, Schlussanträge vom 19.12.2018, *Schrems II*, ECLI:EU:C:2019:1145 Rn. 249; *Botta*, CR 2020, 82 Rn. 15; *Hennemann*, RabelsZ 84 (2020), 864, 891.

[20] Generalanwalt *Saugmandsgaard Øe*, Schlussanträge vom 19.12.2018, *Schrems II*, ECLI:EU:C:2019:1145 Rn. 249.

[21] *Artikel-29-Datenschutzgruppe*, WP 254 Angemessenheit, S. 6.

[22] Cal. Civ. Code § 1798.140(d). Siehe Kapitel 3:B.II.2 (ab S. 56).

[23] Cal. Civ. Code § 1798.140(i). Siehe Kapitel 3:B.II.1 (ab S. 56).

[24] Art. 1 Entscheidung 2002/2/EG der Kommission vom 20. Dezember 2001 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit

auf den Anwendungsbereich des CCPA *de lege lata* jedoch praktisch wertlos, da sich Personen mit Wohnsitz oder gewöhnlichem Aufenthalt in Kalifornien typischerweise nicht in Europa aufhalten.[25]

Ausreichend sind dagegen die Verbraucherrechte des CCPA. Zu den wesentlichen Rechten auf Auskunft, Berichtigung und Löschung der betroffenen Person besteht jeweils ein Äquivalent im CCPA, die abgesehen von rechtskulturellen Unterschieden ähnlich umfassend wie die entsprechenden Rechte der DSGVO sind.[26] Die größere Rolle der Meinungsfreiheit, die im engen Recht auf Löschung des CCPA zum Ausdruck kommt, ist nicht negativ zu werten, da der CCPA dennoch die für die Praxis relevanteren Speicherfristen regelt.[27] Das Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und das Widerspruchsrecht gegen Profiling gemäß Art. 22 Abs. 1 DSGVO haben dagegen bisher noch keine Entsprechung im CCPA.[28] Sie sind jedoch als praktisch weniger relevante Rechte kein Teil der Kernanforderungen des europäischen Datenschutzrechts.[29]

Die Unternehmenspflichten ähneln der DSGVO, auch weil der Gesetzgeber des CCPA die »Referenzgrundlage Angemessenheit« der Artikel-29-Datenschutzgruppe als »Checkliste« für die Unternehmenspflichten verwandte.[30] Sie weichen in zwei Aspekten deutlich voneinander ab: bei internationalen Datentransfers und bei dem fehlenden Prinzip der Rechtmäßigkeit.

Für internationale Datentransfers verfolgt der CCPA eine Vertragslösung: Unternehmen müssen mit allen Empfänger:innen einen Weiterübermittlungsvertrag abschließen. Die Artikel-29-Datenschutzgruppe fordert insoweit keine Übernahme des Regelungskonzepts der Art. 44–50 DSGVO, sondern nur, dass die Weiterübermittlung »Vorschriften (einschließlich vertraglichen Bestimmungen)«

---

des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet, ABl. 2002 L 2, 13;

Art. 1 Beschluss 2010/146/EU der Kommission vom 5. März 2010 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus, den das färöische Gesetz über die Verarbeitung personenbezogener Daten bietet, ABl. 2010 L 58, 17;

Art. 1 Abs. 1 Durchführungsbeschluss (EU) 2019/419 der Kommission vom 23. Januar 2019 nach der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Japan im Rahmen des Gesetzes über den Schutz personenbezogener Informationen, ABl. 2019 L 76, 1.

[25] Ebenso: *Flor*, 96 Notre Dame L. Rev. 2035, 2057; *Greenleaf*, California's CCPA 2.0, S. 3.

[26] Cal. Civ. Code §§ 1798.105, 1798.106, 1798.110, 1798.115. Zum Recht auf Auskunft siehe Kapitel 3:C.III (ab S. 116). Zum Recht auf Berichtigung siehe Kapitel 3:C.V (ab S. 145). Zum Recht auf Löschung siehe Kapitel 3:C.IV (ab S. 134).

[27] Cal. Civ. Code § 1798.100(a)(3). Siehe Kapitel 3:D.III (ab S. 169).

[28] Cal. Civ. Code § 1798.185(a)(16) ermächtigt California Privacy Protection Agency, »access and opt-out rights with respect to businesses' use of automated decisionmaking technology«. Zu diesem unklaren Wortlaut siehe Kapitel 3:E.I.2.c) (ab S. 187).

[29] Vgl. *Artikel-29-Datenschutzgruppe*, WP 254 Angemessenheit, S. 6 f.: nennt ebenfalls diese beiden Rechte nicht.

[30] Siehe Kapitel 3:D.VI.4 (ab S. 180).

unterliegt, welche das Schutzniveau weiter gewährleisten. Der weitere Empfänger soll zudem nach der Rechtsordnung des Drittlands die personenbezogenen Daten nur für festgelegte und begrenzte Zwecke nutzen dürfen.[31] Diesen Anforderungen genügt der Weiterübermittlungsvertrag des CCPA, welcher Empfänger:innen verpflichtet, die empfangenen Daten nur für festgelegte und begrenzte Zwecke zu nutzen und die Anforderungen des CCPA zu beachten.[32] Insoweit ist zu beobachten, ob sich die *transfer impact assessments* tatsächlich in der europäischen Rechtspraxis durchsetzen und so das europäische Datenschutzniveau erhöhen.[33]

Schließlich fehlt im kalifornischen Recht das Prinzip der Rechtmäßigkeit des Art. 5 Abs. 1 lit. a Alt. 1, 6 Abs. 1 DSGVO. Kann ein Rechtssystem gleichwertig sein, das dieses zentrale Prinzip der DSGVO nicht kennt? Entscheidend für die Beantwortung dieser Frage ist, wie das Rechtmäßigkeitsprinzip in der europäischen Rechtspraxis tatsächlich funktioniert. Art. 6 DSGVO sieht verschiedene Rechtsgrundlagen vor, von denen zwei (Art. 6 Abs. 1 S. 1 lit. a, b DSGVO) auf privatautonomen Entscheidungen der betroffenen Personen beruhen, während vier heteronome Entscheidungen (Art. 6 Abs. 1 S. 1 lit. c–f DSGVO) ausdrücken.[34] Die Anforderungen der Art. 6 Abs. 1 S. 1 lit. a, b DSGVO ähneln dem Schutz durch den CCPA, der umfangreiche Informationspflichten und Widerspruchsrechte vorsieht.[35] Auch die Definition der Einwilligung im CCPA ähnelt dem Einwilligungsbegriff der DSGVO stark.[36] Zu Art. 6 Abs. 1 S. 1 lit. c, d DSGVO bestehen vergleichbare Bereichsausnahmen unter dem CCPA.[37] Art. 6 Abs. 1 S. 1 lit. e DSGVO ist angesichts des auf profitorientierte Unternehmen beschränkten Anwendungsbereichs und damit des insoweit beschränkten potenziellen Angemessenheitsbeschlusses irrelevant.

Damit verbleibt die Interessenabwägung gemäß Art. 6 Abs. 1 S. 1 lit. f DSGVO. Diese kennt zwar kein Äquivalent im CCPA. Dennoch scheidet eine Angemessenheit für Kalifornien nicht allein deshalb aus,[38] weil die kalifornischen branchenspezifischen Datenschutzgesetze ein funktionales Äquivalent bilden. Diese reagieren zwar nur *ex post* auf einen festgestellten Missbrauch.[39] Allerdings funktioniert Art. 6 Abs. 1 S. 1 lit. f DSGVO die Interessenabwägung in der Praxis

---

[31] *Artikel-29-Datenschutzgruppe*, WP 254 Angemessenheit, S. 6.

[32] Cal. Civ. Code § 1798.100(d). Siehe Kapitel 3:D.V (ab S. 173).

[33] Vgl. *EDSA*, Opinion 14/2021 United Kingdom, Rn. 87: behauptet, dass diese bereits eine Kernanforderung des europäischen Datenschutzrechts seien. Dies kann angesichts der insoweit fehlenden klaren Vorgaben und faktisch fehlenden Umsetzung nicht überzeugen.

[34] Für diese Unterscheidung: *Sattler* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 225, 245.

[35] Zu den Informationspflichten siehe Kapitel 3:D.I (ab S. 150). Zu dem Widerspruchsrecht gegen Datenhandel siehe Kapitel 3:C.I (ab S. 81).

[36] Cal. Civ. Code § 1798.140(h).

[37] Siehe Kapitel 3:B.IV.1 (ab S. 74).

[38] A.A. *Botta*, PinG 2019, 261, 265.

[39] Siehe Kapitel 2:B.I.2 (ab S. 19).

nur *ex post.* So ist die Interessenabwägung für sich genommen häufig zu offen, um Verantwortliche *ex ante* zur Unterlassung problematischer Verarbeitungen personenbezogener Daten zu zwingen. Verantwortliche sind keine neutralen Dritten, die unbefangen Interessen abwägen. Vielmehr schränkt die Interessensabwägung faktisch Verantwortliche nur dann ein, wenn für die jeweilige Verarbeitungsart Aufsichtsbehörden, Literatur oder Gerichte die Interessenabwägung konkretisiert haben.[40] Dieses Konkretisieren ist mit den branchenspezifischen Gesetzen in Kalifornien vergleichbar, bei denen das kalifornische Parlament anhand konkreter Fälle Datenschutzgesetze erlässt. Dieser Ansatz hat den Nachteil eines lückenhafteren Schutzes – auch wenn Kalifornien mit inzwischen über 100 branchenspezifischen Gesetzen viele praxisrelevante Fälle abgedeckt hat.[41] Er ist aber stärker demokratisch legitimiert, da die Gesetze durch direkt gewählte Volksvertreter:innen verabschiedet werden. Auch führt ein Parlamentsgesetz schneller zu Rechtssicherheit als die im langsamen Austausch zwischen den vielfältigen Akteuren im europäischen Datenschutzdiskurs entstehende Auslegung der offenen Interessenabwägung des Art. 6 Abs. 1 S. 1 lit. f DSGVO.

III. Umsetzung durch Aufsichtsbehörden, Privatklagerechte und Datenschutzorganisation

Die behördliche Rechtsdurchsetzung ist angemessen.[42] Der CCPA kennt nicht nur mit der California Privacy Protection Agency eine unabhängige Datenschutzbehörde, sondern mit dem Attorney General eine weitere mit einem erheblichen Budget ausgestattete Vollzugsbehörde.[43]

Allerdings ist das Privatklagerecht des CCPA stark begrenzt, da es nur Datenpannen erfasst.[44] Insofern ist es zwar durchaus wirksam, weil das amerikanische Prozessrecht die Bündelung mittels Sammelklagen erlaubt.[45] Allerdings schließt der CCPA ein umfassendes Privatklagerecht explizit aus.[46] Daher stünde einer betroffenen Person, wenn ihre personenbezogenen Daten nach Kalifornien übertragen werden, gerade kein wirksamer Rechtsbehelf mehr zur Verfügung – wie ihn Art. 45 Abs. 2 lit. a DSGVO a.E. fordert. Damit läuft die betroffene Person Gefahr, dass sie einen Berichtigungs-, Löschungs- oder Auskunftsanspruch nicht mehr gerichtlich durchsetzen kann, wenn die personenbezogenen Daten nach Kalifornien übertragen werden. Das Beschwerderecht zur California

---

[40] *Hornung/Spiecker gen. Döhmann* in: NK-DatenschutzR, DS-GVO Einl. Rn. 251–254.

[41] Siehe Kapitel 2:B.II (ab S. 27).

[42] A.A. *Lejeune*, PinG 2021, 25, 26 Fn. 22: Bußgeldrahmen sei »völlig unzureichend«. Bei einer Berechnung pro Verletzungserfolg ergeben sich jedoch erhebliche Summen, siehe Kapitel 3:E.I.2.e) (ab S. 191).

[43] Siehe Kapitel 3:E.I.3 (ab S. 194).

[44] Cal. Civ. Code § 1798.150.

[45] Siehe Kapitel 3:E.II (ab S. 204).

[46] Cal. Civ. Code § 1798.150(d).

Privacy Protection Agency wiegt dies nicht auf, da diese nach freiem Ermessen entscheiden kann.[47]

Die Vorgaben für die Datenschutzorganisation sind im CCPA geringer, was allerdings nicht überbewertet werden sollte. Zwar fehlt im CCPA eine Pflicht, Datenschutzbeauftragte zu bestellen und ein Verzeichnis der Verarbeitungstätigkeiten zu erstellen. Kalifornische Praxisratgeber raten aber dennoch dazu, konkrete Beschäftigte mit Datenschutz zu beauftragen und sich einen Überblick über alle Verarbeitungstätigkeiten durch ein zentrales Verzeichnis zu verschaffen.[48] Auch die sonst sehr präskriptive Artikel-29-Datenschutzgruppe ordnet Datenschutzbeauftragte und ein Verzeichnis der Verarbeitungstätigkeiten nur als mögliche Ausgestaltung der praktischen Durchsetzung des Datenschutzes ein, nicht als absolut erforderliches Minimum.[49]

IV. Zugang von Sicherheitsbehörden

Auf Bundesebene verarbeiten Nachrichtendienste weiterhin massenhaft personenbezogene Daten, wobei betroffene Personen ohne amerikanische Staatsangehörigkeit keine gerichtlich durchsetzbaren Rechte haben. Dies war der Grund für den EuGH, in seinem *Schrems-II*-Urteil den *Privacy-Shield*-Beschluss für unwirksam zu erklären.[50] Die vom Irish High Court[51] und EuGH diskutieren FISA Sec. 702,[52] Executive Order 12333[53] und PPD-28[54] bestehen nahezu unverändert weiter. Das U. S. Department of Commerce behauptet zwar in seiner Stellungnahme zum *Schrems-II*-Urteil, dass sich die Rechtslage seit dem Vorlagebeschluss des Irish High Court wesentlich gebessert habe.[55] Tatsächlich ist der FISA Amendments Reauthorization Act of 2017[56] erst nach dem Vorlagebeschluss in Kraft getreten und hat nur insoweit eine kleine Rolle im *Schrems-II*-Verfahren gespielt, als ihn der Generalanwalt Saugmandsgaard Øe nur in einer Fußnote erwähnt hatte.[57] Allerdings enthält der FISA Amendments Reauthorization Act nur Detailänderungen: Einschränkung der internen Zugriffsrechte auf aus Überwachung

---

[47] Cal. Civ. Code § 1798.199.45(b).

[48] Siehe Kapitel 3:D.VI (ab S. 176).

[49] *Artikel-29-Datenschutzgruppe*, WP 254 Angemessenheit, S. 8.

[50] EuGH vom 16.07.2020, *Schrems II*, ECLI:EU:C:2020:559, 178–198. Der *Safe-Harbour*-Beschluss enthielt hierzu keine Feststellungen, weswegen ihn der EuGH schon deshalb verworfen hat: EuGH vom 06.10.2015 – C-362/14, *Schrems I*, ECLI:EU:C:2015:650 Rn. 83–98.

[51] Irish High Court vom 03.10.2017, *Schrems II*, [2017] IEHC 545, Rn. 164–263.

[52] 50 U. S. C. § 1802.

[53] Exec. Order 12,333, 46 Fed. Reg. 235.

[54] *Obama*, Presidential Policy Directive 28, Signals Intelligence Activities.

[55] *U. S. Department of Commerce*, White Paper Schrems II, S. 14 f.

[56] FISA Amendments Reauthorization Act of 2017, Publ. L. No. 115-118, 132 Stat. 3.

[57] Generalanwalt *Saugmandsgaard Øe*, Schlussanträge vom 19.12.2018, *Schrems II*, ECLI:EU:C:2019:1145 Fn. 150.

gewonnener Daten,[58] Datenschutzbeauftragte für FBI und NSA[59] und leicht gesteigerte Transparenzanforderungen.[60] Ein gerichtlicher Rechtsbehelf fehlt weiterhin. Der FISA Amendments Reauthorization Act stellt damit keine nachhaltige Verbesserung dar.[61]

V. Gesamtbewertung

Hindernisse für einen Angemessenheitsbeschluss sind somit die Massenüberwachung durch Nachrichtendienste des Bundes, die fehlende Erstreckung auf Personen außerhalb Kaliforniens und das fehlende umfassende Privatklagerecht. Jeder einzelne dieser drei Aspekte führt schon allein dazu, dass Kalifornien *de lege lata* über kein der Sache nach gleichwertiges Schutzniveau im Sinne des Art. 45 Abs. 1 S. 1 DSGVO verfügt.[62]

Die fehlende Erstreckung auf Personen außerhalb Kaliforniens ließe sich lösen, indem das kalifornische Parlament den Verbraucherbegriff auf alle Individuen erweitert. Dies erscheint auch hinsichtlich der *dormant Commerce Clause* verfassungsrechtlich zulässig. So wären weiterhin Beeinträchtigungen des Handels zwischen den Bundesstaaten ausgeschlossen, da die Ausnahmen für Unternehmen, die nicht in Kalifornien tätig sind, und für Verarbeitungen außerhalb Kaliforniens bestehen blieben. Auch der California Disabled Persons Act, den der für Kalifornien zuständige Court of Appeals for the 9th Circuit als vereinbar mit der *dormant Commerce Clause* hält,[63] schützt Individuen unabhängig von ihrem Wohnsitz.[64]

Ebenso verfassungsrechtlich zulässig wäre ein weiter gefasstes Privatklagerecht.[65] Politisch wird dieses jedoch nur schwierig zu erreichen sein, da Wirtschaftsverbände die damit verbundene Rechtsunsicherheit durch Sammelklagen kritisch sehen.[66]

Kalifornien kann jedoch nicht die Massenüberwachung durch Nachrichtendienste des Bundes lösen.[67] Insoweit werden viele rechtliche Lösungsmöglichkeiten diskutiert, deren Darstellung hier den Rahmen sprengen würde.[68] Es

---

[58] FISA Amendments Reauthorization Act of 2017, Publ. L. No. 115-118, 132 Stat. 3, Sec. 101, amending 50 U.S.C. § 1881a(f).

[59] FISA Amendments Reauthorization Act of 2017, Sec. 109, amending 42 U.S.C. § 2000ee-1(a).

[60] FISA Amendments Reauthorization Act of 2017, Sec. 107, amending 50 U.S.C. § 1807.

[61] *EDSA*, EU – U.S. Privacy Shield – Second Annual Joint Review, Rn. 19.

[62] *Lejeune*, PinG 2021, 25, 27. Ebenso zum CCPA-2018: *Botta*, PinG 2019, 261, 266.

[63] U.S. Court of Appeals 9th Circuit vom 05.02.2014, *Greater L.A. Agency on Deafness, Inc. v. CNN, Inc.*, 742 F.3d 414, 432–434.

[64] Cal. Civ. Code § 54(a).

[65] Die *standing doctrine* gilt nur für Bundesgerichte, siehe Kapitel 3:E.II.2.c) (ab S. 212).

[66] Siehe Kapitel 3:E.II.2.d) (ab S. 214).

[67] *Lejeune*, PinG 2021, 25, 27.

[68] Amend. 100 by MS. Lofgren of California to H.R. 4505 – Commerce, Justice, Science, and Related Agencies Appropriations Act, 117th Cong. (2021); *Privacy and Civil Liberties*

wird allerdings kaum einfach und schnell möglich sein, die amerikanische Massenüberwachung einzuhegen und auf eine rechtsstaatliche Grundlage zu stellen. Für eine umfassende Reform fehlt allerdings der politische Wille, den das *Schrems-II*-Urteil bisher auch nicht anstoßen konnte. So wird Kalifornien ein Angemessenheitsbeschluss auf absehbare Zeit versagt bleiben.

B. Übernahme der Regelung für finanzielle Anreize in das europäische Datenschutzrecht

I. Einleitung: gegenseitiger transatlantischer Austausch

Im europäischen Datenschutzrecht ist das Geschäftsmodell »Leistung gegen Daten« stark umstritten. Die unter diesem Schlagwort diskutierten Datenüberlassungsverträge,[69] bei denen die Bereitstellung personenbezogener Daten die Hauptleistung der betroffenen Person bildet, sind zugleich praxisrelevant wie risikoreich. Bisher besteht jedoch nur eine Regelung, die sowohl unklar ist als auch die wesentlichen Probleme außen vorlässt.[70]

Dabei ist ein Rückgriff auf die kalifornische Sonderregelung zu finanziellen Anreizen[71] naheliegend. Europa und die Vereinigten Staaten sind als Teile des Westens kulturell wie wirtschaftlich eng verwoben. Besonders nahe steht Europa das politisch progressive Kalifornien. Die Internetunternehmen des kalifornischen Silicon Valley prägen zudem auch die europäische Datenwirtschaft.[72] Rechtskulturell bestehen zwar gewisse Unterschiede – beispielsweise bewertet das amerikanische Recht Privatautonomie und Meinungsfreiheit höher als das europäische Recht.[73] Ansonsten verfügen die Vereinigten Staaten und besonders Kalifornien aber neben dem CCPA über zahlreiche weitere Datenschutzgesetze, denen ähnliche Prinzipien wie dem europäischen Datenschutzrecht zugrundeliegen und die teilweise sogar ein höheres Schutzniveau als die DSGVO erreichen.[74]

Aufgrund dieser rechtskulturellen Ähnlichkeiten haben die Vereinigten Staaten und Europa häufig Datenschutznormen des jeweils anderen übernommen. Im Ausland finden sich oft vielfältige Herangehensweisen an auch in Europa und Deutschland bestehende Probleme. Es ist lohnenswert, auf die dort gewonnenen

---

Oversight Board, Chairman's FISA White Paper, S. 22–26; *Christakis*, European Law Blog, Squaring the Circle? (Part 2); *Fennessy*, Lawfare, A Multilateral Surveillance Accord; *Flor*, 96 Notre Dame L. Rev. 2035, 2051–2057; *Ivers*, 62 B.C. L. Rev. 2573, 2615 f.; *Propp/Swire*, Lawfare, After Schrems II.

[69] Geprägt von *Weichert*, NJW 2001, 1463, 1468 f.

[70] Siehe Kapitel 3:C.I.4.c) (ab S. 107).

[71] Siehe Kapitel 3:C.I.4.b) (ab S. 101).

[72] Siehe Kapitel 1:A (ab S. 1).

[73] Siehe Kapitel 3:F.I (ab S. 221).

[74] Siehe Kapitel 2:B.I.2 (ab S. 19).

Erfahrungen zurückzugreifen.[75] Rechtsübernahmen sind daher eines der primären Mittel, um das heimische Recht fortzubilden.[76] Am deutlichsten zeigt sich dieser Einfluss an den zahlreichen punktuellen Rechtsübernahmen des CCPA.[77] Daneben rezipieren Gesetze anderer amerikanischer Bundesstaaten und Gesetzesentwürfe für ein Datenschutzgesetz des Bundes die DSGVO ausgiebig und übernehmen überwiegend mit »controller« und »processor« sogar die Nomenklatur der DSGVO.[78]

Umgekehrt beeinflusst auch das amerikanische Datenschutzrecht Europa. So geht beispielsweise die Datenschutz-Folgenabschätzung des Art. 35 DSGVO auf die angelsächsischen, insbesondere amerikanischen *privacy impact assessments* zurück.[79] Zudem stand der amerikanische COPPA Pate für Art. 8 DSGVO.[80] Auch Kalifornien hat bereits das europäische Datenschutzrecht beeinflusst. Als erster Bundesstaat verpflichtete Kalifornien Unternehmen, Opfer einer Datenpanne zu benachrichtigen – was inzwischen alle anderen 49 Bundesstaaten übernommen haben.[81] Dieses kalifornische Datenpannemeldegesetz ist ein direkter Vorläufer von Art. 33, 34 DSGVO. So diskutierte die von der Europäischen Kommission für die Reform der ePrivacy-RL 2006 in Auftrag gegebene Studie das kalifornische Gesetz ausführlich.[82] Auch der Europäische Datenschutzbeauftragte verwies in seiner Stellungnahme zur Reform der ePrivacy-RL auf die positiven Erfahrungen amerikanischer Bundesstaaten mit Datenpannenmeldepflichten.[83] Dies führte dazu, dass der europäische Gesetzgeber 2009 eine Datenpannenmeldepflicht in Art. 4 Abs. 3 ePrivacy-RL einfügte.[84] Auch der deutsche Gesetzgeber orientierte sich bei der Einführung einer entsprechenden Pflicht in § 42a

---

[75] *Kischel*, Rechtsvergleichung, § 2 Rn. 29; *Zweigert/Kötz*, Einführung in die Rechtsvergleichung, S. 15.

[76] *De Cruz*, Comparative law in a changing world, S. 21f; *Graziadei* in: Reimann/Zimmermann, The Oxford Handbook of Comparative Law, 443, 443; *Watson*, Legal transplants, S. 95; *Zweigert/Kötz*, Einführung in die Rechtsvergleichung, S. 15.

[77] Siehe Kapitel 3:F.IV (ab S. 230).

[78] Colo. Rev. Stat. § 6-1-1303(7),(19); Va. Code § 59.1-571. Manche Mustergesetze übernehmen sogar zusätzlich den Begriff des »data subject«: *American Law Institute*, Principles of the law, data privacy, § 2(c),(e),(f); *Uniform Law Commission*, Uniform Personal Data Protection Act, § 2(3),(4),(12).

[79] Siehe Kapitel 3:D.VI.2 (ab S. 177).

[80] Siehe S. 23.

[81] S.B. 1386, 2001–02 Leg., Reg. Sess. (Cal. 2002), Cal. Stats. 2002 ch. 915, kodifiziert in Cal. Civ. Code § 1798.82. Siehe Kapitel 2:B.II (ab S. 27).

[82] *Hogan & Hartson/Analysys*, Review of the electronic communications regulatory framework: Final Report For the European Commission, S. 252, insb. Fn. 78.

[83] *Europäischer Datenschutzbeauftragter*, Stellungnahme Änderung Richtlinie 2002/58/EG Rn. 26.

[84] Art. 2 Nr. 4 Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der

BDSG-2009 ausweislich der Gesetzesbegründung an »Regelungen im Recht der Vereinigten Staaten von Amerika«.[85] Aufbauend auf Art. 4 Abs. 3 ePrivacy-RL,[86] erstreckte der europäische Gesetzgeber schließlich in Art. 33, 34 DSGVO die Datenpannenmeldepflicht auf alle Verantwortliche. Damit hat Kalifornien das europäische Datenschutzrecht bereits einmal an entscheidender Stelle geprägt.

Daher stellt sich die Frage, ob Europa auch bei Datenüberlassungsverträgen von Kalifornien lernen kann. Zunächst untersucht der nächste Abschnitt den zugrunde liegenden Konflikt zwischen Privatautonomie und grundrechtsgeprägtem europäischem Datenschutzrecht (II.1). Sodann wird die Rechtslage *de lege lata* erörtert (II.2), gefolgt von einem Überblick über die bisher diskutierten Regelungsalternativen *de lege ferenda* (II.3). Aufbauend darauf ist zu untersuchen, inwieweit sich die kalifornische Lösung für diese Regelungslücke eignet (III.1) und wo diese Regelung zu verorten ist (III.2). Schließlich wird ein konkreter Regelungsvorschlag erarbeitet (III.3).

II. Regelungsbedarf

1. Hintergrund: Leistung gegen Daten im grundrechtsgeprägten europäischen Datenschutz

»Es mag wohl einen Markt für personenbezogene Daten geben, sowie es leider auch einen Markt für lebende menschliche Organe gibt, doch bedeutet dies nicht, dass wir diesen Markt mit einem Rechtsinstrument absegnen können oder sollten. Man kann ein Grundrecht nicht zu Geld und zum Gegenstand einer einfachen geschäftlichen Transaktion machen, auch wenn die von den Daten betroffene natürliche Person eine der an der Transaktion beteiligten Parteien ist.«

Giovanni Buttarelli, Europäischer Datenschutzbeauftragter[87]

Dieses Zitat zeigt die in der europäischen Datenschutzdiskussion weit verbreitete Skepsis gegenüber Datenüberlassungsverträgen auf. Das europäische Datenschutzrecht ist stark grundrechtsgeprägt, womit eine Kommerzialisierung personenbezogener Daten nur schwer vereinbar ist. So befürchten Literaturstimmen, dass die individuelle Persönlichkeit lediglich zu einem Objekt wirtschaftlicher Tätigkeit reduziert würde.[88] Bei einer durchgreifenden Kommerzialisierung werde das Individuum zu einer bloßen Sammlung von Daten, die Computer beliebig

elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

[85] BT-Drs. 16/12011, 34.

[86] *Europäische Kommission*, DSGVO-E(KOM), KOM(2012) 11 endg., Begründung Nr. 3.4.4.2.

[87] *Europäischer Datenschutzbeauftragter*, Stellungnahme 4/2017 Digitale-Inhalte-RL, Rn. 17. Ähnlich: *EDSA*, Leitlinien 2/2019 Rechtsgrundlage Vertrag, Rn. 54.

[88] *Peifer*, Individualität im Zivilrecht, S. 291–294; *Simitis*, NJW 1998, 2473, 2477. Vgl. die umfassende Problemdarstellung bei *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 183–198.

kombinieren und auseinandernehmen, um sie zum größtmöglichen Profit zu verwerten.[89] Wenn betroffene Personen ihre personenbezogenen Daten »verkaufen«, führe dies auch zu einem weniger individuellen, marktgängigen Verhalten.[90] Die mit der Zulassung von Datenüberlassungsverträgen verbundene Kommerzialisierung ruft damit Risiken für die betroffene Person hervor.

Ein vollständiges Verbot von Datenüberlassungsverträgen ist allerdings mit der Privatautonomie nicht vereinbar.[91] Vertragsfreiheit ist auch von der GRCh geschützt (Art. 16 GRCh).[92] Besonders bei wenig sensiblen Daten ist eine völlige Kommerzialisierung der Persönlichkeit kaum zu befürchten. Natürlich gibt es keine völlig belanglosen Daten, die keinerlei Regulierung bedürfen.[93] Ist es aber wirklich gerechtfertigt, Prominente vor sich selbst zu schützen, die ihren Namen für Werbung verkaufen wollen?[94] Auch aus praktischen Erwägungen sollte der Kreis der *res ex commercium* möglichst eng gezogen werden. Wenn der Staat ein generelles Verbot ausspricht, verzichtet er auf die Möglichkeit, den Markt zu ordnen. Zugegebenermaßen entfaltet jedes (durchgesetzte) Verbot auch eine gewisse Wirkung. So hat beispielsweise die Alkoholprohibition in den Vereinigten Staaten[95] trotz erheblicher gesellschaftlicher Widerstände durchaus zu weniger Alkoholkonsum geführt.[96] Diese Alkoholprohibition hat dem Staat jedoch vielfältige Regulierungsoptionen genommen, wie Altersgrenzen oder die Kontrolle auf Streckmittel. Ebenso würde ein generelles Verbot von Datenüberlassungsverträgen dem Staat die Möglichkeit nehmen, einen Ordnungsrahmen für dieses Geschäftsmodell zu schaffen.

---

[89] *Simitis*, NJW 1998, 2473, 2477.

[90] *Peifer*, Individualität im Zivilrecht, S. 292.

[91] *Bijok*, Kommerzialisierungsfester Datenschutz, S. 205–209; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 173–183; *ders.*, DuD 2010, 39, 43; *Bunnenberg*, Privates Datenschutzrecht, S. 169–171; *Datenethikkommission*, Gutachten, S. 104; *Engler*, ZD 2018, 55, 56; *Hacker*, Datenprivatrecht, S. 193; *Hofmann* in: Stiftung Datenschutz, Dateneigentum und Datenhandel, 161, 172; *Heckmann/Paschke* in: Ehmann/Selmayr, DS-GVO Art. 7 Rn. 95; *Metzger* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 23, 41 f.; *Rogosch*, Die Einwilligung im Datenschutzrecht, S. 43 f.; *Sattler* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 225, 233–237; *Schantz/Wolff*, Das neue Datenschutzrecht, Rn. 515; *Schrader*, Datenschutz Minderjähriger, S. 194; *Schulz* in: Gola, DS-GVO Art. 7 Rn. 27 a. A. wohl *Dix*, ZEuP 2017, 1, 4: Datenschutzrecht sei nicht disponibel.

[92] EuGH vom 24.09.2020 – C-223/19, *YS u. a.*, ECLI:EU:C:2020:753 Rn. 86; vom 15.04.2021 – C-798/18, *Federazione nazionale delle imprese elettrotecniche ed elettroniche (Anie) u. a.*, ECLI:EU:C:2021:280 Rn. 56.

[93] Diesen *topos* prägend: BVerfG vom 15.12.1983 – 1 BvR 209/83, *Volkszählung*, BVerfGE 65, 1, 45.

[94] Diese Parallele ebenso entwickelnd: *Buchner*, DuD 2010, 39, 43; *Sattler* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 225, 237; *der.*, NJW 2020, 3623 Rn. 31.

[95] U. S. Const. amend. XVIII § 1, repealed by U. S. Const. amend. XXI § 1.

[96] *Blocker*, 96 Am. J. Public Health 233, 236–238; *Miron/Zwiebel*, Alcohol Consumption During Prohibition, S. 4–6: Alkoholkonsum sei nach Einführung auf ca. 30 % des vorherigen Levels, später ca. 60 %, gesunken.

Der europäische Gesetzgeber hat Datenüberlassungsverträge auch entgegen der Meinung des Europäischen Datenschutzbeauftragten bisher nicht verboten. Vielmehr hat er insbesondere bei dem Koppelungsverbot des Art. 7 Abs. 4 DSGVO sich an einer Regelung versucht (2.a). Auch das Telemediendatenschutzrecht (2.b), die Digitale-Inhalte-RL (2.c) und das AGB-Recht (2.d) sind für Datenüberlassungsverträge relevant.

2. *Unzureichende Regelung* de lege lata

a) Koppelungsverbot des Art. 7 Abs. 4 DSGVO

Das Koppelungsverbot des Art. 7 Abs. 4 DSGVO ist die *de lege lata* zentrale Norm für die Zulässigkeit von Datenüberlassungsverträgen. Nach dieser Norm ist bei der Freiwilligkeit einer Einwilligung im »größtmöglichen Umfang« zu berücksichtigen, ob der Verantwortliche die Erfüllung eines Vertrages davon abhängig macht, dass die betroffene Person in eine für die Vertragserfüllung nicht erforderliche Verarbeitung einwilligt. Die Norm gilt weithin als misslungen.[97]

Am Wortlaut ist schon problematisch, dass eine für die Vertragserfüllung erforderliche Verarbeitung personenbezogener Daten bereits aufgrund Art. 6 Abs. 1 S. 1 lit. b DSGVO zulässig ist. Die Formulierung »für die Vertragserfüllung […] erforderlich« ist übereinstimmend mit in Art. 6 Abs. 1 S. 1 lit. b DSGVO auszulegen, weil sie mit dieser Rechtsgrundlage in einem engen systematischen Zusammenhang steht.[98] Die Erforderlichkeit für die Vertragserfüllung lässt sich entweder objektiv oder subjektiv verstehen.[99] Nach der objektiven Ansicht des Europäischen Datenschutzausschusses bezieht sich die Erforderlichkeit auf den grundlegenden Vertragszweck, um Missbrauch durch einseitig gestellte Klauseln zu verhindern.[100] Die subjektive Ansicht knüpft die Erforderlichkeit dagegen an die konkreten Vertragsklauseln, da eine datenschutzrechtliche Inhaltskontrolle

---

[97] *Becker*, CR 2021, 87 Rn. 26; *Bunnenberg*, Privates Datenschutzrecht, S. 70 f.; *Dammann* ZD 2016, 307, 311; *Frenzel* in: Paal/Pauly, DS-GVO Art. 7 Rn. 18; *Funke*, Dogmatik und Voraussetzungen der datenschutzrechtlichen Einwilligung im Zivilrecht, S. 268; *Härting*, Legal Tribune Online, Trilog erfolgreich, Einwilligung tot; *Kühling*, DuD 2021, 783, 787; *Roßnagel/Geminn*, Datenschutz-Grundverordnung verbessern, S. 88; *Schrader*, Datenschutz Minderjähriger, S. 195 f.; *Schulz* in: Gola, DS-GVO Art. 7 Rn. 24; *Stemmer* in: BeckOK DatenschutzR, DS-GVO Art. 7 Rn. 46.2.

[98] *Buchner/Kühling* in: Kühling/Buchner, DS-GVO Art. 7 Rn. 47; *Frenzel* in: Paal/Pauly, DS-GVO Art. 7 Rn. 20; *Hacker*, Datenprivatrecht, S. 182; *Ingold* in: Sydow, DSGVO Art. 7 Rn. 32; *Schulz* in: Gola, DS-GVO Art. 7 Rn. 27; *Stemmer* in: BeckOK DatenschutzR, DS-GVO Art. 7 Rn. 47; a. A. *Voigt*, Die datenschutzrechtliche Einwilligung, S. 371 unter Verweis auf Gesetzgebungsgeschichte.

[99] Diese Unterscheidung entwickelnd: *Engeler*, ZD 2018, 55, 57 f.

[100] *EDSA*, Leitlinien 2/2019 Rechtsgrundlage Vertrag, Rn. 30–32; *Brinkmann* in: BeckOGK, BGB § 307 Datenschutzklausel Rn. 13–16; *Bock*, CR 2020, 173, 176–178; *Becker*, CR 2021, 230 Rn. 27–29; *Buchner/Kühling* in: Kühling/Buchner, DS-GVO Art. 7 Rn. 49–51a; *Golland*, MMR 2018, 130, 131; *Leistner/Antoine/Sagstetter*, Big Data, S. 265 f.; *Stemmer* in: BeckOK DatenschutzR, DS-GVO Art. 7 Rn. 41.

neben dem Vertragsrecht nicht gerechtfertigt sei.[101] Das Problem haben sowohl das OLG Düsseldorf als auch der österreichische OGH dem EuGH vorgelegt.[102]

Die Bedeutung des zweiten Tatbestandselements im »größtmöglichen Umfang« (englisch: »utmost account«) ist ebenfalls unklar. Die deutsche Fassung des Erwägungsgrundes 43 S. 2 spricht davon, dass eine Einwilligung bei einer solchen Koppelung als unfreiwillig »gilt«. Dies legt eine Fiktion nahe.[103] Jedoch verwenden die englische (»presumed«), spanische (»presume«), italienische (»presume«) und französische (»présumé«) Sprachfassung des Erwägungsgrundes 43 S. 2 Begriffe, die für eine Vermutung sprechen.[104] In anderen Rechtsgebieten legt der EuGH »presumed« als widerlegbare Vermutung aus.[105] Erwägungsgrund 43 S. 2 ist damit für die Ermittlung der Reichweite des Koppelungsverbots unergiebig.[106]

Der verwirrende Wortlaut geht darauf zurück, dass das Koppelungsverbot im Gesetzgebungsverfahren stark umstritten war. Gegenüber der DSRL wurden die Anforderungen an die Einwilligung allgemein deutlich verschärft,[107] wobei Art. 7 DSGVO-E(KOM) noch kein Koppelungsverbot enthielt. Das traditionell datenschutzfreundlichere Europäische Parlament schlug daraufhin in Art. 7 Abs. 4 S. 2 DSGVO-E(PARL) ein absolutes Koppelungsverbot (»shall not«) vor. Im Trilog haben Europäische Kommission, Rat und Europäisches Parlament diesen Vorschlag auf »utmost account shall be taken« abgeschwächt und durch den ebenso unscharfen Erwägungsgrund 43 S. 2 ergänzt.

Eine Auslegung als striktes Verbot von Datenüberlassungsverträgen ist mit dieser Gesetzgebungsgeschichte nicht vereinbar.[108] Zudem erwähnen sowohl Art. 3 Abs. 1a Verbraucherrechte-RL als auch Art. 3 Abs. 1 UAbs. 2 Digitale-Inhalte-RL

---

[101] *Engeler*, ZD 2018, 55, 57f; *ders.*, PinG 2019, 149, 150–153; *Hacker*, ZfPW 2019, 148, 157f; *ders.*, Datenprivatrecht, S. 185f.; *Heinzke/Lennart*, ZD 2020, 189, 191; *Jahnel*, DS-GVO Art. 6 Rn. 29.

[102] OLG Düsseldorf vom 24.03.2021 – Kart 2/19 (V), Az. beim EuGH: C-252/21, EuZW 2021, 680, Frage 3; OGH (Österreich) vom 23.06.2021 – 6 Ob 56/21k, Az. beim EuGH: C-446/21, BeckRS 2021, 19302, Frage 1.

[103] *Brinkmann* in: BeckOGK, BGB § 307 Datenschutzklausel Rn. 68; *Engler*, ZD 2018, 55, 59; *Heckmann/Paschke* in: Ehmann/Selmayr, DS-GVO Art. 7 Rn. 99; *Schrader*, Datenschutz Minderjähriger, S. 194; *Taeger* in: Taeger/Gabel, DS-GVO Art. 7 Rn. 99; *Voigt*, Die datenschutzrechtliche Einwilligung, S. 354f.

[104] Ähnlich *Becker*, CR 2021, 230 Rn. 21.

[105] Kartellrecht: EuGH vom 10.09.2009 – C-97/08 P, *Akzo Nobel*, ECLI:EU:C:2009:536 Rn. 60; vom 29.03.2011, *ArcelorMittal*, ECLI:EU:C:2009:547 Rn. 97.
Asylrecht: EuGH vom 21.12.2011, *N.S. u. a.*, ECLI:EU:C:2011:865 Rn. 99–105.

[106] *Becker*, CR 2021, 230 Rn. 22. Ebenso i. Erg., aber gestützt auf einen Widerspruch zwischen Erwägungsgrund und Normtext: *Brinkmann* in: BeckOGK, BGB § 307 Datenschutzklausel Rn. 68; *Engler*, ZD 2018, 55, 59; *Heckmann/Paschke* in: Ehmann/Selmayr, DS-GVO Art. 7 Rn. 99; *Schrader*, Datenschutz Minderjähriger, S. 194; *Voigt*, Die datenschutzrechtliche Einwilligung, S. 354f.

[107] *Funke*, Datenschutzrechtliche Einwilligung im Zivilrecht, S. 267.

[108] *Voigt*, Die datenschutzrechtliche Einwilligung, S. 353.

Verträge, in denen »der Verbraucher dem Unternehmer personenbezogene Daten bereitstellt oder deren Bereitstellung zusagt« und gehen damit ersichtlich von der grundsätzlichen Zulässigkeit des Datenüberlassungsvertrages aus. Bei einem Verbot solcher Verträge würden Art. 3 Abs. 1a Verbraucherrechte-RL und Art. 3 Abs. 1 UAbs. 2 Digitale-Inhalte-RL leerlaufen, was dem Gebot, das Europarecht auch rechtsaktübergreifend einheitlich auszulegen,[109] widersprechen würde. Daher sprechen beide Normen für eine grundsätzliche Zulässigkeit des Geschäftsmodells »Leistung gegen Daten«.[110] Auch der Generalanwalt *Spuznar* geht davon aus, dass Datenüberlassungsverträge an sich zulässig sind.[111] Die Frage ist nur, ob dieses Geschäftsmodell auf der Rechtsgrundlage der Einwilligung (Art. 6 Abs. 1 S. 1 lit. a DSGVO) oder des Vertrages (Art. 6 Abs. 1 S. 1 lit. b DSGVO) beruhen sollte.

Die wohl überwiegende Ansicht will Datenüberlassungsverträge auf eine Einwilligung stützen und das Koppelungsverbot des Art. 7 Abs. 4 DSGVO einschränkend auslegen (datenschutzrechtliche Lösung).[112] So seien nur sachfremde Einwilligungen erfasst, wenn beispielsweise Banken eine Werbeeinwilligung bei Vertragsschluss über einen Kreditvertrag fordern.[113] Auch wird vertreten, dass eine Einwilligung trotz Koppelung mit der Vertragserfüllung freiwillig sei, wenn im Markt ein Alternativangebot existiere; umgekehrt sei bei Monopolen eine Einwilligung unfreiwillig.[114] Die Aufsichtsbehörden und einige weitere Literaturstimmen halten eine Einwilligung trotz Koppelung nur für freiwillig, wenn der

---

[109] EuGH vom 05.07.2012 – C-49/11, *Content Services Ltd.*, ECLI:EU:C:2012:419 Rn. 47; *Riesenhuber* in: Riesenhuber, Europäische Methodenlehre, § 10 Rn. 24.

[110] Ebenso zur Digitale-Inhalte-RL: *Heckmann/Paschke* in: Ehmann/Selmayr, DS-GVO Art. 7 Rn. 95; *Krohm/Müller-Peltzer*, ZD 2017, 551, 553; *Leistner/Antoine/Sagstetter*, Big Data, S. 256; *Metzger* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 23, 34; a. A. *Mischau*, ZEuP 2020, 335, 339: kein Rückschluss wegen Art. 3 Abs. 8 Digitale-Inhalte-RL.

[111] Generalanwalt *Spuznar*, Schlussanträge vom 21.03.2019 – C-673/17, *Planet49 GmbH*, ECLI:EU:C:2019:246 Rn. 98.

[112] Corte Suprema di Cassazione (Italien) vom 02.07.2018 – 17278/2018, *Autorità Garante per la Proezione dei Dati Personali contro AD SPRAY S.r.l.*, http://www.interlex.it/2testi/giurisprudenza/cass18-17278.pdf [perma.cc/RLR2-Y7WP], Nr. 2.5; *EDSA*, Leitlinien 05/2020 Einwilligung, Rn. 37; *Becker*, CR 2021, 230 Rn. 47–49; *Brinkmann* in: BeckOGK, BGB § 307 Datenschutzklausel Rn. 68; *Buchner/Kühling* in: Kühling/Buchner, DS-GVO Art. 7 Rn. 49; *Bunnenberg*, Privates Datenschutzrecht, S. 72–74 und passim; *Frenzel* in: Paal/Pauly, DS-GVO Art. 7 Rn. 21; *Golland*, MMR 2018, 130, 133–135; *Hacker*, Datenprivatrecht, S. 186–204; *Heckmann/Paschke* in: Ehmann/Selmayr, DS-GVO Art. 7 Rn. 98; *Ingold* in: Sydow, DSGVO Art. 7 Rn. 33; *Korch*, ZEuP 2021, 792, 806; *Leistner/Antoine/Sagstetter*, Big Data, S. 256–258; *Schrader*, Datenschutz Minderjähriger, S. 192–198; *Stemmer* in: BeckOK DatenschutzR, DS-GVO Art. 7 Rn. 46.1; *Voigt*, Die datenschutzrechtliche Einwilligung, S. 346–378. Wohl auch: *Schantz/Wolff*, Das neue Datenschutzrecht Rn. 514–516. Offenlassend: OGH (Österreich) vom 31.08.2018 – 6 Ob 140/18h, ZD 2019, 72 Rn. 46.

[113] *Schulz* in: Gola, DS-GVO Art. 7 Rn. 27.

[114] Corte Suprema di Cassazione vom 02.07.2018 – 17278/2018, *Autorità Garante per la Proezione dei Dati Personali contro AD SPRAY S.r.l.*, http://www.interlex.it/2testi/giurisprudenza/cass18-17278.pdf [perma.cc/RLR2-Y7WP], Nr. 2.5; *Frenzel* in: Paal/Pauly, DS-GVO Art. 7

Verantwortliche selbst eine datensparsame Alternative anbietet.[115] Diese müsse in jeder Hinsicht gleichwertig und transparent dargestellt sein.[116]

Andere Stimmen in Literatur und Rechtsprechung stützen die Zulässigkeit des Datenüberlassungsvertrages auf Art. 6 Abs. 1 S. 1 lit. b Alt. 1 DSGVO (schuldrechtliche Lösung).[117] Wenn die Bereitstellung personenbezogener Daten Hauptleistung ist, sei die dafür nötige Verarbeitung personenbezogener Daten für die Vertragserfüllung erforderlich. Der Schutz der betroffenen Person vor unangemessenen Vertragsklauseln solle über das Schuldrecht erfolgen (insbesondere gemäß §§ 138, 242, 307 Abs. 1 BGB).[118] Schuldrecht und Datenschutz laufen nach dieser Ansicht schon deshalb parallel, da ein Vertrag nur eine Rechtsgrundlage bildet, soweit er wirksam ist.

Die schuldrechtliche Lösung ist besser mit dem weit gefassten Wortlaut vereinbar. Art. 7 Abs. 4 DSGVO ist aber insgesamt so unklar formuliert, dass es keine zwingende Entscheidung zwischen schuldrechtlicher und datenschutzrechtlicher Lösung erlaubt. Die Formulierung »im größtmöglichen Umfang« des Art. 7 Abs. 4 DSGVO spricht deutlich für ein (nahezu) absolutes Koppelungsverbot. Es ist angesichts diesem ein nahezu absolutes Koppelungsverbot andeutenden Wortlaut unwahrscheinlich, dass der europäische Gesetzgeber ausgerechnet den klassischen Fall einer Koppelung »Leistung gegen Daten« ausnehmen wollte. Vor allem aber ist die schuldrechtliche Lösung besser mit der Systematik der DSGVO vereinbar.[119] Wenn eine Verarbeitung personenbezogener Daten für die Vertragserfüllung erforderlich ist, besteht mit Art. 6 Abs. 1 S. 1 lit. b Alt. 1 DSGVO bereits eine Rechtsgrundlage. Art. 7 Abs. 4 DSGVO greift im Gegensatz dazu nur, wenn die Einwilligung zur Vertragserfüllung nicht erforderlich ist. Damit kommt dieser Norm letztlich die Funktion zu, ein Umgehen des Art. 6 Abs. 1 S. 1 lit. b Alt. 1 DSGVO zu verhindern. Art. 6 Abs. 1 S. 1 lit. b Alt. 1 DSGVO geht genauso wie die Einwilligung auf die autonome Willensentscheidung der

---

Rn. 21; *Heckmann/Paschke* in: Ehmann/Selmayr, DS-GVO Art. 7 Rn. 98. Zu recht kritisch: *Schrader*, Datenschutz Minderjähriger, S. 199–201.

[115] *EDSA*, Leitlinien 05/2020 Rn. 37; *Buchner/Kühling* in: Kühling/Buchner, DS-GVO Art. 7 Rn. 49; *Bunnenberg*, Privates Datenschutzrecht, S. 72–74; *Golland*, MMR 130, 133–135; *Ingold* in: Sydow, DSGVO Art. 7 Rn. 33; *Stemmer* in: BeckOK DatenschutzR, DS-GVO Art. 7 Rn. 46.1. wohl auch: *Schantz/Wolff*, Das neue Datenschutzrecht Rn. 514–516.

[116] *EDSA*, Leitlinien 05/2020 Einwilligung, Rn. 37; *Bunnenberg*, Privates Datenschutzrecht, S. 271 f.; *Buchner/Kühling* in: Kühling/Buchner, DS-GVO Art. 7 Rn. 52, 53; *Golland*, MMR 130, 134.

[117] OLG Wien vom 07.12.2020 – 11 R 153/20f, 11 R 154/20b, *Maximilian Schrems ./. Facebook Ireland Ltd.*, BeckRS 2020, 49348 Rn. 60; *DPC* (Irland), Draft Decision In the matter of LB (through NOYB) v Facebook Ireland Limited, Rn. 4.31–4.33; *Engeler*, ZD 2018, 55, 56–60; *Hofmann* in: Stiftung Datenschutz, Dateneigentum und Datenhandel, 161, 172; *Kramer* in: Eßer/Kramer/Lewinski, DSGVO Art. 7 Rn. 31; *Indenhuck/Britz*, BB 2019, 1091, 1095; *Schulz* in: Gola, DS-GVO Art. 7 Rn. 30.

[118] OLG Wien vom 07.12.2020 – 11 R 153/20f, 11 R 154/20b, *Maximilian Schrems ./. Facebook Ireland Ltd.*, BeckRS 2020, 49348 Rn. 59; *Engeler*, ZD 2018, 55, 61.

[119] *Engeler*, ZD 2018, 55, 58 f.

betroffenen Person zurück,[120] ist also ebenso sachgerecht für einen freiwillig abgeschlossenen Datenüberlassungsvertrag.

Rechtspolitisch können beide Ansichten nicht überzeugen. Die schuldrechtliche Lösung schränkt das problematische Geschäftsmodell »Leistung gegen Daten« faktisch kaum ein.[121] Aber auch die datenschutzrechtliche Lösung kann aus dem unscharfen Wortlaut des Art. 7 Abs. 4 DSGVO kaum konkrete, allgemein verbindliche Kriterien für ein Alternativangebot und für Informationspflichten entwickeln.

b) TTDSG und geplante ePrivacy-VO

Das Koppelungsverbot des Art. 7 Abs. 4 DSGVO gilt gemäß § 25 Abs. 1 S. 2 TTDSG ebenso für die Einwilligung in die Speicherung von Informationen (insbesondere Cookies) in der Endeinrichtung des Endnutzers. Damit ist die Zulässigkeit eines Datenüberlassungsvertrages ebenso unklar wie unter der DSGVO.

Im Telemediendatenschutz hat sich insbesondere bei österreichischen und deutschen Nachrichtenwebseiten teilweise eine explizite Wahl herausgebildet zwischen einem kostenlosen Angebot mit Werbetracking und einem kostenpflichtigen Angebot ohne Werbetracking. Dieses Modell ist allerdings kaum mehr als ein »Feigenblatt«, da die verlangten Preise nicht ansatzweise im Verhältnis zu dem Wert der personenbezogenen Daten stehen. Ein Seitenaufruf ohne Cookies resultiert in Werbemindereinnahmen von etwa 0,10 € pro 1.000 Seitenaufrufe.[122] Dagegen verlangt beispielsweise »Der Standard« 7 €/Monat für ein »Pur-Abo« ohne Werbetracking[123] – dies entspricht dem Mehrerlös von circa 70.000 Seitenaufrufen ohne Cookies pro Monat. Selbst für das im deutschen Sprachraum momentan günstigste Angebot der Zeitung »Die Zeit« mit 1,20 €/Monat[124] gleicht immer noch dem Gegenwert von 12.000 Seitenaufrufen pro Monat ohne Cookies. Niemand wird 12.000 oder 70.000 Seitenaufrufe pro Monat erreichen; solche Zahlen stellen erst recht nicht den Durchschnitt dar. Dennoch akzeptieren die Aufsichtsbehörden dieses Modell.[125] Die fehlende Regulierung

---

[120] BGH vom 23.06.2020 – KVR 69/19, *Facebook II*, NZKart 2020, 473 Rn. 108; *Sattler* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 225, 245.

[121] Zum AGB-Recht sogleich.

[122] *Marotta/Abhishek/Acquisti*, Online Tracking and Publishers' Revenues: An Empirical Analysis, S. 20.

[123] *Der Standard*, Abo & Angebote: Fragen & Antworten.

[124] *Die Zeit*, Pur-Abo.

[125] *Datenschutzbehörde (Österreich)*, vom 30.11.2018, DSB-D122.931/0003-DSB/2018, D.1.c. Ebenso nach Medienberichten die deutschen Aufsichtsbehörden: *Eberl*, Netzpolitik.org, Tracking auf Nachrichtenseiten: Datenschutzbehörden erhöhen den Druck auf Verlage. Die französische Aufsichtsbehörde will dagegen im Einzelfall prüfen, ob der Preis angemessen ist: *National Commission for Computing and Liberties* (Frankreich), Cookie walls : la CNIL publie des premiers critères d'évaluation, paid, Alternative payante : le tarif est-il raisonnable ? Inzwischen hat die von *Maximilian Schrems* geleitete Organisation noyb Beschwerde gegen

führt dazu, dass Webseitenbetreiber auf eine Wahlmöglichkeit verweisen können, die sie aber nur zu weit vom tatsächlichen Datenwert entfernten Preisen anbieten.

Unter der zukünftigen ePrivacy-VO ist umstritten, ob und wieweit solche Koppelungen ausgeschlossen werden sollen. Das Europäische Parlament hat in Art. 8 Abs. 1a ePrivacy-VO-E(PARL) ein striktes Koppelungsverbot aufgenommen, während Art. 8 ePrivacy-VO-E(KOM) und Art. 8 ePrivacy-VO-E(RAT) keinerlei Koppelungsverbot beinhalten. Auch hier zeichnet sich keine sachgerechte Lösung ab, sondern nur ein weiteres unscharfes Koppelungsverbot mit dem sich der europäische Gesetzgeber letztlich aus der Verantwortung stiehlt.

c) Digitale-Inhalte-RL und §§ 327–327u BGB

Erwägungsgrund 24 S. 3 der Digitale-Inhalte-RL spricht die ambivalente Haltung des europäischen Gesetzgebers besonders deutlich aus: er erkenne zwar »in vollem Umfang« an, dass Datenschutz »ein Grundrecht ist und daher personenbezogene Daten nicht als Ware betrachtet werden können«. Dennoch sei nach Erwägungsgrund 24 S. 3 ein Erstrecken der Anforderungen der Digitale-Inhalte-RL auf solche Geschäftsmodelle sinnvoll, womit die Digitale-Inhalte-RL letztlich deren Zulässigkeit unterstellt.[126]

Dementsprechend ist diese gemäß Art. 3 Abs. 1 UAbs. 2 Digitale-Inhalte-RL auch auf Verträge anwendbar, »bei denen der Verbraucher personenbezogene Daten bereitstellt oder deren Bereitstellung zusagt, außer wenn der Unternehmer die personenbezogenen Daten ausschließlich zur Bereitstellung digitaler Inhalte oder digitaler Dienstleistungen oder zur Erfüllung rechtlicher Anforderungen nutzt«. Anders als der Kommissionsvorschlag bezeichnet diese Definition wegen der grundrechtlichen Dimension des Datenschutzes personenbezogene Daten nicht als Gegenleistung, behandelt sie jedoch faktisch als solche.[127]

Inhaltlich stellt die Digitale-Inhalte-RL Leistungsstörungen bei Datenüberlassungsverträgen weitgehend Verträgen gleich, bei denen der Verbraucher ein monetäres Entgelt zahlt. So sind auf Datenüberlassungsverträgen gleichermaßen die Regelungen über die Vertragsmäßigkeit digitaler Produkte und die Nacherfüllungs- und Schadensersatzrechte anwendbar (Art. 6–13 Digitale-Inhalte-RL). Allerdings scheidet eine Preisminderung bei solchen Verträgen gemäß Art. 14 Abs. 4 Alt. 1 Digitale-Inhalte-RL aus, da die Digitale-Inhalte-RL – anders als der CCPA – personenbezogenen Daten keinen bezifferbaren Wert zuweist. Dies ist bedauernswert, weil die Wertberechnung einen Einblick in die wirtschaftlichen

---

diese Angebote eingelegt, vgl. *noyb*, News Sites: Readers need to »buy back« their own data at an exorbitant price?!.

[126] *Heckmann/Paschke* in: Ehmann/Selmayr, DS-GVO Art. 7 Rn. 95; *Loosen*, Die Rückabwicklung des Vertrages Daten gegen Leistung, S. 50, 53 f.; *Krohm/Müller-Peltzer*, ZD 2017, 551, 553; *Leistner/Antoine/Sagstetter*, Big Data, S. 256; *Metzger* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 23, 34; a. A. *Mischau*, ZEuP 2020, 335, 339 (kein Rückschluss wegen Art. 3 Abs. 8 Digitale-Inhalte-RL).

[127] *Staudenmayer*, ZEuP 2019, 663, 679.

Grundlagen des Geschäftsmodells »Leistung gegen Daten« gewähren würde.[128] Zum Ausgleich der fehlenden Preisminderung ist eine Beendigung des Vertrages auch bei geringfügigen Vertragsverstößen des Unternehmers möglich (Art. 14 Abs. 6 Digitale-Inhalte-RL *e contrario*).[129] Ansonsten lässt die Digitale-Inhalte-RL die DSGVO und die ePrivacy-RL unberührt (Art. 3 Abs. 8 UAbs. 2 Digitale-Inhalte-RL).

Der deutsche Gesetzgeber folgt mit den am 01.01.2022 in Kraft getretenen §§ 327–327u BGB eng der vollharmonisierenden Digitale-Inhalte-RL und geht inhaltlich kaum über diese hinaus.[130] Er übernimmt den Begriff der Verträge, »bei denen der Verbraucher dem Unternehmer personenbezogene Daten bereitstellt oder sich hierzu verpflichtet«, nahezu gleichlautend. Über eine reine Umsetzung der Digitale-Inhalte-RL hinausgehend bleibt gemäß § 327q Abs. 1 BGB der Vertrag wirksam, wenn der Verbraucher datenschutzrechtliche Rechte ausübt oder Erklärungen abgibt. Bei Dauerschuldverhältnissen räumt § 327q Abs. 2 BGB dem Unternehmer ein Sonderkündigungsrecht ein, wenn der Verbraucher eine datenschutzrechtliche Einwilligung widerruft und die weitere Fortsetzung des Vertrages dem Unternehmer nicht mehr zumutbar ist. Ersatzansprüche des Unternehmers sind bei einem Widerruf ausgeschlossen (§ 327q Abs. 3 BGB). Somit führt der Gesetzgeber eine klare Trennung zwischen der datenschutzrechtlichen und schuldrechtlichen Ebene herbei.[131]

d) Klausel-RL und §§ 305–310 BGB

Das AGB-Recht ist grundsätzlich auch auf vorformulierte Einwilligungserklärungen anwendbar.[132] Es ist allerdings unklar, ob das Datenschutzrecht als *lex specialis* die Inhaltskontrolle nach §§ 307 Abs. 1 S. 1, 308, 309 BGB verdrängt. So hat der BGH in *Payback* und *Happy Digits* vor Inkrafttreten der DSGVO entschieden, dass eine mit dem BDSG a.F. vereinbare Einwilligung keine von Rechtsvorschriften abweichende oder diese ergänzende Regelung sei und deswegen gemäß § 307 Abs. 3 S. 1 BGB nicht der Inhaltskontrolle unterliege.[133] Die DSGVO spricht nun in Erwägungsgrund 42 S. 3 davon, dass vorformulierte Einwilligungserklärungen keine »missbräuchlichen« Klauseln gemäß der Klausel-RL enthalten dürfen. Damit geht

---

[128] *Sattler*, CR 2020, 145, Rn. 57.

[129] Dies hält Erwägungsgrund 67 S. 2 der Digitale-Inhalte-RL explizit fest.

[130] *Rosenkranz*, ZUM 2021, 195, 200; *Spindler*, MMR 2021, 451, 457; *ders.*, MMR 2021, 528, 533.

[131] *Korch*, ZEuP 2021, 792, 794; *Sattler*, NJW 2020, 3623 Rn. 34–36; *Spindler*, MMR 2021, 528, 531.

[132] BGH vom 16.07.2008 – VIII ZR 348/06, Payback, NJW 2008, 3055 Rn. 18; vom 11.11.2009 – VIII ZR 12/08, *Happy Digits*, NJW 2010, 864 Rn. 14; *Bijok*, Kommerzialisierungsfester Datenschutz, S. 424; *Bunnenberg*, Privates Datenschutzrecht, S. 221 f.; *Engeler*, ZD 2018, 55, 56.

[133] BGH vom 16.07.2008 – VIII ZR 348/06, *Payback*, NJW 2008, 3055 Rn. 41; BGH vom 11.11.2009 – VIII ZR 12/08, *Happy Digits*, NJW 2010, 864 Rn. 16.

die DSGVO offensichtlich davon aus, dass der Maßstab der Missbräuchlichkeit des Art. 3 Klausel-RL bei vorformulierten Einwilligungserklärungen einen eigenständigen Anwendungsbereich hat.[134] Die Rechtsprechung des BGH ist daher wohl nicht mehr fortzuführen.[135]

Jedenfalls ist bei Datenüberlassungsverträgen die Inhaltskontrolle gemäß § 307 Abs. 3 S. 1 BGB unanwendbar, weil die personenbezogenen Daten als Hauptleistung oder zumindest als Bedingung für die Gegenleistung gewährt werden.[136] § 307 Abs. 3 S. 1 BGB erfasst nach seinem Wortlaut nur Regelungen, die von Rechtsvorschriften abweichen oder diese ergänzen. Insoweit ist diese Norm allerdings richtlinienkonform nach Art. 1 Abs. 2, 4 Abs. 2 Klausel-RL auszulegen.[137] Sie will nicht nur den – hier mangels bindendender Rechtsvorschriften nicht einschlägigen Art. 1 Abs. 2 Klausel-RL umsetzen, sondern auch Art. 4 Abs. 2 Klausel-RL. Hiernach erfasst die Inhaltskontrolle weder den »Hauptgegenstand« des Vertrages noch die Angemessenheit zwischen »dem Preis bzw. dem Entgelt« und Gegenleistung. Nur Klauseln, die Hauptleistungen festlegen und charakterisieren, bilden den Hauptgegenstand des Vertrages.[138] Dagegen regeln Klauseln mit akzessorischem Charakter nicht den Hauptgegenstand des Vertrages; Kriterien für die Abgrenzung sind die Natur, die Systematik und der rechtliche und tatsächliche Kontext des Vertrages.[139] Die zweite Ausnahme des Art. 4 Abs. 2 Klausel-RL (Angemessenheit von »Preis bzw. Entgelt«) hat nur einen engen Anwendungsbereich.[140] Klauseln sind trotz dieser Ausnahme

---

[134] *Bijok*, Kommerzialisierungsfester Datenschutz, S. 424; *Bunnenberg*, Privates Datenschutzrecht, S. 224; *Engeler*, ZD 2018, 55, 56; *Hacker*, Datenprivatrecht, S. 433; *Leistner/Antoine/Sagstetter*, Big Data, S. 269; *Wendehorst/Westphalen*, NJW 2016, 3745, 3748.

[135] *Bijok*, Kommerzialisierungsfester Datenschutz, S. 424; *Bunnenberg*, Privates Datenschutzrecht, S. 224 f.; *Engeler*, ZD 2018, 55, 56; *Hacker*, Datenprivatrecht, S. 433; *Langhanke*, Daten als Leistung, S. 222 f.; *Leistner/Antoine/Sagstetter*, Big Data, S. 269; *Wendehorst/Westphalen*, NJW 2016, 3745, 3748 f.

[136] *Korch*, ZEuP 2021, 792, 808–810; *Leistner/Antoine/Sagstetter*, Big Data, S. 269; *Loosen*, Die Rückabwicklung des Vertrages Daten gegen Leistung, S. 54–58; *Wendehorst/Westphalen*, NJW 2016, 3745, 3748.

[137] *Wurmnest* in: MükoBGB, BGB § 307 Rn. 13.

[138] EuGH vom 30.04.2014 – C-26/13, *Kásler und Káslerné Rábai*, ECLI:EU:C:2014:282 Rn. 49; vom 26.02.2015 – C-143/13, *Matei*, ECLI:EU:C:2015:127 Rn. 54; vom 03.10.2019 – C621/17, *Andriciuc u. a.*, ECLI:EU:C:2019:820 Rn. 35; vom 03.10.2019 – C-621/17, *Kiss und CIB Bank*, ECLI:EU:C:2019:820 Rn. 32; vom 16.07.2020 – C-224/19, *Caixabank*, ECLI:EU:C:2020:578 Rn. 62.

[139] EuGH vom 30.04.2014 – C-26/13, *Kásler und Káslerné Rábai*, ECLI:EU:C:2014:282 Rn. 51; vom 26.02.2015 – C-143/13, *Matei*, ECLI:EU:C:2015:127 Rn. 54; vom 03.10.2019 – C-621/17, *Kiss und CIB Bank*, ECLI:EU:C:2019:820 Rn. 33; vom 16.07.2020 – C-224/19, *Caixabank*, ECLI:EU:C:2020:578 Rn. 63.

[140] EuGH vom 30.04.2014 – C-26/13, *Kásler und Káslerné Rábai*, ECLI:EU:C:2014:282 Rn. 54 f.; EuGH vom 26.02.2015 – C-143/13, *Matei*, ECLI:EU:C:2015:127 Rn. 55; vom 03.10.2019 – C621/17, *Andriciuc u. a.*, ECLI:EU:C:2019:820; vom 03.10.2019 – C-621/17, *Kiss und CIB Bank*, ECLI:EU:C:2019:820 Rn. 34; vom 16.07.2020 – C-224/19, *Caixabank*, ECLI:EU:C:2020:578 Rn. 65.

kontrollfähig, wenn sie bloß einen Preis modifizieren oder Kosten für Leistungen umlegen, die auch im Interesse des Unternehmers liegen.[141]

Insoweit sind personenbezogene Daten als Gegenleistung nicht anders als ein monetäres Entgelt zu behandeln und damit als Hauptgegenstand nicht kontrollfähig.[142] Zwar mag zivilrechtlich die Bereitstellung von personenbezogenen Daten nicht als Gegenleistung einzuordnen sein, sondern als Bedingung für die Erbringung der Gegenleistung.[143] Allerdings ist die Bereitstellung personenbezogener Daten einer »echten« Hauptleistung weitgehend gleichgestellt (Art. 3 Abs. 1 UAbs. 2 Digitale-Inhalte-RL, § 312 Abs. 1a BGB). Auch lassen der Wortlaut des Art. 4 Abs. 2 Klausel-RL (»dem Preis bzw. dem Entgelt«) als auch der ohnehin offen formulierte § 307 Abs. 3 S. 1 BGB die Einordnung von personenbezogenen Daten als Entgelt zu.

Auch Klauseln, die den Hauptgegenstand festlegen, unterliegen zwar nach Art. 4 Abs. 2 Klausel-RL, § 307 Abs. 3 S. 2, Abs. 1 S. 2 BGB dem Transparenzgebot. Verwender:innen müssen jedoch nach dem Transparenzgebot keine über Art. 13, 14 DSGVO hinausgehenden Informationen mitteilen.[144] Damit ist auch die Transparenzkontrolle bei Datenüberlassungsverträgen nicht hilfreich, da Kerninformationen über die wirtschaftliche Transaktion wie der Datenwert fehlen.

Als Lösungsmöglichkeit will *Hacker* Art. 4 Abs. 2 Klausel-RL bei Datenüberlassungsverträgen teleologisch reduzieren und diese damit der Inhaltskontrolle unterwerfen.[145] Verbraucher:innen würden nur einem Preis in Geld Aufmerksamkeit schenken. Eine datenbasierte Gegenleistung sei dagegen für Verbraucher:innen kaum verständlich und werde ignoriert.[146] Auch könnten Verbraucher:innen den Wert ihrer personenbezogenen Daten nicht einschätzen, weshalb Preisbildungsmechanismen nicht funktionierten.[147] Das daraus resultierende rationale Desinteresse sei gerade die Situation, welche die Klausel-RL lösen will.[148] Daran ist korrekt, dass für viele Verbraucher Datenüberlassungsverträge

---

[141] EuGH vom 26.02.2015 – C-143/13, *Matei*, ECLI:EU:C:2015:127 Rn. 56.

[142] *Leistner/Antoine/Sagstetter*, Big Data, S. 269; *Wendehorst/Westphalen*, NJW 2016, 3745, 3748.

[143] Für eine Gegenleistungspflicht: *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 268; *Leinemann*, Personenbezogene Daten als Entgelt, S. 100–120; *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, Rn. 343; *dies.*, JZ 2017, 763, 768 f.; *Langhanke*, Daten als Leistung, S. 97 f.; *Metzger*, 216 AcP 216 (2016), 817, 833–835. Für eine Bedingung: *Hacker*, ZfPW 2019, 148, 167–177.

[144] BGH vom 28.05.2020, *App-Zentrum*, juris Rn. 28– 30: Art. 12–14 DSGVO seien »maßgeblich« für Informationspflichten nach § 307 BGB; *Hacker*, Datenprivatrecht, S. 426–430 m. w. N. zu Rechtsprechung unter der DSRL; *Wendehorst/Westphalen*, NJW 2016, 3745, 3748.

[145] *Hacker*, Datenprivatrecht, S. 435–439; *ders.* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 47, 64–69; *ders.*, ZfPW 2019, 148, 187 f.

[146] *Hacker*, Datenprivatrecht, S. 438.

[147] Ebd., S. 438.

[148] Ebd., S. 439.

de lege lata schwer verständlich sind. Allerdings sieht Art. 4 Abs. 2 Klausel-RL das Problem intransparenter Hauptleistung durchaus. Nach dieser Norm müssen Klauseln, die den Hauptgegenstand bilden, nur »klar und verständlich« sein, während eine Inhaltskontrolle auch bei einem intransparentem Hauptgegenstand nicht erfolgt. Außerdem führt der Unangemessenheitsmaßstab mangels klarer Kriterien für die Angemessenheit von »Datenpreis« und Leistung zu erheblicher Rechtsunsicherheit – wie auch *Hacker* selbst einräumt.[149]

Insgesamt ist das bisherige Datenschutz- und Datenschuldrechts unzureichend. Sowohl Art. 7 Abs. 4 DSGVO als auch Art. 3 Abs. 1a Digitale-Inhalte-RL sind politische Minimalkompromisse, welche die problematischen Fragen weitgehend umschiffen. Auch bei der ePrivacy-VO zeichnet sich keine Lösung ab. Die Klausel-RL löst das Problem ebenso wenig, da sie nicht auf den Hauptgegenstand des Vertrages anwendbar ist. Der deutsche Gesetzgeber beschränkt sich vor allem darauf, die Digitale-Inhalte-RL und Klausel-RL umzusetzen, und regelt nur einzelne schuldrechtliche Folgen dieses Vertragstyps.

3. Regelungsalternativen de lege ferenda *im Überblick*

In der deutschen Rechtswissenschaft hat sich angesichts der unzureichenden gesetzlichen Regelung eine umfangreiche Diskussion über die Regulierung des Geschäftsmodells »Leistung gegen Daten« *de lege ferenda* entwickelt.[150] Diese zunächst eher vage Diskussion hat sich immer mehr auf konkrete Lösungsvorschläge zugespitzt.[151]

Anfangs wurde häufig unter dem plakativem Schlagwort »Dateneigentum« die Schaffung eines Ausschließlichkeitsrecht an personenbezogenen und nichtpersonenbezogenen Daten diskutiert.[152] Ein solches *erga omnes* wirkendes, übertragbares Recht hat sicherlich viele Vorteile. So existieren mit dem Eigentumsrecht, Besitzrecht und Urheberrecht bereits etablierte und ausdifferenzierte Rechtsinstitute, an denen man sich orientieren könnte.[153] Auch könnte ein

---

[149] Ebd., S. 459. Hacker schlägt insoweit eine Reform der §§ 308 f. BGB vor. Diese könnte, wenn man *Hackers* Bedingungen folgt, sich auch an den unten dargestellten Grundsätzen orientieren.

[150] Allein themenspezifische Monografien und Sammelbände (jeweils passim): *Bijok*, Kommerzialisierungsfester Datenschutz; *Haag*, Bonusprogramme; *Haustein*, Möglichkeiten und Grenzen von Dateneigentum; *Loosen*, Die Rückabwicklung des Vertrages Daten gegen Leistung; *Jöns*, Daten als Handelsware; *Langhanke*, Daten als Leistung; *Leinemann*, Personenbezogene Daten als Entgelt; Lohsse/Schulze/Staudenmayer, Data as Counter-Performance; *Schmidt*, Datenschutz als Vermögensrecht; Stiftung Datenschutz, Dateneigentum und Datenhandel; Pertot, Rechte an Daten.

[151] *Leistner/Antoine/Sagstetter*, Big Data, S. 24.

[152] Diesen Begriff prägend: *Hoeren*, MMR-Beil. 1998, 6, 9; *ders.*, MMR 2013, 486–491. *Hoeren* hat im Nachgang betont, dass er sich nur zu einer Analogie zu § 903 BGB *de lege lata* äußern wollte, vgl. *Hoeren* in: Pertot, Rechte an Daten, 37, 39.

[153] Besitz als Vorbild: *Hoeren*, MMR 2019, 5–8. Eigentum als Vorbild: *Amstutz*, AcP 218 (2018), 438, 541–551; *Haustein*, Möglichkeiten und Grenzen von Dateneigentum, S. 195 f.

Dateneigentum Datensouveränität begründen, indem es Individuen Kontrolle über ihre Daten ermöglicht.[154] Allerdings führt ein Ausschließlichkeitsrecht potenziell zu einer stärkeren Konzentration auf besonders große, datenmächtige Unternehmen, die dadurch Konkurrenten ausschließen könnten.[155] Zudem ist ein solches Dateneigentum nur schwer mit dem bisherigen Datenschutzrecht kompatibel.[156] Damit wirft ein Dateneigentum letztlich mehr Probleme auf, als es löst. Die Europäische Kommission zeigte sich zwar 2017 gegenüber der Einführung eines Dateneigentums offen,[157] erwähnt das Dateneigentum aber in ihrer neusten Datenstrategie nicht mehr.[158] Auch auf nationaler Ebene lehnen sowohl die Datenethikkommission[159] als auch die Datenstrategie der Bundesregierung[160] ein Dateneigentum explizit ab. Damit gilt die Dateneigentums-Diskussion weitgehend als beendet.[161]

Stattdessen wird vor allem eine evolutive Reform des bestehenden Datenschutz- und Datenschuldrecht erwogen. Für manche Konstellationen mag eine Datentreuhand zwischen betroffenen Personen und Datennutzende eine sachgerechte Lösung sein, wie sie insbesondere die Data-Governance-VO vorsieht.[162] Ein solcher Intermediär ergänzt jedoch eher die privatautonome Entscheidung der jeweiligen betroffenen Person. So sollen die Datenvermittlungsdienste der Data-Governance-VO betroffene Personen im Hinblick auf die Vertragsbedingungen nur »beraten« (Art. 12 lit. m Data-Governace-VO), sodass die Entscheidung über den Vertragsschluss weiterhin bei den betroffenen Personen bleibt. Inwieweit Datenüberlassungsverträge zulässig sind, wäre weiterhin unklar. Zusätzliche Auskunfts- oder Portabilitätsrechte könnten ebenfalls hilfreich sein,[163] setzen aber

---

Urheberrecht als Vorbild: *Jöns*, Daten als Handelsware, S. 188–257. Übersicht m. w. N.: *Bijok*, Kommerzialisierungsfester Datenschutz, S. 373–378.

[154] *Bijok*, Kommerzialisierungsfester Datenschutz, S. 393–395, 424f; *Kilian* in: Stiftung Datenschutz, Dateneigentum und Datenhandel, 191, 201.

[155] *Drexl et al.*, GRUR Int. 2016, 914 Rn. 6; *Kühling/Sackmann*, ZD 2020, 24, 27 f.; *Riechert* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 267, 269.

[156] *Dix*, ZEuP 2017, 1, 2 f.; *Richter/Hilty* in: Stiftung Datenschutz, Dateneigentum und Datenhandel, 241, 252–254. Ebenso in der parallelen amerikanischen Diskussion: *Determann*, 70 Hastings L. J. 1, 37–38.

[157] *Europäische Kommission*, Europäische Datenwirtschaft, COM(2017) 9 final, Nr. 3.3.

[158] *Europäische Kommission*, Europäische Datenstrategie, COM(2020) 66 final, passim.

[159] *Datenethikkommission*, Gutachten, S. 104.

[160] *Bundesregierung*, Datenstrategie der Bundesregierung, S. 23. Auch der Koalitionsvertrag der »Ampelkoalition« erwähnt kein Dateneigentum: *SPD/Bündnis 90/Die Grünen/FDP*, Koalitionsvertrag 2021–2025, passim.

[161] *Hoeren* in: Pertot, Rechte an Daten, 37, 40; *Korch*, ZEuP 2021, 792 Fn. 3; *Leistner/Antoine/Sagstetter*, Big Data, S. 23; *Westphalen*, IWRZ 2018, 9, 14.

[162] Siehe Kapitel 3:C.I.2.d)dd) (ab S. 97).

[163] *Drexl* in: Bundesministerium der Justiz und für Verbraucherschutz/Max-Planck-Institut für Innovation und Wettbewerb, Data Access, Consumer Interests and Public Welfare, 477, 499–525, *ders*, NZKart 2017, 415; *Richter/Hilty* in: Stiftung Datenschutz, Dateneigentum und Datenhandel, 241, 256–258.

ebenso eine privatautonome Entscheidung zur Kommerzialisierung personenbezogener Daten voraus. Weiterhin sind Vorschläge, die ein Marktversagen in einer bestimmten Branche lösen wollen,[164] keine Alternative zu einer allgemeinen Regulierung von Datenüberlassungsverträgen, sondern eine Ergänzung.

Das Einschalten einer Verwertungsgesellschaft für eine kollektive Vergütung kommerzialisierter personenbezogener Daten spielt eine kleinere Rolle in der gegenwärtigen Diskussion.[165] Auch der kalifornische Gouverneur *Gavin Newsoom* hat mit seiner »Data Dividend« ein ähnliches Konzept vorgeschlagen.[166] Sowohl in Deutschland als auch in Kalifornien stößt aber auf Skepsis, ob die Kollektivierung dieser Rechte wirklich sinnvoll ist.[167] Sie ist zumindest dann überflüssig, wenn auch eine an der Privatautonomie orientierte Regulierung von Daten als Gegenleistung möglich ist.[168]

III. Entwicklung eines Regelungsvorschlags

1. Eignung der kalifornischen Lösung

Als solche privatautonome Regelungsalternative bietet sich die Regelung zu finanziellen Anreizen des CCPA an. Sie ist hochgradig entwickelt und detailreich kodifiziert,[169] was ihre Übernahme erleichtert. Gleichzeitig ist sie inhaltlich ausgewogen.

Der kalifornischen Lösung gelingt der Spagat zwischen Privatautonomie und Schutz vor einer übermäßigen Kommerzialisierung. Sie nimmt Privatautonomie ernst, indem sie die Zulässigkeit von Daten als Gegenleistung explizit anerkennt.[170] Zudem schafft sie durch die verpflichtende Angabe des Datenwerts Transparenz. Betroffene Personen können so erkennen, dass es sich um eine wirtschaftliche Transaktion handelt und grob den Marktwert ihrer personenbezogenen Daten einschätzen. Die Pflicht zu einem Alternativangebot, das sich am Datenwert orientiert, stellt sicher, dass es sich wirklich um eine freiwillige Wahl handelt.

Gleichzeitig nimmt der CCPA Risiken einer Kommerzialisierung personenbezogener Daten ernst. So erfasst die Ausnahme für finanzielle Anreize nicht das Recht auf Beschränkung sensibler Informationen.[171] Damit unterliegen gerade

---

[164] Einen solchen Vorschlag entwickelt insbesondere *Hacker*, Datenprivatrecht, S. 620–656.

[165] Ein solches Rechtsinstitut entwickelnd: *Fezer*, Repräsentatives Dateneigentum, S. 77–85.

[166] *Au-Yeung*, Forbes, California Wants To Copy Alaska And Pay People A 'Data Dividend.' Is It Realistic?

[167] Skeptisch zu *Fezers* Vorschlag: *Leistner/Antoine/Sagstetter*, Big Data, S. 24. Skeptisch zu parallelen amerikanischen Vorschlägen: *Harris*, 54 Loy. L. A. L. Rev. 197, 224 f.; *Lyon/Moerel*, Privacy Perspectives, Why placing a price tag on personal data may harm consumer privacy; *Tsukayama*, Electronic Frontier Foundation, Why Getting Paid for Your Data Is a Bad Deal.

[168] *Leistner/Antoine/Sagstetter*, Big Data, S. 24.

[169] Cal. Civ. Code § 1798.125(b), 11 C. C. R. § 7016, 336, 337.

[170] Cal. Civ. Code § 1798.125(b)(1).

[171] Siehe Kapitel 3:C.II.2 (ab S. 114).

die besonders sensiblen, für betroffene Personen risikoreichen Informationen nicht einer Kommerzialisierung.

Es ist allerdings sinnvoll, nur die Regelung finanzieller Anreize selbst zu übernehmen, nicht das Maßregelungsverbot in Gänze.[172] Die Regelung finanzieller Anreize ist nur deshalb im allgemeinen Maßregelungsverbot verankert, weil der CCPA einen *opt-out*-Mechanismus verfolgt: Verbraucher:innen müssen zuerst dem Datenhandel widersprechen.[173] Erst dann ist ein vergleichbarer Zustand mit dem in Europa *ipso iure* geltenden Verbot mit Erlaubnisvorbehalt des Art. 6 Abs. 1 DSGVO hergestellt. Eine bloße Übernahme des Maßregelungsverbots würde dem nicht gerecht werden, da sie nur die Rechte der Art. 15–22 DSGVO erfassen würde, nicht aber das Verbot mit Erlaubnisvorbehalt des Art. 6 DSGVO. Die Regelung finanzieller Anreize ist vom Maßregelungsverbot abtrennbar, da der Gesetzgeber des CCPA den *opt-out*-Mechanismus ohnehin nur aufgrund der überragenden Bedeutung der Meinungsfreiheit gewählt hat.[174] Die Regelung muss allerdings an das Verbot mit Erlaubnisvorbehalt angepasst werden, das in praktischer Konsequenz einen *opt-in*-Mechanismus für Datenüberlassungsverträge etabliert.[175]

Eine solche punktuelle Lösung ist realistischer als eine umfassende Reform des Datenschutzrechts. Es ist kaum damit zu rechnen, dass der europäische Gesetzgeber das weit entwickelte europäische Datenschutzrecht grundlegend ändert. So ähnelte auch die DSGVO der DSRL bereits stark.[176] Zwar plant die EU mit dem Gesetz über digitale Dienste,[177] dem Gesetz über digitale Märkte[178] und der bereits oben diskutierten Data-Governance-VO[179] durchaus eine weitere Regulierung des digitalen Binnenmarkts. Diese lassen die DSGVO allerdings unberührt (Art. 1 Abs. 4 lit. g Gesetz-über-digitale-Dienste-E, Art. 1 Abs. 3 Data-Governance-VO, Art. 1 Abs. 5 lit. i Gesetz-über-digitale Märkte-E), genauso wie schon zuvor die Digitale-Inhalte-RL (Art. 3 Abs. 8 UAbs. 2 Digitale-Inhalte-RL). Eine revolutionäre Änderung des Datenschutzrechts ist demnach nicht zu erwarten.

---

[172] Eine Übernahme des Maßregelungsverbots andenkend: *Specht-Riemenschneider* in: Bundesministerium der Justiz und für Verbraucherschutz/Max-Planck-Institut für Innovation und Wettbewerb, Data access, consumer interests and public welfare, 401, 414.

[173] Cal. Civ. Code § 1798.120(a). Siehe Kapitel 3:C.II.2 (ab S. 114).

[174] Siehe Kapitel 3:C.I.1 (ab S. 81).

[175] Siehe Kapitel 3:C.I.2.d)bb) (ab S. 95).

[176] *Kühling/Martini*, EuZW 2016, 448, 454.

[177] *Europäisches Parlament*, Legislative Entschließung zum Gesetz über digitale Märkte (COM(2020)0842 – C9-0419/2020 – 2020/0374(COD)). Die Veröffentlichung im Amtsblatt nach der Einigung im Trilog steht noch aus.

[178] *Europäisches Parlament*, Legislative Entschließung zum Gesetz über digitale Dienste (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD)). Die Veröffentlichung im Amtsblatt nach der Einigung im Trilog steht ebenfalls noch aus.

[179] Siehe Kapitel 3:C.I.2.d)dd) (ab S. 97).

Dennoch ist das Europarecht nicht in Stein gemeißelt. Punktuelle Änderungen wie bei der Überarbeitung der ePrivacy-RL 2009, bei welcher der europäische Gesetzgeber die kalifornische Datenmeldepflicht übernahm, sind durchaus realistisch. Sie müssen sich allerdings in das bisherige Recht einfügen.

2. Regelungsstandort: neuer Art. 8a DSGVO-E

a) Verankerung im europäischen oder nationalen Recht?

Zuerst ist zu klären, ob die Regelung auf nationaler oder europäischer Ebene zu verorten ist. Auf nationaler Ebene wäre eine Aufnahme in das allgemeine Schuldrecht des BGB naheliegend, da Datenüberlassungsverträge unabhängig vom Vertragstyp regulierungsbedürftig sind. Allerdings würde eine Aufnahme in das nationale Schuldrecht notwendigerweise zu Konflikten mit der vorrangig anwendbaren DSGVO führen. Angesichts des konfusen Koppelungsverbots (Art. 7 Abs. 4 DSGVO), aus dem die datenschutzrechtliche Lösung konkrete Anforderungen für Datenüberlassungsverträge ableitet, ist ein direkter Konflikt denkbar. Wenn man – wie hier vertreten – der schuldrechtlichen Lösung folgt, spielt das nationale Schuldrecht *de lege lata* eine größere Rolle.[180] Es ist dafür maßgeblich, welche Verträge wirksam sind und damit ob der Verantwortliche seine Datenverarbeitung auf Art. 6 Abs. 1 S. 1 lit. b DSGVO stützen kann.
Allerdings steht eine Regelung auch nach der schuldrechtlichen Lösung unter dem Vorbehalt, dem *effet utile* der DSGVO (Art. 4 Abs. 3 EUV) nicht zu widersprechen. Damit ist der Spielraum des nationalen Gesetzgebers vergleichsweise klein.[181] Denn die DSGVO regelt nicht nur einen Mindeststandard, sondern auch einen Höchststandard für Datenschutz. Sie will auch Handelshemmnisse durch unterschiedliche Datenschutzanforderungen der Mitgliedsstaaten verhindern (Erwägungsgrund 2 S. 2 der DSGVO). Unterschiedliche Anforderungen an die Zulässigkeit des Geschäftsmodells »Leistung gegen Daten« würden wohl solche Handelshemmnisse begründen. So verstößt beispielsweise ein Mitgliedsstaat angesichts der umfangreichen Informationspflichten des Art. 13, 14 DSGVO gegen deren *effet utile*, wenn er für bestimmte Datenverarbeitungen zusätzliche Informationspflichten einführt.[182]

Datenüberlassungsverträge stehen an der Schnittstelle von Datenschutz- und Datenschuldrecht, ohne dass sie klar und überzeugend einer Materie komplett zugeordnet werden könnten. Eine Lösung im nationalen Schuldrecht steht damit im potenziellen Widerspruch zum europaweit einheitlichen Datenschutzrecht. Auch eine knapp den *effet utile* umschiffende Lösung würde erhebliche Rechtsunsicherheit auslösen, da stets unklar wäre, ob sie gegen die vorrangig anwendbare und hinsichtlich Datenüberlassungsverträgen unscharfe DSGVO verstoßen könnte. Daher ist es vorzugswürdig, das Problem auf europäischer Ebene zu lösen.

---

[180] *Engeler*, ZD 2018, 55, 61.
[181] *Korch*, ZEuP 2021, 792, 810–813.
[182] Umfassend zum *effet utile* im Datenschutzrecht: *Hacker*, Datenprivatrecht, S. 326–343.

b) Aufnahme in Digitale-Inhalte-RL, Klausel-RL oder DSGVO?

Im europäischen Recht kommt zunächst eine Verortung in der Digitale-Inhalte-RL in Betracht, die explizit Datenüberlassungsverträge anspricht (Art. 3 Abs. 1 UAbs. 2 Digitale-Inhalte-RL) und Leistungsstörungen bei solchen Verträgen bereits regelt (Art. 6–21 Digitale-Inhalte-RL). Allerdings will sie nach ihrer bisherigen Systematik nicht den Datenschutz mitregeln, sondern die DSGVO unberührt lassen (Art. 3 Abs. 8 UAbs. 2 Digitale-Inhalte-RL).[183] Auch würde eine Verankerung der Regelung innerhalb der Digitale-Inhalte-RL nur Verträge erfassen, bei denen ein Unternehmer dem Verbraucher digitale Inhalte oder digitale Dienstleistungen bereitstellt (Art. 3 Abs. 1 Digitale-Inhalte-RL). Damit wären Datenüberlassungsverträge in der analogen Welt nicht erfasst. Diese sind aber durchaus praxisrelevant, wie auch die Gesetzesbegründung des deutschen Umsetzungsgesetzes zur Digitale-Inhalte-RL betont – insbesondere sind Rabatte als Gegenleistung für die Datensammlung durch Kundenkartensysteme weit verbreitet.[184]

Auch auf Verträge in der analogen Welt anwendbar und damit ein weiterer möglicher Regelungsstandort ist die Klausel-RL. *Ratio legis* der Klausel-RL ist, dass sich der Verbraucher in einer schwächeren Verhandlungsposition befindet und über weniger Informationen verfügt.[185] Genau diese Situation liegt *de lege lata* bei dem Datenüberlassungsverträgen vor: betroffene Personen kennen den Wert ihrer Daten nicht und sind damit in einer schwachen Position.[186] Allerdings will die Klausel-RL gerade das »Kleingedruckte« regulieren, das Verbraucher typischerweise nicht wahrnehmen. Bei dem Hauptgegenstand des Vertrages findet gemäß Art. 4 Abs. 2 Klausel-RL gerade keine Inhaltskontrolle statt, da dieser der Aufmerksamkeit der Vertragsparteien unterliegt.[187] Daher wäre eine Regelung in der Klausel-RL ein Fremdkörper

Daneben ist auch eine Aufnahme in die Verbraucherrechte-RL denkbar, da die Regelung finanzieller Anreize des CCPA vor allem auf Verbraucher:innen zugeschnitten ist. Allerdings regelt die Verbraucherrechte-RL bisher nur die Modalitäten des Vertragsschlusses, nicht die Zulässigkeit von Vertragstypen.

Die Regelung passt somit am besten in die DSGVO, die als die zentrale europäische Datenschutzregulierung die Abwägung zwischen Kommerzialisierung der Persönlichkeit und Privatautonomie treffen sollte. Eine Regelung direkt in der DSGVO kann der europäische Gesetzgeber besser mit dem Koppelungsverbot des Art. 7 Abs. 4 DSGVO und den Informationspflichten des Art. 13, 14 DSGVO abstimmen. Dem könnte man entgegen, dass die Regelung zivilrechtlich sei

[183] Vgl. *Mischau*, ZEuP 2020, 335, 341: Digitale-Inhalte-RL schütze Verbraucher im »vertragsrechtlichen Kontext«, DSGVO verteidige Grundrechte der betroffenen Personen.

[184] BT-Drs. 19/27653, 35. Ebenso: *Buchner*, DuD 2010, 39, 39; *Mischau*, ZEuP 2020, 335, 353.

[185] EuGH vom 30.04.2014 – C-26/13, *Kásler und Káslerné Rábai*, ECLI:EU:C:2014:282 Rn. 39; vom 26.02.2015 – C-143/13, *Matei*, ECLI:EU:C:2015:127 Rn. 51.

[186] *Hacker*, Datenprivatrecht, S. 438.

[187] *Wurmnest* in: MükoBGB, BGB § 307 Rn. 13.

und daher besser in das Datenschuldrecht passt. Allerdings enthält die DSGVO auch sonst zahlreiche zivilrechtliche Regelungen.[188] So sind die Art. 15–21, 82 DSGVO originär zivilrechtliche Ansprüche. Auch beinhalten Art. 26 Abs. 1 S. 2, Abs 2, 28 Abs. 3 UAbs. 1 DSGVO detaillierte Vorgaben für den Inhalt bestimmter zivilrechtlicher Verträge. Ähnlich zu diesen Verträgen ist es sinnvoll, die Zulässigkeit von Datenüberlassungsverträgen und die damit verbundenen Informationspflichten in der DSGVO zu regeln. Der Vertragsschluss selbst und die Leistungsstörungen sollten dagegen weiterhin der Digitale-Inhalte-RL, der Verbraucherrechte-RL und dem nationalen Datenschuldrecht überlassen bleiben.

c) Verortung innerhalb der DSGVO

An welcher Stelle ist eine solche Regelung in der DSGVO zu verankern? Um mit der bisherigen Systematik der DSGVO vereinbar zu sein, muss die Regelung an eine der bestehenden Rechtsgrundlagen des Art. 6 Abs. 1 S. 1 DSGVO anknüpfen. Diese bilden eine Stufenleiter der Privatautonomie:[189] die Einwilligung des Art. 6 Abs. 1 S. 1 lit. a DSGVO drückt den höchsten Grad der Privatautonomie aus, während die Rechtsgrundlage Vertrag Art. 6 Abs. 1 S. 1 lit. b DSGVO auf einer leicht schwächeren privatautonomen Entscheidung beruht. Demgegenüber basieren Art. 6 Abs. 1 S. 1 lit. c–f DSGVO auf einer heteronomen Entscheidung und sind daher für privatautonome Datenüberlassungsverträge nicht geeignet. Man könnte zunächst an die Rechtsgrundlage der Einwilligung des Art. 6 Abs. 1 S. 1 lit. a DSGVO anknüpfen, die besonders hohe Anforderungen an die autonome Entscheidung der betroffenen Person stellt. So muss die betroffene Person gemäß Art. 4 Nr. 11 DSGVO freiwillig, informiert, spezifisch und unmissverständlich einwilligen. Freiwillig handelt nur, wer bei Verweigerung oder Zurückziehen der Einwilligung keine Nachteile befürchten muss (Erwägungsgrund 42 S. 5 der DSGVO). Bei einem klaren Ungleichgewicht zwischen betroffener Person und Verantwortlichem scheidet Freiwilligkeit dagegen aus (Erwägungsgrund 43 S. 1 der DSGVO). Dieser Grad an Freiwilligkeit ist sehr hoch. Beispielsweise ist die Einwilligung nach dem Europäischen Datenschutzausschuss selbst bei den – hohen ethischen Standards unterliegenden – medizinischen Studien »in den meisten Fällen«[190] unfreiwillig, da schon das Angehören zu einer sozial benachteiligten Gruppe oder ein schlechter Gesundheitszustand Freiwilligkeit ausschließe. Überdies kann die betroffene Person ihre Einwilligung gemäß Art. 7 Abs. 3 S. 1 DSGVO jederzeit ohne Angabe eines Grundes widerrufen, was zwingendes Recht ist.[191] Solch beträchtliche Vorgaben an die autonome Entscheidung

[188] *Hacker*, ZfPW 2019, 148, 150.

[189] Eine solche Unterscheidung nach Autonomiestufen entwickelnd: *Sattler* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 225, 245. Eine »Stufenleiter der Gestattungen« hat erstmals entwickelt: *Ohly*, Volenti non fit iniuria, S. 141–177.

[190] *EDSA*, Stellungnahme 3/2019 Verordnung über klinische Prüfungen, Rn. 20.

[191] *Schmidt-Kessel* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 129, 138; *Spindler/Dalby* in: Spindler/Schuster, DS-GVO Art. 7 Rn. 12; *Stemmer* in: BeckOK

lassen die Einwilligung kaum für Datenüberlassungsverträge geeignet erscheinen, selbst wenn man vom Koppelungsverbot des Art. 7 Abs. 4 DSGVO absieht. *Sattler* will insoweit verschiedene Stufen der Einwilligung schaffen und an eine schuldrechtliche Einwilligung niedrigere Maßstäbe anlegen.[192]

Dafür besteht aber kein Bedarf, da für Verträge bereits die besser geeignete Rechtsgrundlage des Art. 6 Abs. 1 S. 1 lit. b DSGVO greift. Diese steht auf der Stufenleiter der Privatautonomie niedriger als die Einwilligung, beruht aber dennoch auf der privatautonomen Entscheidung der betroffenen Person zum Vertragsschluss.[193] Es ist auch systematisch sachgerecht, für Datenüberlassungsverträge an der primären Rechtsgrundlage für Verträge anzuknüpfen. Zwar besteht bei Art. 6 Abs. 1 S. 1 lit. b DSGVO kein Widerrufsrecht. Die betroffene Person ist allerdings nicht schutzlos gestellt, da sie immer noch den Vertrag kündigen kann. Auch der Widerruf der Einwilligung wirkt nur *ex nunc* (Art. 7 Abs. 3 S. 2 DSGVO). Zuzugeben ist, dass die betroffene Person eine vertragliche oder gesetzliche Kündigungsfrist abwarten muss. Dies ist aber angesichts der bewussten Entscheidung für den Vertrag gerechtfertigt. Damit besteht im Rahmen der DSGVO kein Bedürfnis, eine schwächere Form der Einwilligung zu schaffen. Vielmehr ist es vorzugswürdig, die Regelung der Datenüberlassungsverträge an Art. 6 Abs. 1 S. 1 lit. b DSGVO anzuknüpfen.[194]

Die neue Regelung sollte der europäische Gesetzgeber nach den Art. 7, 8 DSGVO einfügen, welche die Einwilligung als die in Art. 6 Abs. S. 1 DSGVO zuerst genannte Rechtsgrundlage näher bestimmen. Parallel dazu könnte die zweitgenannte Rechtsgrundlage in einer darauffolgenden Norm konkretisiert werden. Um eine Verschiebung aller nachfolgenden 91 Artikel zu vermeiden, sollte die neue Norm als Buchstabennorm eingefügt werden, wie sie auch sonst im europäischen Recht üblich sind.[195] Damit bietet sich an, die Regelung als »Artikel 8a« in die DSGVO aufzunehmen. Als Überschrift ist »Bedingungen für Datenüberlassungsverträge« sinnvoll. »Datenüberlassungsverträge« fasst die Sachlage gut zusammen: die betroffene Person überlässt personenbezogene Daten, überträgt aber kein Ausschließlichkeitsrecht an diesen. »Bedingungen« knüpft an die amtliche Überschrift der Art. 7, 8 DSGVO an.

DatenschutzR, DS-GVO Art. 7 Rn. 90 a. A. *Sattler* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 225, 246–248; *ders.*, NJW 2020, 3623 Rn. 38.

[192] *Sattler* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 225, 243–248 a. A. *Hacker*, Datenprivatrecht, S. 162 f.

[193] BGH vom 23.06.2020, *Facebook II*, NZKart 2020, 473 Rn. 108, *Sattler* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 225, 245.

[194] Die Regelung finanzieller Anreize eignet sich aber genauso für ein Anknüpfen an Art. 6 Abs. 1 S. 1 lit. a DSGVO. Auch der unten entworfene Regelungsvorschlag könnte im Wesentlichen hierfür übernommen werden.

[195] Z. B. Art. 2a Richtlinie 2010/31/EU des Europäischen Parlaments und des Rates vom 19. Mai 2010 über die Gesamtenergieeffizienz von Gebäuden, Art. 1a, 3a Verordnung (EU) Nr. 1352/2014 des Rates vom 18. Dezember 2014 über restriktive Maßnahmen angesichts der Lage in Jemen.

Der neue Art. 8a DSGVO-E wird im Folgenden nach dem kalifornischen Vorbild näher ausgestaltet. Es ist zwar sicher möglich, an der einen oder anderen Stelle eine andere Meinung zu vertreten. Ein konkreter Regelungsvorschlag ist aber dennoch sinnvoll, um die bisher nebulöse und unscharfe Debatte um Datenüberlassungsverträge voranzubringen.

3. Inhalt des neuen Art. 8a DSGVO-E »Bedingungen für Datenüberlassungsverträge«

a) Absatz 1: Grundsätzliche Zulässigkeit des Datenüberlassungsvertrages

Wie ist der Begriff »Datenüberlassungsverträge« zu definieren? Eine trennscharfe Definition ist von zentraler Bedeutung, da der Gesetzgeber sonst »im Nebel stochert«. Unter dem Schlagwort »Leistung gegen Daten« werden zahlreiche verschiedene Geschäftsmodelle diskutiert, die meist nur eine Verarbeitung personenbezogener Daten in einem kommerziellen Zusammenhang gemein haben. Teilweise heißt es sogar polemisch: »Wenn es dich nichts kostet, bist du das Produkt.«[196] Nicht jedes kostenlose Angebot, bei dem der Verantwortliche personenbezogene Daten erhebt, finanziert sich aber durch diese personenbezogenen Daten.[197] Es ist jedoch nur dann sinnvoll, Leistungen als Gegenleistung zu behandeln, wenn diese wirtschaftlich betrachtet tatsächlich eine Gegenleistung sind. Das heißt nicht, dass die weiteren unter dem Schlagwort »Leistung gegen Daten« diskutierten Geschäftsmodelle nicht regulierungsbedürftig sind, sondern nur, dass eine auf Hauptleistungen zugeschnittene Regelung wie die finanziellen Anreize des CCPA unpassend wäre. Eine klare Abgrenzung verhindert auch, dass Verantwortliche beliebige übermäßige Datensammelei als privatautonome Entscheidung der betroffenen Person legitimieren.[198]

Ein in der Praxis lang etablierter Datenüberlassungsvertrag ist die Erhebung von personenbezogenen Daten für Marktforschung im Gegenzug für die Erbringung eines Dienstes oder der Gewährung eines Rabattes.[199] Ein Beispiel sind Kundenkartensysteme, bei denen Kund:innen einen Rabatt erhalten, wenn sie im Gegenzug die Erhebung von Daten über ihr Einkaufsverhalten gestatten.[200] Ein ähnliches Modell verfolgt Microsoft Corp., das Testversionen von Windows auch ohne monetäres Entgelt anbietet, wenn Nutzer:innen das Sammeln von umfassenden Nutzungsdaten zur Fehlerbehebung gestatten.[201] Ein weiterer

---

[196] *Tönnesmann*, Die Zeit, Das Produkt bist du.

[197] Ebenfalls für ein enges Verständnis von »Leistung gegen Daten«: *Härting*, CR 2016, 735, 737 f. Für ein weites Verständnis: *Hacker*, Datenprivatrecht, S. 53–55; *Rogosch*, Die Einwilligung im Datenschutzrecht, S. 41f; *Unseld*, Die Kommerzialisierung personenbezogener Daten, S. 3–5.

[198] *Waldman*, Privacy, Practice, and Performance, S. 37–41, der dieses Argumentationsmuster treffend »weaponizing consent« nennt.

[199] *Hacker*, Datenprivatrecht, S. 54; *ders.*, ZfPW 2019, 148, 154.

[200] BT-Drs. 19/27653, 35; *Rogosch*, Die Einwilligung im Datenschutzrecht, S. 41.

[201] *Microsoft*, Microsoft Windows Insider Program Agreement, 3.

klassischer Anwendungsfall sind Gewinnspiele, bei denen Teilnehmende ihre personenbezogenen Daten für Werbezwecke im Gegenzug für eine Gewinnchance bereitstellen.[202]

Dagegen ist bei Freemium-Geschäftsmodellen die Bereitstellung der personenbezogenen Daten keine Hauptleistung. Bei diesen wird eine Basisversion kostenlos angeboten, während die Vollversion kostenpflichtig ist.[203] Die kostenlose Probeversion ermöglicht es dem Anbieter, zahlreiche Kund:innen zu gewinnen, die wiederum über Mundpropaganda weitere Kundschaft anwerben.[204] Schon ein kleiner Anteil zahlender Kund:innen kann ausreichen, um einen Gewinn zu erzielen, da bei internetbasierten Diensten ein zusätzlicher Kunde oder eine zusätzliche Kundin vernachlässigbare Grenzkosten erzeugt. Wenn die kostenlose Version nur ein »Lockangebot« darstellt, ist es aber unzutreffend, die sowohl bei der kostenlosen als auch kostenpflichtigen Version erhobenen personenbezogenen Daten als Hauptleistung einzuordnen.[205]

Komplexer ist die Abgrenzung bei werbefinanzierten Internetdiensten. Diese zeichnen sich durch einen dreiseitigen Markt aus: die betroffene Person kann den Dienst kostenlos nutzen, der Verantwortliche im Gegenzug dafür Werbeanzeigen schalten, für welche Werbende eine Vergütung zahlen. Die primäre Gegenleistung der betroffenen Person ist das Konsumieren der Werbung, während die Bereitstellung personenbezogener Daten nur nebensächlich ist. Bei personalisierter Werbung zahlen Werbende typischerweise höhere Preise, da mehr personenbezogene Daten zielgerichtetere Werbung erlauben.[206] Somit ist aber die Bereitstellung der personenbezogenen Daten nur insoweit Gegenleistung, als die betroffene Person zusätzliche für die Durchführung des Dienstes nicht erforderliche personenbezogene Daten übermittelt oder deren Übertragung an Werbende gestattet. Keine Hauptleistung ist die Bereitstellung personenbezogener Daten, wenn diese bereits für Erbringung des Dienstes erforderlich sind und nur sekundär für Werbung genutzt werden.[207] Die Zulässigkeit einer bloß sekundären Nutzung ist mehr Frage des AGB-Rechts. Auch die Regelung finanzieller Anreize erfasst nur an Dritte weitergegebene personenbezogene Daten, da sie an die Datenhandelsdefinition anknüpft, die eine Weitergabe an Dritte erfordert.[208]

Die Definition sollte diese zentralen Geschäftsmodelle abdecken, aber auch für zukünftige Entwicklungen der Datenwirtschaft flexibel genug sein. Als Ausgangspunkt bietet sich die Definition finanzieller Anreize des CCPA an:

---

[202] *Schulz* in: Gola, DS-GVO Art. 7 Rn. 31.

[203] *Kumar*, Harvard Business Review, Making "Freemium" Work.

[204] *Kumar*, Harvard Business Review, Making "Freemium" Work.

[205] A. A. *Hacker*, Datenprivatrecht, S. 53 f., *ders.*, ZfPW 2019, 148, 154: Freemium-Modell sei datenfinanziert, weil Basisversion kostenlos.

[206] Siehe Kapitel 3:C.I.4.b)bb) (ab S. 104).

[207] Ähnlich *Bunnenberg*, Privates Datenschutzrecht, S. 268 f.

[208] Siehe Kapitel 3:C.I.4.b)aa) (ab S. 101).

»program, benefit, or other offering, including payments to consumers, related to the collection, deletion, or sale of personal information.«[209] Diese ist allerdings an das bestehende europäische Recht anzupassen und zu konkretisieren. Sie muss insbesondere mit der Digitale-Inhalte-RL und der Klausel-RL vereinbar sein. Die Digitale-Inhalte-RL enthält eine weitere Defintion in Art. 3 Abs. 1 UAbs. 1 Digitale-Inhalte-RL, die auf das Bereitstellen oder das Zusagen der Bereitstellung personenbezogener Daten in einem Vertrag durch die betroffene Person abstellt. Diese Definition hat den Vorteil, dass sie auch nationalen Rechten gerecht wird, die nicht zwischen Verpflichtungs- und Verfügungsgeschäft unterscheiden.[210] Die Definition des Art. 3 Abs. 1 UAbs. 1 Digitale-Inhalte-RL ist allerdings für den Regelungsgegenstand zu weit, da sie nicht danach unterscheidet, ob es sich um eine Hauptleistung handelt oder nicht.

Zur weiteren Eingrenzung knüpft die vorgeschlagene Definition an den Begriff des »Hauptgegenstandes des Vertrages« des Art. 4 Abs. 2 Klausel-RL an. Dieser ist durch die Rechtsprechung des EuGH bereits etabliert und konkretisiert.[211] Der Bezug auf diese Norm bietet zudem den Vorteil, dass sie klar abgrenzt, welche Teile des Vertrages Art. 8a DSGVO-E und welche Teile der Inhaltskontrolle gemäß Art. 3, 4 Abs. 1 Klausel-RL unterfallen. Die Bereitstellung personenbezogener Daten als Hauptgegenstand ist dann unter den Bedingungen des Art. 8a DSGVO-E der Privatautonomie der Parteien selbst überlassen. Etwaige sonstige Klauseln unterliegen hingegen der gemäß Art. 3, 4 Abs. 1 Klausel-RL vorgegebenen Inhaltskontrolle.
Art. 8a Abs. 1 DSGVO-E sollte damit lauten:

(1) [1]Die Verarbeitung personenbezogener Daten auf Basis eines Vertrages gemäß Artikel 6 Absatz 1 Buchtstabe b ist nur unter den Bedingungen dieses Artikels zulässig, wenn die betroffene Person in dem Vertrag dem Verantwortlichen für einen Preis, Rabatt oder sonstigen Vorteil personenbezogene Daten bereitstellt oder deren Bereitstellung zusagt und diese Bereitstellung den Hauptgegenstand des Vertrages bildet. [2]Die Bereitstellung bildet insbesondere nicht den Hauptgegenstand, wenn der Verantwortliche die von der betroffenen Person bereitgestellten personenbezogenen Daten ausschließlich zur Bereitstellung seiner Dienstleistung oder zur Lieferung von Waren oder digitaler Inhalte oder für die Erfüllung von rechtlichen Anforderungen gemäß Artikel 6 Absatz 1 Buchstabe c verarbeitet.

---

[209] 11 C.C.R. § 7001(j).

[210] *Faust*, Stellungnahme Umsetzungsgesetz Digitale-Inhalte-RL, S. 3.

[211] EuGH vom 30.04.2014 – C-26/13, *Kásler und Káslerné Rábai*, ECLI:EU:C:2014:282 Rn. 36–59; vom 26.02.2015 – C-143/13, *Matei*, ECLI:EU:C:2015:127 Rn. 47–78; vom 03.10.2019 – C621/17, *Andriciuc u. a.*, ECLI:EU:C:2019:820 Rn. 32–41; vom 03.10.2019 – C-621/17, *Kiss und CIB Bank*, ECLI:EU:C:2019:820 Rn. 30–45; vom 16.07.2020 – C-224/19, *Caixabank*, ECLI:EU:C:2020:578 Rn. 56–71.

b) Absatz 2: Angemessenes Alternativangebot

Erst eine gleichwertige Alternative ermöglicht eine privatautonome Entscheidung für und gegen eine Kommerzialisierung der eigenen personenbezogenen Daten.[212] Ein solch explizites Alternativangebot durch den Verantwortlichen selbst kann zudem dazu führen, dass betroffene Personen sich mehr Gedanken über die jeweiligen Datenverarbeitungen machen.[213]

Dieser Teil der Regelung finanzieller Anreize kann nahezu unverändert übernommen werden. Insbesondere führt die Pflicht, dass sich das Alternativangebot an dem Wert der personenbezogenen Daten orientieren muss, dazu, dass das Alternativangebot mehr als ein bloßes »Feigenblatt« darstellt.[214] Dabei ist eine Festlegung auf eine Orientierung (»reasonably related«)[215] am Datenwert wie beim CCPA ausreichend genau, da der Datenwert ohnehin nicht hundertprozentig exakt bestimmt werden kann. Die in der Durchführungsverordnung des CCPA explizit aufgeführten Regelbeispiele für verschiedene Branchen[216] sind allerdings angesichts des technologieneutralen Ansatzes der DSGVO zu spezifisch. Es ist daher nicht sinnvoll, sie zu übernehmen.
Art. 8a Abs. 2 DSGVO-E sollte daher lauten:

(2) [1]Der Verantwortliche muss seine Dienstleistung, Ware, digitale Dienstleistung oder digitalen Inhalt auch ohne Vertrag im Sinne des Absatz 1 anbieten. [2]Der Preis, Rabatt oder beliebige Vorteil im Sinne des Absatz 1 gegenüber diesem Alternativangebot muss sich am Wert der personenbezogenen Daten orientieren.

c) Absatz 3: Informationspflichten

Bisher besteht bei Datenüberlassungsverträgen eine erhebliche Informationsasymmetrie. Betroffene Personen können ohne Kenntnis des Wertes ihrer personenbezogenen Daten kaum erkennen, ob es sich um ein ausgewogenes Geschäft handelt.[217] Daher ist die Übernahme der Pflicht zur Angabe eines monetären Datenwerts des CCPA sinnvoll.

Eine Pflicht der stärkeren Vertragspartei, den Wert der Gegenleistung der schwächeren Vertragspartei anzugeben, ist dem europäischen Recht nicht fremd. So muss der Unternehmer dem Verbraucher den Gesamtpreis der Waren oder Dienstleistungen einschließlich aller Steuern und Abgaben und aller sonstigen

---

[212] *Bunnenberg*, Privates Datenschutzrecht, S. 271f; *Datenethikkommission*, Gutachten, S. 106; *Hacker*, Datenprivatrecht, S. 620.

[213] *Bunnenberg*, Privates Datenschutzrecht, S. 272.

[214] Siehe Kapitel 3:C.I.4.b)bb) (ab S. 104).

[215] Cal. Civ. Code § 1798.125(b)(1).

[216] 11 C.C.R. § 7080(d).

[217] *Hacker* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 47, 53; *Hoofnagle/Whittington*, 61 UCLA L. Rev. 606, 639; *Kilian* in: Stiftung Datenschutz, Dateneigentum und Datenhandel, 191, 203; *Kretschmer*, Wirtschaftsdienst 2018, 459, 460; *Schur*, Die Lizenzierung von Daten, S. 277.

Kosten mitteilen (Art. 5 Abs. 1 lit. c, 6 Abs. 1 lit. e Verbraucherrechte-RL). In den Fällen, in denen der Preis aufgrund der Beschaffenheit der Waren oder Dienstleistungen nicht im Voraus berechnet werden kann, ist nach Erwägungsgrund 36 S. 5 der Verbraucherrechte-RL die Art der Preisberechnung samt einer realistischen Schätzung der Höchstkosten anzugeben. Dies ähnelt stark der Situation bei Datenüberlassungsverträgen, bei denen der Verantwortliche als »Herr der Datenverarbeitung« und typischerweise wirtschaftlich stärkere Person besser den Wert der personenbezogenen Daten feststellen kann.

Neben der Angabe des Datenwerts ist die vom CCPA geforderte kurze Zusammenfassung der Herleitung hilfreich.[218] Ein solcher »Rechenweg« ermächtigt die betroffene Person, das datenfinanzierte Geschäftsmodell zu verstehen. Zusätzlich erlaubt sie der Öffentlichkeit, zu prüfen, ob der Datenwert plausibel ist.[219] Dabei ziehen sich Unternehmen unter dem CCPA häufig auf eine abstrakte Beschreibung zurück.[220] Daher sollten Verantwortliche über den CCPA hinausgehend die konkreten der Berechnung zugrundliegenden Zahlen offenlegen, da nur so die Öffentlichkeit die Plausibilität der Herleitung prüfen kann. Eine Offenlegung der Zahlen mag Unternehmen unrecht sein, da sie so Transparenz über ihr Geschäftsmodell schaffen müssen. Dies ist aber angesichts des öffentlichen Transparenzinteresses bei der besonders grundrechtssensiblen Kommerzialisierung personenbezogener Daten hinzunehmen.

Ebenso für Transparenz sorgt die Angabe der betroffenen Kategorien der persönlichen Informationen[221] und die Beschreibung des finanziellen Anreizes.[222] Weniger hilfreich ist hingegen die vom CCPA vorgesehene Beschreibung der Widerrufsmöglichkeit,[223] wenn man die Regelung, wie hier vertreten, bei Art. 6 Abs. 1 S. 1 lit. b DSGVO verortet. Bei Verträgen gegenüber Verbrauchern muss ein Unternehmer ohnehin klar und verständlich über Bedingungen der Kündigung informieren (Art. 5 Abs. 1 lit. f, 6 Abs. 1 lit. o Verbraucherrechte-RL). Auch ist, anders als bei den finanziellen Anreizen des CCPA,[224] keine Information über die Modalitäten des Vertragsschlusses nötig, da dieser bei Fernabsatzverträgen und außerhalb von Geschäftsräumen geschlossenen Verträgen verbrauchergünstig formalisiert (Art. 7, 8 Verbraucherrechte-RL).

Doch wo sollte der Gesetzgeber die Informationspflichten für Datenüberlassungsverträge innerhalb der DSGVO regeln? Man könnte die zusätzliche Informationen in Art. 13 DSGVO integrieren. Dieser ist allerdings schon bisher überladen,[225] sodass sich darin die speziellen Informationen für Daten-

[218] 11 C. C. R. § 7016(b)(5)(B).
[219] *Cal. Attorney General*, Initial Statement of Reasons, S. 38.
[220] Siehe Kapitel 3:C.I.4.b)bb) (ab S. 104).
[221] 11 C. C. R. § 7016(b)(2).
[222] 11 C. C. R. § 7016(b)(1).
[223] 11 C. C. R. § 7016(b)(4).
[224] 11 C. C. R. § 7016(b)(3).
[225] Siehe Kapitel 3:D.I.2.c) (ab S. 160).

überlassungsverträge verlieren würden. Daher ist eine separate Erklärung vorzugswürdig, wie sie auch der CCPA enthält.[226]

Diese Erklärung muss stetig fortentwickelt werden können, da Informationspflichten so komplex sind, dass sie stets auf Entwicklungen in der Praxis angepasst werden müssen.[227] Hierzu ist ähnlich zu Art. 12 Abs. 8 DSGVO eine Delegation auf die Europäische Kommission sinnvoll.
Art. 8a Abs. 3 DSGVO-E sollte daher lauten:

(3) [1]Bevor die betroffene Person an einen Vertrag oder an ein Angebot gebunden ist, informiert der Unternehmer sie in klarer und verständlicher Weise über Folgendes:[228]
a) eine kurze Beschreibung des Preises, Rabattes oder sonstigen Vorteils;
b) die betroffenen Kategorien personenbezogener Daten;
c) den Wert der personenbezogenen Daten und
d) wie der Verantwortliche den Wert der personenbezogenen Daten berechnet als kurze Beschreibung unter Angabe der relevanten Zahlen.
[2]Der Kommission wird die Befugnis übertragen, gemäß Artikel 92 delegierte Rechtsakte zur Modifizierung der mitzuteilenden Informationen und deren standardisierten Mitteilung zu erlassen.

d) Absatz 4: Bestimmung des Datenwerts

Zentral für das angemessene Alternativangebot und die Informationspflichten ist eine Methode zur Bestimmung des Wertes der personenbezogenen Daten. Die deutsche Literatur hält die Bestimmung eines exakten Datenwerts für wünschenswert, aber unmöglich.[229] Zugegebenermaßen ist der konkrete Wert der personenbezogenen Daten einer bestimmten betroffenen Person nicht vollständig präzise berechenbar. Er hängt stark vom Kontext ab, in dem die personenbezogenen Daten verarbeitet werden. Allerdings bietet bereits ein plausibel berechneter Durchschnittswert einen Orientierungspunkt für die betroffene Person.

Die Durchführungsverordnung des CCPA enthält hierfür ein an der einschlägigen wirtschaftswissenschaftlichen Literatur orientiertes,[230] gut durchdachtes Konzept. Dabei ist der Gewinn des Unternehmens[231] aufgrund der jeweiligen persönlichen Informationen[232] maßgeblich.[233] Das Unternehmen hat einen

---

[226] 11 C.C.R. § 7016. Es ist allerdings zulässig, diese Erklärung auf derselben Webseite wie die umfassende Datenschutzerklärung vorzuhalten, solange der Link sie direkt zu diesem Abschnitt führt, 11 C.C.R. § 7016(a)(3).

[227] Siehe Kapitel 3:D.I.2.a)bb) (ab S. 154).

[228] Diese Formulierung orientiert sich an Art. 5, 6 Abs. 1 Verbraucherrechte-RL a.A.

[229] *Hacker* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 47, 53; *Heller* in: *Leupold/Wiebe/Glossner*, IT-Recht, Teil 6.2 Rn. 9.; *Sattler*, CR 2020, 145 Rn. 57. Ähnlich *Schur*, Die Lizenzierung von Daten, S. 266–268: messbarer Datenwert habe sich in der fragmentierten Datenwirtschaft noch nicht herausgebildet.

[230] Cal. Attorney General, Initial Statement of Reasons, S. 38.

[231] Das Äquivalent zum Verantwortlichen, siehe Kapitel 3:B.II.2 (ab S. 56).

[232] Zum Begriff siehe Kapitel 3:B.I.1.a) (ab S. 43).

[233] 11 C.C.R. § 7081(a)(7).

gewissen Spielraum, Einnahmen und Ausgaben zuzuordnen, da hierfür keine exakten Maßstäbe bestehen,[234] wobei die Zuordnung allerdings »reasonable« sein muss.[235] Das Unternehmen kann entweder den Gewinn individuell pro Verbraucher:in berechnen[236] oder – praxisrelevanter – als Durchschnitt bezogen auf Kalifornien oder die gesamten Vereinigten Staaten.[237] Daneben ist auch eine andere Berechnungsweise zulässig, wenn diese zu nachvollziehbaren, zuverlässigen Ergebnisse führt und praktikabel ist.[238]

Diese flexible und kontextbasierte Methode ist dem Regelungsgegenstand angemessen. Ein klarer, objektiver Maßstab, personenbezogene Daten zu bewerten, existiert bisher nicht.[239] Die Auswahl einer marktbezogenen Methode durch den CCPA ist konsequent, da ein Unternehmen den Wert für die betroffene Person kaum selbst bestimmen kann.[240] Zudem ist der Wert für die jeweilige betroffene Person subjektiv und kaum rechtssicher bestimmbar.[241] Alternativ wäre ein Abstellen auf den konkreten Marktpreis auf legalen oder illegalen Datenmärkten denkbar.[242] Preise auf existierenden Datenmärkten haben den Vorteil, dass sie eine konkrete Geldsumme abbilden und sich aus Angebot und Nachfrage ergeben. Allerdings hängt der Datenwert stark vom Kontext des jeweiligen Unternehmens ab.[243] Zudem kann die Qualität der personenbezogenen Daten eines Datenhändlers in der Regel nicht *ex ante* festgestellt werden, was zu einer potenziell niedrigen Bewertung führt.[244] Schließlich bewegen sich Datenhändler unter der DSGVO am Rande zur Illegalität, was die Preisbildung intransparent und unzuverlässig macht.[245]

Der gewinnorientierte Ansatz des CCPA scheint in der derzeitigen Datenwirtschaft gut umsetzbar zu sein. Er basiert auf für Unternehmen leicht feststellbaren

---

[234] *Cal. Attorney General*, Initial Statement of Reasons, S. 39.

[235] 11 C.C.R. § 7081(a) a. A.

[236] 11 C. C. R. § 7081(a)(1).

[237] 11 C. C. R. § 7081(a)(2),(b).

[238] 11 C. C. R. § 7081(a)(8).

[239] *Hacker* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 47, 53; *Heller* in: *Leupold/Wiebe/Glossner*, IT-Recht, Teil 6.2 Rn. 9; *Nguyen/Paczos*, Economic Value of Data and Cross-Border Data Flows, S. 31; *OECD*, Exploring the Economics of Personal Data, S. 10; *Schur*, Die Lizenzierung von Daten, S. 266–268; *Spiekermann/Korunovska*, Journal of Information Technology 72 (2017), 62, 63.

[240] Ähnlich *Hacker* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, 47, 53: marktbasierte Maßstäbe seien für staatliche Regulierung besser geeignet.

[241] *Solove*, 89 Geo. Wash. L. Rev. 1, 31–33; *Spiekermann/Korunovska*, Journal of Information Technology 72 (2017), 62, 75: Umfrage zu Datenwert unter Facebook-Nutzer:innen.

[242] *OECD*, Exploring the Economics of Personal Data, S. 19.

[243] *Nguyen/Paczos*, Economic Value of Data and Cross-Border Data Flows, S. 32; *OECD*, Exploring the Economics of Personal Data, S. 27; *Short/Todd*, MITSloan 17, 18.

[244] *OECD*, Exploring the Economics of Personal Data, S. 27.

[245] Zu der bei Datenhandel typischerweise fehlenden Rechtsgrundlage siehe Kapitel 3:C.I.2.d) (ab S. 94). Zu den negativen Auswirkungen auf die Verlässlichkeit des Datenwerts: *OECD*, Exploring the Economics of Personal Data, S. 28 f.

Zahlen, da Unternehmen ohnehin Einnahmen und Ausgaben ermitteln.[246] Auch wird sich zumindest nachvollziehbar zuordnen lassen, wie groß der Einfluss einzelner Verarbeitungstätigkeiten auf den Umsatz ist. Beispielsweise wird eine nicht-öffentliche Stelle Marktforschung nur in dem Umfang betreiben wollen, wie sie dazu beiträgt, Kosten zu senken oder den Umsatz zu erhöhen. Die Zuordnung wird nicht immer vollständig präzise möglich sein. Es ist aber die Kernkompetenz eines wirtschaftlich handelnden Unternehmens, den Nutzen einzelner Aktivitäten und die ihnen zuzuweisenden Ressourcen zu ermitteln. Typischerweise wird es Unternehmen möglich sein, den Anteil personenbezogener Daten am Gewinn der jeweiligen Geschäftseinheit zumindest annähernd zu bestimmen. Ein solcher Anhaltspunkt ist bereits wertvoll für betroffene Personen, um die Informationsasymmetrie zum Verantwortlichen auszugleichen.

Sollte neben der Anknüpfung an den durchschnittlichen Wert für alle betroffenen Personen auch eine Anknüpfung an betroffene Personen in einem bestimmten Mitgliedsstaat zulässig sein? Auch der CCPA lässt mit dem alternativen Abstellen auf Kalifornien und die Vereinigten Staaten länderspezifische Durchschnittswerte zu.[247] Der Wert personenbezogener Daten von betroffenen Personen aus unterschiedlichen Mitgliedsstaaten unterscheidet sich teilweise erheblich, da die Mitgliedsstaaten über eine unterschiedliche Wirtschaftskraft verfügen. Die DSGVO verfolgt zwar ausdrücklich auch das Ziel eines harmonisierten Binnenmarkts (Art. 1 Abs. 1 Alt. 2 DSGVO), dem unterschiedliche Wertangaben für personenbezogene Daten und damit verbunden unterschiedliche Preise für Alternativangebote widersprechen könnten. Allerdings verbietet auch Art. 4 Abs. 1, 2 Geoblocking-VO keine länderspezifischen Angebote, sondern nur solche, die innerhalb desselben Gebiets Personen aus anderen Mitgliedstaaten diskriminieren.[248] Vergleichbar dazu ist es sinnvoll, auch für die Festlegung des Datenwerts länderspezifische Durchschnittswerte zuzulassen.

Die Generalklausel für andere Berechnungsmethoden[249] kann ebenfalls beibehalten werden. Zwar begründet sie eine gewisse Missbrauchsgefahr, da sie Verantwortlichen viel Spielraum einräumt. Allerdings ist sie durch das Erfordernis einer nachvollziehbaren und zuverlässigen Berechnungsmethode eingeschränkt.[250] Das europäische Datenschutzrecht kennt zudem bereits viele Generalklauseln, die das Wechselspiel von Aufsichtsbehörden, Literatur und Rechtsprechung konkretisiert. Zudem wird die Regelung so für zukünftige Entwicklungen geöffnet, beispielsweise, falls sich in der Zukunft doch ein objektiver Marktwert für bestimmte Kategorien personenbezogener Daten herausbildet. Art. 8a Abs. 4 DSGVO-E sollte damit lauten:

---

[246] Ähnlich *Hacker* in: Lohsse/Schulze/Staudenmayer, Data as Counter-Performance, S. 49; *OECD*, Exploring the Economics of Personal Data, S. 24.

[247] 11 C.C.R. § 7081(b).

[248] *Kohler*, ZEuP 2020, 253, 255.

[249] 11 C.C.R. § 7081(a)(8).

[250] 11 C.C.R. § 7081(a)(8).

(4) Der Verantwortliche muss bei Datenüberlassungsverträgen den Wert der personenbezogenen Daten nach Treu und Glauben unter Nutzung einer der folgenden Methoden ermitteln:
a) den Gewinn aus der Bereitstellung personenbezogener Daten der jeweiligen betroffenen Person. Der Verantwortliche muss nach Treu und Glauben Einnahmen und Ausgaben den personenbezogenen Daten einer bestimmten betroffenen Person zuordnen;
b) den durchschnittlichen Gewinn aus der Verarbeitung der aus der Bereitstellung der personenbezogenen Daten aller betroffenen Personen. Der Verantwortliche kann auch auf den durchschnittlichen Gewinn bezüglich der betroffenen Personen aus einem Mitgliedstaat oder einem Drittstaat abstellen. Der Verantwortliche muss nach Treu und Glauben Einnahmen und Ausgaben den personenbezogenen Daten der jeweiligen Personengruppe zuordnen;
c) eine andere nach Treu und Glauben nachvollziehbare und zuverlässige Berechnungsmethode.

e) Absatz 5: Ausnahme für Unternehmer als betroffene Person

Die bisher diskutierten Bedingungen für Datenüberlassungsverträge sind nur sinnvoll, wenn die betroffene Person Verbraucher im Sinne des Art. 2 Nr. 1 Verbraucherrechte-RL ist.[251] Die Regelung finanzieller Anreize ist auf Verbraucher:innen zugeschnitten, die den Wert ihrer persönlichen Informationen nicht kennen. Auch Unternehmer im Sinne des Art. 2 Nr. 2 Verbraucherrechte-RL schließen allerdings bisweilen Datenüberlassungsverträge ab, wie beispielsweise die bereits oben diskutierten Merchandisingverträge mit Prominenten.[252] Sie sind aber nicht schutzbedürftig. Prominente kennen ihren Marktwert und lassen sich typischerweise professionell beraten. Es besteht keine Informationsasymmetrie, wie sie Art. 8a DSGVO-E lösen soll.

Damit sind Unternehmer in Art. 8a Abs. 5 DSGVO-E vom Anwendungsbereich der Regelung auszunehmen:

(5) Dieser Artikel findet keine Anwendung, soweit die betroffene Person Unternehmer ist. In diesen Fall sind Datenüberlassungsverträge auch ohne Einhaltung der Bedingungen dieses Artikels zulässig.

f) Absatz 6: Verhältnis zu Artikel 9 und dem Vertragsrecht der Mitgliedstaaten

aa) Satz 1: Verhältnis zu Art. 9 DSGVO

Die Gefahren für die betroffene Person sind umso größer, je eher der Kern der Persönlichkeit betroffen ist. Sowohl der CCPA als auch die DSGVO schützen daher sensible Daten stärker.[253] Der CCPA nimmt sie auch von der Regelung finanzieller Anreize aus, da diese das Recht auf Beschränkung sensibler Informationen nicht erfassen.[254] Es ist sinnvoll, diese Beschränkung auch für Art. 8a

[251] Zum weiteren Verbraucherbegriff des CCPA siehe Kapitel 3:B.II.1 (ab S. 56).
[252] Siehe Kapitel 4:B.II.1 (ab S. 243).
[253] Siehe Kapitel 3:C.II (ab S. 109).
[254] Cal. Civ. Code § 1798.125(b)(1). Siehe Kapitel 3:C.II.2 (ab S. 114).

DSGVO-E zu übernehmen und dabei an die in der europäischen Rechtstradition verwurzelten besonderen Kategorien des Art. 9 Abs. 1 DSGVO anzuknüpfen.[255]

Gerade bei sensiblen Daten im Sinne des Art. 9 Abs. 1 DSGVO besteht die Gefahr einer Kommerzialisierung des Persönlichkeitskerns, da diese höchstpersönlich und identitätsstiftend sind.[256] Wenn schon das pragmatische Verbraucherschutzgesetz CCPA sensible Informationen nicht als Wirtschaftsgut behandelt, muss dies im grundrechtsgeprägten europäischen Datenschutzrecht erst recht gelten. Schon *de lege lata* findet Art. 6 Abs. 1 S. 1 lit. b DSGVO keine Entsprechung in Art. 9 Abs. 2 DSGVO. Darin kommt die deutliche Wertung zum Ausdruck, dass besondere Kategorien personenbezogener Daten nicht kommerzialisiert werden sollten. Das Medizinrecht enthält einen ähnlichen Gedanken: bei klinischen Studien sind Vergütungen, die über eine Aufwandsentschädigung hinausgehen, nur unter strengen Bedingungen zulässig. Nach der am 31.01.2022[257] in Kraft getretenen Humanarzneimittel-Prüf-VO sind bei besonders schutzwürdigen Gruppen nur eine Aufwandsentschädigung für Auslagen und Verdienstausfall zulässig.[258] Andere Prüfungsteilnehmer dürfen zwar eine Vergütung erhalten, diese unterliegt aber der eingehenden Prüfung der betroffenen Mitgliedsstaaten (Art. 7 Abs. 2 lit. b Humanarzneimittel-Prüf-VO). Dem lässt sich entnehmen, dass eine freie Preisbildung bei höchstpersönlichen Gesundheitsdaten gerade nicht gewollt ist.

Auch die anderen besonderen Kategorien personenbezogener Daten des Art. 9 Abs. 1 DSGVO sollten nicht kommerzialisiert werden. So bergen die rassische oder ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung, die Gewerkschaftsangehörigkeit und sexuelle Orientierung ein besonderes Diskriminierungspotenzial.[259] Gerade eine Kommerzialisierung politischer Ansichten würde die besondere Gefahr hervorrufen, durch erhöhte

---

[255] Bereits ein Anknüpfen der Zulässigkeit der Kommerzialisierung an diese Trennlinie andenkend: *Sattler* in: Bakhoum et al., Personal Data in Competition, Consumer Protection and Intellectual Property Law, S. 27.

[256] *Bunnenberg*, Privates Datenschutzrecht, S. 249–254; *Frenzel* in: Paal/Pauly, DS-GVO Art. 9 Rn. 6; *Sattler* in: Pertot, Rechte an Daten, 49, 63; *Weichert* in: Kühling/Buchner, DS-GVO Art. 9 Rn. 17. Kritisch zur Einteilung in sensible und nicht-sensible Daten: *Schneider*, ZD 2017, 303, 305.

[257] Art. 99 Abs. 2 Humanarzneimittel-Prüf-VO i. V. m. Art. 1 Beschluss (EU) 2021/1240 der Kommission vom 13. Juli 2021 über die Übereinstimmung des EU-Portals und der EU-Datenbank für klinische Prüfungen mit Humanarzneimitteln mit den Anforderungen gemäß Artikel 82 Absatz 2 der Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates, C/2021/5063, ABl. 2021 L 275, 1.

[258] Nicht einwilligungsfähige Prüfungsteilnehmer gemäß Art. 31 Abs. 1 lit. d, Minderjährige gemäß Art. 32 Abs. 1 lit. d und schwangere oder stillende Frauen gemäß Art. 33 Abs. 1 lit. d Humanarzneimittel-Prüf-VO.

[259] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 195; *Bunnenberg*, Privates Datenschutzrecht, S. 250; *Franzen* in: Franzen/Gallner/Oetker, Europäisches Arbeitsrecht, EU (VO) 2016/679 Art. 9 Rn. 2; *Petri* in: NK-DatenschutzR, DS-GVO Art. 9 Rn. 10; *Weichert* in: Kühling/Buchner, DS-GVO Art. 9 Rn. 2.

Marktgängigkeit im politischen Diskurs Vielfalt zu verlieren.[260] Insoweit steht die Privatautonomie im Konflikt mit sozialstaatlichen Zielen: die nicht-diskriminierte Mehrheit könnte bedenkenlos ihre sensiblen Daten im Sinne des Art. 9 Abs. 1 DSGVO kommerzialisieren. Dagegen wäre bei diskriminierten Minderheiten ein Rückschluss durch deren Nicht-Teilnahme an Datenüberlassungsverträgen möglich.[261]

Regelungstechnisch ergibt sich der Ausschluss von besonderen Kategorien personenbezogener Daten zwanglos daraus, dass die Rechtsgrundlage des Art. 6 Abs. 1 S. 1 lit. b DSGVO in Art. 9 Abs. 2 DSGVO keine Entsprechung hat. Wenn wie nach der Humanarzneimittel-Prüf-VO eine Derogation des Art. 9 Abs. 2 DSGVO vorliegt, ist auch dagegen die Verarbeitung personenbezogener Daten auf Basis eines Datenüberlassungsvertrags zulässig. Dies ist kurz klarzustellen. Art. 8a Abs. 6 S. 1 DSGVO-E sollte damit lauten:

(6) [1]Dieser Artikel lässt Artikel 9 unberührt.

bb) Satz 2: Verhältnis zum Vertragsrecht der Mitgliedsstaaten

Die Regelung steht an der Schnittstelle zwischen Datenschutz und Datenschuldrecht. Das Verhältnis zum nationalen Datenschuldrecht muss daher nach dem Vorbild der Unberührtheitsregelung des Art. 8 Abs. 3 DSGVO kurz klargestellt werden.
Art. 8a Abs. 6 S. 2 DSGVO-E sollte damit lauten:

[2]Dieser Artikel lässt das allgemeine Vertragsrecht der Mitgliedsstaaten, wie etwa die Vorschriften zum Zustandekommen oder zu den Rechtsfolgen eines Datenüberlassungsvertrages, unberührt.

4. Folgeänderungen

Das unklare Koppelungsverbot des Art. 7 Abs. 4 DSGVO muss präzisiert werden. Durch die separate Regelung von Datenüberlassungsverträgen verbleiben sachfremde Koppelungen, bei denen der Verantwortliche die Vertragserfüllung von der Einwilligung zu einer Datenverarbeitung abhängig macht, die ohne Bezug zum Vertragsinhalt ist. Diese können für generell unzulässig erklärt werden, sodass eine klare Trennung zu Art. 6 Abs. 1 S. 1 lit. b DSGVO entsteht. Zudem ist klarzustellen, dass auch eine Koppelung mit dem Vertragsschluss unzulässig ist. Dies entspricht bereits *de lege lata* der allgemeinen Auffassung, lässt sich aber aus dem Wortlaut (»Erfüllung des Vertrages«) nicht eindeutig entnehmen.[262]

---

[260] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 191–193.

[261] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 197 f.

[262] *Becker*, CR 2021, 230 Rn. 24 f.; *Heckmann/Paschke* in: Ehmann/Selmayr, DS-GVO Art. 7 Rn. 98; *Ingold* in: Sydow, DSGVO Art. 7 Rn. 31; *Taeger* in: Taeger/Gabel, DS-GVO Art. 7 Rn. 98; *Voigt*, Die datenschutzrechtliche Einwilligung, S. 137.

Art. 7 Abs. 4 DSGVO-E sollte daher lauten (Streichungen durchgestrichen, Einfügungen kursiv):

(4) ~~Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem~~ *Eine Einwilligung ist nicht freiwillig, wenn* das Zustandekommen oder die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

Die Definition des Unternehmers wurde in Art. 8a Abs. 5 DSGVO-E verwendet. Sie muss daher in Art. 4 Nr. 27 DSGVO-E ergänzt werden:

27. »Unternehmer« eine natürliche Person im Sinne des Artikel 2 Nummer 2 der Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates.(*)

———

(*) Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG des Rates und der Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 85/577/EWG des Rates und der Richtlinie 97/7/EG des Europäischen Parlaments und des Rates.

Schließlich sollten auch die Modalitäten für die transparente Art der Information in Art. 12 DSGVO an die neue Informationspflicht angepasst werden (Einfügungen in kursiv):

(1) [1]Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß *dem Artikel 8a Absatz 3 sowie* den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. [2]Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. [3]Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

...

(5) [1]Informationen gemäß *dem Artikel 8a Absatz 3 sowie* den Artikeln 13 und 14 sowie alle Mitteilungen und Maßnahmen gemäß den Artikeln 15 bis 22 und Artikel 34 werden unentgeltlich zur Verfügung gestellt. [2]Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder

a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder

b) sich weigern, aufgrund des Antrags tätig zu werden.

[3]Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.

Der Regelungsvorschlag ist inhaltlich auch auf die ePrivacy-VO übertragbar. Insoweit sollte im Hinblick auf deren beschränkten Anwendungsbereich eine einheitliche Lösung mit der DSGVO erfolgen. Die genaue Ausgestaltung ist

aber angesichts des Trilogs noch zu sehr im Fluss, zumal eine isolierte Regelung nur in der ePrivacy-VO angesichts deren beschränkten Anwendungsbereichs nicht sinnvoll ist.

IV. Abschließender Regelungsvorschlag

Die Verordnung (EU) 2016/679 wird wie folgt geändert:
1. In Artikel 4 wird folgende Nummer eingefügt:

27. »Unternehmer« eine natürliche Person im Sinne des Artikel 2 Nummer 2 der Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates.(*)

(*) Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG des Rates und der Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 85/577/EWG des Rates und der Richtlinie 97/7/EG des Europäischen Parlaments und des Rates.

2. In Artikel 7 erhält Absatz 4 folgende Fassung:

(4) Eine Einwilligung ist nicht freiwillig, wenn das Zustandekommen oder die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

3. Der folgende Artikel wird eingefügt:

Artikel 8a Bedingungen für Datenüberlassungsverträge
(1) [1]Die Verarbeitung personenbezogener Daten auf Basis eines Vertrages gemäß Artikel 6 Absatz 1 Buchtstabe b ist nur unter den Bedingungen dieses Artikels zulässig, wenn die betroffene Person in dem Vertrag dem Verantwortlichen für einen Preis, Rabatt oder sonstigen Vorteil personenbezogene Daten bereitstellt oder deren Bereitstellung zusagt und diese Bereitstellung den Hauptgegenstand des Vertrages bildet. [2]Die Bereitstellung bildet insbesondere nicht den Hauptgegenstand, wenn der Verantwortliche die von der betroffenen Person bereitgestellten personenbezogenen Daten ausschließlich zur Bereitstellung seiner Dienstleistung oder zur Lieferung von Waren oder digitaler Inhalte oder für die Erfüllung von rechtlichen Anforderungen gemäß Artikel 6 Absatz 1 Buchstabe c verarbeitet.
(2) [1]Der Verantwortliche muss seine Dienstleistung, Ware, digitale Dienstleistung oder digitalen Inhalt auch ohne Vertrag im Sinne des Absatz 1 anbieten. [2]Der Preis, Rabatt oder beliebige Vorteil im Sinne des Absatz 1 gegenüber diesem Alternativangebot muss sich am Wert der personenbezogenen Daten orientieren.
(3) [1]Bevor die betroffene Person an einen Vertrag oder an ein Angebot gebunden ist, informiert der Unternehmer sie in klarer und verständlicher Weise über Folgendes:[263]
a) eine kurze Beschreibung des Preises, Rabattes oder sonstigen Vorteils;
b) die betroffenen Kategorien personenbezogener Daten;
c) den Wert der personenbezogenen Daten und
d) wie der Verantwortliche den Wert der personenbezogenen Daten berechnet als kurze Beschreibung unter Angabe der relevanten Zahlen.

[263] Diese Formulierung orientiert sich an Art. 5, 6 Abs. 1 Verbraucherrechte-RL a. A.

[2]Der Kommission wird die Befugnis übertragen, gemäß Artikel 92 delegierte Rechtsakte zur Modifizierung der mitzuteilenden Informationen und deren standardisierten Mitteilung zu erlassen.
(4) Der Verantwortliche muss bei Datenüberlassungsverträgen den Wert der personenbezogenen Daten nach Treu und Glauben unter Nutzung einer der folgenden Methoden ermitteln:
a) den Gewinn aus der Bereitstellung personenbezogener Daten der jeweiligen betroffenen Person. Der Verantwortliche muss nach Treu und Glauben Einnahmen und Ausgaben den personenbezogenen Daten einer bestimmten betroffenen Person zuordnen;
b) den durchschnittlichen Gewinn aus der Verarbeitung der aus der Bereitstellung der personenbezogenen Daten aller betroffenen Personen. Der Verantwortliche kann auch auf den durchschnittlichen Gewinn bezüglich der betroffenen Personen aus einem Mitgliedstaat oder einem Drittstaat abstellen. Der Verantwortliche muss nach Treu und Glauben Einnahmen und Ausgaben den personenbezogenen Daten der jeweiligen Personengruppe zuordnen;
c) eine andere nach Treu und Glauben nachvollziehbare und zuverlässige Berechnungsmethode.
(5) Dieser Artikel findet keine Anwendung, soweit die betroffene Person Unternehmer ist. In diesen Fall sind Datenüberlassungsverträge auch ohne Einhaltung der Bedingungen dieses Artikels zulässig.
(6) [1]Dieser Artikel lässt Artikel 9 unberührt. [2]Dieser Artikel lässt das allgemeine Vertragsrecht der Mitgliedsstaaten, wie etwa die Vorschriften zum Zustandekommen oder zu den Rechtsfolgen eines Datenüberlassungsvertrages unberührt.

4. Artikel 12 wird wie folgt geändert:
a) Absatz 1 erhält folgende Fassung:

(1) [1]Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß dem Artikel 8a Absatz 3 sowie den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. [2]Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. [3]Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

b) Absatz 5 erhält folgende Fassung:

(5) [1]Informationen gemäß dem Artikel 8a Absatz 3 sowie den Artikeln 13 und 14 sowie alle Mitteilungen und Maßnahmen gemäß den Artikeln 15 bis 22 und Artikel 34 werden unentgeltlich zur Verfügung gestellt. [2]Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder
a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder
b) sich weigern, aufgrund des Antrags tätig zu werden.
[3]Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.

Kapitel 5

Fazit

A. Zusammenfassung der Ergebnisse

I. Hintergrund und Gesetzgebungsgeschichte

1. Verfassungsrechtlicher Hintergrund

Die U. S. Constitution ist auf freien Informationsfluss statt auf einen starken Privatsphäreschutz ausgerichtet. So kennt die U. S. Constitution kein explizites Recht auf Privatsphäre, sondern schützt diese nur indirekt und in geringem Maß. Vor allem aber verteidigt die U. S. Constitution den öffentlichen Diskurs gegen staatliche Einschränkungen durch die Meinungsfreiheit des *First Amendment,* die im amerikanischen Verfassungsrecht eine überragende Bedeutung hat. Anders als im europäischen und deutschen Verständnis behandelt der U. S. Supreme Court auch die Weiterübermittlung personenbezogener Daten als Meinungsäußerung. Im *marketplace of ideas* sollen dabei Informationen frei fließen, was Datenschutzgesetze deutlich einschränkt.

Im Gegensatz dazu enthält die California Constitution ein explizites Recht auf Privatsphäre, welches ein Volksentscheid 1972 eingeführt hatte. Die Rechtsprechung des California Supreme Court ist dementsprechend deutlich datenschutzfreundlicher.

2. Amerikanisches Datenschutzrecht

Das Bild eines Zwiespalts zwischen einem datenschutzskeptischen Bund und einem datenschutzfreundlichen Kalifornien setzt sich auf einfachgesetzlicher Ebene fort.

Der Gesetzgeber auf Bundesebene hat sich für einen branchenspezifischen Regulierungsansatz entschieden, der zwar für manche Branchen einen hohen Schutzstandard erreicht, insgesamt aber lückenhaft bleibt.

Diese Lücken füllt die Bundesbehörde Federal Trade Commission (FTC). Sie hat seit den 1990ern eine bewusst offen formulierte Generalklausel für Verbraucherschutz genutzt, um zur primären Regulierungsbehörde für Datenschutz in den Vereinigten Staaten zu werden. Deren auf Privatautonomie und Datensicherheit fokussierte Verwaltungspraxis prägt das amerikanische Datenschutzrecht nachhaltig. So hat die FTC drei der fünf größten amerikanischen Unternehmen umfangreiche datenschutzrechtliche Pflichten nach einem von ihr

festgestellten Datenschutzverstoß auferlegt. Das *notice-and-choice*-Modell der Wettbewerbsbehörde FTC ist stark auf die freie Entscheidung eines informierten Individuums fokussiert, die sich in der Praxis häufig als dessen Überforderung herausstellt.

Kalifornien ergänzte dies bereits vor dem CCPA durch über hundert zusätzliche Datenschutzgesetze. Diese beeinflussen häufig das gesamte amerikanische Recht: so hat Kalifornien als erster Bundesstaat eine Datenpannenmeldepflicht eingeführt, die inzwischen alle anderen 49 Bundesstaaten übernommen haben und auf die auch Art. 4 Abs. 3 ePrivacy-RL, Art. 33, 34 DSGVO zurückzuführen sind.[1]

3. Gesetzgebungsgeschichte

In dem datenschutzfreundlicheren Klima Kaliforniens war es naheliegend, dass Verbraucherschutzorganisationen versuchen, die vielen losen Fäden der branchenspezifischen Gesetze und der Verwaltungspraxis der FTC zu einem umfassenden Datenschutzgesetz zusammenzuführen. Dies ist der neu gegründeten Bürgeriniative Californians for Consumer Privacy erstmals 2018 gelungen, als sie das kalifornische Parlament dazu veranlasste, ihr Volksbegehren weitgehend unverändert anzunehmen. Im Jahr 2020 hat Californians for Consumer Privacy in dem erfolgreichen Volksentscheid Proposition 24 eine deutliche Erweiterung des CCPA erreicht.

II. Analyse des CCPA und Vergleich mit europäischem Datenschutzrecht

1. Anwendungsbereich

Aus diesem Volksbegehren ist ein umfassendes Datenschutzgesetz für die Privatwirtschaft entstanden, das für diese über einen mit der DSGVO vergleichbaren Anwendungsbereich verfügt.

Der Kernbegriff der persönlichen Informationen (»personal information«) des CCPA ist ähnlich weit wie der Begriff der personenbezogenen Daten des Art. 4 Nr. 1 DSGVO. Insbesondere genügt ein nur indirekter Personenbezug. Die Ausnahme aggregierter und deidentifizierter Informationen ähnelt den anonymen Daten der DSGVO, wobei der CCPA Restrisiken unzureichender Deidentifizierung mit fortgeltenden, reduzierten Pflichten begegnet. Öffentliche Informationen sind pauschal von der Definition persönlicher Informationen ausgenommen. Darin spiegelt sich die überragende Bedeutung der Meinungsfreiheit des *First Amendments*, welche den öffentlichen Diskurs umfassend schützt. Die weniger an der Meinungsfreiheit orientierte DSGVO reduziert den Schutz öffentlicher personenbezogener Daten hingegen nur punktuell.

Der persönliche Anwendungsbereich des CCPA ist hingegen kleiner als derjenige der DSGVO. Nur gewinnorientierte Gesellschaften einer gewissen Größe

[1] Zu der Übernahme durch die EU siehe Kapitel 4:B.I (ab S. 241).

sind als Unternehmen (»business«) primäre Adressaten der Rechte und Pflichten des CCPA. Der wichtigste Schwellenwert ist ein Jahresumsatz von 25.000.000 $. Hingegen sind Verantwortliche im Sinne des Art. 4 Nr. 1 DSGVO auch Behörden, kleinere Gesellschaften und grundsätzlich sogar Privatpersonen. Sekundär verpflichtet der CCPA auch Dienstleister (»service providers« und »contrators«), die mit den Auftragsverarbeitern des Art. 4 Nr. 8, 28 DSGVO vergleichbar sind.

Auch der räumliche Anwendungsbereich ist enger als derjenige der DSGVO, um die *dormant Commerce Clause* der U. S. Consitution zu umschiffen. Nur Verarbeitungen mit gewissem Bezug zu Kalifornien sind erfasst. Zudem sind nur Personen mit Wohnsitz in Kalifornien geschützt (missverständlich als »consumer«, d. h. Verbraucher:innen, benannt).

2. Verbraucherrechte

a) Widerspruchsrecht gegen Datenhandel

Das Widerspruchsrecht gegen Datenhandel des CCPA ermöglicht es Verbraucher:innen, die kommerzielle Weiterverbreitung ihrer persönlichen Informationen zu verhindern. Die Legaldefinition des Datenhandels (»selling or sharing«) umfasst jede Weiterübermittlung persönlicher Informationen an Dritte für eine weit verstandene Gegenleistung, insbesondere eine Weitergabe für personalisierte Werbung. Keinen Datenhandel stellen dagegen Übermittlungen an Dritte dar, die für den Geschäftsbetrieb des Unternehmen nötig sind. Bemerkenswert ist, wie pauschal der Widerspruch ausgestaltet ist, der wertungsmäßig nach der Konzeption des CCPA der Standardfall sein sollte. Dementsprechend genügt bereits ein automatisches Widerspruchssignal durch ein Gerät oder einen Browser. Ergänzend müssen Unternehmen, die mit persönlichen Informationen handeln, in der Regel einen auffälligen Widerspruchslink auf ihrer Webseite platzieren und den Widerspruch durch eine Datenschutzagentur akzeptieren. Wenn Verbraucher:innen widersprochen haben, darf das Unternehmen ihnen finanzielle Anreize anbieten, damit sie doch in den Datenhandel einwilligen. Dies ist eine detaillierte Sonderregelung des Geschäftsmodells »Leistung gegen Daten«. Das Unternehmen muss umfangreiche Informationen offenlegen, damit Verbraucher:innen sich bewusst und informiert für oder gegen die finanziellen Anreize entscheiden können. Es muss insbesondere den Wert der persönlichen Informationen schätzen und über diesen sowie dessen Herleitung informieren. Der monetäre Gegenwert der finanziellen Anreize muss sich an dem so geschätzten Wert der persönlichen Informationen orientieren. Eine Nutzung der durch das Unternehmen angebotenen Dienstleistung muss auch ohne Einwilligung in Datenhandel möglich sein. Auch sonst darf das Unternehmen Verbraucher:innen nicht wegen der Ausübung ihrer Rechte diskriminieren.

Mit persönlichen Informationen von Minderjährigen unter 16 Jahren dürfen Unternehmen unter dem CCPA nur handeln, wenn die Minderjährigen

(beziehungsweise bei Minderjährigen unter 13 Jahren deren Erziehungsberechtigte) aktiv in den Datenhandel einwilligen.

Die DSGVO regelt kein Widerspruchsrecht gegen Datenhandel, kommt allerdings bereits *ipso iure* der Situation nach einem Widerspruch nahe: Datenhandel kann ein Verantwortlicher nur auf die Rechtsgrundlagen der Einwilligung (Art. 6 Abs. 1 S. 1 lit. a DSGVO) und des Vertrages (Art. 6 Abs. 1 S. 1 lit. b DSGVO) stützen, die beide eine privatautonome Entscheidung der betroffenen Person voraussetzen. Die Zulässigkeit des Geschäftsmodells »Leistung gegen Daten« regelt die DSGVO nur durch das unscharfe Kopplungsverbot des Art. 7 Abs. 4 DSGVO.

b) Recht auf Beschränkung sensibler Informationen

Das zweite Kernrecht des CCPA ist das Recht auf Beschränkung sensibler Informationen. Die Definition sensibler Informationen (»sensitive personal information«) orientiert sich an Art. 9 Abs. 1 DSGVO, passt diesen jedoch an das amerikanische Verständnis von Privatsphäre an, indem sie bestimmte Kategorien entfernt oder hinzufügt. Anders als unter Art. 9 Abs. 1 DSGVO ist die Nutzung sensibler Informationen nur eingeschränkt, wenn Verbraucher:innen dieses Recht ausüben, und auch dann leichter möglich als unter Art. 9 Abs. 2 DSGVO. Die Ausübung dieses Rechts ist ebenso einfach und pauschal gestaltet wie beim Widerspruchsrecht gegen Datenhandel.

c) Recht auf Auskunft, Recht auf Löschung und Recht auf Berichtigung

Das Auskunftsrecht ist umfassend und weicht nur in Details von Art. 15 DSGVO ab. Es sind dabei die konkret gespeicherten persönlichen Informationen mitzuteilen, was unter der DSGVO stark umstritten ist. Der CCPA regelt eingehend durch zahlreiche Ausnahmen, welche persönlichen Informationen mitzuteilen sind und bei welchen persönlichen Informationen das Interesse des Unternehmens oder Dritter überwiegt.

Das Recht auf Löschung des CCPA ist deutlich enger als Art. 17 DSGVO. Grund ist die höhere Bedeutung der Meinungsfreiheit des *First Amendments*, mit der ein Recht auf Vergessenwerden schon auf einer grundlegenden Ebene unvereinbar wäre. Dementsprechend ist das Recht auf die Kontrolle der selbst bereitgestellten personenbezogenen Daten beschränkt und schützt nicht das eigene Bild in der Öffentlichkeit.

Besser mit dem Leitbild einer Kontrolle über die eigenen persönlichen Informationen vereinbar ist das Berichtigungsrecht. Dieses ist im CCPA daher ähnlich weit gefasst wie in Art. 16 DSGVO.

3. Unternehmenspflichten

Die Unternehmenspflichten des CCPA sind geringer als die Verbraucherrechte ausgeprägt. Sie legen Unternehmen insbesondere kaum auf eine bestimmte

Datenschutzorganisation fest. Weitergehend als die DSGVO sind dagegen die eingehend geregelten Informationspflichten, die auch eine zweistufige Information aus kurzem Datenschutzhinweis für Verbraucher:innen und eine umfassende Datenschutzerklärung für die Öffentlichkeit als Ganzes vorsehen. Insoweit ist die spezifische Regelungstechnik des CCPA besser für Informationspflichten geeignet als die offene, technologieneutrale Regelungstechnik der DSGVO.

Nur gering ausgeprägt sind die Prinzipien der Zweckbindung, Datenminimierung und Speicherfristbegrenzung. Ersichtlich zielte Proposition 24 mit der Einführung dieser Unternehmenspflichten nur darauf ab, einen Angemessenheitsbeschluss zu erreichen, und hat dementsprechend die »Referenzgrundlage Angemessenheit« der Artikel-29-Datenschutzgruppe wie eine Checkliste abgearbeitet.

Die Datensicherheitspflicht inkorporiert nur ein früheres kalifornisches Datensicherheitsgesetz in den CCPA. Die verpflichtenden Weiterübermittlungs- und Dienstleisterverträge sollen für Rechenschaft in Übermittlungsketten sorgen und so die Reichweite des CCPA faktisch auch über Kalifornien hinaus erstrecken.

4. Rechtsdurchsetzung

Zentral für die Durchsetzung des CCPA ist die durch Proposition 24 geschaffene unabhängige California Privacy Protection Agency, die sich noch im Aufbau befindet. Vergleichbar mit den Aufsichtsbehörden der DSGVO kann sie Bußgelder festsetzen und die Öffentlichkeit über Datenschutz aufklären. Anders als diese verfügt sie jedoch über eine umfassende Verordnungskompetenz und ein garantiertes Mindestbudget. Bußgelder setzt sie in einem für das amerikanische Recht typischen transparentem Verfahren fest, indem sie nicht nur den endgültigen Bußgeldbescheid unter Namensnennung veröffentlicht, sondern auch die Vorberatungen ihres Leitungsgremium öffentlich führt.

Die zweite wichtige Aufsichtsbehörde leitet der direkt gewählte kalifornische Attorney General, der Straf- und Zivilgesetze Kaliforniens aller Art vollstreckt. Dieser kann auf Verhängung einer *civil penalty* klagen. *Civil penalties* sind die im amerikanischen Recht typischen Unternehmenssanktionen und werden im Zivilprozess durch ein Gerichtsurteil verhängt. Ergänzend können District und City Attorneys, die allerdings nur über geringe Ressourcen verfügen, kleinere Fälle übernehmen.

Die gleichzeitige Zuständigkeit verschiedener Aufsichtsbehörden ist Ausdruck der starken Gewaltenteilung im amerikanischen Recht. Die Aufsichtsstruktur der DSGVO ist dagegen wesentlich mehr auf einheitliche Entscheidungen ausgerichtet, bei der nach dem *One-Stop-Shop*-Verfahren immer nur eine Aufsichtsbehörde zuständig ist.

Daneben kennt der CCPA ein auf Datenpannen beschränktes Privatklagerecht, das auf Sammelklagen zugeschnitten ist. Dieser ermöglicht durch eine Schadensersatz-Pauschale eine sachgerechte Abwicklung der hierdurch entstandenen Massenschäden. Art. 79, 82 DSGVO sind materiell-rechtlich weiter

gefasste Ansprüche, allerdings zumindest in Deutschland in ein prozessuales Umfeld eingebettet, in dem eine kollektive Rechtsdurchsetzung kaum möglich ist.

5. Rechtsvergleichendes Fazit

Leitbild des CCPA ist die Privatautonomie, während die DSGVO auf eine mittelbare Drittwirkung der Art. 7, 8 GRCh abzielt. Privatautonomie ist generell ein zentrales Prinzip des amerikanischen und kalifornischen Zivilrechts, was sich an der nur minimal ausgeprägten AGB-Kontrolle zeigt. Ähnlich dazu ist das amerikanische und kalifornische Datenschutzrecht von der Zielsetzung einer größtmöglichen Kontrolle über die eigenen persönlichen Informationen geprägt, welcher auch in acht Erwägungsgründen des CCPA zum Ausdruck kommt. Dementsprechend kennt der CCPA umfangreiche Verbraucherrechte, jedoch weniger *ipso iure* geltende Unternehmenspflichten. Dies setzt aktivere Verbraucher:innen voraus, die sich selbst informieren und ihre Rechte ausüben, als die eher passiven »betroffenen Personen« der DSGVO. Ob Verbraucher:innen in der Praxis wirklich so aktiv sind, ist zweifelhaft.

Eng verbunden mit der Privatautonomie ist das Ideal des freien Informationsflusses und der Transparenz, das sich durch den gesamten CCPA zieht. Dies kommt neben den umfassenden Informationspflichten auch in den hohen Anforderungen an die Transparenz der California Privacy Protection Agency zum Ausdruck. Andererseits schränkt dieses Leitbild auch den Umfang des CCPA deutlich ein. So sind öffentliche Informationen pauschal vom Anwendungsbereich des CCPA ausgenommen. Ebenfalls kennt der CCPA kein Recht auf Vergessenwerden.

Der Einfluss der DSGVO auf den CCPA ist dagegen eher oberflächlich. Der CCPA ist auf der Umsetzungsebene um Kompatibilität mit der DSGVO bemüht, damit weltweit tätige Unternehmen ihre bereits für die DSGVO entwickelten Datenschutzprozesse nutzen können. Dies gilt aber nicht für mit der Regelungsphilosophie des CCPA unvereinbare Rechte und Pflichten wie das Verbot mit Erlaubnisvorbehalt des Art. 6 Abs. 1 DSGVO. Zudem nutzt der CCPA die DSGVO an vielen Stellen als Fundus für Formulierungen.

Diese »Gesetzgebung nach dem *copy-and-paste*-Verfahren« ist wohl auf den Ursprung des CCPA als Volksbegehren zurückzuführen. Der von der kleinen Bürgeriniative Californians for Consumer Privacy entwickelte CCPA enthält zahlreiche Redaktionsfehler, die auch in der amerikanischen Literatur vielfach kritisiert werden. Andererseits ist der CCPA an vielen Stellen hochgradig spezifisch, weil das amerikanische Recht wortlautorientiert ausgelegt wird.

III. Schlussfolgerungen aus der Analyse

1. Kein Angemessenheitsbeschluss für Kalifornien

Kalifornien verfügt trotz des CCPA über kein angemessenes Schutzniveau nach Art. 45 Abs. 1 S. 1 DSGVO. Dafür ist nach dem ergebnisorientierten Maßstab des EuGH ein der Sache nach gleichwertiges Schutzniveau erforderlich.

Der enge Anwendungsbereich des CCPA schließt derzeit einen Angemessenheitsbeschluss aus. Das Schutzniveau ist zumindest für Personen mit Wohnsitz innerhalb des Europäischen Wirtschaftsraums nicht gleichwertig, da der CCPA diese von seiner Definition der Verbraucher:innen ausnimmt und somit nicht schützt. Dieses Hindernis könnte Kalifornien allerdings wohl in Angemessenheitsverhandlungen durch eine einfache Gesetzesänderung lösen.

Dagegen kann Kalifornien nicht die Massenüberwachung durch die U. S. Geheimdienste beeinflussen. Allein diese hat dem EuGH in *Schrems II* genügt, um ein angemessenes Schutzniveau zu verneinen. Für eine umfassende Reform der Massenüberwachung auf Bundesebene fehlt der politische Wille. Damit wird Kalifornien wohl auf absehbare Zeit ein Angemessenheitsbeschluss versagt bleiben.

2. Übernahme der Regelung finanzieller Anreize

Das Geschäftsmodell »Leistung gegen Daten« ist in der europäischen rechtswissenschaftlichen Diskussion stark umstritten. Ein völliges Verbot der Bereitstellung personenbezogener Daten als die Gegenleistung der betroffenen Person (im folgenden: Datenüberlassungsvertrag) ist rechtspolitisch nicht überzeugend, da auch ein solcher Vertrag von der Privatautonomie umfasst ist.

Datenüberlassungsverträge sind *de lege lata* nur unzureichend reguliert. Das für diese Vertragsart zentrale Koppelungsverbot des Art. 7 Abs. 4 DSGVO ist nur konfus geregelt. Dem unklaren Wortlaut dieser Norm (»im größtmöglichen Umfang«) lässt sich keine umfassende Regulierung der Zulässigkeit von Datenüberlassungsverträgen entnehmen. Eine solche enthält auch die Digitale-Inhalte-RL und deren deutsche Umsetzung (§§ 327–327u BGB) nicht, welche nur Leistungsstörungen und die Folgen der Ausübung datenschutzrechtlicher Rechte bei Datenüberlassungsverträgen regeln.

Einigkeit besteht nur darüber, dass die Rechtslage *de lege ferenda* reformbedürftig ist. Der Vorschlag eines Dateneigentums gilt als weitgehend gescheitert. Andere konkrete Lösungsvorschläge sind noch zu wenig entwickelt oder ergänzen nur eine Regelung zur Zulässigkeit der Datenüberlassungsverträge.

Die Regelung finanzieller Anreize des CCPA ist gut geeignet, diese Lücke zu füllen. Sie stellt einen ausgewogenen Kompromiss dar: weder bevormundet sie die betroffene Person noch regelt sie eine grenzenlose Privatautonomie. Zwar sind Datenüberlassungsverträge nach der kalifornischen Lösung an sich zulässig. Unternehmen müssen aber auch eingehend über sie informieren und insbesondere den Datenwert angeben. Dass Unternehmen eine finanziell ungefähr gleichwertige Alternative anbieten müssen, stellt die Freiwilligkeit sicher. Bei

sensiblen Informationen sind finanzielle Anreize nach dem CCPA unzulässig, sodass gerade die besonders risikoreichen und höchstpersönlichen Informationen von der Regelung ausgenommen sind.

Die Rechtsübernahme finanzieller Anreize sollte auf europäischer Ebene in die DSGVO aufgenommen werden. Damit kann die Zulässigkeit von Datenüberlassungsverträgen europaweit einheitlich geregelt werden. Dabei sollte die Regelung an die Rechtsgrundlage des Vertrages gemäß Art. 6 Abs. 1 S. 1 lit. b DSGVO anknüpfen. Dieser ist für Datenüberlassungsverträge durch einen neu zu schaffenden Art. 8a DSGVO-E zu konkretisieren. Die Definition der Datenüberlassungsverträge sollte sich dabei an der Definition finanzieller Anreize und des Hauptgegenstandes des Art. 4 Abs. 2 Klausel-RL orientieren (Art. 8a Abs. 1 DSGVO-E). Darauf folgend können die Pflicht eines angemessen Alternativangebots, die Informationspflichten und die Berechnungsmethode des Datenwerts der Regelung finanzieller Anreize minimal angepasst übernommen werden (Art. 8a Abs. 2–4 DSGVO-E). Unternehmer als betroffene Personen (insbesondere Prominente) sind auszunehmen, da sie nicht schutzwürdig sind (Art. 8a Abs. 5 DSGVO-E). Art. 9 DSGVO sollte unberührt bleiben, damit bei den höchstpersönlichen besonderen Kategorien personenbezogener Daten eine Kommerzialisierung in der Regel ausscheidet (Art. 8a Abs. 6 S. 1 DSGVO-E). Der Vertragsschluss und die Rechtsfolgen eines Datenüberlassungsvertrags können weiterhin dem nationalen Schuldrecht überlassen werden (Art. 8a Abs. 6 S. 2 DSGVO). So kann diese bisher nebulöse Diskussion einer sachgerechten, ausgewogenen Lösung zugeführt werden.

B. Ausblick

Wird der U. S. Kongress den CCPA übernehmen? Bereits seit den 1970ern hat dieser wiederholt ein umfassendes Datenschutzgesetz erwogen, welches allerdings stets am Widerstand der Wirtschaftsverbände gescheitert ist.[2] Mit dem Inkrafttreten des CCPA ist dieser Widerstand schlagartig wesentlich geschwächt worden, da in den gesamten Vereinigten Staaten tätige Unternehmen ohnehin die Datenschutzpflichten des CCPA einhalten müssen.[3] Die Furcht vor einer Rechtszersplitterung führt sogar dazu, dass Wirtschaftsverbände jetzt ein umfassendes Datenschutzgesetz befürworten.[4] Auf Bundesebene besteht damit

[2] Siehe Kapitel 2:B.I.2 (ab S. 19).

[3] *Büyuksagis*, 30 Fordham Intell. Prop. Media & Ent. L. J. 139, 181 f.; *Gassner*, 12 U.C. Irvine L. Rev. 267, 302; *Hartzog/Richards*, 61 B.C. L. Rev. 1687, 1692; *Whitney*, 96 Denv. L. Rev. Online 176, 179.

[4] *Hartzog/Richards*, 61 B.C. L. Rev. 1687, 1692; *Solove/Schwartz*, ALI Data Privacy: Overview and Black Letter Text, S. 4; *Whitney*, 96 Denv. L. Rev. Online 176, 179.

Einigkeit, dass der U. S. Kongress ein umfassendes Datenschutzgesetz erlassen sollte.[5] Die Frage ist nur: welches?

Angesichts der Abstimmungsregeln im U. S.-Senat sind faktisch 60 von 100 Stimmen erforderlich,[6] was nur mit einem überparteilichen Konsens möglich ist. Ein solcher Konsens ist freilich zwischen massiv zerstrittenen Demokraten und Republikanern selbst über Routinebeschlüsse kaum zu erreichen – so war die U. S. Regierung in den letzten Jahren regelmäßig für mehrere Tage zahlungsunfähig, weil der U. S. Kongress zwar Ausgaben beschließt, aber nicht rechtzeitig das Schuldenlimit im gleichen Maß anhebt.[7]

Dementsprechend hat sich derzeit die amerikanische Datenschutzdebatte auf einzelstaatliche Gesetze fokussiert, die oft stark durch den CCPA beeinflusst sind.[8] Diese Entwicklung in Gang zu setzen, war explizites Ziel beider dem CCPA zugrundeliegenden Volksbegehren.[9] Seit 2018 haben Abgeordnete in den Parlamenten von 29 der 49 anderen Bundesstaaten Gesetzesentwürfe für ein umfassendes Datenschutzgesetz eingebracht.[10]

Davon waren bisher vier Gesetze erfolgreich: der Colorado Privacy Act,[11] der Connecticut Act Concerning Personal Data Privacy and Online Monitoring,[12] der Utah Consumer Privacy Act[13] und der Virgina Consumer Data Protection Act.[14] Die durch diese vier Gesetze statuierten Rechte und Pflichten ähneln dem CCPA stark.[15] Gesetzesentwürfe, die sich wie der Washington Privacy Act stärker an der DSGVO orientierten, sind dagegen bisher gescheitert. Damit spricht einiges dafür, dass sich noch weitere Bundesstaaten an dem tief im amerikanischen Recht verwurzelten CCPA orientieren werden.

Wird dieser Trend wiederum zu einem umfassenden U. S.-Datenschutzgesetz führen? Zwar zeigt die Datenpannen-Meldepflicht, dass auch eine parallele

---

[5] *Büyuksagis*, 30 Fordham Intell. Prop. Media & Ent. L. J. 139, 182; *Feld*, 24 N.C. Banking Inst. 481, 497; *Hartzog/Richards*, 61 B.C. L. Rev. 1687, 1692; *Solove/Schwartz*, ALI Data Privacy: Overview and Black Letter Text, S. 4; *Wilson*, The Time is Ripe for Federal Privacy Legislation, S. 2.

[6] *Dauster*, 19 N.Y.U. J. Legis. & Pub. Pol'y 631, 639–645.

[7] *Brass et al.*, Shutdown of the Federal Government, S. 3 f. Die Schuldenbremse selbst ist geregelt in: 31 U.S.C. § 3101(b).

[8] *Büyuksagis*, 30 Fordham Intell. Prop. Media & Ent. L. J. 139; *Flor*, 96 Notre Dame L. Rev. 2035, 2403; *Manheim/Kaplan*, 21 Yale J. L. & Tech. 106; *Monnin*, 95 N. D. L. Rev. 345, 363; *Ormerod*, Privacy Qui Tam, S. 11; *Park*, 10 UC Irvine L. Rev. 1455, 1488; *Yallen*, 53 Loy. L. A. L. Rev. 787, 818. Zum »Kalifornien-Effekt« siehe Kapitel 2:B.II (ab S. 27).

[9] Zum CCPA-2018: *Lapowsky*, Bill Could Give Californians Unprecedented Control Over Data. Zu Proposition 24: *Californians for Consumer Privacy*, Prop 24 Webinar, 13m:00s.

[10] *DataGuidance*, USA State Law Tracker.

[11] Colo. Rev. Stat. §§ 6-1-1301 bis 6-1-1313.

[12] Conn. Public Act No. 22-15.

[13] Utah Code Ann. § 13-61-101 bis 13-404.

[14] Va. Code Ann. §§ 59.1-571 bis 59.1-581.

[15] *Duball*, The Privacy Advisor, Colorado Privacy Act passes, professionals ponder effects; *Goldman*, Internet Law, S. 383; *Southwell et al.*, Virginia Passes Comprehensive Privacy Law, S. 1.

Regelung durch alle 50 Bundesstaaten möglich ist. Datenschutzgesetze erzeugen aber höhere Umsetzungskosten bei Abweichungen, da sie nicht nur einmalig bei der Datenpannenmeldung, sondern fortlaufend einzuhalten sind. In den gesamten Vereinigten Staaten tätige Unternehmen haben damit ein deutliches Interesse an einem vorrangig anwendbaren Bundesdatenschutzgesetz. Umgekehrt sinkt aber das Interesse von Verbraucherschutzorganisationen an einem Bundesdatenschutzgesetz, wenn sie ihr Ziel eines stärkeren Datenschutzes auch durch zahlreiche einzelstaatliche Datenschutzgesetze erreichen können. Damit haben sie nur einen Anreiz, ein vorrangig anwendbares Bundesdatenschutzgesetz zu unterstützen, wenn dieses stärker als der CCPA wäre. Dementsprechend hat die demokratische Sprecherin des U. S. Repräsentantenhauses *Nancy Pelosi* eine Zustimmung zu einem Bundesdatenschutzgesetz ausgeschlossen, wenn dieses den CCPA schwächt.[16]

Somit ergeben sich zwei Varianten für die Zukunft des CCPA. Erstens könnte der U. S.-Kongress ein umfassendes Datenschutzgesetz erlassen. Dieses wird sich wohl eng am CCPA orientieren, weil eine Abschwächung des CCPA für die in Kalifornien traditionell starke demokratische Partei nur schwer vertretbar ist, zumal der CCPA durch einen Volksentscheid legitimiert ist. Zweitens könnte sich auch der bisherige Trend einzelstaatlicher Datenschutzgesetze dauerhaft fortsetzen und verstetigen. Auch in dieser Alternative wäre der CCPA wegen des »Kalifornien-Effekts«[17] für das amerikanische Datenschutzrecht prägend.

Damit zeigt sich Kalifornien als Demokratielabor, das mit dem Experiment CCPA die Entwicklung eines originär amerikanischen, liberalen Datenschutzes entscheidend voranbringt. Wie weit, wird die Zukunft zeigen.

[16] So die Sprecherin des Repräsentantenhauses *Nancy Pelosi* in: *Swisher*, Interview with Nancy Pelosi.

[17] Siehe Kapitel 2:B.II (ab S. 27).

Anhang 1: California Consumer Privacy Act[1]

Cal. Civ. Code § 1798.100. General Duties of Businesses that Collect Personal Information

(a) A business that controls the collection of a consumer's personal information shall, at or before the point of collection, inform consumers of the following:

(1) The categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared. A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected without providing the consumer with notice consistent with this section.

(2) If the business collects sensitive personal information, the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used, and whether that information is sold or shared. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected without providing the consumer with notice consistent with this section.

(3) The length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine that period provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose.

(b) A business that, acting as a third party, controls the collection of personal information about a consumer may satisfy its obligation under subdivision (a) by providing the required information prominently and conspicuously on the homepage of its internet website. In addition, if a business acting as a third party controls the collection of personal information about a consumer on its premises, including in a vehicle, then the business shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information are used, and whether that personal information is sold, in a clear and conspicuous manner at the location.

(c) A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.

[1] Aktuelle Fassung im Juli 2022 aufgrund der letzten Änderung zum 01.01.2022. Die ab 01.01.2023 anwendbaren Änderungen durch Proposition 24 sind bereits berücksichtigt.

(d) A business that collects a consumer's personal information and that sells that personal information to, or shares it with, a third party or that discloses it to a service provider or contractor for a business purpose shall enter into an agreement with the third party, service provider, or contractor, that:

(1) Specifies that the personal information is sold or disclosed by the business only for limited and specified purposes.

(2) Obligates the third party, service provider, or contractor to comply with applicable obligations under this title and obligate those persons to provide the same level of privacy protection as is required by this title.

(3) Grants the business rights to take reasonable and appropriate steps to help ensure that the third party, service provider, or contractor uses the personal information transferred in a manner consistent with the business' obligations under this title.

(4) Requires the third party, service provider, or contractor to notify the business if it makes a determination that it can no longer meet its obligations under this title.

(5) Grants the business the right, upon notice, including under paragraph (4), to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

(e) A business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Section 1798.81.5.

(f) Nothing in this section shall require a business to disclose trade secrets, as specified in regulations adopted pursuant to paragraph (3) of subdivision (a) of Section 1798.185.

Cal. Civ. Code § 1798.105. Consumers' Right to Delete Personal Information

(a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's rights to request the deletion of the consumer's personal information.

(c) (1) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records, notify any service providers or contractors to delete the consumer's personal information from their records, and notify all third parties to whom the business has sold or shared the personal information to delete the consumer's personal information unless this proves impossible or involves disproportionate effort.

(2) The business may maintain a confidential record of deletion requests solely for the purpose of preventing the personal information of a consumer who has submitted a deletion request from being sold, for compliance with laws or for other purposes, solely to the extent permissible under this title.

(3) A service provider or contractor shall cooperate with the business in responding to a verifiable consumer request, and at the direction of the business, shall delete, or enable the business to delete and shall notify any of its own service providers or contractors to delete personal information about the consumer collected, used, processed, or retained by the service provider or the contractor. The service provider or contractor shall notify any service providers, contractors, or third parties who may have accessed personal information from or through the service provider or contractor, unless the information was accessed at the direction of the business, to delete the consumer's personal information unless this proves impossible or involves

disproportionate effort. A service provider or contractor shall not be required to comply with a deletion request submitted by the consumer directly to the service provider or contractor to the extent that the service provider or contractor has collected, used, processed, or retained the consumer's personal information in its role as a service provider or contractor to the business.

(d) A business, or a service provider or contractor acting pursuant to its contract with the business, another service provider, or another contractor, shall not be required to comply with a consumer's request to delete the consumer's personal information if it is reasonably necessary for the business, service provider, or contractor to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated by the consumer within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(2) Help to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for those purposes.

(3) Debug to identify and repair errors that impair existing intended functionality.

(4) Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law.

(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.

(6) Engage in public or peer-reviewed scientific, historical, or statistical research that conforms or adheres to all other applicable ethics and privacy laws, when the business' deletion of the information is likely to render impossible or seriously impair the ability to complete such research, if the consumer has provided informed consent.

(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business and compatible with the context in which the consumer provided the information.

(8) Comply with a legal obligation.

Cal. Civ. Code § 1798.106. Consumers' Right to Correct Inaccurate Personal Information

(a) A consumer shall have the right to request a business that maintains inaccurate personal information about the consumer to correct that inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's right to request correction of inaccurate personal information.

(c) A business that receives a verifiable consumer request to correct inaccurate personal information shall use commercially reasonable efforts to correct the inaccurate personal information as directed by the consumer, pursuant to Section 1798.130 and regulations adopted pursuant to paragraph (8) of subdivision (a) of Section 1798.185.

Cal. Civ. Code § 1798.110. Consumers' Right to Know What Personal Information is Being Collected. Right to Access Personal Information

(a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

(1) The categories of personal information it has collected about that consumer.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting, selling, or sharing personal information.

(4) The categories of third parties to whom the business discloses personal information.

(5) The specific pieces of personal information it has collected about that consumer.

(b) A business that collects personal information about a consumer shall disclose to the consumer, pursuant to subparagraph (B) of paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer, provided that a business shall be deemed to be in compliance with paragraphs (1) to (4), inclusive, of subdivision (a) to the extent that the categories of information and the business or commercial purpose for collecting, selling, or sharing personal information it would be required to disclose to the consumer pursuant to paragraphs (1) to (4), inclusive, of subdivision (a) is the same as the information it has disclosed pursuant to paragraphs (1) to (4), inclusive, of subdivision (c).

(c) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The categories of personal information it has collected about consumers.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting, selling, or sharing personal information.

(4) The categories of third parties to whom the business discloses personal information.

(5) That a consumer has the right to request the specific pieces of personal information the business has collected about that consumer.

Cal. Civ. Code § 1798.115. Consumers' Right to Know What Personal Information is Sold or Shared and to Whom

(a) A consumer shall have the right to request that a business that sells or shares the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

(1) The categories of personal information that the business collected about the consumer.

(2) The categories of personal information that the business sold or shared about the consumer and the categories of third parties to whom the personal information was sold or shared, by category or categories of personal information for each category of third parties to whom the personal information was sold or shared.

(3) The categories of personal information that the business disclosed about the consumer for a business purpose and the categories of persons to whom it was disclosed for a business purpose.

(b) A business that sells or shares personal information about a consumer, or that discloses a consumer's personal information for a business purpose, shall disclose, pursuant to paragraph (4) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) to the consumer upon receipt of a verifiable consumer request from the consumer.

(c) A business that sells or shares consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose, pursuant to subparagraph (C) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The category or categories of consumers' personal information it has sold or shared, or if the business has not sold or shared consumers' personal information, it shall disclose that fact.

(2) The category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed consumers' personal information for a business purpose, it shall disclose that fact.

(d) A third party shall not sell or share personal information about a consumer that has been sold to, or shared with, the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120.

Cal. Civ. Code § 1798.120. Consumers' Right to Opt Out of Sale or Sharing of Personal Information

(a) A consumer shall have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information. This right may be referred to as the right to opt-out of sale or sharing.

(b) A business that sells consumers' personal information to, or shares it with, third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold or shared and that consumers have the "right to opt-out" of the sale or sharing of their personal information.

(c) Notwithstanding subdivision (a), a business shall not sell or share the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale or sharing of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age.

(d) A business that has received direction from a consumer not to sell or share the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell or share the minor consumer's personal information, shall be prohibited, pursuant to paragraph (4) of subdivision (c) of Section 1798.135, from selling or sharing the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides consent, for the sale or sharing of the consumer's personal information.

Cal. Civ. Code § 1798.121. Consumers' Right to Limit Use and Disclosure of Sensitive Personal Information

(a) A consumer shall have the right, at any time, to direct a business that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services, to perform the services set forth in paragraphs (2), (4), (5), and (8) of subdivision (e) of Section 1798.140, and as authorized by regulations adopted pursuant to subparagraph (C) of paragraph (19) of subdivision (a) of Section 1798.185. A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in this subdivision shall provide

notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be used, or disclosed to a service provider or contractor, for additional, specified purposes and that consumers have the right to limit the use or disclosure of their sensitive personal information.

(b) A business that has received direction from a consumer not to use or disclose the consumer's sensitive personal information, except as authorized by subdivision (a), shall be prohibited, pursuant to paragraph (4) of subdivision (c) of Section 1798.135, from using or disclosing the consumer's sensitive personal information for any other purpose after its receipt of the consumer's direction unless the consumer subsequently provides consent for the use or disclosure of the consumer's sensitive personal information for additional purposes.

(c) A service provider or contractor that assists a business in performing the purposes authorized by subdivision (a) may not use the sensitive personal information after it has received instructions from the business and to the extent it has actual knowledge that the personal information is sensitive personal information for any other purpose. A service provider or contractor is only required to limit its use of sensitive personal information received pursuant to a written contract with the business in response to instructions from the business and only with respect to its relationship with that business.

(d) Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to this section, as further defined in regulations adopted pursuant to subparagraph (C) of paragraph (19) of subdivision (a) of Section 1798.185, and shall be treated as personal information for purposes of all other sections of this act, including Section 1798.100.

Cal. Civ. Code § 1798.125. Consumers' Right of No Retaliation Following Opt Out or Exercise of Other Rights

(a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(E) Retaliating against an employee, applicant for employment, or independent contractor, as defined in subparagraph (A) of paragraph (2) of subdivision (m) of Section 1798.145, for exercising their rights under this title.

(2) Nothing in this subdivision prohibits a business, pursuant to subdivision (b), from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.

(3) This subdivision does not prohibit a business from offering loyalty, rewards, premium features, discounts, or club card programs consistent with this title.

(b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale or sharing of personal information, or the retention of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is reasonably related to the value provided to the business by the consumer's data.

(2) A business that offers any financial incentives pursuant to this subdivision, shall notify consumers of the financial incentives pursuant to Section 1798.130.

(3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.130 that clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time. If a consumer refuses to provide opt-in consent, then the business shall wait for at least 12 months before next requesting that the consumer provide opt-in consent, or as prescribed by regulations adopted pursuant to Section 1798.185.

(4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

Cal. Civ. Code § 1798.130. Notice, Disclosure, Correction, and Deletion Requirements

(a) In order to comply with Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:

(1) (A) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, or requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively, including, at a minimum, a toll-free telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, or for requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively.

(B) If the business maintains an internet website, make the internet website available to consumers to submit requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, or requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively.

(2) (A) Disclose and deliver the required information to a consumer free of charge, correct inaccurate personal information, or delete a consumer's personal information, based on the consumer's request, within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business's duty to disclose and deliver the information, to correct inaccurate personal information, or to delete personal information within 45 days of receipt of the consumer's request. The time period to provide the required information, to correct inaccurate personal information, or to delete personal information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure of the required information shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but shall not require the consumer to create an account with the business in order to make a verifiable consumer request provided that if the consumer, has an account with the business, the business may require the consumer to use that account to submit a verifiable consumer request.

(B) The disclosure of the required information shall cover the 12-month period preceding the business' receipt of the verifiable consumer request provided that, upon the adoption of a

regulation pursuant to paragraph (9) of subdivision (a) of Section 1798.185, a consumer may request that the business disclose the required information beyond the 12-month period, and the business shall be required to provide that information unless doing so proves impossible or would involve a disproportionate effort. A consumer's right to request required information beyond the 12-month period, and a business's obligation to provide that information, shall only apply to personal information collected on or after January 1, 2022. Nothing in this subparagraph shall require a business to keep personal information for any length of time.

(3) (A) A business that receives a verifiable consumer request pursuant to Section 1798.110 or 1798.115 shall disclose any personal information it has collected about a consumer, directly or indirectly, including through or by a service provider or contractor, to the consumer. A service provider or contractor shall not be required to comply with a verifiable consumer request received directly from a consumer or a consumer's authorized agent, pursuant to Section 1798.110 or 1798.115, to the extent that the service provider or contractor has collected personal information about the consumer in its role as a service provider or contractor. A service provider or contractor shall provide assistance to a business with which it has a contractual relationship with respect to the business' response to a verifiable consumer request, including, but not limited to, by providing to the business the consumer's personal information in the service provider or contractor's possession, which the service provider or contractor obtained as a result of providing services to the business, and by correcting inaccurate information or by enabling the business to do the same. A service provider or contractor that collects personal information pursuant to a written contract with a business shall be required to assist the business through appropriate technical and organizational measures in complying with the requirements of subdivisions (d) to (f), inclusive, of Section 1798.100, taking into account the nature of the processing.

(B) For purposes of subdivision (b) of Section 1798.110:

(i) To identify the consumer, associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(ii) Identify by category or categories the personal information collected about the consumer for the applicable period of time by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected; the categories of sources from which the consumer's personal information was collected; the business or commercial purpose for collecting, selling, or sharing the consumer's personal information; and the categories of third parties to whom the business discloses the consumer's personal information.

(iii) Provide the specific pieces of personal information obtained from the consumer in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity at the consumer's request without hindrance. "Specific pieces of information" do not include data generated to help ensure security and integrity or as prescribed by regulation. Personal information is not considered to have been disclosed by a business when a consumer instructs a business to transfer the consumer's personal information from one business to another in the context of switching services.

(4) For purposes of subdivision (b) of Section 1798.115:

(A) Identify the consumer and associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information of the consumer that the business sold or shared during the applicable period of time by reference to the enumerated

category in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was sold or shared during the applicable period of time by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold or shared. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (C).

(C) Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose during the applicable period of time by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information, and provide the categories of persons to whom the consumer's personal information was disclosed for a business purpose during the applicable period of time by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B).

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its internet website, and update that information at least once every 12 months:

(A) A description of a consumer's rights pursuant to Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, and 1798.125 and two or more designated methods for submitting requests, except as provided in subparagraph (A) of paragraph (1) of subdivision (a).

(B) For purposes of subdivision (c) of Section 1798.110:

(i) A list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.

(ii) The categories of sources from which consumers' personal information is collected.

(iii) The business or commercial purpose for collecting, selling, or sharing consumers' personal information.

(iv) The categories of third parties to whom the business discloses consumers' personal information.

(C) For purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115, two separate lists:

(i) A list of the categories of personal information it has sold or shared about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold or shared, or if the business has not sold or shared consumers' personal information in the preceding 12 months, the business shall prominently disclose that fact in its privacy policy.

(ii) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describes the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business' privacy practices or the business' compliance with this title are informed of all requirements in Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.125, and this section, and how to direct consumers to exercise their rights under those sections.

(7) Use any personal information collected from the consumer in connection with the business' verification of the consumer's request solely for the purposes of verification and shall

not further disclose the personal information, retain it longer than necessary for purposes of verification, or use it for unrelated purposes.

(b) A business is not obligated to provide the information required by Sections 1798.110 and 1798.115 to the same consumer more than twice in a 12-month period.

(c) The categories of personal information required to be disclosed pursuant to Sections 1798.100, 1798.110, and 1798.115 shall follow the definitions of personal information and sensitive personal information in Section 1798.140 by describing the categories of personal information using the specific terms set forth in subparagraphs (A) to (K), inclusive, of paragraph (1) of subdivision (v) of Section 1798.140 and by describing the categories of sensitive personal information using the specific terms set forth in paragraphs (1) to (9), inclusive, of subdivision (ae) of Section 1798.140.

Cal. Civ. Code § 1798.135. Methods of Limiting Sale, Sharing, and Use of Personal Information and Use of Sensitive Personal Information

(a) A business that sells or shares consumers' personal information or uses or discloses consumers' sensitive personal information for purposes other than those authorized by subdivision (a) of Section 1798.121 shall, in a form that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business's internet homepages, titled "Do Not Sell or Share My Personal Information," to an internet web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale or sharing of the consumer's personal information.

(2) Provide a clear and conspicuous link on the business' internet homepages, titled "Limit the Use of My Sensitive Personal Information," that enables a consumer, or a person authorized by the consumer, to limit the use or disclosure of the consumer's sensitive personal information to those uses authorized by subdivision (a) of Section 1798.121.

(3) At the business' discretion, utilize a single, clearly labeled link on the business' internet homepages, in lieu of complying with paragraphs (1) and (2), if that link easily allows a consumer to opt out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information.

(4) In the event that a business responds to opt-out requests received pursuant to paragraph (1), (2), or (3) by informing the consumer of a charge for the use of any product or service, present the terms of any financial incentive offered pursuant to subdivision (b) of Section 1798.125 for the retention, use, sale, or sharing of the consumer's personal information.

(b) (1) A business shall not be required to comply with subdivision (a) if the business allows consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism, based on technical specifications set forth in regulations adopted pursuant to paragraph (20) of subdivision (a) of Section 1798.185, to the business indicating the consumer's intent to opt out of the business' sale or sharing of the consumer's personal information or to limit the use or disclosure of the consumer's sensitive personal information, or both.

(2) A business that allows consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information pursuant to paragraph (1) may provide a link to a web page that enables the consumer to consent to the business ignoring the opt-out preference signal with respect to that business' sale or sharing of the consumer's personal information or the use of the consumer's sensitive personal information for additional purposes provided that:

(A) The consent web page also allows the consumer or a person authorized by the consumer to revoke the consent as easily as it is affirmatively provided.

(B) The link to the web page does not degrade the consumer's experience on the web page the consumer intends to visit and has a similar look, feel, and size relative to other links on the same web page.

(C) The consent web page complies with technical specifications set forth in regulations adopted pursuant to paragraph (20) of subdivision (a) of Section 1798.185.

(3) A business that complies with subdivision (a) is not required to comply with subdivision (b). For the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b).

(c) A business that is subject to this section shall:

(1) Not require a consumer to create an account or provide additional information beyond what is necessary in order to direct the business not to sell or share the consumer's personal information or to limit use or disclosure of the consumer's sensitive personal information.

(2) Include a description of a consumer's rights pursuant to Sections 1798.120 and 1798.121, along with a separate link to the "Do Not Sell or Share My Personal Information" internet web page and a separate link to the "Limit the Use of My Sensitive Personal Information" internet web page, if applicable, or a single link to both choices, or a statement that the business responds to and abides by opt-out preference signals sent by a platform, technology, or mechanism in accordance with subdivision (b), in:

(A) Its online privacy policy or policies if the business has an online privacy policy or policies.

(B) Any California-specific description of consumers' privacy rights.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Sections 1798.120, 1798.121, and this section and how to direct consumers to exercise their rights under those sections.

(4) For consumers who exercise their right to opt-out of the sale or sharing of their personal information or limit the use or disclosure of their sensitive personal information, refrain from selling or sharing the consumer's personal information or using or disclosing the consumer's sensitive personal information and wait for at least 12 months before requesting that the consumer authorize the sale or sharing of the consumer's personal information or the use and disclosure of the consumer's sensitive personal information for additional purposes, or as authorized by regulations.

(5) For consumers under 16 years of age who do not consent to the sale or sharing of their personal information, refrain from selling or sharing the personal information of the consumer under 16 years of age and wait for at least 12 months before requesting the consumer's consent again, or as authorized by regulations or until the consumer attains 16 years of age.

(6) Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.

(d) Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

(e) A consumer may authorize another person to opt-out of the sale or sharing of the consumer's personal information and to limit the use of the consumer's sensitive personal

information on the consumer's behalf, including through an opt-out preference signal, as defined in paragraph (1) of subdivision (b), indicating the consumer's intent to opt out, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General regardless of whether the business has elected to comply with subdivision (a) or (b). For purposes of clarity, a business that elects to comply with subdivision (a) may respond to the consumer's opt-out consistent with Section 1798.125.

(f) If a business communicates a consumer's opt-out request to any person authorized by the business to collect personal information, the person shall thereafter only use that consumer's personal information for a business purpose specified by the business, or as otherwise permitted by this title, and shall be prohibited from:

(1) Selling or sharing the personal information.

(2) Retaining, using, or disclosing that consumer's personal information.

(A) For any purpose other than for the specific purpose of performing the services offered to the business.

(B) Outside of the direct business relationship between the person and the business.

(C) For a commercial purpose other than providing the services to the business.

(g) A business that communicates a consumer's opt-out request to a person pursuant to subdivision (f) shall not be liable under this title if the person receiving the opt-out request violates the restrictions set forth in the title provided that, at the time of communicating the opt-out request, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation. Any provision of a contract or agreement of any kind that purports to waive or limit in any way this subdivision shall be void and unenforceable.

Cal. Civ. Code § 1798.140. Definitions

For purposes of this title:

(a) "Advertising and marketing" means a communication by a business or a person acting on the business' behalf in any medium intended to induce a consumer to obtain goods, services, or employment.

(b) "Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.

(c) "Biometric information" means an individual's physiological, biological, or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that is used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(d) "Business" means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes

and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, sells, or shares the personal information of 100,000 or more consumers or households.

(C) Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information.

(2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business and with whom the business shares consumers' personal information. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark that the average consumer would understand that two or more entities are commonly owned.

(3) A joint venture or partnership composed of businesses in which each business has at least a 40 percent interest. For purposes of this title, the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business.

(4) A person that does business in California, that is not covered by paragraph (1), (2), or (3), and that voluntarily certifies to the California Privacy Protection Agency that it is in compliance with, and agrees to be bound by, this title.

(e) "Business purpose" means the use of personal information for the business' operational purposes, or other notified purposes, or for the service provider or contractor's operational purposes, as defined by regulations adopted pursuant to paragraph (11) of subdivision (a) of Section 1798.185, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed or for another purpose that is compatible with the context in which the personal information was collected. Business purposes are:

(1) Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) Helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes.

(3) Debugging to identify and repair errors that impair existing intended functionality.

(4) Short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.

(5) Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.

(6) Providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer provided that, for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers that

the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or persons or collects from its own interaction with consumers.

(7) Undertaking internal research for technological development and demonstration.

(8) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

(f) "Collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.

(g) "Commercial purposes" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction.

(h) "Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent.

(i) "Consumer" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

(j) (1) "Contractor" means a person to whom the business makes available a consumer's personal information for a business purpose, pursuant to a written contract with the business, provided that the contract:

(A) Prohibits the contractor from:

(i) Selling or sharing the personal information.

(ii) Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract, or as otherwise permitted by this title.

(iii) Retaining, using, or disclosing the information outside of the direct business relationship between the contractor and the business.

(iv) Combining the personal information that the contractor receives pursuant to a written contract with the business with personal information that it receives from or on behalf of another person or persons, or collects from its own interaction with the consumer, provided that the contractor may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) and in regulations adopted by the California Privacy Protection Agency.

(B) Includes a certification made by the contractor that the contractor understands the restrictions in subparagraph (A) and will comply with them.

(C) Permits, subject to agreement with the contractor, the business to monitor the contractor's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.

(2) If a contractor engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the contractor engages another person to assist in processing personal information for that business purpose, it shall notify the business of that engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).

(k) "Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.

(l) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation.

(m) "Deidentified" means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the business that possesses the information:

(1) Takes reasonable measures to ensure that the information cannot be associated with a consumer or household.

(2) Publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision.

(3) Contractually obligates any recipients of the information to comply with all provisions of this subdivision.

(n) "Designated methods for submitting requests" means a mailing address, email address, internet web page, internet web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.

(o) "Device" means any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device.

(p) "Homepage" means the introductory page of an internet website and any internet web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, "About," "Information,'' or settings page, and any other location that allows consumers to review the notices required by this title, including, but not limited to, before downloading the application.

(q) "Household" means a group, however identified, of consumers who cohabitate with one another at the same residential address and share use of common devices or services.

(r) "Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

(s) "Intentionally interacts" means when the consumer intends to interact with a person, or disclose personal information to a person, via one or more deliberate interactions, including visiting the person's website or purchasing a good or service from the person. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a person.

(t) "Nonpersonalized advertising" means advertising and marketing that is based solely on a consumer's personal information derived from the consumer's current interaction with the business with the exception of the consumer's precise geolocation.

(u) "Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

(v) (1) "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

(B) Any personal information described in subdivision (e) of Section 1798.80.

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(L) Sensitive personal information.

(2) "Personal information" does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. For purposes of this paragraph, "publicly available" means: information that is lawfully made available from federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

(3) "Personal information" does not include consumer information that is deidentified or aggregate consumer information.

(w) "Precise geolocation" means any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet, except as prescribed by regulations.

(x) "Probabilistic identifier" means the identification of a consumer or a consumer's device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

(y) "Processing" means any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means.

(z) "Profiling" means any form of automated processing of personal information, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of Section 1798.185, to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(aa) "Pseudonymize" or "Pseudonymization" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

(ab) "Research" means scientific analysis, systematic study, and observation, including basic research or applied research that is designed to develop or contribute to public or scientific knowledge and that adheres or otherwise conforms to all other applicable ethics and privacy laws, including, but not limited to, studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business' service or device for other purposes shall be:

(1) Compatible with the business purpose for which the personal information was collected.

(2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, by a business.

(3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain, other than as needed to support the research.

(4) Subject to business processes that specifically prohibit reidentification of the information, other than as needed to support the research.

(5) Made subject to business processes to prevent inadvertent release of deidentified information.

(6) Protected from any reidentification attempts.

(7) Used solely for research purposes that are compatible with the context in which the personal information was collected.

(8) Subjected by the business conducting the research to additional security controls that limit access to the research data to only those individuals as are necessary to carry out the research purpose.

(ac) "Security and integrity" means the ability of:

(1) Networks or information systems to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information.

(2) Businesses to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions and to help prosecute those responsible for those actions.

(3) Businesses to ensure the physical safety of natural persons.

(ad) (1) "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration.

(2) For purposes of this title, a business does not sell personal information when:

(A) A consumer uses or directs the business to intentionally:

(i) Disclose personal information.

(ii) Interact with one or more third parties.

(B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information or limited the use of the consumer's sensitive personal information for the purposes of alerting persons that the consumer has opted out of the sale of the consumer's personal information or limited the use of the consumer's sensitive personal information.

(C) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with this title. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with this title. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(ae) "Sensitive personal information" means:

(1) Personal information that reveals:

(A) A consumer's social security, driver's license, state identification card, or passport number.

(B) A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

(C) A consumer's precise geolocation.

(D) A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership.

(E) The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.

(F) A consumer's genetic data.

(2) (A) The processing of biometric information for the purpose of uniquely identifying a consumer.

(B) Personal information collected and analyzed concerning a consumer's health.

(C) Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

(3) Sensitive personal information that is "publicly available" pursuant to paragraph (2) of subdivision (v) shall not be considered sensitive personal information or personal information.

(af) "Service" or "services" means work, labor, and services, including services furnished in connection with the sale or repair of goods.

(ag) (1) "Service provider" means a person that processes personal information on behalf of a business and that receives from or on behalf of the business consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the person from:

(A) Selling or sharing the personal information.

(B) Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract for the business, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract with the business, or as otherwise permitted by this title.

(C) Retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business.

(D) Combining the personal information that the service provider receives from, or on behalf of, the business with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that the service provider may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) of this section and in regulations adopted by the California Privacy Protection Agency. The contract may, subject to agreement with the service provider, permit the business to monitor the service provider's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.

(2) If a service provider engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the service provider engages another person to assist in processing personal information for that business purpose, it shall notify the business of that engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).

(ah) (1) "Share," "shared," or "sharing" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

(2) For purposes of this title, a business does not share personal information when:

(A) A consumer uses or directs the business to intentionally disclose personal information or intentionally interact with one or more third parties.

(B) The business uses or shares an identifier for a consumer who has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information for the purposes of alerting persons that the consumer has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information.

(C) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with this title. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with this title. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(ai) "Third party" means a person who is not any of the following:

(1) The business with whom the consumer intentionally interacts and that collects personal information from the consumer as part of the consumer's current interaction with the business under this title.

(2) A service provider to the business.

(3) A contractor.

(aj) "Unique identifier" or "unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device that is linked to a consumer or family. For purposes of this subdivision, "family" means a custodial parent or guardian and any children under 18 years of age over which the parent or guardian has custody.

(ak) "Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, or by a person who has power of attorney or is acting as a conservator for the consumer, and that the business can verify, using commercially reasonable methods, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115, to delete personal information pursuant to Section 1798.105, or to correct inaccurate personal information pursuant to Section 1798.106, if the business cannot verify, pursuant to this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

Cal. Civ. Code § 1798.145. Exemptions

(a) The obligations imposed on businesses by this title shall not restrict a business' ability to:

(1) Comply with federal, state, or local laws or comply with a court order or subpoena to provide information.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities. Law enforcement agencies, including police and sheriff's departments, may direct a business pursuant to a law enforcement agency-approved investigation with an active case number not to delete a consumer's personal information, and, upon receipt of that direction, a business shall not delete the personal information for 90 days in order to allow the law enforcement agency to obtain a court-issued subpoena, order, or warrant to obtain a consumer's personal information. For good cause and only to the extent necessary for investigatory purposes, a law enforcement agency may direct a business not to delete the consumer's personal information for additional 90-day periods. A business that has received direction from a law enforcement agency not to delete the personal information of a consumer who has requested deletion of the consumer's personal information shall not use the consumer's personal information for any purpose other than retaining it to produce to law enforcement in response to a court-issued subpoena, order, or warrant unless the consumer's deletion request is subject to an exemption from deletion under this title.

(3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(4) Cooperate with a government agency request for emergency access to a consumer's personal information if a natural person is at risk or danger of death or serious physical injury provided that:

(A) The request is approved by a high-ranking agency officer for emergency access to a consumer's personal information.

(B) The request is based on the agency's good faith determination that it has a lawful basis to access the information on a nonemergency basis.

(C) The agency agrees to petition a court for an appropriate order within three days and to destroy the information if that order is not granted.

(5) Exercise or defend legal claims.

(6) Collect, use, retain, sell, share, or disclose consumers' personal information that is deidentified or aggregate consumer information.

(7) Collect, sell, or share a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not prohibit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

(b) The obligations imposed on businesses by Sections 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, and 1798.135 shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

(c) (1) This title shall not apply to any of the following:

(A) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

(B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

(C) Personal information collected as part of a clinical trial or other biomedical research study subject to, or conducted in accordance with, the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration, provided that the information is not sold or shared in a manner not permitted by this subparagraph, and, if it is inconsistent, that participants be informed of that use and provide consent.

(2) For purposes of this subdivision, the definitions of "medical information" and "provider of health care" in Section 56.05 shall apply and the definitions of "business associate," "covered entity," and "protected health information" in Section 160.103 of Title 45 of the Code of Federal Regulations shall apply.

(d) (1) This title shall not apply to an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in subdivision (f) of Section 1681a of Title 15 of the United States Code, by a furnisher of information, as set forth in Section 1681s-2 of Title 15 of the United States Code, who provides information for use in a consumer report, as defined in subdivision (d) of Section 1681a of Title 15 of the United States Code, and by a user of a consumer report as set forth in Section 1681b of Title 15 of the United States Code.

(2) Paragraph (1) shall apply only to the extent that such activity involving the collection, maintenance, disclosure, sale, communication, or use of such information by that agency, furnisher, or user is subject to regulation under the Fair Credit Reporting Act, Section 1681 et seq., Title 15 of the United States Code and the information is not collected, maintained, used, communicated, disclosed, or sold except as authorized by the Fair Credit Reporting Act.

(3) This subdivision shall not apply to Section 1798.150.

(e) This title shall not apply to personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code), or the federal Farm Credit Act of 1971 (as amended in 12 U.S.C. 2001-2279cc and implementing regulations, 12 C.F.R. 600, et seq.). This subdivision shall not apply to Section 1798.150.

(f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.). This subdivision shall not apply to Section 1798.150.

(g) (1) Section 1798.120 shall not apply to vehicle information or ownership information retained or shared between a new motor vehicle dealer, as defined in Section 426 of the Vehicle Code, and the vehicle's manufacturer, as defined in Section 672 of the Vehicle Code, if the vehicle information or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall conducted pursuant to Sections 30118 to 30120, inclusive, of Title 49 of the United States Code, provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose.

(2) Section 1798.120 shall not apply to vessel information or ownership information retained or shared between a vessel dealer and the vessel's manufacturer, as defined in Section 651 of the Harbors and Navigation Code, if the vessel information or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vessel repair covered by a vessel warranty or a recall conducted pursuant to Section 4310 of Title 46 of the United States Code, provided that the vessel dealer or vessel manufacturer with which that vessel information or ownership information is shared does not sell, share, or use that information for any other purpose.

(3) For purposes of this subdivision:

(A) "Ownership information" means the name or names of the registered owner or owners and the contact information for the owner or owners.

(B) "Vehicle information" means the vehicle information number, make, model, year, and odometer reading.

(C) "Vessel dealer" means a person who is engaged, wholly or in part, in the business of selling or offering for sale, buying or taking in trade for the purpose of resale, or exchanging, any vessel or vessels, as defined in Section 651 of the Harbors and Navigation Code, and receives or expects to receive money, profit, or any other thing of value.

(D) "Vessel information" means the hull identification number, model, year, month and year of production, and information describing any of the following equipment as shipped, transferred, or sold from the place of manufacture, including all attached parts and accessories:

(i) An inboard engine.

(ii) An outboard engine.

(iii) A stern drive unit.

(iv) An inflatable personal floatation device approved under Section 160.076 of Title 46 of the Code of Federal Regulations.

(h) Notwithstanding a business' obligations to respond to and honor consumer rights requests pursuant to this title:

(1) A time period for a business to respond to a consumer for any verifiable consumer request may be extended by up to a total of 90 days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(2) If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

(3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any verifiable consumer request is manifestly unfounded or excessive.

(i) (1) A business that discloses personal information to a service provider or contractor in compliance with this title shall not be liable under this title if the service provider or contractor receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider or contractor intends to commit such a violation. A service provider or contractor shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title provided that the service provider or contractor shall be liable for its own violations of this title.

(2) A business that discloses personal information of a consumer, with the exception of consumers who have exercised their right to opt out of the sale or sharing of their personal information, consumers who have limited the use or disclosure of their sensitive personal information, and minor consumers who have not opted in to the collection or sale of their personal information, to a third party pursuant to a written contract that requires the third party to provide the same level of protection of the consumer's rights under this title as provided by the business shall not be liable under this title if the third party receiving the personal information uses it in violation of the restrictions set forth in this title provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the third party intends to commit such a violation.

(j) This title shall not be construed to require a business, service provider, or contractor to:

(1) Reidentify or otherwise link information that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

(2) Retain any personal information about a consumer if, in the ordinary course of business, that information about the consumer would not be retained.

(3) Maintain information in identifiable, linkable, or associable form, or collect, obtain, retain, or access any data or technology, in order to be capable of linking or associating a verifiable consumer request with personal information.

(k) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other natural persons. A verifiable consumer request for specific pieces of personal information pursuant to Section 1798.110, to delete a consumer's personal information pursuant to Section 1798.105, or to correct inaccurate personal information pursuant to Section 1798.106, shall not extend to personal information about the consumer that belongs to, or the business maintains on behalf of, another natural person. A business may rely on representations made in a verifiable consumer request as to rights with respect to personal information and is under no legal requirement to seek out other persons that may have or claim to have rights to personal information, and a business is under no legal obligation under this title or any other provision of law to take any action under this title in the event of a dispute between or among persons claiming rights to personal information in the business' possession.

(l) The rights afforded to consumers and the obligations imposed on any business under this title shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the California Constitution.

(m) (1) This title shall not apply to any of the following:

(A) Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or an independent contractor of, that business.

(B) Personal information that is collected by a business that is emergency contact information of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, that business to the extent that the personal information is collected and used solely within the context of having an emergency contact on file.

(C) Personal information that is necessary for the business to retain to administer benefits for another natural person relating to the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, that business to the extent that the personal information is collected and used solely within the context of administering those benefits.

(2) For purposes of this subdivision:

(A) "Independent contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as director, or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Medical staff member" means a licensed physician and surgeon, dentist, or podiatrist, licensed pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code and a clinical psychologist as defined in Section 1316.5 of the Health and Safety Code.

(D) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, including a chief executive officer, president, secretary, or treasurer.

(E) "Owner" means a natural person who meets one of the following criteria:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall not apply to subdivision (a) of Section 1798.100 or Section 1798.150.

(4) This subdivision shall become inoperative on January 1, 2023.

(n) (1) The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.121, 1798.130, and 1798.135 shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who acted or is acting as an employee, owner, director, officer, or independent contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit, or government agency.

(2) For purposes of this subdivision:

(A) "Independent contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(D) "Owner" means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall become inoperative on January 1, 2023.

(o) (1) Sections 1798.105 and 1798.120 shall not apply to a commercial credit reporting agency's collection, processing, sale, or disclosure of business controller information to the extent the commercial credit reporting agency uses the business controller information solely to identify the relationship of a consumer to a business that the consumer owns or contact the consumer only in the consumer's role as the owner, director, officer, or management employee of the business.

(2) For the purposes of this subdivision:

(A) "Business controller information" means the name or names of the owner or owners, director, officer, or management employee of a business and the contact information, including a business title, for the owner or owners, director, officer, or management employee.

(B) "Commercial credit reporting agency" has the meaning set forth in subdivision (b) of Section 1785.42.

(C) "Owner" means a natural person that meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(D) "Director" means a natural person designated in the articles of incorporation of a business as director, or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(E) "Officer" means a natural person elected or appointed by the board of directors of a business to manage the daily operations of a corporation, including a chief executive officer, president, secretary, or treasurer.

(F) "Management employee" means a natural person whose name and contact information is reported to or collected by a commercial credit reporting agency as the primary manager of a business and used solely within the context of the natural person's role as the primary manager of the business.

(p) The obligations imposed on businesses in Sections 1798.105, 1798.106, 1798.110, and 1798.115 shall not apply to household data.

(q) (1) This title does not require a business to comply with a verifiable consumer request to delete a consumer's personal information under Section 1798.105 to the extent the verifiable consumer request applies to a student's grades, educational scores, or educational test results that the business holds on behalf of a local educational agency, as defined in subdivision (d) of Section 49073.1 of the Education Code, at which the student is currently enrolled. If a business does not comply with a request pursuant to this section, it shall notify the consumer that it is acting pursuant to this exception.

(2) This title does not require, in response to a request pursuant to Section 1798.110, that a business disclose on educational standardized assessment or educational assessment or a consumer's specific responses to the educational standardized assessment or educational assessment if consumer access, possession, or control would jeopardize the validity and reliability of that educational standardized assessment or educational assessment. If a business does not comply with a request pursuant to this section, it shall notify the consumer that it is acting pursuant to this exception.

(3) For purposes of this subdivision:

(A) "Educational standardized assessment or educational assessment" means a standardized or nonstandardized quiz, test, or other assessment used to evaluate students in or for entry to kindergarten and grades 1 to 12, inclusive, schools, postsecondary institutions, vocational programs, and postgraduate programs that are accredited by an accrediting agency or organization recognized by the State of California or the United States Department of Education, as well as certification and licensure examinations used to determine competency and eligibility to receive certification or licensure from a government agency or government certification body.

(B) "Jeopardize the validity and reliability of that educational standardized assessment or educational assessment" means releasing information that would provide an advantage to the consumer who has submitted a verifiable consumer request or to another natural person.

(r) Sections 1798.105 and 1798.120 shall not apply to a business' use, disclosure, or sale of particular pieces of a consumer's personal information if the consumer has consented to the business' use, disclosure, or sale of that information to produce a physical item, including a school yearbook containing the consumer's photograph if:

(1) The business has incurred significant expense in reliance on the consumer's consent.

(2) Compliance with the consumer's request to opt out of the sale of the consumer's personal information or to delete the consumer's personal information would not be commercially reasonable.

(3) The business complies with the consumer's request as soon as it is commercially reasonable to do so.

Cal. Civ. Code § 1798.146. [Deidentified Medical Data]

(a) This title shall not apply to any of the following:

(1) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the federal Health Information Technology for Economic and Clinical Health Act, Title XIII of the federal American Recovery and Reinvestment Act of 2009 (Public Law 111-5).

(2) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains, uses, and discloses patient information in the same manner as medical information or protected health information as described in paragraph (1).

(3) A business associate of a covered entity governed by the privacy, security, and data breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the federal Health Information Technology for Economic and Clinical Health Act, Title XIII of the federal American Recovery and Reinvestment Act of 2009 (Public Law 111-5), to the extent that the business associate maintains, uses, and discloses patient information in the same manner as medical information or protected health information as described in paragraph (1).

(4) (A) Information that meets both of the following conditions:

(i) It is deidentified in accordance with the requirements for deidentification set forth in Section 164.514 of Part 164 of Title 45 of the Code of Federal Regulations.

(ii) It is derived from patient information that was originally collected, created, transmitted, or maintained by an entity regulated by the Health Insurance Portability and Accountability Act, the Confidentiality Of Medical Information Act, or the Federal Policy for the Protection of Human Subjects, also known as the Common Rule.

(B) Information that met the requirements of subparagraph (A) but is subsequently reidentified shall no longer be eligible for the exemption in this paragraph, and shall be subject to applicable federal and state data privacy and security laws, including, but not limited to, the Health Insurance Portability and Accountability Act, the Confidentiality Of Medical Information Act, and this title.

(5) Information that is collected, used, or disclosed in research, as defined in Section 164.501 of Title 45 of the Code of Federal Regulations, including, but not limited to, a clinical trial, and that is conducted in accordance with applicable ethics, confidentiality, privacy, and security rules of Part 164 of Title 45 of the Code of Federal Regulations, the Federal Policy for

the Protection of Human Subjects, also known as the Common Rule, good clinical practice guidelines issued by the International Council for Harmonisation, or human subject protection requirements of the United States Food and Drug Administration.

(b) For purposes of this section, all of the following shall apply:

(1) "Business associate" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(2) "Covered entity" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(3) "Identifiable private information" has the same meaning as defined in Section 46.102 of Title 45 of the Code of Federal Regulations.

(4) "Individually identifiable health information" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(5) "Medical information" has the same meaning as defined in Section 56.05.

(6) "Patient information" shall mean identifiable private information, protected health information, individually identifiable health information, or medical information.

(7) "Protected health information" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(8) "Provider of health care" has the same meaning as defined in Section 56.05.

Cal. Civ. Code § 1798.148. [Safeguards for Deidentified Medical Data]

(a) A business or other person shall not reidentify, or attempt to reidentify, information that has met the requirements of paragraph (4) of subdivision (a) of Section 1798.146, except for one or more of the following purposes:

(1) Treatment, payment, or health care operations conducted by a covered entity or business associate acting on behalf of, and at the written direction of, the covered entity. For purposes of this paragraph, "treatment," "payment," "health care operations," "covered entity," and "business associate" have the same meaning as defined in Section 164.501 of Title 45 of the Code of Federal Regulations.

(2) Public health activities or purposes as described in Section 164.512 of Title 45 of the Code of Federal Regulations.

(3) Research, as defined in Section 164.501 of Title 45 of the Code of Federal Regulations, that is conducted in accordance with Part 46 of Title 45 of the Code of Federal Regulations, the Federal Policy for the Protection of Human Subjects, also known as the Common Rule.

(4) Pursuant to a contract where the lawful holder of the deidentified information that met the requirements of paragraph (4) of subdivision (a) of Section 1798.146 expressly engages a person or entity to attempt to reidentify the deidentified information in order to conduct testing, analysis, or validation of deidentification, or related statistical techniques, if the contract bans any other use or disclosure of the reidentified information and requires the return or destruction of the information that was reidentified upon completion of the contract.

(5) If otherwise required by law.

(b) In accordance with paragraph (4) of subdivision (a) of Section 1798.146, information reidentified pursuant this section shall be subject to applicable federal and state data privacy and security laws including, but not limited to, the Health Insurance Portability and Accountability Act, the Confidentiality of Medical Information Act, and this title.

(c) Beginning January 1, 2021, any contract for the sale or license of deidentified information that has met the requirements of paragraph (4) of subdivision (a) of Section 1798.146,

where one of the parties is a person residing or doing business in the state, shall include the following, or substantially similar, provisions:

(1) A statement that the deidentified information being sold or licensed includes deidentified patient information.

(2) A statement that reidentification, and attempted reidentification, of the deidentified information by the purchaser or licensee of the information is prohibited pursuant to this section.

(3) A requirement that, unless otherwise required by law, the purchaser or licensee of the deidentified information may not further disclose the deidentified information to any third party unless the third party is contractually bound by the same or stricter restrictions and conditions.

(d) For purposes of this section, "reidentify" means the process of reversal of deidentification techniques, including, but not limited to, the addition of specific pieces of information or data elements that can, individually or in combination, be used to uniquely identify an individual or usage of any statistical method, contrivance, computer software, or other means that have the effect of associating deidentified information with a specific identifiable individual.

Cal. Civ. Code § 1798.150. Personal Information Security Breaches

(a) (1) Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, or whose email address in combination with a password or security question and answer that would permit access to the account is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

(2) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

(b) Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. The implementation and maintenance of reasonable security procedures and practices pursuant to Section 1798.81.5 following a breach does not constitute a cure with respect to that breach. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for

each breach of the express written statement, as well as any other violation of the title that postdates the written statement.

(c) The cause of action established by this section shall apply only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.

Cal. Civ. Code § 1798.155. Administrative Enforcement

(a) Any business, service provider, contractor, or other person that violates this title shall be liable for an administrative fine of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation or violations involving the personal information of consumers whom the business, service provider, contractor, or other person has actual knowledge are under 16 years of age, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185, in an administrative enforcement action brought by the California Privacy Protection Agency.

(b) Any administrative fine assessed for a violation of this title, and the proceeds of any settlement of an action brought pursuant to subdivision (a), shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160 with the intent to fully offset any costs incurred by the state courts, the Attorney General, and the California Privacy Protection Agency in connection with this title.

Cal. Civ. Code § 1798.160. Consumer Privacy Fund

(a) A special fund to be known as the "Consumer Privacy Fund" is hereby created within the General Fund in the State Treasury, and is available upon appropriation by the Legislature first to offset any costs incurred by the state courts in connection with actions brought to enforce this title, the costs incurred by the Attorney General in carrying out the Attorney General's duties under this title, and then for the purposes of establishing an investment fund in the State Treasury, with any earnings or interest from the fund to be deposited in the General Fund, and making grants to promote and protect consumer privacy, educate children in the area of online privacy, and fund cooperative programs with international law enforcement organizations to combat fraudulent activities with respect to consumer data breaches.

(b) Funds transferred to the Consumer Privacy Fund shall be used exclusively as follows:

(1) To offset any costs incurred by the state courts and the Attorney General in connection with this title.

(2) After satisfying the obligations under paragraph (1), the remaining funds shall be allocated each fiscal year as follows:

(A) Ninety-one percent shall be invested by the Treasurer in financial assets with the goal of maximizing long term yields consistent with a prudent level of risk. The principal shall not be subject to transfer or appropriation, provided that any interest and earnings shall be transferred on an annual basis to the General Fund for appropriation by the Legislature for General Fund purposes.

(B) Nine percent shall be made available to the California Privacy Protection Agency for the purposes of making grants in California, with 3 percent allocated to each of the following grant recipients:

(i) Nonprofit organizations to promote and protect consumer privacy.

(ii) Nonprofit organizations and public agencies, including school districts, to educate children in the area of online privacy.

(iii) State and local law enforcement agencies to fund cooperative programs with international law enforcement organizations to combat fraudulent activities with respect to consumer data breaches.

(c) Funds in the Consumer Privacy Fund shall not be subject to appropriation or transfer by the Legislature for any other purpose.

Cal. Civ. Code § 1798.175. Conflicting Provisions

This title is intended to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information, including, but not limited to, Chapter 22 (commencing with Section 22575) of Division 8 of the Business and Professions Code and Title 1.81 (commencing with Section 1798.80). The provisions of this title are not limited to information collected electronically or over the Internet, but apply to the collection and sale of all personal information collected by a business from consumers. Wherever possible, law relating to consumers' personal information should be construed to harmonize with the provisions of this title, but in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

Cal. Civ. Code § 1798.180. Preemption

This title is a matter of statewide concern and supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection and sale of consumers' personal information by a business.

Cal. Civ. Code § 1798.185. Regulations

(a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas:

(1) Updating or adding categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision (v) of Section 1798.140, and updating or adding categories of sensitive personal information to those enumerated in subdivision (ae) of Section 1798.140 in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.

(2) Updating as needed the definitions of "deidentified" and "unique identifier" to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and adding, modifying, or deleting categories to the definition of designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business pursuant to Section 1798.130. The authority to update the definition of "deidentified" shall not apply to deidentification standards set forth in Section 164.514 of Title 45 of the Code of Federal Regulations, where such information previously was "protected health information" as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter, with the intention that trade secrets should not be disclosed in response to a verifiable consumer request.

(4) Establishing rules and procedures for the following:

(A) To facilitate and govern the submission of a request by a consumer to opt-out of the sale or sharing of personal information pursuant to Section 1798.120 and to limit the use of a consumer's sensitive personal information pursuant to Section 1798.121 to ensure that consumers have the ability to exercise their choices without undue burden and to prevent business from engaging in deceptive or harassing conduct, including in retaliation against consumers for exercising their rights, while allowing businesses to inform consumers of the consequences of their decision to opt out of the sale or sharing of their personal information or to limit the use of their sensitive personal information.

(B) To govern business compliance with a consumer's opt-out request.

(C) For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

(5) Adjusting the monetary thresholds, in January of every odd-numbered year to reflect any increase in the Consumer Price Index, in: subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.140; subparagraph (A) of paragraph (1) of subdivision (a) of Section 1798.150; subdivision (a) of Section 1798.155; Section 1798.199.25; and subdivision (a) of Section 1798.199.90.

(6) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentives within one year of passage of this title and as needed thereafter.

(7) Establishing rules and procedures to further the purposes of Sections 1798.105, 1798.106, 1798.110, and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to delete personal information, correct inaccurate personal information pursuant to Section 1798.106, or obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business's determination that a request for information received from a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.

(8) Establishing how often, and under what circumstances, a consumer may request a correction pursuant to Section 1798.106, including standards governing the following:

(A) How a business responds to a request for correction, including exceptions for requests to which a response is impossible or would involve disproportionate effort, and requests for correction of accurate information.

(B) How concerns regarding the accuracy of the information may be resolved.

(C) The steps a business may take to prevent fraud.

(D) If a business rejects a request to correct personal information collected and analyzed concerning a consumer's health, the right of a consumer to provide a written addendum to the business with respect to any item or statement regarding any such personal information that the consumer believes to be incomplete or incorrect. The addendum shall be limited to 250 words per alleged incomplete or incorrect item and shall clearly indicate in writing that the consumer requests the addendum to be made a part of the consumer's record.

(9) Establishing the standard to govern a business' determination, pursuant to subparagraph (B) of paragraph (2) of subdivision (a) of Section 1798.130, that providing information beyond the 12-month period in a response to a verifiable consumer request is impossible or would involve a disproportionate effort.

(10) Issuing regulations further defining and adding to the business purposes, including other notified purposes, for which businesses, service providers, and contractors may use consumers' personal information consistent with consumers' expectations, and further defining the business purposes for which service providers and contractors may combine consumers' personal information obtained from different sources, except as provided for in paragraph (6) of subdivision (e) of Section 1798.140.

(11) Issuing regulations identifying those business purposes, including other notified purposes, for which service providers and contractors may use consumers' personal information received pursuant to a written contract with a business, for the service provider or contractor's own business purposes, with the goal of maximizing consumer privacy.

(12) Issuing regulations to further define "intentionally interacts," with the goal of maximizing consumer privacy.

(13) Issuing regulations to further define "precise geolocation," including if the size defined is not sufficient to protect consumer privacy in sparsely populated areas or when the personal information is used for normal operational purposes, including billing.

(14) Issuing regulations to define the term "specific pieces of information obtained from the consumer" with the goal of maximizing a consumer's right to access relevant personal information while minimizing the delivery of information to a consumer that would not be useful to the consumer, including system log information and other technical data. For delivery of the most sensitive personal information, the regulations may require a higher standard of authentication provided that the agency shall monitor the impact of the higher standard on the right of consumers to obtain their personal information to ensure that the requirements of verification do not result in the unreasonable denial of verifiable consumer requests.

(15) Issuing regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to:

(A) Perform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent. The factors to be considered in determining when processing may result in significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities.

(B) Submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public. Nothing in this section shall require a business to divulge trade secrets.

(16) Issuing regulations governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer.

(17) Issuing regulations to further define a "law enforcement agency-approved investigation" for purposes of the exception in paragraph (2) of subdivision (a) of Section 1798.145.

(18) Issuing regulations to define the scope and process for the exercise of the agency's audit authority, to establish criteria for selection of persons to audit, and to protect consumers' personal information from disclosure to an auditor in the absence of a court order, warrant, or subpoena.

(19) (A) Issuing regulations to define the requirements and technical specifications for an opt-out preference signal sent by a platform, technology, or mechanism, to indicate a consumer's intent to opt out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information. The requirements and specifications for the opt-out preference signal should be updated from time to time to reflect the means by which consumers interact with businesses, and should:

(i) Ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business.

(ii) Ensure that the opt-out preference signal is consumer-friendly, clearly described, and easy to use by an average consumer and does not require that the consumer provide additional information beyond what is necessary.

(iii) Clearly represent a consumer's intent and be free of defaults constraining or presupposing that intent.

(iv) Ensure that the opt-out preference signal does not conflict with other commonly used privacy settings or tools that consumers may employ.

(v) Provide a mechanism for the consumer to selectively consent to a business' sale of the consumer's personal information, or the use or disclosure of the consumer's sensitive personal information, without affecting the consumer's preferences with respect to other businesses or disabling the opt-out preference signal globally.

(vi) State that in the case of a page or setting view that the consumer accesses to set the opt-out preference signal, the consumer should see up to three choices, including:

(I) Global opt out from sale and sharing of personal information, including a direction to limit the use of sensitive personal information.

(II) Choice to "Limit the Use of My Sensitive Personal Information."

(III) Choice titled "Do Not Sell/Do Not Share My Personal Information for Cross-Context Behavioral Advertising."

(B) Issuing regulations to establish technical specifications for an opt-out preference signal that allows the consumer, or the consumer's parent or guardian, to specify that the consumer is less than 13 years of age or at least 13 years of age and less than 16 years of age.

(C) Issuing regulations, with the goal of strengthening consumer privacy while considering the legitimate operational interests of businesses, to govern the use or disclosure of a consumer's sensitive personal information, notwithstanding the consumer's direction to limit the use or disclosure of the consumer's sensitive personal information, including:

(i) Determining any additional purposes for which a business may use or disclose a consumer's sensitive personal information.

(ii) Determining the scope of activities permitted under paragraph (8) of subdivision (e) of Section 1798.140, as authorized by subdivision (a) of Section 1798.121, to ensure that the activities do not involve health-related research.

(iii) Ensuring the functionality of the business' operations.

(iv) Ensuring that the exemption in subdivision (d) of Section 1798.121 for sensitive personal information applies to information that is collected or processed incidentally, or without the purpose of inferring characteristics about a consumer, while ensuring that businesses do not use the exemption for the purpose of evading consumers' rights to limit the use and disclosure of their sensitive personal information under Section 1798.121.

(20) Issuing regulations to govern how a business that has elected to comply with subdivision (b) of Section 1798.135 responds to the opt-out preference signal and provides consumers with the opportunity subsequently to consent to the sale or sharing of their personal information or the use and disclosure of their sensitive personal information for purposes in addition to those authorized by subdivision (a) of Section 1798.121. The regulations should:

(A) Strive to promote competition and consumer choice and be technology neutral.

(B) Ensure that the business does not respond to an opt-out preference signal by:

(i) Intentionally degrading the functionality of the consumer experience.

(ii) Charging the consumer a fee in response to the consumer's opt-out preferences.

(iii) Making any products or services not function properly or fully for the consumer, as compared to consumers who do not use the opt-out preference signal.

(iv) Attempting to coerce the consumer to opt in to the sale or sharing of the consumer's personal information, or the use or disclosure of the consumer's sensitive personal information, by stating or implying that the use of the opt-out preference signal will adversely affect the consumer as compared to consumers who do not use the opt-out preference signal, including stating or implying that the consumer will not be able to use the business' products or services or that those products or services may not function properly or fully.

(v) Displaying any notification or pop-up in response to the consumer's opt-out preference signal.

(C) Ensure that any link to a web page or its supporting content that allows the consumer to consent to opt in:

(i) Is not part of a popup, notice, banner, or other intrusive design that obscures any part of the web page the consumer intended to visit from full view or that interferes with or impedes in any way the consumer's experience visiting or browsing the web page or website the consumer intended to visit.

(ii) Does not require or imply that the consumer must click the link to receive full functionality of any products or services, including the website.

(iii) Does not make use of any dark patterns.

(iv) Applies only to the business with which the consumer intends to interact.

(D) Strive to curb coercive or deceptive practices in response to an opt-out preference signal but should not unduly restrict businesses that are trying in good faith to comply with Section 1798.135.

(21) Review existing Insurance Code provisions and regulations relating to consumer privacy, except those relating to insurance rates or pricing, to determine whether any provisions of the Insurance Code provide greater protection to consumers than the provisions of this title. Upon completing its review, the agency shall adopt a regulation that applies only the more protective provisions of this title to insurance companies. For the purpose of clarity, the Insurance Commissioner shall have jurisdiction over insurance rates and pricing.

(22) Harmonizing the regulations governing opt-out mechanisms, notices to consumers, and other operational mechanisms in this title to promote clarity and the functionality of this title for consumers.

(b) The Attorney General may adopt additional regulations as necessary to further the purposes of this title.

(c) The Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner.

(d) Notwithstanding subdivision (a), the timeline for adopting final regulations required by the act adding this subdivision shall be July 1, 2022. Beginning the later of July 1, 2021, or six months after the agency provides notice to the Attorney General that it is prepared to

begin rulemaking under this title, the authority assigned to the Attorney General to adopt regulations under this section shall be exercised by the California Privacy Protection Agency. Notwithstanding any other law, civil and administrative enforcement of the provisions of law added or amended by this act shall not commence until July 1, 2023, and shall only apply to violations occurring on or after that date. Enforcement of provisions of law contained in the California Consumer Privacy Act of 2018 amended by this act shall remain in effect and shall be enforceable until the same provisions of this act become enforceable.

Cal. Civ. Code § 1798.190. Anti-Avoidance

A court or the agency shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title:

(a) If a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this title, including the disclosure of information by a business to a third party in order to avoid the definition of sell or share.

(b) If steps or transactions were taken to purposely avoid the definition of sell or share by eliminating any monetary or other valuable consideration, including by entering into contracts that do not include an exchange for monetary or other valuable consideration, but where a party is obtaining something of value or use.

Cal. Civ. Code § 1798.192. Waiver

Any provision of a contract or agreement of any kind, including a representative action waiver, that purports to waive or limit in any way rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable. This section shall not prevent a consumer from declining to request information from a business, declining to opt out of a business's sale of the consumer's personal information, or authorizing a business to sell or share the consumer's personal information after previously opting out.

Cal. Civ. Code § 1798.194. [Construction]

This title shall be liberally construed to effectuate its purposes.

Cal. Civ. Code § 1798.196. [Conflicting Federal Laws]

This title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution.

Cal. Civ. Code § 1798.198. [Taking Effect]

(a) Subject to limitation provided in subdivision (b), and in Section 1798.199, this title shall be operative January 1, 2020.

(b) This title shall become operative only if initiative measure No. 17-0039, The Consumer Right to Privacy Act of 2018, is withdrawn from the ballot pursuant to Section 9604 of the Elections Code.

Cal. Civ. Code § 1798.199. [Taking Effect of Section 1798.180]

Notwithstanding Section 1798.198, Section 1798.180 shall be operative on the effective date of the act adding this section.

Cal. Civ. Code § 1798.199.10. [California Privacy Protection Agency]

(a) There is hereby established in state government the California Privacy Protection Agency, which is vested with full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018. The agency shall be governed by a five-member board, including the chairperson. The chairperson and one member of the board shall be appointed by the Governor. The Attorney General, Senate Rules Committee, and Speaker of the Assembly shall each appoint one member. These appointments should be made from among Californians with expertise in the areas of privacy, technology, and consumer rights.

(b) The initial appointments to the agency shall be made within 90 days of the effective date of the act adding this section.

Cal. Civ. Code § 1798.199.15. [Board]

Members of the agency board shall:

(a) Have qualifications, experience, and skills, in particular in the areas of privacy and technology, required to perform the duties of the agency and exercise its powers.

(b) Maintain the confidentiality of information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers, except to the extent that disclosure is required by the Public Records Act.

(c) Remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from another.

(d) Refrain from any action incompatible with their duties and engaging in any incompatible occupation, whether gainful or not, during their term.

(e) Have the right of access to all information made available by the agency to the chairperson.

(f) Be precluded, for a period of one year after leaving office, from accepting employment with a business that was subject to an enforcement action or civil action under this title during the member's tenure or during the five-year period preceding the member's appointment.

(g) Be precluded for a period of two years after leaving office from acting, for compensation, as an agent or attorney for, or otherwise representing, any other person in a matter pending before the agency if the purpose is to influence an action of the agency.

Cal. Civ. Code § 1798.199.20. [Length of Term]

Members of the agency board, including the chairperson, shall serve at the pleasure of their appointing authority but shall serve for no longer than eight consecutive years.

Cal. Civ. Code § 1798.199.25.[Compensation]

For each day on which they engage in official duties, members of the agency board shall be compensated at the rate of one hundred dollars ($100), adjusted biennially to reflect changes in the cost of living, and shall be reimbursed for expenses incurred in performance of their official duties.

Cal. Civ. Code § 1798.199.30. [Employees]

The agency board shall appoint an executive director who shall act in accordance with agency policies and regulations and with applicable law. The agency shall appoint and discharge officers, counsel, and employees, consistent with applicable civil service laws, and shall fix the compensation of employees and prescribe their duties. The agency may contract for services that cannot be provided by its employees.

Cal. Civ. Code § 1798.199.35. [Delegation of Authority]

The agency board may delegate authority to the chairperson or the executive director to act in the name of the agency between meetings of the agency, except with respect to resolution of enforcement actions and rulemaking authority.

Cal. Civ. Code § 1798.199.40. [Functions]

The agency shall perform the following functions:

(a) Administer, implement, and enforce through administrative actions this title.

(b) On and after the later of July 1, 2021, or within six months of the agency providing the Attorney General with notice that it is prepared to assume rulemaking responsibilities under this title, adopt, amend, and rescind regulations pursuant to Section 1798.185 to carry out the purposes and provisions of the California Consumer Privacy Act of 2018, including regulations specifying recordkeeping requirements for businesses to ensure compliance with this title.

(c) Through the implementation of this title, protect the fundamental privacy rights of natural persons with respect to the use of their personal information.

(d) Promote public awareness and understanding of the risks, rules, responsibilities, safeguards, and rights in relation to the collection, use, sale, and disclosure of personal information, including the rights of minors with respect to their own information, and provide a public report summarizing the risk assessments filed with the agency pursuant to paragraph (15) of subdivision (a) of Section 1798.185 while ensuring that data security is not compromised.

(e) Provide guidance to consumers regarding their rights under this title.

(f) Provide guidance to businesses regarding their duties and responsibilities under this title and appoint a Chief Privacy Auditor to conduct audits of businesses to ensure compliance with this title pursuant to regulations adopted pursuant to paragraph (18) of subdivision (a) of Section 1798.185.

(g) Provide technical assistance and advice to the Legislature, upon request, with respect to privacy-related legislation.

(h) Monitor relevant developments relating to the protection of personal information and, in particular, the development of information and communication technologies and commercial practices.

(i) Cooperate with other agencies with jurisdiction over privacy laws and with data processing authorities in California, other states, territories, and countries to ensure consistent application of privacy protections.

(j) Establish a mechanism pursuant to which persons doing business in California that do not meet the definition of business set forth in paragraph (1), (2), or (3) of subdivision (d) of Section 1798.140 may voluntarily certify that they are in compliance with this title, as set forth in paragraph (4) of subdivision (d) of Section 1798.140, and make a list of those entities available to the public.

(k) Solicit, review, and approve applications for grants to the extent funds are available pursuant to paragraph (2) of subdivision (b) of Section 1798.160.

(l) Perform all other acts necessary or appropriate in the exercise of its power, authority, and jurisdiction and seek to balance the goals of strengthening consumer privacy while giving attention to the impact on businesses.

Cal. Civ. Code § 1798.199.45. [Investigations]

(a) Upon the sworn complaint of any person or on its own initiative, the agency may investigate possible violations of this title relating to any business, service provider, contractor, or person. The agency may decide not to investigate a complaint or decide to provide a business with a time period to cure the alleged violation. In making a decision not to investigate or provide more time to cure, the agency may consider the following:

(1) Lack of intent to violate this title.

(2) Voluntary efforts undertaken by the business, service provider, contractor, or person to cure the alleged violation prior to being notified by the agency of the complaint.

(b) The agency shall notify in writing the person who made the complaint of the action, if any, the agency has taken or plans to take on the complaint, together with the reasons for that action or nonaction.

Cal. Civ. Code § 1798.199.50. [Notice to Alleged Violator]

No finding of probable cause to believe this title has been violated shall be made by the agency unless, at least 30 days prior to the agency's consideration of the alleged violation, the business, service provider, contractor, or person alleged to have violated this title is notified of the violation by service of process or registered mail with return receipt requested, provided with a summary of the evidence, and informed of their right to be present in person and represented by counsel at any proceeding of the agency held for the purpose of considering whether probable cause exists for believing the person violated this title. Notice to the alleged violator shall be deemed made on the date of service, the date the registered mail receipt is signed, or if the registered mail receipt is not signed, the date returned by the post office. A proceeding held for the purpose of considering probable cause shall be private unless the alleged violator files with the agency a written request that the proceeding be public.

Cal. Civ. Code § 1798.199.55. [Hearing]

(a) When the agency determines there is probable cause for believing this title has been violated, it shall hold a hearing to determine if a violation has or violations have occurred. Notice shall be given and the hearing conducted in accordance with the Administrative Procedure Act (Chapter 5 (commencing with Section 11500), Part 1, Division 3, Title 2, Government Code). The agency shall have all the powers granted by that chapter. If the agency determines on the basis of the hearing conducted pursuant to this subdivision that a violation or violations have occurred, it shall issue an order that may require the violator to do all or any of the following:

(1) Cease and desist violation of this title.

(2) Subject to Section 1798.155, pay an administrative fine of up to two thousand five hundred dollars ($2,500) for each violation, or up to seven thousand five hundred dollars ($7,500) for each intentional violation and each violation involving the personal information of minor consumers to the Consumer Privacy Fund within the General Fund of the state. When the agency determines that no violation has occurred, it shall publish a declaration so stating.

(b) If two or more persons are responsible for any violation or violations, they shall be jointly and severally liable.

Cal. Civ. Code § 1798.199.60. [Rejection of Decision by Administrative Law Judge]

Whenever the agency rejects the decision of an administrative law judge made pursuant to Section 11517 of the Government Code, the agency shall state the reasons in writing for rejecting the decision.

Cal. Civ. Code § 1798.199.65. [Taking Evidence]

The agency may subpoena witnesses, compel their attendance and testimony, administer oaths and affirmations, take evidence and require by subpoena the production of any books, papers, records, or other items material to the performance of the agency's duties or exercise of its powers, including, but not limited to, its power to audit a business' compliance with this title.

Cal. Civ. Code § 1798.199.70. [Statute of Limitations]

No administrative action brought pursuant to this title alleging a violation of any of the provisions of this title shall be commenced more than five years after the date on which the violation occurred.

(a) The service of the probable cause hearing notice, as required by Section 1798.199.50, upon the person alleged to have violated this title shall constitute the commencement of the administrative action.

(b) If the person alleged to have violated this title engages in the fraudulent concealment of the person's acts or identity, the five-year period shall be tolled for the period of the concealment. For purposes of this subdivision, "fraudulent concealment" means the person knows of material facts related to the person's duties under this title and knowingly conceals them in performing or omitting to perform those duties for the purpose of defrauding the public of information to which it is entitled under this title.

(c) If, upon being ordered by a superior court to produce any documents sought by a subpoena in any administrative proceeding under this title, the person alleged to have violated this title fails to produce documents in response to the order by the date ordered to comply therewith, the five-year period shall be tolled for the period of the delay from the date of filing of the motion to compel until the date the documents are produced.

Cal. Civ. Code § 1798.199.75. [Collection of Fines Through Civil Action]

(a) In addition to any other available remedies, the agency may bring a civil action and obtain a judgment in superior court for the purpose of collecting any unpaid administrative fines imposed pursuant to this title after exhaustion of judicial review of the agency's action. The action may be filed as a small claims, limited civil, or unlimited civil case depending on the jurisdictional amount. The venue for this action shall be in the county where the administrative fines were imposed by the agency. In order to obtain a judgment in a proceeding under this section, the agency shall show, following the procedures and rules of evidence as applied in ordinary civil actions, all of the following:

(1) That the administrative fines were imposed following the procedures set forth in this title and implementing regulations.

(2) That the defendant or defendants in the action were notified, by actual or constructive notice, of the imposition of the administrative fines.

(3) That a demand for payment has been made by the agency and full payment has not been received.

(b) A civil action brought pursuant to subdivision (a) shall be commenced within four years after the date on which the administrative fines were imposed.

Cal. Civ. Code § 1798.199.80. [Collection of Fines]

(a) If the time for judicial review of a final agency order or decision has lapsed, or if all means of judicial review of the order or decision have been exhausted, the agency may apply to the clerk of the court for a judgment to collect the administrative fines imposed by the order or decision, or the order as modified in accordance with a decision on judicial review.

(b) The application, which shall include a certified copy of the order or decision, or the order as modified in accordance with a decision on judicial review, and proof of service of the order or decision, constitutes a sufficient showing to warrant issuance of the judgment to collect the administrative fines. The clerk of the court shall enter the judgment immediately in conformity with the application.

(c) An application made pursuant to this section shall be made to the clerk of the superior court in the county where the administrative fines were imposed by the agency.

(d) A judgment entered in accordance with this section has the same force and effect as, and is subject to all the provisions of law relating to, a judgment in a civil action and may be enforced in the same manner as any other judgment of the court in which it is entered.

(e) The agency may bring an application pursuant to this section only within four years after the date on which all means of judicial review of the order or decision have been exhausted.

(f) The remedy available under this section is in addition to those available under any other law.

Cal. Civ. Code § 1798.199.85. [Judicial Review]

Any decision of the agency with respect to a complaint or administrative fine shall be subject to judicial review in an action brought by an interested party to the complaint or administrative fine and shall be subject to an abuse of discretion standard.

Cal. Civ. Code § 1798.199.90. [Civil Penalties]

(a) Any business, service provider, contractor, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation and each violation involving the personal information of minor consumers, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The court may consider the good faith cooperation of the business, service provider, contractor, or other person in determining the amount of the civil penalty.

(b) Any civil penalty recovered by an action brought by the Attorney General for a violation of this title, and the proceeds of any settlement of any said action, shall be deposited in the Consumer Privacy Fund.

(c) The agency shall, upon request by the Attorney General, stay an administrative action or investigation under this title to permit the Attorney General to proceed with an investigation or civil action and shall not pursue an administrative action or investigation, unless the Attorney General subsequently determines not to pursue an investigation or civil action. The agency may not limit the authority of the Attorney General to enforce this title.

(d) No civil action may be filed by the Attorney General under this section for any violation of this title after the agency has issued a decision pursuant to Section 1798.199.85 or an order pursuant to Section 1798.199.55 against that person for the same violation.

(e) This section shall not affect the private right of action provided for in Section 1798.150.

Cal. Civ. Code § 1798.199.95. [Budget]

(a) There is hereby appropriated from the General Fund of the state to the agency the sum of five million dollars ($5,000,000) during the fiscal year 2020–2021, and the sum of ten million dollars ($10,000,000) adjusted for cost-of-living changes, during each fiscal year thereafter, for expenditure to support the operations of the agency pursuant to this title. The expenditure of funds under this appropriation shall be subject to the normal administrative review given to other state appropriations. The Legislature shall appropriate those additional amounts to the commission and other agencies as may be necessary to carry out the provisions of this title.

(b) The Department of Finance, in preparing the state budget and the Budget Act bill submitted to the Legislature, shall include an item for the support of this title that shall indicate all of the following:

(1) The amounts to be appropriated to other agencies to carry out their duties under this title, which amounts shall be in augmentation of the support items of those agencies.

(2) The additional amounts required to be appropriated by the Legislature to the agency to carry out the purposes of this title, as provided for in this section.

(3) In parentheses, for informational purposes, the continuing appropriation during each fiscal year of ten million dollars ($10,000,000), adjusted for cost-of-living changes made pursuant to this section.

(c) The Attorney General shall provide staff support to the agency until the agency has hired its own staff. The Attorney General shall be reimbursed by the agency for these services.

Cal. Civ. Code § 1798.199.100. [Cooperation of the Violator]

The agency and any court, as applicable, shall consider the good faith cooperation of the business, service provider, contractor, or other person in determining the amount of any administrative fine or civil penalty for a violation of this title. A business shall not be required by the agency, a court, or otherwise to pay both an administrative fine and a civil penalty for the same violation.

Anhang 2: California Consumer Privacy Act Regulations[1]

Article 1. General Provisions

11 C.C.R. § 7000. Title and Scope.

(a) This Chapter shall be known as the California Consumer Privacy Act Regulations. It may be cited as such and will be referred to in this Chapter as "these regulations." These regulations govern compliance with the California Consumer Privacy Act and do not limit any other rights that consumers may have.

(b) A violation of these regulations shall constitute a violation of the CCPA and be subject to the remedies provided for therein.

11 C.C.R. § 7001. Definitions.

In addition to the definitions set forth in Civil Code section 1798.140, for purposes of these regulations:

(a) "Affirmative authorization" means an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information. Within the context of a parent or guardian acting on behalf of a consumer under 13 years of age, it means that the parent or guardian has provided consent to the sale of the consumer's personal information in accordance with the methods set forth in section 7070. For consumers 13 years of age and older, it is demonstrated through a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.

(b) "Attorney General" means the California Attorney General or any officer or employee of the California Department of Justice acting under the authority of the California Attorney General.

(c) "Authorized agent" means a natural person or a business entity registered with the Secretary of State to conduct business in California that a consumer has authorized to act on their behalf subject to the requirements set forth in section 7063.

(d) "Categories of sources" means types or groupings of persons or entities from which a business collects personal information about consumers, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity. They may include the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

(e) "Categories of third parties" means types or groupings of third parties with whom the business shares personal information, described with enough particularity to provide consumers

[1] Aktuelle Fassung im Juli 2022 aufgrund der letzten Änderung zum 05.05.2022.

with a meaningful understanding of the type of third party. They may include advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

(f) "CCPA" means the California Consumer Privacy Act of 2018, Civil Code sections 1798.100 et seq.

(g) "COPPA" means the Children's Online Privacy Protection Act, 15 U. S.C. sections 6501 to 6508 and 16 Code of Federal Regulations part 312.5.

(h) "Employment benefits" means retirement, health, and other benefit programs, services, or products to which consumers and their dependents or their beneficiaries receive access through the consumer's employer.

(i) "Employment-related information" means personal information that is collected by the business about a natural person for the reasons identified in Civil Code section 1798.145, subdivision (h)(1). The collection of employment-related information, including for the purpose of administering employment benefits, shall be considered a business purpose.

(j) "Financial incentive" means a program, benefit, or other offering, including payments to consumers, related to the collection, deletion, or sale of personal information.

(k) "Household" means a person or group of people who: (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier.

(l) "Notice at collection" means the notice given by a business to a consumer at or before the point at which a business collects personal information from the consumer as required by Civil Code section 1798.100, subdivision (b), and specified in these regulations.

(m) "Notice of right to opt-out" means the notice given by a business informing consumers of their right to opt-out of the sale of their personal information as required by Civil Code sections 1798.120 and 1798.135 and specified in these regulations.

(n) "Notice of financial incentive" means the notice given by a business explaining each financial incentive or price or service difference as required by Civil Code section 1798.125, subdivision (b), and specified in these regulations.

(o) "Price or service difference" means (1) any difference in the price or rate charged for any goods or services to any consumer related to the collection, retention, or sale of personal information, including through the use of discounts, financial payments, or other benefits or penalties; or (2) any difference in the level or quality of any goods or services offered to any consumer related to the collection, retention, or sale of personal information, including the denial of goods or services to the consumer.

(p) "Privacy policy," as referred to in Civil Code section 1798.130, subdivision (a)(5), means the statement that a business shall make available to consumers describing the business's practices, both online and offline, regarding the collection, use, disclosure, and sale of personal information, and of the rights of consumers regarding their own personal information.

(q) "Request to delete" means a consumer request that a business delete personal information about the consumer that the business has collected from the consumer, pursuant to Civil Code section 1798.105.

(r) "Request to know" means a consumer request that a business disclose personal information that it has collected about the consumer pursuant to Civil Code sections 1798.100, 1798.110, or 1798.115. It includes a request for any or all of the following:

(1) Specific pieces of personal information that a business has collected about the consumer;

(2) Categories of personal information it has collected about the consumer;

(3) Categories of sources from which the personal information is collected;

(4) Categories of personal information that the business sold or disclosed for a business purpose about the consumer;

(5) Categories of third parties to whom the personal information was sold or disclosed for a business purpose; and

(6) The business or commercial purpose for collecting or selling personal information.

(s) "Request to opt-in" means the affirmative authorization that the business may sell personal information about the consumer by a parent or guardian of a consumer less than 13 years of age, by a consumer at least 13 and less than 16 years of age, or by a consumer who had previously opted out of the sale of their personal information.

(t) "Request to opt-out" means a consumer request that a business not sell the consumer's personal information to third parties, pursuant to Civil Code section 1798.120, subdivision (a).

(u) "Signed" means that the written attestation, declaration, or permission has either been physically signed or provided electronically in accordance with the Uniform Electronic Transactions Act, Civil Code section 1633.1 et seq.

(v) "Third-party identity verification service" means a security process offered by an independent third party that verifies the identity of the consumer making a request to the business. Third-party identity verification services are subject to the requirements set forth in Article 4 regarding requests to know and requests to delete.

(w) "Value of the consumer's data" means the value provided to the business by the consumer's data as calculated under section 7081.

(x) "Verify" means to determine that the consumer making a request to know or request to delete is the consumer about whom the business has collected information, or if that consumer is less than 13 years of age, the consumer's parent or legal guardian.

Article 2. Notices to Consumers

11 C.C.R. § 7010. Overview of Required Notices.

(a) Every business that must comply with the CCPA and these regulations shall provide a privacy policy in accordance with the CCPA and section 7011.

(b) A business that collects personal information from a consumer shall provide a notice at collection in accordance with the CCPA and section 7012.

(c) A business that sells personal information shall provide a notice of right to opt-out in accordance with the CCPA and section 7013.

(d) A business that offers a financial incentive or price or service difference shall provide a notice of financial incentive in accordance with the CCPA and section 7016.

11 C.C.R. § 7011. Privacy Policy.

(a) Purpose and General Principles

(1) The purpose of the privacy policy is to provide consumers with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their personal information.

(2) The privacy policy shall be designed and presented in a way that is easy to read and understandable to consumers. The policy shall:

(A) Use plain, straightforward language and avoid technical or legal jargon.

(B) Use a format that makes the policy readable, including on smaller screens, if applicable.

(C) Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.

(D) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium,

incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the policy in an alternative format.

(E) Be available in a format that allows a consumer to print it out as a document.

(b) The privacy policy shall be posted online through a conspicuous link using the word "privacy" on the business's website homepage or on the download or landing page of a mobile application. If the business has a California-specific description of consumers' privacy rights on its website, then the privacy policy shall be included in that description. A business that does not operate a website shall make the privacy policy conspicuously available to consumers. A mobile application may include a link to the privacy policy in the application's settings menu.

(c) The privacy policy shall include the following information:

(1) Right to Know About Personal Information Collected, Disclosed, or Sold.

(A) Explanation that a consumer has the right to request that the business disclose what personal information it collects, uses, discloses, and sells.

(B) Instructions for submitting a verifiable consumer request to know and links to an online request form or portal for making the request, if offered by the business.

(C) General description of the process the business will use to verify the consumer request, including any information the consumer must provide.

(D) Identification of the categories of personal information the business has collected about consumers in the preceding 12 months. The categories shall be described in a manner that provides consumers a meaningful understanding of the information being collected.

(E) Identification of the categories of sources from which the personal information is collected.

(F) Identification of the business or commercial purpose for collecting or selling personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is collected or sold.

(G) Disclosure or Sale of Personal Information.

1. Identification of the categories of personal information, if any, that the business has disclosed for a business purpose or sold to third parties in the preceding 12 months.

2. For each category of personal information identified, the categories of third parties to whom the information was disclosed or sold.

3. Statement regarding whether the business has actual knowledge that it sells the personal information of consumers under 16 years of age.

(2) Right to Request Deletion of Personal Information.

(A) Explanation that the consumer has a right to request the deletion of their personal information collected by the business.

(B) Instructions for submitting a verifiable consumer request to delete and links to an online request form or portal for making the request, if offered by the business.

(C) General description of the process the business will use to verify the consumer request, including any information the consumer must provide.

(3) Right to Opt-Out of the Sale of Personal Information.

(A) Explanation that the consumer has a right to opt-out of the sale of their personal information by a business.

(B) Statement regarding whether or not the business sells personal information. If the business sells personal information, include either the contents of the notice of right to opt-out or a link to it in accordance with section 7013.

(4) Right to Non-Discrimination for the Exercise of a Consumer's Privacy Rights.

(A) Explanation that the consumer has a right not to receive discriminatory treatment by the business for the exercise of the privacy rights conferred by the CCPA.

(5) Authorized Agent.

(A) Instructions on how an authorized agent can make a request under the CCPA on the consumer's behalf.

(6) Contact for More Information.

(A) A contact for questions or concerns about the business's privacy policies and practices using a method reflecting the manner in which the business primarily interacts with the consumer.

(7) Date the privacy policy was last updated.

(8) If subject to the requirements set forth in section 7102, subsection (a), the information compiled in section 7023, subsection (a)(1), or a link to it.

(9) If the business has actual knowledge that it sells the personal information of consumers under 16 years of age, a description of the processes required by sections 7070 and 7071.

11 C.C.R. § 7012. Notice at Collection of Personal Information.

(a) Purpose and General Principles

(1) The purpose of the notice at collection is to provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them and the purposes for which the personal information will be used.

(2) The notice at collection shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:

(A) Use plain, straightforward language and avoid technical or legal jargon.

(B) Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.

(C) Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.

(D) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.

(3) The notice at collection shall be made readily available where consumers will encounter it at or before the point of collection of any personal information. Illustrative examples follow:

(A) When a business collects consumers' personal information online, it may post a conspicuous link to the notice on the introductory page of the business's website and on all webpages where personal information is collected.

(B) When a business collects personal information through a mobile application, it may provide a link to the notice on the mobile application's download page and within the application, such as through the application's settings menu.

(C) When a business collects consumers' personal information offline, it may include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online.

(D) When a business collects personal information over the telephone or in person, it may provide the notice orally.

(4) When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it shall provide a just-in-time notice containing a summary of the categories of personal information being collected and a link to the full notice at collection. For example, if the business offers a flashlight application and the application collects geolocation information, the business shall provide a just-in-time

notice, such as through a popststate-up window when the consumer opens the application, that contains the information required by this subsection.

(5) A business shall not collect categories of personal information other than those disclosed in the notice at collection. If the business intends to collect additional categories of personal information, the business shall provide a new notice at collection.

(6) If a business does not give the notice at collection to the consumer at or before the point of collection of their personal information, the business shall not collect personal information from the consumer.

(b) A business shall include the following in its notice at collection:

(1) A list of the categories of personal information about consumers to be collected. Each category of personal information shall be written in a manner that provides consumers a meaningful understanding of the information being collected.

(2) The business or commercial purpose(s) for which the categories of personal information will be used.

(3) If the business sells personal information, the link titled "Do Not Sell My Personal Information" required by section 7026, subsection (a), or in the case of offline notices, where the webpage can be found online.

(4) A link to the business's privacy policy, or in the case of offline notices, where the privacy policy can be found online.

(c) If a business collects personal information from a consumer online, the notice at collection may be given to the consumer by providing a link to the section of the business's privacy policy that contains the information required in subsection (b).

(d) A business that does not collect personal information directly from the consumer does not need to provide a notice at collection to the consumer if it does not sell the consumer's personal information.

(e) A data broker registered with the Attorney General pursuant to Civil Code section 1798.99.80 et seq. does not need to provide a notice at collection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out.

(f) A business collecting employment-related information shall comply with the provisions of section 7012 except with regard to the following:

(1) The notice at collection of employment-related information does not need to include the link or web address to the link titled "Do Not Sell My Personal Information".

(2) The notice at collection of employment-related information is not required to provide a link to the business's privacy policy.

(g) Subsection (f) shall become inoperative on January 1, 2021, unless the CCPA is amended otherwise.

11 C.C.R. § 7013. Notice of Right to Opt-Out of Sale of Personal Information.

(a) Purpose and General Principles

(1) The purpose of the notice of right to opt-out is to inform consumers of their right to direct a business that sells their personal information to stop selling their personal information.

(2) The notice of right to opt-out shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:

(A) Use plain, straightforward language and avoid technical or legal jargon.

(B) Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.

(C) Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.

(D) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.

(b) A business that sells the personal information of consumers shall provide the notice of right to opt-out to consumers as follows:

(1) A business shall post the notice of right to opt-out on the Internet webpage to which the consumer is directed after clicking on the "Do Not Sell My Personal Information" link on the website homepage or the download or landing page of a mobile application. In addition, a business that collects personal information through a mobile application may provide a link to the notice within the application, such as through the application's settings menu. The notice shall include the information specified in subsection (c) or link to the section of the business's privacy policy that contains the same information.

(2) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to opt-out. That method shall comply with the requirements set forth in subsection (a)(2).

(3) A business that sells personal information that it collects in the course of interacting with consumers offline shall also inform consumers by an offline method of their right to opt-out and provide instructions on how to submit a request to opt-out. Illustrative examples follow:

(A) A business that sells personal information that it collects from consumers in a brick-and-mortar store may inform consumers of their right to opt-out on the paper forms that collect the personal information or by posting signage in the area where the personal information is collected directing consumers to where the opt-out information can be found online.

(B) A business that sells personal information that it collects over the phone may inform consumers of their right to opt-out orally during the call when the information is collected.

(c) A business shall include the following in its notice of right to opt-out:

(1) A description of the consumer's right to opt-out of the sale of their personal information by the business;

(2) The interactive form by which the consumer can submit their request to opt-out online, as required by section 7026, subsection (a), or if the business does not operate a website, the offline method by which the consumer can submit their request to opt-out; and

(3) Instructions for any other method by which the consumer may submit their request to opt-out.

(d) A business does not need to provide a notice of right to opt-out if:

(1) It does not sell personal information; and

(2) It states in its privacy policy that it does not sell personal information.

(e) A business shall not sell the personal information it collected during the time the business did not have a notice of right to opt-out posted unless it obtains the affirmative authorization of the consumer.

(f) Opt-Out Icon.

(1) The following opt-out icon may be used in addition to posting the notice of right to opt-out, but not in lieu of any requirement to post the notice of right to opt-out or a "Do Not Sell My Personal Information" link as required by Civil Code section 1798.135 and these regulations.

(2) The icon shall be approximately the same size as any other icons used by the business on its webpage.

11 C.C.R. § 7016. Notice of Financial Incentive.

(a) Purpose and General Principles

(1) The purpose of the notice of financial incentive is to explain to the consumer the material terms of a financial incentive or price or service difference the business is offering so that the consumer may make an informed decision about whether to participate. A business that does not offer a financial incentive or price or service difference is not required to provide a notice of financial incentive.

(2) The notice of financial incentive shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:

(A) Use plain, straightforward language and avoid technical or legal jargon.

(B) Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.

(C) Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.

(D) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.

(E) Be readily available where consumers will encounter it before opting-in to the financial incentive or price or service difference.

(3) If the business offers the financial incentive or price or service difference online, the notice may be given by providing a link to the section of a business's privacy policy that contains the information required in subsection (b).

(b) A business shall include the following in its notice of financial incentive:

(1) A succinct summary of the financial incentive or price or service difference offered;

(2) A description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference and the value of the consumer's data;

(3) How the consumer can opt-in to the financial incentive or price or service difference;

(4) A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and

(5) An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including:

(A) A good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and

(B) A description of the method the business used to calculate the value of the consumer's data.

Article 3. Business Practices for Handling Consumer Requests

11 C.C.R. § 7020. Methods for Submitting Requests to Know and Requests to Delete.

(a) A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address

for submitting requests to know. All other businesses shall provide two or more designated methods for submitting requests to know, including, at a minimum, a toll-free telephone number. Other acceptable methods for submitting these requests include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail.

(b) A business shall provide two or more designated methods for submitting requests to delete. Acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a link or form available online through a business's website, a designated email address, a form submitted in person, and a form submitted through the mail.

(c) A business shall consider the methods by which it primarily interacts with consumers when determining which methods to provide for submitting requests to know and requests to delete. If the business interacts with consumers in person, the business shall consider providing an in-person method such as a printed form the consumer can directly submit or send by mail, a tablet or computer portal that allows the consumer to complete and submit an online form, or a telephone with which the consumer can call the business's toll-free number.

(d) A business may use a two-step process for online requests to delete where the consumer must first, submit the request to delete and then second, separately confirm that they want their personal information deleted.

(e) If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, the business shall either:

(1) Treat the request as if it had been submitted in accordance with the business's designated manner, or

(2) Provide the consumer with information on how to submit the request or remedy any deficiencies with the request, if applicable.

11 C.C.R. § 7021. Timelines for Responding to Requests to Know and Requests to Delete.

(a) Upon receiving a request to know or a request to delete, a business shall confirm receipt of the request within 10 business days and provide information about how the business will process the request. The information provided shall describe in general the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request. The confirmation may be given in the same manner in which the request was received. For example, if the request is made over the phone, the confirmation may be given orally during the phone call.

(b) Businesses shall respond to requests to know and requests to delete within 45 calendar days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request. If the business cannot verify the consumer within the 45-day time period, the business may deny the request. If necessary, businesses may take up to an additional 45 calendar days to respond to the consumer's request, for a maximum total of 90 calendar days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.

11 C.C.R. § 7022. Requests to Delete.

(a) For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 5, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified.

(b) A business shall comply with a consumer's request to delete their personal information by:

(1) Permanently and completely erasing the personal information on its existing systems with the exception of archived or back-up systems;

(2) Deidentifying the personal information; or

(3) Aggregating the consumer information.

(c) If a business stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or next accessed or used for a sale, disclosure, or commercial purpose.

(d) In responding to a request to delete, a business shall inform the consumer whether or not it has complied with the consumer's request.

(e) If the business complies with the consumer's request, the business shall inform the consumer that it will maintain a record of the request as required by section 7030, subsection (b). A business may retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from the business's records.

(f) In cases where a business denies a consumer's request to delete, the business shall do all of the following:

(1) Inform the consumer that it will not comply with the consumer's request and describe the basis for the denial, including any conflict with federal or state law, or exception to the CCPA, unless prohibited from doing so by law;

(2) Delete the consumer's personal information that is not subject to the exception; and

(3) Not use the consumer's personal information retained for any other purpose than provided for by that exception.

(g) If a business that denies a consumer's request to delete sells personal information and the consumer has not already made a request to opt-out, the business shall ask the consumer if they would like to opt-out of the sale of their personal information and shall include either the contents of, or a link to, the notice of right to opt-out in accordance with section 7013.

(h) In responding to a request to delete, a business may present the consumer with the choice to delete select portions of their personal information only if a global option to delete all personal information is also offered and more prominently presented than the other choices.

11 C.C.R. § 7024 Requests to Know.

(a) For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 45, the business shall not disclose any specific pieces of personal information to the requestor and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall also evaluate the consumer's request as if it is seeking the disclosure of categories of personal information about the consumer pursuant to subsection (b).

(b) For requests that seek the disclosure of categories of personal information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 45, the business may deny the request to disclose the categories and other information requested and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall provide or direct the consumer to its general business practices regarding the collection, maintenance, and sale of personal information set forth in its privacy policy.

(c) In responding to a request to know, a business is not required to search for personal information if all of the following conditions are met:

(1) The business does not maintain the personal information in a searchable or reasonably accessible format;

(2) The business maintains the personal information solely for legal or compliance purposes;

(3) The business does not sell the personal information and does not use it for any commercial purpose; and

(4) The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.

(d) A business shall not disclose in response to a request to know a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics. The business shall, however, inform the consumer with sufficient particularity that it has collected the type of information. For example, a business shall respond that it collects "unique biometric data including a fingerprint scan" without disclosing the actual fingerprint scan data.

(e) If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business shall inform the requestor and explain the basis for the denial, unless prohibited from doing so by law. If the request is denied only in part, the business shall disclose the other information sought by the consumer.

(f) A business shall use reasonable security measures when transmitting personal information to the consumer.

(g) If a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 45.

(h) Unless otherwise specified by the business to cover a longer period of time, the 12-month period covered by a consumer's verifiable request to know referenced in Civil Code section 1798.130, subdivision (a)(2), shall run from the date the business receives the request, regardless of the time required to verify the request.

(i) In responding to a consumer's verified request to know categories of personal information, categories of sources, and/or categories of third parties, a business shall provide an individualized response to the consumer as required by the CCPA. It shall not refer the consumer to the businesses' general practices outlined in its privacy policy unless its response would be the same for all consumers and the privacy policy discloses all the information that is otherwise required to be in a response to a request to know such categories.

(j) In responding to a verified request to know categories of personal information, the business shall provide:

(1) The categories of personal information the business has collected about the consumer in the preceding 12 months;

(2) The categories of sources from which the personal information was collected;

(3) The business or commercial purpose for which it collected or sold the personal information;

(4) The categories of third parties with whom the business shares personal information;

(5) The categories of personal information that the business sold in the preceding 12 months, and for each category identified, the categories of third parties to whom it sold that particular category of personal information; and

(6) The categories of personal information that the business disclosed for a business purpose in the preceding 12 months, and for each category identified, the categories of third parties to whom it disclosed that particular category of personal information.

(k) A business shall identify the categories of personal information, categories of sources of personal information, and categories of third parties to whom a business sold or disclosed personal information, in a manner that provides consumers a meaningful understanding of the categories listed.

11 C.C.R. § 7026. Requests to Opt-Out.

(a) A business shall provide two or more designated methods for submitting requests to opt-out, including an interactive form accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information," on the business's website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information.

(b) A business shall consider the methods by which it interacts with consumers, the manner in which the business sells personal information to third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer.

(c) If a business collects personal information from consumers online, the business shall treat user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer.

(1) Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to opt-out of the sale of personal information.

(2) If a global privacy control conflicts with a consumer's existing business-specific privacy setting or their participation in a business's financial incentive program, the business shall respect the global privacy control but may notify the consumer of the conflict and give the consumer the choice to confirm the business-specific privacy setting or participation in the financial incentive program.

(d) In responding to a request to opt-out, a business may present the consumer with the choice to opt-out of sale for certain uses of personal information as long as a global option to opt-out of the sale of all personal information is more prominently presented than the other choices.

(e) A business shall comply with a request to opt-out as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. If a business sells a consumer's personal information to any third parties after the consumer submits their request but before the business complies with that request, it shall notify those third parties that the consumer has exercised their right to opt-out and shall direct those third parties not to sell that consumer's information.

(f) A consumer may use an authorized agent to submit a request to opt-out on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer.

A business may deny a request from an authorized agent if the agent cannot provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf. User-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information shall be considered a request directly from the consumer, not through an authorized agent.

(g) A request to opt-out need not be a verifiable consumer request. If a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent.

(h) A business's methods for submitting request to opt-out shall be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out. A business shall not use a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out. Illustrative examples follow:

(1) The business's process for submitting a request to opt-out shall not require more steps than that business's process for a consumer to opt-in to the sale of personal information after having previously opted out. The number of steps for submitting a request to opt-out is measured from when the consumer clicks on the "Do Not Sell My Personal Information" link to completion of the request. The number of steps for submitting a request to opt-in to the sale of personal information is measured from the first indication by the consumer to the business of their interest to opt-out in completion of the request.

(2) A business shall not use confusing language, such as double-negatives (e.g., "Don't Not Sell My Personal Information"), when providing consumers the choice to opt-out.

(3) Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request.

(4) The business's process for submitting a request to opt-out shall not require the consumer to provide personal information that is not necessary to implement the request.

(5) Upon clicking the "Do Not Sell My Personal Information" link, the business shall not require the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out.

11 C.C.R. § 7028. Requests to Opt-In After Opting-Out of the Sale of Personal Information.

(a) Requests to opt-in to the sale of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.

(b) If a consumer who has opted-out of the sale of their personal information initiates a transaction or attempts to use a product or service that requires the sale of their personal information, a business may inform the consumer that the transaction, product, or service requires the sale of their personal information and provide instructions on how the consumer can opt-in.

11 C.C.R. § 7031. Requests to Know or Delete Household Information.

(a) Where a household does not have a password-protected account with a business, a business shall not comply with a request to know specific pieces of personal information about the household or a request to delete household personal information unless all of the following conditions are satisfied:

(1) All consumers of the household jointly request to know specific pieces of information for the household or the deletion of household personal information;

(2) The business individually verifies all the members of the household subject to the verification requirements set forth in section 7062; and

(3) The business verifies that each member making the request is currently a member of the household.

(b) Where a consumer has a password-protected account with a business that collects personal information about a household, the business may process requests to know and requests to delete relating to household information through the business's existing business practices and in compliance with these regulations.

(c) If a member of a household is a consumer under the age of 13, a business must obtain verifiable parental consent before complying with a request to know specific pieces of information for the household or the deletion of household personal information pursuant to the parental consent provisions in section 7070.

Article 4. Service Providers

11 C.C.R. § 7051. Service Providers.

(a) A business that provides services to a person or organization that is not a business, and that would otherwise meet the requirements and obligations of a "service provider" under the CCPA and these regulations, shall be deemed a service provider for purposes of the CCPA and these regulations.

(b) To the extent that a business directs a second entity to collect personal information directly from a consumer, or about a consumer, on the first business's behalf, and the second entity would otherwise meet the requirements and obligations of a "service provider" under the CCPA and these regulations, the second entity shall be deemed a service provider of the first business for purposes of the CCPA and these regulations.

(c) A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except:

(1) To process or maintain personal information on behalf of the business that provided the personal information or directed the service provider to collect the personal information, and in compliance with the written contract for services required by the CCPA;

(2) To retain and employ another service provider as a subcontractor, where the subcontractor meets the requirements for a service provider under the CCPA and these regulations;

(3) For internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles to use in providing services to another business, or correcting or augmenting data acquired from another source;

(4) To detect data security incidents or protect against fraudulent or illegal activity; or

(5) For the purposes enumerated in Civil Code section 1798.145, subdivisions (a)(1) through (a)(4).

(d) A service provider shall not sell data on behalf of a business when a consumer has opted-out of the sale of their personal information with the business.

(e) If a service provider receives a request to know or a request to delete from a consumer, the service provider shall either act on behalf of the business in responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider.

(f) A service provider that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider.

Article 5. Verification of Requests

11 C.C.R. § 7060. General Rules Regarding Verification.

(a) A business shall establish, document, and comply with a reasonable method for verifying that the person making a request to know or a request to delete is the consumer about whom the business has collected information.

(b) In determining the method by which the business will verify the consumer's identity, the business shall:

(1) Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service that complies with this section.

(2) Avoid collecting the types of personal information identified in Civil Code section 1798.81.5, subdivision (d), unless necessary for the purpose of verifying the consumer.

(3) Consider the following factors:

(A) The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive or valuable personal information shall warrant a more stringent verification process. The types of personal information identified in Civil Code section 1798.81.5, subdivision (d), shall be considered presumptively sensitive;

(B) The risk of harm to the consumer posed by any unauthorized access or deletion. A greater risk of harm to the consumer by unauthorized access or deletion shall warrant a more stringent verification process;

(C) The likelihood that fraudulent or malicious actors would seek the personal information. The higher the likelihood, the more stringent the verification process shall be;

(D) Whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated;

(E) The manner in which the business interacts with the consumer; and

(F) Available technology for verification.

(c) A business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, security, or fraud-prevention. The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with section 7101.

(d) A business shall not require the consumer or the consumer's authorized agent to pay a fee for the verification of their request to know or request to delete. For example, a business may not require a consumer to provide a notarized affidavit to verify their identity unless the business compensates the consumer for the cost of notarization.

(e) A business shall implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer's personal information.

(f) If a business maintains consumer information that is deidentified, a business is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request.

11 C.C.R. § 7061. Verification for Password-Protected Accounts.

(a) If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in section 7060. The business shall also require a consumer to re-authenticate themself before disclosing or deleting the consumer's data.

(b) If a business suspects fraudulent or malicious activity on or from the password-protected account, the business shall not comply with a consumer's request to know or request to delete until further verification procedures determine that the consumer request is authentic and the consumer making the request is the person about whom the business has collected information. The business may use the procedures set forth in section 7062 to further verify the identity of the consumer.

11 C.C.R. § 7062. Verification for Non-Accountholders.

(a) If a consumer does not have or cannot access a password-protected account with a business, the business shall comply with this section, in addition to section 7060.

(b) A business's compliance with a request to know categories of personal information requires that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may include matching at least two data points provided by the consumer with data points maintained by the business that it has determined to be reliable for the purpose of verifying the consumer.

(c) A business's compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. If a business uses this method for verification, the business shall maintain all signed declarations as part of its record-keeping obligations.

(d) A business's compliance with a request to delete may require that the business verify the identity of the consumer to a reasonable or reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion. For example, the deletion of family photographs may require a reasonably high degree of certainty, while the deletion of browsing history may require only a reasonable degree of certainty. A business shall act in good faith when determining the appropriate standard to apply when verifying the consumer in accordance with these regulations.

(e) Illustrative examples follow:

(1) Example 1: If a business maintains personal information in a manner associated with a named actual person, the business may verify the consumer by requiring the consumer to provide evidence that matches the personal information maintained by the business. For example, if a retailer maintains a record of purchases made by a consumer, the business may require the consumer to identify items that they recently purchased from the store or the dollar amount of their most recent purchase to verify their identity to a reasonable degree of certainty.

(2) Example 2: If a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the personal information. For example, a business may have a mobile application that collects personal information about

the consumer but does not require an account. The business may determine whether, based on the facts and considering the factors set forth in section 7060, subsection (b)(3), it may reasonably verify a consumer by asking them to provide information that only the person who used the mobile application may know or by requiring the consumer to respond to a notification sent to their device.

(f) A business shall deny a request to know specific pieces of personal information if it cannot verify the identity of the requestor pursuant to these regulations.

(g) If there is no reasonable method by which a business can verify the identity of the consumer to the degree of certainty required by this section, the business shall state so in response to any request and explain why it has no reasonable method by which it can verify the identity of the requestor. If the business has no reasonable method by which it can verify any consumer, the business shall explain why it has no reasonable verification method in its privacy policy. The business shall evaluate and document whether a reasonable method can be established at least once every 12 months, in connection with the requirement to update the privacy policy set forth in Civil Code section 1798.130, subdivision (a)(5).

11 C.C.R. § 7063. Authorized Agent.

(a) When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. The business may also require the consumer to do either of the following:

(1) Verify their own identity directly with the business.

(2) Directly confirm with the business that they provided the authorized agent permission to submit the request.

(b) Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4121 to 4130.

(c) An authorized agent shall implement and maintain reasonable security procedures and practices to protect the consumer's information.

(d) An authorized agent shall not use a consumer's personal information, or any information collected from or about the consumer, for any purposes other than to fulfill the consumer's requests, verification, or fraud prevention.

Article 6. Special Rules Regarding Consumers Under 16 Years of Age

11 C.C.R. § 7070. Consumers Under 13 Years of Age.

(a) Process for Opting-In to Sale of Personal Information

(1) A business that has actual knowledge that it sells the personal information of a consumer under the age of 13 shall establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. This affirmative authorization is in addition to any verifiable parental consent required under COPPA.

(2) Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include, but are not limited to:

(A) Providing a consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan;

(B) Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

(C) Having a parent or guardian call a toll-free telephone number staffed by trained personnel;

(D) Having a parent or guardian connect to trained personnel via video-conference;

(E) Having a parent or guardian communicate in person with trained personnel; and

(F) Verifying a parent or guardian's identity by checking a form of government-issued identification against databases of such information, as long as the parent or guardian's identification is deleted by the business from its records promptly after such verification is complete.

(b) When a business receives an affirmative authorization pursuant to subsection (a), the business shall inform the parent or guardian of the right to opt-out and of the process for doing so on behalf of their child pursuant to section 7026, subsections (a)-(f).

(c) A business shall establish, document, and comply with a reasonable method, in accordance with the methods set forth in subsection (a)(2), for determining that a person submitting a request to know or a request to delete the personal information of a child under the age of 13 is the parent or guardian of that child.

11 C.C.R. § 7071. Consumers 13 to 15 Years of Age.

(a) A business that has actual knowledge that it sells the personal information of consumers at least 13 years of age and less than 16 years of age shall establish, document, and comply with a reasonable process for allowing such consumers to opt-in to the sale of their personal information, pursuant to section 7028.

(b) When a business receives a request to opt-in to the sale of personal information from a consumer at least 13 years of age and less than 16 years of age, the business shall inform the consumer of the right to opt-out at a later date and of the process for doing so pursuant to section 7026.

11 C.C.R. § 7072. Notices to Consumers Under 16 Years of Age.

(a) A business subject to sections 7070 and/or 7071 shall include a description of the processes set forth in those sections in its privacy policy.

(b) A business that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell the personal information without the affirmative authorization of consumers at least 13 years of age and less than 16 years of age, or the affirmative authorization of their parent or guardian for consumers under 13 years of age, is not required to provide the notice of right to opt-out.

Article 7. Non-Discrimination

11 C.C.R. § 7080. Discriminatory Practices.

(a) A financial incentive or a price or service difference is discriminatory, and therefore prohibited by Civil Code section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or these regulations.

(b) A business may offer a financial incentive or price or service difference if it is reasonably related to the value of the consumer's data. If a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the financial incentive or price or service difference.

(c) A business's denial of a consumer's request to know, request to delete, or request to opt-out for reasons permitted by the CCPA or these regulations shall not be considered discriminatory.

(d) Illustrative examples follow:

(1) Example 1: A music streaming business offers a free service as well as a premium service that costs $5 per month. If only the consumers who pay for the music streaming service are allowed to opt-out of the sale of their personal information, then the practice is discriminatory, unless the $5-per-month payment is reasonably related to the value of the consumer's data to the business.

(2) Example 2: A clothing business offers a loyalty program whereby customers receive a $5-off coupon by email after spending $100 with the business. A consumer submits a request to delete all personal information the business has collected about them but also informs the business that they want to continue to participate in the loyalty program. The business may deny their request to delete with regard to their email address and the amount the consumer has spent with the business because that information is necessary for the business to provide the loyalty program requested by the consumer and is reasonably anticipated within the context of the business's ongoing relationship with them pursuant to Civil Code section 1798.105, subdivision (d)(1).

(3) Example 3: A grocery store offers a loyalty program whereby consumers receive coupons and special discounts when they provide their phone numbers. A consumer submits a request to opt-out of the sale of their personal information. The retailer complies with their request but no longer allows the consumer to participate in the loyalty program. This practice is discriminatory unless the grocery store can demonstrate that the value of the coupons and special discounts are reasonably related to the value of the consumer's data to the business.

(4) Example 4: An online bookseller collects information about consumers, including their email addresses. It offers coupons to consumers through browser pop-up windows while the consumer uses the bookseller's website. A consumer submits a request to delete all personal information that the bookseller has collected about them, including their email address and their browsing and purchasing history. The bookseller complies with the request but stops providing the periodic coupons to the consumer. The bookseller's failure to provide coupons is discriminatory unless the value of the coupons is reasonably related to the value provided to the business by the consumer's data. The bookseller may not deny the consumer's request to delete with regard to the email address because the email address is not necessary to provide the coupons or reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

(e) A business shall notify consumers of any financial incentive or price or service difference subject to Civil Code section 1798.125 that it offers in accordance with section 7016.

(f) A business's charging of a reasonable fee pursuant to Civil Code section 1798.145, subdivision (i)(3), shall not be considered a financial incentive subject to these regulations.

(g) A price or service difference that is the direct result of compliance with a state or federal law shall not be considered discriminatory.

11 C.C.R. § 7081. Calculating the Value of Consumer Data

(a) A business offering a financial incentive or price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer's data. The business shall consider one or more of the following:

(1) The marginal value to the business of the sale, collection, or deletion of a consumer's data.

(2) The average value to the business of the sale, collection, or deletion of a consumer's data.

(3) The aggregate value to the business of the sale, collection, or deletion of consumers' data divided by the total number of consumers.

(4) Revenue generated by the business from sale, collection, or retention of consumers' personal information.

(5) Expenses related to the sale, collection, or retention of consumers' personal information.

(6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference.

(7) Profit generated by the business from sale, collection, or retention of consumers' personal information.

(8) Any other practical and reasonably reliable method of calculation used in good faith.

(b) For the purpose of calculating the value of consumer data, a business may consider the value to the business of the data of all natural persons in the United States and not just consumers.

Article 8. Training, Record-Keeping

11 C.C.R. § 7100. Training.

(a) All individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA shall be informed of all of the requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations.

(b) A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall-establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests made under the CCPA or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA.

11 C.C.R. § 7101. Record-Keeping.

(a) A business shall maintain records of consumer requests made pursuant to the CCPA and how it responded to the requests for at least 24 months. The business shall implement and maintain reasonable security procedures and practices in maintaining these records.

(b) The records may be maintained in a ticket or log format provided that the ticket or log includes the date of request, nature of request, manner in which the request was made, the date of the business's response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part.

(c) A business's maintenance of the information required by this section, where that information is not used for any other purpose, does not taken alone violate the CCPA or these regulations.

(d) Information maintained for record-keeping purposes shall not be used for any other purpose except as reasonably necessary for the business to review and modify its processes for compliance with the CCPA and these regulations. Information maintained for record-keeping purposes shall not be shared with any third party except as necessary to comply with a legal obligation.

(e) Other than as required by subsection (a), a business is not required to retain personal information solely for the purpose of fulfilling a consumer request made under the CCPA.

11 C.C.R. § 7102. Requirements for Businesses Collecting Large Amounts of Personal Information.

(a) A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall:

(1) Compile the following metrics for the previous calendar year:

(A) The number of requests to know that the business received, complied with in whole or in part, and denied;

(B) The number of requests to delete that the business received, complied with in whole or in part, and denied;

(C) The number of requests to opt-out that the business received, complied with in whole or in part, and denied; and

(D) The median or mean number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out.

(2) Disclose, by July 1 of every calendar year, the information compiled in subsection (a)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy.

(A) In its disclosure pursuant to subsection (a)(2), a business may choose to disclose the number of requests that it denied in whole or in part because the request was not verifiable, was not made by a consumer, called for information exempt from disclosure, or was denied on other grounds.

(b) A business may choose to compile and disclose the information required by subsection (a)(1) for requests received from all individuals, rather than requests received from consumers. The business shall state whether it has done so in its disclosure and shall, upon request, compile and provide to the Attorney General the information required by subsection (a)(1) for requests received from consumers.

Literatur- und Quellenverzeichnis

Adams, Henry, The Federalist Regulation of Privacy: The Happy Incidents of State Regulatory Activity and Costs of Preemptive Federal Action, 84 Mo. L. Rev. 1055–1094.

Adams, Kristen David, Blaming the Mirror: The Restatements and the Common Law, 40 Ind. L. Rev. 205–270.

Adler, Steve, HIPAA Journal, 2020 HIPAA Violation Cases and Penalties, 2021, https://www.hipaajournal.com/2020-hipaa-violation-cases-and-penalties/ [perma.cc/5987-MN4B].[1]

Agencia Española Protectección Datos (Spanien), Resolución De Procedimiento Sancionador, Expediente Nº: PS/00003/2021, https://www.aepd.es/es/documento/ps-00003-2021.pdf [perma.cc/TTJ2-QZHK].

Albers, Marion, Informationelle Selbstbestimmung, Baden-Baden 2005.

Alexander, Christopher Bret, The General Data Protection Regulation and California Consumer Privacy Act: The Economic Impact and Future of Data Privacy Regulations, 32 Loy. Consumer L. Rev. 199–245.

Allmendinger, Christoph, Company Law in the European Union and the United States: A Comparative Analysis of the Impact of the EU Freedoms of Establishment and Capital and the U. S. Interstate Commerce Clause, 4 Wm. & Mary Bus. L. Rev. 67–110.

Alpert, David, Beyond Request-and-Respond: Why Data Access Will Be Insufficient to Tame Big Tech, 120 Colum. L. Rev. 1215–1254.

Al-Saif, Sulaf, Animal Healthcare Robots: The Case for Privacy Regulation, 14 Wash. J.L. Tech. & Arts 77–102.

Alza, Gustavo Jr., Blockchain & CCPA, 37 Santa Clara High Tech. L. J. 231–255.

American Civil Liberties Union, 5 Problems with National ID Cards, https://www.aclu.org/other/5-problems-national-id-cards [perma.cc/QW8T-9PKT].

American Civil Liberties Union of California/California Public Interest Research Group/Center for Digital Democracy/Common Sense Media/Consumer Action/Consumer Federation of America/Consumer Reports/Electronic Frontier Foundation/Media Alliance/Oakland Privacy/Privacy Rights Clearinghouse, California Privacy Rights and Enforcement Act – Privacy Coalition Comments, 2019, https://www.eff.org/files/2019/10/29/2019-10-23_-_privacy_coalition_comments_on_cprea.pdf [perma.cc/R57V-VRCL].

American Law Institute, Restatement of the law, second, Torts, St. Paul, Minnesota 1977.

–, Principles of the law, data privacy, Philadelphia 2020.

Amstutz, Marc, Dateneigentum, AcP 218 (2018), 438–551.

Anderson, Bryan, The Sacramento Bee, California's new initiative process, 02.07.2018, https://www.sacbee.com/news/politics-government/capitol-alert/article214110874.html [perma.cc/7ZDW-534R].

[1] Die zitierten Internetquellen sind unter jeweils angegebenen perma.cc-URL dauerhaft archiviert. Das Datum des letzten Abrufs entspricht dem im perma.cc-Archiv angegebenen Datum. Perma.cc ist ein Angebot der Universitätsbibliothek Harvard, dessen dauerhafte Erreichbarkeit gesichert ist, vgl. *Zittrain/Albert/Lessig*, 127 Harv. L. Rev. 176–199.

Angwin, Julia, The Markup, Tech on the Ballot: Interview with Ashkan Soltani, 2020, https://www.getrevue.co/profile/themarkup/issues/tech-on-the-ballot-286520 [perma.cc/L5XJ-HPR2].

Apple, Apple Legal, Your California Privacy Disclosures, 2021, https://www.apple.com/legal/privacy/california/ [perma.cc/4ETA-E45Q].

Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136, 2007, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_de.pdf [perma.cc/R4LK-SD5T] (zitiert als: *Artikel-29-Datenschutzgruppe*, WP 136 Personenbezogene Daten).

–, Stellungnahme 13/2011 zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten, WP 185, 2011, https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/wp185_de.pdf [perma.cc/Q9F6-7CJM] (zitiert als: *Artikel-29-Datenschutzgruppe*, WP 185 Geolokalisierungsdienste).

–, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216, 2014, https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/wp216_de.pdf [perma.cc/HM4N-2U7L] (zitiert als: *Artikel-29-Datenschutzgruppe*, WP 216 Anonymisierung).

–, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG. WP 217, 2014, https://www.datenschutzstelle.li/application/files/2915/5914/1746/WP217_Opinion62014LegitimateInterest.pdf [perma.cc/GW6X-KLUE] (zitiert als: *Artikel-29-Datenschutzgruppe*, WP 217 Berechtigtes Interesse).

–, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242, 2017, https://datenschutz-hamburg.de/assets/pdf/wp242rev01_de.pdf [perma.cc/M3HG-49E4] (zitiert als: *Artikel-29-Datenschutzgruppe*, WP 242 Datenübertragbarkeit).

–, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 wahrscheinlich ein hohes Risiko mit sich bringt, WP 248, 2017, https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48464 [perma.cc/4VYU-LWVZ] (zitiert als: *Artikel-29-Datenschutzgruppe*, WP 248 DSFA).

–, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260, 2017, https://ec.europa.eu/newsroom/article29/redirection/document/54194 [perma.cc/F2U3-ERJA] (zitiert als: *Artikel-29-Datenschutzgruppe*, WP 260 Transparenz).

–, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, WP251, 2018, https://ec.europa.eu/newsroom/article29/redirection/document/54169 [perma.cc/BC7H-4ZCQ] (zitiert als: *Artikel-29-Datenschutzgruppe*, WP 251 Profiling).

–, Referenzgrundlage für Angemessenheit, WP 254, 2018, https://ec.europa.eu/newsroom/article29/redirection/document/54200 [perma.cc/NUB5-N73U] (zitiert als: *Artikel-29-Datenschutzgruppe*, WP 254 Angemessenheit).

Ashman, Noah, Outed by Advertisements: How LGBTQ Internet Users Present a Case for Federal Privacy Legislation Comment, 99 Or. L. Rev. 523–556.

Association of National Advertisers/American Association of Advertising Agencies/American Advertising Federation/Interactive Advertising Bureau/California Grocers Association/Digital Advertising Alliance/Email Sender & Provider Coalition/National Business Coalition on E-Commerce and Privacy/Network Advertising Initiative/Insights Association/NetChoice, Statement of Opposition to Proposition 24: The California Privacy Rights Act of 2020 Ballot Initiative, 2020, https://www.networkadvertising.org/sites/default/files/joint_industry_letter_in_opposition_to_cpra_final.pdf [perma.cc/5P3H-GYVC].

Aubuchon, Alyssa L., Getting into Court When the Data Has Gotten out: A Two-Part Framework, 98 Wash. U. L. Rev. 1289–1312.

Auer-Reinsdorff, Astrid/Conrad, Isabell (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Auflage, München 2019.

Auswärtiges Amt, Verzeichnis der Staatennamen für den amtlichen Gebrauch in der Bundesrepublik Deutschland, 2021, https://www.auswaertiges-amt.de/blob/199312/9ebddb339f025f8ce355b1aa253d453b/staatennamen-data.pdf [perma.cc/X2ES-KC6V].

Autorité de protection des données (Belgien), Cookies et autres traceurs, https://www.autoriteprotectiondonnees.be/cookies [perma.cc/L3QM-K8RW].

–, Decision on the merits 21/2022 of 2 February 2022; Case number: DOS-2019-01377; Concerning: Complaint relating to Transparency & Consent Framework, 2022, https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf [perma.cc/W4JD-FRX3].

Autoriteit Persoonsgegevens (Niederlande), Beleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van bestuurlijke boetes [Richtlinie vom 19.02.2019 zur Bußgeldbemessung], 2019, https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-14586_0.pdf [perma.cc/ZP5L-Z2ST].

–, Dutch DPA imposes fine of €525,000 on Locatefamily.com, 2021, https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-imposes-fine-%E2%82%AC525000-locatefamilycom [perma.cc/T6WQ-J5A9].

–, DPA fines DPG Media for unnecessarily requesting copies of identity documents, 2022, https://www.autoriteitpersoonsgegevens.nl/en/news/dpa-fines-dpg-media-unnecessarily-requesting-copies-identity-documents [perma.cc/S8Z9-VY6T].

Au-Yeung, Angel, Forbes, California Wants To Copy Alaska And Pay People A 'Data Dividend.' Is It Realistic?, 2019, https://www.forbes.com/sites/angelauyeung/2019/02/14/california-wants-to-copy-alaska-and-pay-people-a-data-dividend--is-it-realistic/ [perma.cc/99J2-ZL86].

Axicom, US Products Privacy Policy, 2021, https://www.acxiom.com/about-us/privacy/highlights-for-us-products-privacy-policy/ [perma.cc/6836-Y7L6].

Baik, Jeeyun Sophia, Data Privacy Against Innovation or Against Discrimination?: The Case of the California Consumer Privacy Act (CCPA), 2020, https://papers.ssrn.com/abstract=3624850 [perma.cc/4EZQ-BPSP].

Ballon, Ian C, E-commerce & Internet law: treatise with forms, Eagan, Minnesota 2019.

Barbas, Samantha, The Sidis Case and the Origins of Modern Privacy Law, 36 Colum. J.L. & Arts 21–70.

Barber, Daniel, Privacy Tech, Benchmarking CCPA-related data subject requests, 2020, https://iapp.org/news/a/at-midyear-companies-seeing-both-do-not-sell-ccpa-requests-and-fraudulent-requests-for-access/ [perma.cc/NR4T-BEVR].

Barkow, Rachel E., Insulating Agencies: Avoiding Capture Through Institutional Design, 89 Tex. L. Rev. 15–79.

Bauer, Martin/Böhle, Thomas/Ecker, Gerhard (Hrsg.), Bayerische Kommunalgesetze: Gemeindeordnung, Landkreisordnung, Bezirksordnung: Kommentar, München, Stand: 108. EL 2021. (zitiert als: *Bearbeiter* in: Bauer/Böhle/Ecker, Bayerische Kommunalgesetze).

Baumann, Bastian, Datenschutzkonflikte zwischen der EU und den USA, Berlin 2016.

BayLDA (Bayerisches Landesamt für Datenschutzaufsicht), 6. Tätigkeitsbericht des Bayerischen Landesamtes für Datenschutzaufsicht für die Jahre 2013 und 2014, 2015, https://www.lda.bayern.de/media/baylda_report_06.pdf [perma.cc/97UK-VDMS] (zitiert als: *BayLDA,* Tätigkeitsbericht 2013/2014).

–, FAQ zur DSGVO: Informationspflicht bei ausländischen Kunden, 2018, https://www.lda.bayern.de/media/FAQ_Informationspflichten_Sprache.pdf [perma.cc/G6CW-MNMM].

–, Auskunft, https://www.lda.bayern.de/de/thema_auskunft.html [perma.cc/V3QM-8RSM].

BayLfD (Bayerischer Landesbeauftragter für den Datenschutz), 17. Tätigkeitsbericht 1996, 1996, https://www.datenschutz-bayern.de/tbs/tb17/tb17.pdf [perma.cc/GUD4-YQZ4].

–, Das Recht auf Auskunft nach der Datenschutz-Grundverordnung: Orientierungshilfe, 2019, https://www.datenschutz-bayern.de/verwaltung/OH_Recht_auf_Auskunft.pdf [perma.cc/C9KE-3DEM] (zitiert als: *BayLfD,* Orientierungshilfe Auskunft).

Becerra, Xavier, Testimony of Xavier Becerra, California Attorney General, 2020, https://oag.ca.gov/sites/default/files/Testimony%20of%20Xavier%20Becerra%2C%20CA%20Attorney%20General%5B2%5D%5B1%5D%20copy_0.pdf [perma.cc/SQ2L-2HBX].

Becker, Maximilian, Eine Materialisierung des datenschutzrechtlichen Koppelungsverbots, CR 2021, 230–243.

BeckOGK: Gsell, Beate/Krüger, Wolfgang/Lorenz, *Stephan/Reymann, Christoph (Hrsg.)*, beck-online.Grosskommentar zum Zivilrecht, Stand: 01.11.2021, München (zitiert als: *Bearbeiter* in: BeckOGK).

BeckOK DatenschutzR: Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.), BeckOK Datenschutzrecht, 40. Edition Stand: 01.05.2022 (zitiert als: *Bearbeiter* in: BeckOK DatenschutzR).

Becker, Tyler, When Congress Makes No Policy Choice: The Case of FTC Data Security Enforcement, 120 Colum. L. Rev. Forum 134–152.

Benedict, Jörg, Consideration Formalismus und Realismus im Common Law of Contract Consideration Formalismus und Realismus im Common Law of Contract, RabelsZ 69 (2005), 1–46.

Bennett, Steven C., The Right to Be Forgotten: Reconciling EU and US Perspectives, 30 Berkeley J. Int'l L. 161–195.

Bensinger, Greg, N.Y. Times, A Privacy Measure That's Hard to Like, 28.10.2020, https://www.nytimes.com/2020/10/28/opinion/california-prop-24-privacy.html [perma.cc/5HKQ-VCLX].

Bergt, Matthias, Sanktionierung von Verstößen gegen die Datenschutz-Grundverordnung, DuD 2017, 555–561.

Bertenthal, Alyse, Administrative Reasonableness: An Empirical Analysis, 2020 Wis. L. Rev. 85–140.

BfDI (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit), Arbeitshilfe Artikel 15 Jobcenter, 2020, https://www.bfdi.bund.de/DE/Infothek/Transparenz/Accessforone Accessforall/2020/2020-Arbeitshilfe-Artikel-15-Jobcenter.pdf?__blob=publicationFile&v=1 [perma.cc/9Q3Y-NK66].

–, Tätigkeitsbericht 2020: 29. Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit, 2021, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/29TB_20.pdf?__blob=publicationFile&v=3 [perma.cc/97MH-JRK3] (zitiert als: *BfDI,* Tätigkeitsbericht 2020).

–, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, 2020, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Positionspapier-Anonymisierung.pdf?__blob=publicationFile&v=4 [perma.cc/7KY6-HLLB] (zitiert als: *BfDI,* Anonymisierung).

–, Tätigkeitsbericht 2017 und 2018 zum Datenschutz, 2019, https://www.zaftda.de/tb-bfdi/705-27-tb-bfdi-bund-2017-18-ohne-drs-nr-vom-08-05-2019/file [perma.cc/K6AP-686N].

Bhagwat, Ashutosh, The Test that Ate Everything Intermediate Scrutiny in First Amendment Jurisprudence, 2007 U. Ill. L. Rev. 783–838.

Biderman, David/Shelton Leipzig, Dominique, Decrypted Unscripted: Dr. Johnny Ryan: Senior Fellow at The Irish Council for Civil Liberties | Fighting for Digital Rights – Episode 38, 16.12.2021, https://www.perkinscoie.com/en/news-insights/decrypted-unscripted.html [perma.cc/W99M-VGHD].

Bietti, Elettra, Consent as a Free Pass: Platform Power and the Limits of the Informational Turn, 40 Pace L. Rev. 310–398.

Bijok, Alexander, Kommerzialisierungsfester Datenschutz: Rechtliche Problemlagen der Datennutzung in der Informationswirtschaft, Baden-Baden 2020.

Bitkom, Mustervertragsanlage: Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO), 2017, https://www.bitkom.org/sites/default/files/file/import/170515-Auftragsverarbeitung-Anlage-Mustervertrag-online.pdf [perma.cc/S2G3-NYQ8] (zitiert als: *Bitkom*, Mustervertragsanlage Auftragsverarbeitung).

Blanke, Jordan M., Carpenter v. United States Begs For Action, 2018 U. Ill. L. Rev. Online 260–266.

–, Protection for „Inferences Drawn:" A Comparison between the General Data Protection Rule and the California Consumer Privacy Act, 1 Global Privacy Rev. 81–92.

BlnBDI (Berliner Beauftragte für Datenschutz und Informationsfreiheit), Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten, 2021, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf [perma.cc/7WXE-D5XS].

Blocker, Jack S., Did prohibition really work? Alcohol prohibition as a public health innovation, 96 Am. J. Public Health 233–243.

Blom, Robin, Naming Crime Suspects in the News: "Seek Truth and Report It" vs. "Minimizing Harm", in: Khosrow-Pour, Mehdi (Hrsg.), Media controversy: breakthroughs in research and practice, Hershey, Pennsylvania 2020.

Bock, Kirsten, Beschränkt Datenschutzrecht die Vertragsgestaltungsfreiheit?, CR 2020, 173–178.

Bodoni, Stephanie, Bloomberg.com, Amazon Gets Record $888 Million EU Fine Over Data Violations, 30.07.2021, https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach [perma.cc/8WCW-JMTD].

Booher, Kimberly Dempsey/Robins, Martin, American Privacy Law at the Dawn of a New Decade (and the CCPA and COVID-19): Overview and Practitioner Critique, 2020, https://papers.ssrn.com/abstract=3658495 [perma.cc/CZ7F-ZNHC] (zitiert als: *Booher/Robins*, American Privacy Law at the Dawn of a New Decade).

Botta, Jonas, Der California Consumer Privacy Act: Wegbereiter eines angemessenen Datenschutzniveaus im Silicon Valley? Eine rechtsvergleichende Analyse des neuen kalifornischen Datenschutzgesetzes am Maßstab des Art. 45 DSGVO, PinG 2019, 261–266 (Zweitveröffentlichung: *ders.,* Der California Consumer Privacy Act und die DSGVO: Ein transatlantisches Zwillingspaar?, in: Baumgärtel, Matthias (Hrsg.), DGRI Jahrbuch 2019/2020, Köln 2021, 29–44).

–, Eine Frage des Niveaus: Angemessenheit drittstaatlicher Datenschutzregime im Lichte der Schlussanträge in „Schrems II", CR 2020, 82–89.

Bracy, Jedidiah, Podcast: Alastair Mactaggart on California's Prop 24, 2020, https://iapp.org/news/a/podcast-alastair-mactaggart-on-californias-prop-24/ [perma.cc/GL4T-TKEM].

Bradford, Anu, The Brussels Effect, 107 Nw. U. L. Rev. 1–68.

Brandeis, Louis D., Other people's money, and how the bankers use it, New York City 1914.

Brass, Clinton T./Brudnick, Ida A./Keegan, Natalie/McMillion, Barry J./Rollins, John W./Yeh, Brian T., Congressional Research Service Report: Shutdown of the Federal Government: Causes, Processes, and Effects, 2018, https://sgp.fas.org/crs/misc/RL34680.pdf [perma.cc/P2LE-YL34] (zitiert als: *Brass et al.*, Shutdown of the Federal Government).

Braun, Sven, Vorherige Konsultation der Datenschutzaufsicht nach Folgenabschätzung, ZD 2021, 297–302.

Brauneck, Jens, Privacy Shield – zu Recht für ungültig erklärt?, EuZW 2020, 933–941.

Brendle-Weith, Anne-Katrin, Datenhandel im Rahmen der Datenschutzgrundverordnung, VuR 2018, 331–337.

Brennan, Mark/Denvil, James/Jin, Shee/Hirsch, Jonathan, HL Chronicle of Data Protection, California Consumer Privacy Act: The Challenge Ahead – The CCPA's Anti-Discrimination Clause, 2018, https://www.hldataprotection.com/2018/12/articles/consumer-privacy/

california-consumer-privacy-act-the-challenge-ahead-the-ccpas-anti-discrimination-clause/ [perma.cc/6XEW-JWF5].

Britz, Thomas/Indenhuck, Moritz/Langerhans, Tom, Die Verarbeitung „zufällig" sensibler Daten, ZD 2021, 559–564.

Buchner, Benedikt, Informationelle Selbstbestimmung im Privatrecht, Tübingen 2006.

–, Die Einwilligung im Datenschutzrecht, DuD 2010, 39.

Bukaty, Preston, California Consumer Privacy Act (CCPA): An implementation guide, Ely 2019 (zitiert als: *Bukaty*, CCPA Implementation Guide).

Bundesamt für Justiz, Klageregister, https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Klageregister/Bekanntmachungen/Klagen_node.html [perma.cc/4BK9-J79D].

Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-1: Managementsysteme für Informationssicherheit, 2017, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.pdf?__blob=publicationFile&v=2 [perma.cc/3ANT-JECC].

–, Die Lage der IT-Sicherheit in Deutschland 2021, 2021, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf?__blob=publicationFile&v=3 [perma.cc/V2JP-THGR].

Bundesministerium der Justiz und für Verbraucherschutz, Bundesministerium der Justiz und für Verbraucherschutz, »One-Pager" – Muster für transparente Datenschutzhinweise, 2016, https://www.bmjv.de/SharedDocs/Downloads/DE/Verbraucherportal/OnePager/11192915_OnePager-Datenschutzhinweise.html [perma.cc/YV9S-QTPS].

Bundesministerium des Innern, für Bau und Heimat, Evaluierung des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, 2021, https://www.bmi.bund.de/SharedDocs/evaluierung-von-gesetzen/downloads/berichte/evaluierung-bdsg.pdf?__blob=publicationFile [perma.cc/7EBT-2XJ5].

Bundesregierung, Datenstrategie der Bundesregierung, 2021, https://www.bundesregierung.de/resource/blob/992814/1845634/f073096a398e59573c7526feaadd43c4/datenstrategie-der-bundesregierung-download-bpa-data.pdf [perma.cc/74AH-DR7P].

Bunnenberg, Jan Niklas, Privates Datenschutzrecht: über Privatautonomie im Datenschutzrecht – unter besonderer Berücksichtigung der Einwilligung und ihrer vertraglichen Kopplung nach Art. 7 Abs. 4 DS-GVO, Baden-Baden 2020 (zitiert als: *Bunnenberg*, Privates Datenschutzrecht).

Burbank, Stephen B./Farhang, Sean, Class Actions and the Counterrevolution Against Federal Litigation, 165 U. Pa. L. Rev. 1495–1530.

Buresh, Donald L., A Comparison between the European and the American Approaches to Privacy, 6 The Indonesian Journal of International & Comparative Law 257–285.

–, Should Personal Information and Biometric Data Be Protected Under a Comprehensive Federal Privacy Statute That Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?, 38 Santa Clara High Tech. L.J. 39–93.

Burt, Andrew, NAVEX Global, CPRA: 7 Key Changes to California's Data Privacy Laws, 2021, https://www.navexglobal.com/blog/article/cpra-7-changes-californias-data-privacy-laws/ [perma.cc/Z5XM-RPML].

Busse, Philipp/Dallmann, Michael, Verarbeitung von öffentlich zugänglichen personenbezogenen Daten, ZD 2019, 394–399.

Büyuksagis, Erdem, Towards a Transatlantic Concept of Data Privacy, 30 Fordham Intell. Prop. Media & Ent. L.J. 139–221.

Byun, Diane Y., Privacy Or Protection: The Catch-22 of the CCPA, 32 Loy. Consumer L. Rev. 246–265.

Cadwalladr, Carole/Graham-Harrison, Emma, The Guardian, Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, 17.03.2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [perma.cc/G3AX-6JP5].

Cahill, Kevin F./Harris, David J./Browne, Mark/Bonaccorsi, Hilary/Hespeler, Colleen, California Consumer Privacy Act: Potential Impact and Key Takeaways, 30 IPTJL 11–18.

Cal. Attorney General, State of California – Department of Justice – Office of the Attorney General, History of the Office of the Attorney General, 2011, https://oag.ca.gov/history [perma.cc/9566-7M5K].

–, California Data Breach Report 2016, 2016, https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf [perma.cc/JG45-KHKR].

–, California Consumer Privacy Act of 2018, 2018, https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2018/08/ag-becerras-letter-re-california-consumer-privacy-act.pdf [perma.cc/SU6L-JAAS].

–, State of California – Department of Justice – Office of the Attorney General, California Consumer Privacy Act: Frequently Asked Questions, 2018, https://oag.ca.gov/privacy/ccpa [perma.cc/64FZ-WPJE].

–, Budget Change Proposal – California Consumer Privacy Act of 2018 (AB 375 & SB 1121), 2019, https://esd.dof.ca.gov/Documents/bcp/1920/FY1920_ORG0820_BCP2916.pdf [perma.cc/ZPB8-UBTX] (zitiert als: *Cal. Attorney General*, Budget Change Proposal).

–, Initial Statement of Reasons, 2019, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf [perma.cc/K5WN-Q8NE].

–, Text of Proposed Regulations – California Consumer Privacy Act (CCPA), 2019, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf [perma.cc/DJ7A-HZSH] (zitiert als: *Cal. Attorney General*, Proposed Regulations).

–, CCPA: Text of First Set of Modifications, 2020, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-redline-020720.pdf [perma.cc/HG5B-L4XW].

–, Summary and Response to Comments Submitted during 2nd 15-Day Comment Period, 2020, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-e.pdf [perma.cc/4ZHZ-KQUQ].

–, Summary and Response to Comments Submitted During 45-Day Period, 2020, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-a.pdf [perma.cc/LCN3-NALM].

–, Final Statement of Reasons, 2020, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor.pdf [perma.cc/5WZ5-CNGS].

–, Written Comments 45-Day Period, 2020, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-a.pdf [perma.cc/ZDR5-ERUW].

–, California Officials Announce California Privacy Protection Agency Board Appointments, 2021, https://oag.ca.gov/news/press-releases/california-officials-announce-california-privacy-protection-agency-board [perma.cc/X75X-7FU3].

–, State of California – Department of Justice – Office of the Attorney General, CCPA Enforcement Case Examples, 2021, https://oag.ca.gov/privacy/ccpa/enforcement [perma.cc/Y98H-GMXZ].

–, State of California – Department of Justice – Office of the Attorney General, Privacy Laws, https://oag.ca.gov/privacy/privacy-laws [perma.cc/CD5Y-ZPJ9].

–, Opinion No. 20-303, 2022, https://oag.ca.gov/system/files/opinions/pdfs/20-303.pdf {perma.cc/46S9-HFKT}.

Cal. Legislature, Legislative Information: AB-375 Privacy: personal information: businesses. (2017-2018): Current Version: 06/28/18 – Chaptered Compared to Version: 06/21/18

– Amended Senate, 2018, https://leginfo.legislature.ca.gov/faces/billVersionsCompareClient.xhtml?bill_id=201720180AB375&cversion=20170AB37594AMD [perma.cc/MCJ3-Q72Y].
–, Legislative Information: AB-375 Privacy: personal information: businesses. (2017-2018): Votes, http://leginfo.legislature.ca.gov/faces/billVotesClient.xhtml?bill_id=201720180AB375 [perma.cc/UY6E-BQA9].
Cal. Office of Administrative Law, Notice of Approval in Part and Withdrawal in Part of Regulatory Action, 2020, https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-notice-approval.pdf? [perma.cc/T6CX-HYQC].
Cal. Privacy Protection Agency, Conflict of Interest Code, 2021, https://cppa.ca.gov/meetings/materials/20211018_item11.pdf [perma.cc/GRX3-EUQS].
–, California Privacy Protection Agency Board Meeting: June 14, 2021: Meeting Minutes, 2021, https://cppa.ca.gov/meetings/minutes/20210614.pdf [perma.cc/5YMC-DBLB] (zitiert als: *Cal. Privacy Protection Agency*, Board Meeting June 14, 2021 Minutes).
–, Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020, 2021, https://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf [perma.cc/Z9G3-XL9Q] (zitiert als: *Cal. Privacy Protection Agency*, Invitation Preliminary Comments).
–, Ashkan Soltani Selected as California Privacy Protection Agency Executive Director, 2021, https://cppa.ca.gov/announcements/ [perma.cc/3KQQ-WVTB].
–, California Privacy Protection Agency Board Meeting: October 18, 2021: Meeting Minutes, 2021, https://cppa.ca.gov/meetings/minutes/20211018.pdf [perma.cc/DJM5-DWJ9] (zitiert als: *Cal. Privacy Protection Agency*, Board Meeting October 18, 2021 Minutes).
–, „Per Diem" Policy as Approved in September 7, 2021 Board Meeting, 2021, https://cppa.ca.gov/meetings/materials/20210907_9.pdf [perma.cc/58VC-AZZN].
–, Notes on Economic Impact Estimates for Form 399, 2022, https://cppa.ca.gov/regulations/pdf/std_399_attachment.pdf [perma.cc/5Z3G-FYRM].
–, Text of Proposed Regulations, 2022, https://cppa.ca.gov/regulations/pdf/20220708_text_proposed_regs.pdf [perma.cc/V8F4-F243] (zitiert als: Cal. Privacy Protection Agency, Proposed Regulations).
–, Initial Statement of Reasons, 2022, https://cppa.ca.gov/meetings/materials/20220608_item3_isr.pdf [perma.cc/3W9H-MXEB].
Cal. Secretary of State, Proponents Withdraw Initiative to Establish New Consumer Privacy Rights; Expand Liability for Consumer Data Breaches, 2018, https://www.sos.ca.gov/administration/news-releases-and-advisories/2018-news-releases-and-advisories/proponents-withdraw-initiative-establish-new-consumer-privacy-rights-expand-liability-consumer-data-breaches/ [perma.cc/FL86-RDFV].
–, CalAccess – Campaign Finance: Committee to Protect California Jobs, Sponsored by the California Chamber of Commerce, 2018, https://cal-access.sos.ca.gov/Campaign/Committees/Detail.aspx?id=1401518&session=2017 [perma.cc/XNU6-BN4P].
–, Official Voter Information Guide, California General Election: Tuesday, November 3, 2020, 2020, https://vig.cdn.sos.ca.gov/2020/general/pdf/complete-vig.pdf [perma.cc/5HG6-GM4P] (zitiert als: *Cal. Secretary of State*, Voter Guide 2020).
–, CalAccess – Campaign Finance: California Consumer and Privacy Advocates Against Prop 24, Sponsored by California Nurses Association, 2020, https://cal-access.sos.ca.gov/Campaign/Committees/Detail.aspx?id=1428087&session=2019&view=received [perma.cc/F3BG-A2GX].
–, Statement of Vote: General Election November 3, 2020, 2020, https://elections.cdn.sos.ca.gov/sov/2020-general/sov/complete-sov.pdf [perma.cc/S5TA-YQ2A].

Cal. Senate Judiciary Comm., AB 1950 Bill Analysis, 2004, https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=200320040AB1950 [perma.cc/7D3R-S3LM].
–, AB 375 Bill Analysis, 2018, https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=20172018oAB375# [perma.cc/GG6M-4Z49].
–, AB 1146 Bill Analysis, 2019, https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201920200AB1146# [perma.cc/8R7S-PFZX].
Cal. Senate Judiciary Committee, Cal. Senate Judiciary Committee: AB 1564, 2019, https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201920200AB1564 [perma.cc/92UG-G8YD].
Californian Republican Party, Endorsements, 2020, https://www.cagop.org/s/endorsements [perma.cc/P9RD-94MX].
Californians for Consumer Privacy, The Consumer Right to Privacy Act of 2018, 2017, https://www.oag.ca.gov/system/files/initiatives/pdfs/17-0039%20%28Consumer%20Privacy%20V2%29.pdf [perma.cc/2AXP-QQVE].
–, Submission of Amendments to The California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021, and Request to Prepare Circulating Title and Summary (Amendment), 2019, https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf [perma.cc/UK99-XYY8] (zitiert als: *Californians for Consumer Privacy*, California Privacy Rights and Enforcement Act of 2020, Version 3).
–, The California Privacy Rights and Enforcement Act of 2020, 2019, https://uploads-ssl.webflow.com/5aa18a452485b60001c301de/5d8bc3342a72fc8145920a32_CPREA_2020_092519_Annotated_.pdf [perma.cc/DHC5-5ZPF].
–, Yes on Prop 24, CPRA Ballot Signatures Submitted, 2020, https://www.caprivacy.org/californians-for-consumer-privacy-submits-signatures-to-qualify-the-california-privacy-rights-act-for-november-2020-ballot/ [perma.cc/EDN8-CMW5].
–, Yes on Prop 24, CPRA Qualifies for Nov 2020 Ballot, 2020, https://www.caprivacy.org/california-privacy-rights-act-cpra-qualifies-for-the-november-2020-ballot/ [perma.cc/RZL3-PLVJ].
–, Prop 24 Limits the Tracking of Geolocation, 2020, https://www.caprivacy.org/how-prop-24-can-limit-businesses-from-tracking-your-geolocation-and-using-your-sensitive-personal-information/ [perma.cc/43GD-VB77].
–, How Prop 24 Adds Even More Privacy Rights Compared to the CCPA, 2020, https://www.caprivacy.org/how-prop-24-adds-even-more-privacy-rights-compared-to-the-ccpa/ [perma.cc/PU7F-JBV4].
–, Prop 24 Webinar: „Your Privacy on the Ballot: Prop 24 and the California Privacy Rights Act“, 2020, https://www.youtube.com/watch?v=66UZB9tFmdA [perma.cc/L5QD-S5PB] (zitiert als: *Californians for Consumer Privacy*, Prop 24 Webinar).
–, Annotated Text of the CPRA with CCPA Changes, 2021, https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/ [perma.cc/YK2A-PCJP].
Carrillo, David A., SCOCAblog, How California lives with two legislatures, 2020, http://scocablog.com/how-california-lives-with-two-legislatures/ [perma.cc/D47R-M88E].
Carrillo, David A./Duvernay, Stephen M./Gevercer, Benjamin/Fenzel, Meghan, California Constitutional Law: Direct Democracy, 92 S. Cal. L. Rev. 557–652.
Carson, Angelique, The Privacy Advisor, On keynote stage, Mactaggart addresses his „new“ CCPA, 2019, https://iapp.org/news/a/on-keynote-stage-mactaggart-addresses-his-new-ccpa/ [perma.cc/WY22-WYA5].
Caspar, Johannes, Zwischen Symbolik und Gestaltungskraft – Ist die EU-DSGVO eine Mogelpackung?, vorgänge 231/232 (2020), 99–116.
Catalog Choice, CatalogChoice Mail Preference Service, About Us, https://catalogchoice.org [perma.cc/P3FX-7ANF].

Cate, Fred H./Litan, Robert, Constitutional Issues in Information Privacy, 9 Mich. Telecomm. & Tech. L. Rev. 35–63.

Center for Internet Security, CIS Controls Version 8, 2021, https://learn.cisecurity.org/l/799323/2021-05-18/47qgs [perma.cc/5NQ2-VY7F].

Chander, Anupam/Abraham, Meaza/Chandy, Sandeep/Fang, Yuan/Park, Dayoung/Yu, Isabel, Achieving Privacy, 74 SMU L. Rev. 607–664.

Chander, Anupam/Kaminski, Margot/McGeveran, William, Catalyzing Privacy Law, 105 Minn. L.Rev. 1733–1805.

Chanin, Rachel L., Calfornia's Authority to Regulate Mobile Source Greenhouse Gas Emissions, 58 N.Y.U. Ann. Surv. Am. L. 699–754.

Chen, Jianqing/Stallaert, Jan, An Economic Analysis of Online Advertising Using Behavioral Targeting, 38 MIS Quarterly 429–449.

Christakis, Theodore, European Law Blog, Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 2), 2021, https://europeanlawblog.eu/2021/04/13/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part2/ [perma.cc/4TLW-M5SJ].

Citron, Danielle K., Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age, 80 Cal. L. Rev. 241–297.

–, The Privacy Policymaking of State Attorneys General, 92 Notre Dame L. Rev. 747–816.

Clark, James/Halpert, James, California Consumer Privacy Act and the GDPR – where do they overlap?, 17 PDP 7.

Cohen, Bret/Hall, Britanie/Woo, Ryan, JD Supra, California Consumer Privacy Act: The Challenge Ahead – A Comparison of 10 Key Aspects of The GDPR and The CCPA, 2018, https://www.jdsupra.com/legalnews/california-consumer-privacy-act-the-73267/ [perma.cc/HJ6Z-YK8K].

Cohen, Bret/Otto, Paul/Salminen, Nathan/Perna, Morgan, HL Chronicle of Data Protection, California Consumer Privacy Act: The Challenge Ahead – The CCPA's „Reasonable" Security Requirement, 2019, https://www.hldataprotection.com/2019/02/articles/consumer-privacy/california-consumer-privacy-act-the-challenge-ahead-the-ccpas-reasonable-security-requirement/ [perma.cc/R5P8-KCAB].

Columbia Law Review/Harvard Law Review/University of Pennsylvania Law Review/Yale Law Review (Hrsg.), The Bluebook: A uniform system of citation, 21. Auflage, Cambridge, Massachusetts, 2020.

Comber, Geoffrey, I Presume We're (Commercially) Speaking Privately: Clarifying the Court's Approach to the First Amendment Implications of Data Privacy Regulations, 89 Geo. Wash. L. Rev. 202–232.

Confessore, Nicholas, The N.Y. Times, The Unlikely Activists Who Took On Silicon Valley – and Won., 14.08.2018, https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html [perma.cc/PDD2-LF66].

–, N.Y. Times, Demystifying Online Privacy, 18.08.2018, https://www.nytimes.com/2018/08/18/insider/online-privacy-facebook-data-google.html [perma.cc/5Q2M-USGN].

Cooper, James C./Kobayashi, Bruce H., An Unreasonable Solution: Rethinking the FTC's Current Approach to Data Security, 2020, https://papers.ssrn.com/abstract=3660116 [perma.cc/RLU3-Q5BA].

Corbin, Kenneth, Internetnews, FTC Mulls Browser-Based Block for Online Ads, 2010, http://www.internetnews.com/ec-news/article.php/3895496/FTC+Mulls+BrowserBased+Block+for+Online+Ads.htm [perma.cc/5Y36-7EPK].

Cormack, Andrew, Is the Subject Access Right Now Too Great a Threat to Privacy, 2 EPDL 15–27.

Cosgrove, Cathy, The Privacy Advisor, Top-10 operational impacts of the CPRA: Part 2 – Defining „business" under the law, 2020, https://iapp.org/news/a/cpras-top-operational-impacts-part-2-defining-business/ [perma.cc/BY5X-2RKC].

Cranor, Lorrie Faith/Habib, Hana/Zou, Yixin/Acquisti, Alessandro/Reidenberg, Joel R./Sadeh, Norman/Schaub, Florian, User Testing of the Proposed CCPA Do-Not-Sell Icon, 2020, http://cups.cs.cmu.edu/pubs/CCPA2020Feb24.pdf [perma.cc/HMQ3-RCGN].

Criscione, Hunter, Forgetting the Right to be Forgotten: The Everlasting Negative Implications of a Right to be Dereferenced on Global Freedom in the Wake of Google v. CNIL, 32 Pace Int'l L. Rev. 315–358.

Cross, Frank B., America the Adversarial Book Review, 89 Va. L. Rev. 189–238.

D'Amico, Alex R./Rumph, Karl, Morrison Mahoney, California Ballot Initiative Signals a Sea Change in US Data Privacy Law but Should Not Be Reason for Fear, 2020, https://www.morrisonmahoney.com/blog/545-california-ballot-initiative-signals-a-sea-change-in-us-data-privacy-law-but-should-not-be-reason-for-fear [perma.cc/8SDP-WHZQ].

Dammann, Ulrich, Erfolge und Defizite der EU-Datenschutzgrundverordnung: Erwarteter Fortschritt, Schwächen und überraschende Innovationen, ZD 2016, 307–314.

DataGrail, The State of CCPA, 2021, https://www.datagrail.io/the-state-of-ccpa/ [perma.cc/CD6W-WVCN].

DataGuidance, USA State Law Tracker, 2019, https://www.dataguidance.com/comparisons/usa-state-law-tracker [perma.cc/D3UH-B9YC].

Datenethikkommission, Gutachten der Datenethikkommission, 2019, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile [perma.cc/38B6-HY3M].

Datenschutzbehörde (Österreich), Datenschutzbericht 2020, 67.

Dauster, William G., The Senate in Transition or How I Learned to Stop Worrying and Love the Nuclear Option, 19 N.Y.U. J. Legis. & Pub. Pol'y 631–683.

Davis, Lauren, The Impact of the California Consumer Privacy Act on Financial Instutions Across the Nation, 24 N.C. Banking Inst. 499–525.

De Cruz, Peter, Comparative law in a changing world, 3. Auflage, London 2007.

De la Lama, Amy/Hengesbaugh, Brian, The Privacy Advisor, How to know if your vendor is a „service provider" under CCPA, 2019, https://iapp.org/news/a/how-to-know-if-your-vendor-is-a-service-provider-under-ccpa/ [perma.cc/H6XK-GDB7].

De la Lama, Amy/Markert, Sara L., Bryan Cave Leighton Paisner, The Expanded Private Right of Action under the CPRA, 2020, https://www.bclplaw.com/en-US/insights/the-expanded-private-right-of-action-under-the-cpra.html [perma.cc/4V8D-ME3Y].

De la Torre, Lydia F., Golden Data, What is a 'sale' under CCPA?, 2020, https://medium.com/golden-data/what-is-a-sale-under-ccpa-b27fbe8a527 [perma.cc/AA4N-NBN9].

–, Written testimony for California Senate Judicial Committee, 2020, https://medium.com/golden-data/written-testimony-for-california-senate-judicial-committee-9e3185910e60 [perma.cc/4F9R-BAQG].

–, Golden Data, What is (and is not) personal information under the California Privacy Rights Act?, 2020, https://medium.com/golden-data/what-is-and-is-not-personal-information-under-the-california-privacy-rights-act-89a1d377c483 [perma.cc/4ZNW-BP6W].

–, Golden Data, What is a business under CPRA?, 2020, https://medium.com/golden-data/what-is-a-business-under-cpra-41794347370b [perma.cc/RJ9S-G4U6].

De la Torre, Lydia F./Brown, Glenn, The Privacy Advisor, What is the California Privacy Protection Agency?, 2020, https://iapp.org/news/a/what-is-the-california-privacy-protection-agency/ [perma.cc/C8QY-QYVE].

De la Torre, Lydia F./Rupp, Sebastiano, The Privacy Advisor, What does „valuable consideration" mean under the CCPA?, 2018, https://iapp.org/news/a/what-does-valuable-consideration-mean-under-the-ccpa/ [perma.cc/8X3Z-49QJ].

Deb, Gitanjali, The Data Privacy Landscape During COVID-19: An Exploration of Some of the Major Data Privacy Regulations and Trends, 31 DePaul J. Art Tech. & Intell. Prop. L. 115–145.

Der Standard, Abo & Angebote: Fragen & Antworten, https://abo.derstandard.at/fragen-antworten/ [perma.cc/KKE7-FD4J].

Determann, Lothar, Social Media Privacy: A Dozen Myths and Facts, 2012 Stan. Tech. L. Rev. 7.

–, Adequacy of data protection in the USA: myths and facts, 6 International Data Privacy Law 244–250.

–, Kalifornisches Gesetz gegen Datenhandel, ZD 2018, 443–448 (Zweitveröffentlichung: *ders.,* New California Law Against Data Sharing, CRi 2018, 117–124).

–, Healthy Data Protection, 26 Mich. Tech. L. Rev. 229–278.

–, California Privacy Law: Pratical Guide and Commentary: U. S. Federal and California Law, 4. Auflage, Portsmouth 2020 (zitiert als: *Determann*, California Privacy Law).

–, Kaliforniens erste Datenschutzbehörde – dank Volksentscheid, ZD 2021, 69–74.

–, Electronic Form Over Substance – eSignature Laws Need Upgrades, 72 Hastings L.J. 1385–1452.

Determann, Lothar/Tam, Jonathan, The California Privacy Rights Act of 2020: A broad and complex data processing regulation that applies to businesses worldwide, JDPP 2021, 7–21.

Del Rosario, Luis, On the Propertization of Data and the Harmonization Imperative, 90 Fordham L. Rev. 1699.

Diamond, Mark, Creating a California Consumer Privacy Act Action Plan, 22 Journal of Internet Law 1–22.

Die Zeit, Pur-Abo, https://premium.zeit.de/faq/pur [perma.cc/3V6M-HZ46].

Dix, Alexander, Daten als Bezahlung – Zum Verhältnis zwischen Zivilrecht und Datenschutzrecht, ZEuP 2017, 1–5.

–, Motor oder Flaschenhals? Die Regeln der Datenschutz-Grundverordnung zur Zusammenarbeit und Kohärenz der Datenschutzaufsicht, vorgänge 231/232 (2020), 87–98.

Dodd, Bill, Virtual Town Hall – The Future of Privacy, 2020, https://sd03.senate.ca.gov/video/20201208-town-hall [perma.cc/XYC5-PNBS].

DPC (Data Protection Commission; Irland), Draft Decision In the matter of LB (through NOYB) v Facebook Ireland Limited, 2021, https://noyb.eu/sites/default/files/2021-10/IN%2018-5-5%20Draft%20Decision%20of%20the%20IE%20SA.pdf [perma.cc/HT7B-JWBH].

Drexl, Josef, Neue Regeln für die Europäische Datenwirtschaft?, NZKart 2017, 415–421.

–, Connected devices – An unfair competition law approach to data access rights of users, in: Bundesministerium der Justiz und für Verbraucherschutz/Max-Planck-Institut für Innovation und Wettbewerb (Hrsg.), Data access, consumer interests and public welfare, Baden-Baden 2021, 477–527.

DSGVO-Portal, DSGVO Bußgeld Datenbank, https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank.php [perma.cc/3T8T-3WEM].

DSK (Datenschutzkonferenz), Kurzpapier Nr. 1 Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO, 2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_1.pdf [perma.cc/S9AE-EHV5] (zitiert als: *DSK,* Kurzpapier Nr. 1 – Art. 30 DS-GVO).

–, Kurzpapier Nr. 15: Videoüberwachung nach der Datenschutz-Grundverordnung, 2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_15.pdf [perma.cc/GM99-596S].

–, Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen, 2019, https://www.

datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf [perma.cc/4A8D-ZXQ3] (zitiert als: *DSK,* Konzept Bußgeldzumessung).

–, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021), 2021, https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf (zitiert als: *DSK,* OH Telemedien 2021).

–, Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. April 2019: Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten!, https://www.datenschutzkonferenz-online.de/media/en/20190405_Entschliessung_Unternehmenshaftung.pdf [perma.cc/LM4F-LPVN] (zitiert als: *DSK,* Entschließung Unternehmenshaftung).

Duball, Joseph, The Privacy Advisor, Are companies using semantics to get around CCPA's „sale" provision?, 2020, https://iapp.org/news/a/blinders-up-how-organizations-dance-around-sale-under-ccpa/ [perma.cc/LF5E-WQ75].

–, The Privacy Advisor, What the CPPA's appointments say about enforcement priorities, strategy, 2021, https://iapp.org/news/a/do-cppa-appointments-say-anything-about-priorities-strategy/ [perma.cc/F663-MEYA].

–, The Privacy Advisor, Colorado Privacy Act passes, professionals ponder effects, 2021, https://iapp.org/news/a/colorado-privacy-act-passes-professionals-ponder-effects/ [perma.cc/XJ4G-7HK4].

Düsseldorfer Kreis, Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen", 2014, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2014/03/OH-V%C3%9C-durch-nicht-%C3%B6ffentliche-Stellen.pdf [perma.cc/MT8H-HQBU].

Dyadkina, Raisa/de la Torre, Lydia F./Bryan, Kristin, Consumer Privacy World, First CCPA Settlement Reached in Hanna Andersson Case, 2020, https://www.consumerprivacyworld.com/2020/12/first-ccpa-settlement-reached-in-hanna-andersson-case/ [perma.cc/B5PB-8GCL].

Eberl, Matthias, Netzpolitik.org, Tracking auf Nachrichtenseiten: Datenschutzbehörden erhöhen den Druck auf Verlage, 2020, https://netzpolitik.org/2020/datenschutzbehoerden-erhoehen-den-druck-auf-verlage/ [perma.cc/JLQ2-9S7M].

EDSA (Europäischer Datenschutzausschuss), Endorsement 1/2018, 2018, https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents_en_0.pdf [perma.cc/U9D5-ZEBX].

–, EU – U.S. Privacy Shield – Second Annual Joint Review, 2019, https://edpb.europa.eu/sites/default/files/files/file1/20190122edpb_2ndprivacyshieldreviewreport_final_en.pdf [perma.cc/6NNT-LAU8].

–, Stellungnahme 3/2019 zu den Fragen und Antworten zum Zusammenspiel der Verordnung über klinische Prüfungen und der Datenschutz-Grundverordnung (DSGVO) (Artikel 70 Absatz 1 Buchstabe b), 2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb_opinionctrq_a_final_de.pdf [perma.cc/SU4Y-3UWZ] (zitiert als: *EDSA,* Stellungnahme 3/2019 Verordnung über klinische Prüfungen).

–, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_de_0.pdf [perma.cc/2FY6-YW8T] (zitiert als: *EDSA,* Leitlinien 2/2019 Rechtsgrundlage Vertrag).

–, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_de.pdf [perma.cc/3JD6-UZ74] (zitiert als: *EDSA,* Leitlinien 05/2020 Einwilligung).

–, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte: Version 2.0, 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_de.pdf [perma.cc/KUZ8-64DL] (zitiert als: *EDSA,* Leitlinien 3/2019 Videogeräte).
–, Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19, 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_de_0.pdf [perma.cc/RFS8-XM9W] (zitiert als: *EDSA,* Leitlinien 04/2020).
–, Beschluss 01/2020 zur Streitigkeit nach Artikel 65 Absatz 1 Buchstabe a der DSGVO über den Beschlussentwurf der irischen Aufsichtsbehörde bezüglich der Twitter International Company, 2020, https://edpb.europa.eu/system/files/2021-04/edpb_bindingdecision01_2020_de.pdf [perma.cc/HN4N-Z7KY] (zitiert als: *EDSA,* Beschluss 01/2020 Twitter).
–, Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom, 2021, https://edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf [perma.cc/Y7DY-EN5D] (zitiert als: *EDSA,* Opinion 14/2021 United Kingdom).
–, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 2.0, 2021, https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf [perma.cc/X9N6-ZGJ3] (zitiert als: *EDSA,* Guidelines 07/2020 Controller Processor).
–, Guidelines on data subject rights – Right of access, version 1.0, 2022, https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf#page12 [perma.cc/5LG9-8T8U] (zitiert als: *EDSA,* Guidelines 01/2022 Right of access)
–, Guidelines 04/2022 on the calculation of administrative fines under the GDPR, 2022, https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf [perma.cc/6F9Y-5HSE] (zitiert als: EDSA (Europäischer Datenschutzausschuss), Guidelines 04/2022 Calculation of fines)
–, DSGVO: Leitlinien, Empfehlungen, bewährte Verfahren, https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_de [perma.cc/2QAB-GJN2].
–, Final One Stop Shop Decisions, https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_ro?f%5B0%5D=article_60_types_of_decision%3AAdministrative%20fine [perma.cc/D6QM-GWXB].
Ehmann, Eugen/Selmayr, Martin, Datenschutz-Grundverordnung: Kommentar, 2. Auflage, München 2018.
Eig, Larry M., Statutory Interpretation: General Principles and Recent Trends, 2014, https://sgp.fas.org/crs/misc/97-589.pdf [perma.cc/W3SA-LSEW].
Eilperin, Juliet/Grandoni, Dino, Washington Post, EPA moves to give California right to set climate limits on cars, SUVs, 26.04.2021, https://www.washingtonpost.com/climate-environment/2021/04/26/california-car-climate-waiver/ [perma.cc/C9MT-N87A].
Ellger, Reinhard, Der Datenschutz im grenzüberschreitenden Datenverkehr: eine rechtsvergleichende und kollisionsrechtliche Untersuchung, Baden-Baden 1990 (zitiert als: *Ellger*, Datenschutz im grenzüberschreitenden Datenverkehr).
–, Vertragslösungen als Ersatz für ein angemessenes Schutzniveau bei Datenübermittlungen in Drittstaaten nach dem neuen Europäischen Datenschutzrecht, 60 RabelsZ 60 (1996), 738–770.
Elliott, Taryn, Standing a Chance: Does Spokeo Preclude Claims Alleging the Violation of Certain State Data Breach Laws?, 49 Seton Hall L. Rev. 233–254.
Engeler, Malte, Das überschätzte Kopplungsverbot, ZD 2018, 55–62.
–, The EDPB's guidelines 02/2019 on Art. 6(1)(b) GDPR, PinG 2019, 149–154.
Engeler, Malte/Quiel, Philipp, Recht auf Kopie und Auskunftsanspruch im Datenschutzrecht, NJW 2019, 2201–2206.

Entrikin, J. Lyn, The Death of Common Law, 42 Harv. J.L. & Pub. Pol'y 351–487.

EPA (Enviromental Protection Agency), California State Motor Vehicle Pollution Control Standards; Advanced Clean Car Program; Reconsideration of a Previous Withdrawal of a Waiver of Preemption; Notice of Decision, 87 F.R. 14332, 2022, https://www.federalregister.gov/documents/2022/03/14/2022-05227/california-state-motor-vehicle-pollution-control-standards-advanced-clean-car-program [perma.cc/Z42T-PGPS].

Europäische Kommission, Entscheidung 2002/2/EG der Kommission vom 20. Dezember 2001 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet, ABl. 2002 L 2, 13., 2001, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32002D0002&from=en [perma.cc/5GCD-FBFU].

–, Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endg., 2012, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:de:PDF [perma.cc/WGW8-4BHK] (zitiert als: *Europäische Kommission*, DSGVO-E(KOM), KOM(2012) 11 endg.).

–, Data Protection Day 2014: Full Speed on EU Data Protection Reform, MEMO/14/60, 2014, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_14_60 [perma.cc/2R38-UX6B].

–, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: „Aufbau einer Europäischen Datenwirtschaft", COM(2017) 9 final, 2017, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52017DC0009&from=EN [perma.cc/9RTE-UCMJ] (zitiert als: *Europäische Kommission*, Europäische Datenwirtschaft, KOM(2017) 9 endg.).

–, Durchführungsbeschluss (EU) 2019/419 der Kommission vom 23. Januar 2019 nach der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Japan im Rahmen des Gesetzes über den Schutz personenbezogener Informationen, ABl. 2019 L 76, 1, 2019, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019D0419&from=EN [perma.cc/96PH-PHHT].

–, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Eine europäische Datenstrategie, COM(2020) 66 final, 2020, https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A52020DC0066 [perma.cc/KPL5-MLZN] (zitiert als: *Europäische Kommission*, Europäische Datenstrategie, COM(2020) 66 final).

–, Commission Staff Working Document: Accompanying the Document Communication from the Commission to the European Parliament and the Council: Data protection rules as a pillar of citizens empowerment and EUs approach to digital transition – two years of application of the General Data Protection Regulation, SWD/2020/115 final, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020SC0115 [perma.cc/8577-TPJ2] (zitiert als: *Europäische Kommission*, Commission Staff Working Document: two years of application of GDPR, SWD/2020/115 final).

–, Datenschutztag: Europäische Datenschutzregeln sind Goldstandard, 2021, https://ec.europa.eu/germany/news/20210127-datenschutztag_de [perma.cc/MFP3-7WHD].

–, Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, ABl. 2021 L 199, 31, 2021, https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de&uri=CELEX%3A32021D0914 [perma.cc/S77W-QCSB].

–, Beschluss (EU) 2021/1240 der Kommission vom 13. Juli 2021 über die Übereinstimmung des EU-Portals und der EU-Datenbank für klinische Prüfungen mit Humanarzneimitteln mit den Anforderungen gemäß Artikel 82 Absatz 2 der Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates, ABl. 2021 L 275, 1., 2021, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32021D1240&from=EN [perma.cc/2WBL-UNP6].

Europäischer Datenschutzbeauftragter, Stellungnahme des Europäischen Datenschutzbeauftragten zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung unter anderem der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Richtlinie über den Schutz der Privatsphäre und elektronische Kommunikation), 2008, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:de:PDF [perma.cc/W2YQ-NXLC] (zitiert als: *Europäischer Datenschutzbeauftragter*, Stellungnahme Änderung Richtlinie 2002/58/EG).

–, Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – „A comprehensive approach on personal data protection in the European Union", 2011, https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_en.pdf [perma.cc/BCC8-LZ5T] (zitiert als: *Europäischer Datenschutzbeauftragter*, Opinion on the Communication from the Commission „A comprehensive approach on personal data protection in the European Union").

–, Stellungnahme 4/2017 zu dem Vorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, 2017, https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_de.pdf [perma.cc/V2DD-3984] (zitiert als: *Europäischer Datenschutzbeauftragter*, Stellungnahme 4/2017 Digitale-Inhalte-RL).

Europäisches Parlament, Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 2012, https://www.europarl.europa.eu/doceo/document/A-7-2013-0402_DE.html [perma.cc/CTE3-EMFC].

–, 4 column table on the General Data Protection Regulation, 2015, https://www.datenschutzgrundverordnung.eu/wp-content/uploads/2016/01/s_2014_2019_plmrep_COMMITTEES_LIBE_DV_2015_12-17_3_4column_table_EN.pdf [perma.cc/QNM5-6S5X].

–, Legislative Entschließung des Europäischen Parlaments vom 5. Juli 2022 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte) (COM(2020)0842 – C9-0419/2020 – 2020/0374(COD)), 2022, https://www.europarl.europa.eu/doceo/document/TA-9-2022-0270_DE.html [perma.cc/S4AH-9SYV] (zitiert als: *Europäisches Parlament*, Legislative Entschließung zum Gesetz über digitale Märkte (COM(2020)0842 – C9-0419/2020 – 2020/0374(COD))).

–, Legislative Entschließung des Europäischen Parlaments vom 5. Juli 2022 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD)), 2022, https://www.europarl.europa.eu/doceo/document/TA-9-2022-0269_DE.html [perma.cc/R4F2-BJA6] (zitiert als: *Europäisches Parlament*, Legislative Entschließung zum Gesetz über digitale Dienste (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD)).

Facebook. (damaliger Name von: Meta Platforms), About Facebook, An Update on Our Plans to Restrict Data Access on Facebook, 2018, https://about.fb.com/news/2018/04/restricting-data-access/ [perma.cc/MML5-LBGH].

–, California Privacy Rights Report, 2021, https://www.facebook.com/legal/policy/ccpa/transparencyreport [perma.cc/72RC-J59Z].

Faison, Alicia, TikTok Might Stop: Why the IEEPA Cannot Regulate Personal Data Privacy and the Need for a Comprehensive Solution, 16 Duke J. Const. L. & Pub. Pol'y Sidebar 115–145.

Fallon, Richard H. Jr., The Statutory Interpretation Muddle, 114 Nw. U. L. Rev. 269–334.

Fang, Jianyan, Health Data at Your Fingertips Federal Regulatory Proposals for Consumer-Generated Mobile Health Data, 4 Geo. L. Tech. Rev. 125–180.

Fang, Lee, The Intercept, Google and Facebook Are Quietly Fighting California's Privacy Rights Initiative, Emails Reveal, 2018, https://theintercept.com/2018/06/26/google-and-facebook-are-quietly-fighting-californias-privacy-rights-initiative-emails-reveal/ [perma.cc/RL82-YCMB].

Faust, Florian, Stellungnahme zu den Entwürfen eines Gesetzes zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen und eines Gesetzes zur Regelung des Verkaufs von Sachen mit digitalen Elementen und anderer Aspekte des Kaufvertrags, 2021, https://dserver.bundestag.de/btd/19/311/1931116.pdf [perma.cc/XLT5-MRQA].

Feld, Elizabeth L., The Domino Effect After the GDPR, 24 N.C. Banking Inst. 481–498.

Fennessy, Caitlin, Lawfare, A Multilateral Surveillance Accord: Setting the Table, 2021, https://www.lawfareblog.com/multilateral-surveillance-accord-setting-table [perma.cc/V7K9-23FU].

Fezer, Karl-Heinz, Repräsentatives Dateneigentum: ein zivilgesellschaftliches Bürgerrecht: Studie im Auftrag der Konrad-Adenauer-Stiftung e.V. zum Thema „Einführung eines besonderes Rechts an Daten", 2018, https://www.kas.de/c/document_library/get_file?uuid=f828a351-a2f6-11c1-b720-1aa08eaccff9&groupId=252038 [perma.cc/T6LT-PSB6].

Finanzbehörden des Bundes und der Länder, Allgemeine Informationen zur Umsetzung der datenschutzrechtlichen Vorgaben der Artikel 12 bis 14 der Datenschutz-Grundverordnung in der Steuerverwaltung, https://www.finanzamt.bayern.de/Informationen/Datenschutz/21_05_14_Allgemeines-Informationsschreiben-Steuerverwaltung.pdf [perma.cc/8ND2-R4D9].

Finnegan, Shannon, How Facebook Beat The Children's Online Privacy Protection Act: A Look into the Continued Ineffectiveness of COPPA and How to Hold Social Media Sites Accountable in the Future, 50 Seton Hall L. Rev. 827–854.

Flor, Andraya, The Impact of Schrems II: Next Steps for U. S. Data Privacy Law, 96 Notre Dame L. Rev. 2035–2058.

Forgó, Nikolaus/Helfrich, Marcus/Schneider, Jochen (Hrsg.), Betrieblicher Datenschutz: Rechtshandbuch, 3. Auflage, München 2019 (zitiert als: *Bearbeiter* in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz).

Forsheit, Tanya, Technology & Marketing Law Blog, And At the End of the Day, the CCPA Remains Very Much the Same, 2019, https://blog.ericgoldman.org/archives/2019/09/and-at-the-end-of-the-day-the-ccpa-remains-very-much-the-same-guest-blog-post.htm [perma.cc/Z9N3-B2MP].

Fowler, Geoffrey A., Washington Post, Privacy advocates battle each other over whether California's Proposition 24 better protects consumers, 04.08.2020, https://www.washingtonpost.com/politics/2020/08/04/technology-202-privacy-advocates-battle-each-other-over-whether-california-proposition-24-better-protects-consumers/ [perma.cc/K7UD-HRKQ].

Fox News Network, California Consumer Privacy Act Recordkeeping, 2021, https://www.foxnews.com/recordkeeping [perma.cc/U448-RD3T].

Franchise Tax Board, Doing business in California threshold amounts updated for 2020, 2020, https://www.ftb.ca.gov/about-ftb/newsroom/tax-news/october-2020/doing-business-in-california-threshold-amounts-updated-for-2020.html [perma.cc/RK59-S57P].

Franzen, Martin, Persönlichkeitsrecht und Datenschutz im Arbeitsverhältnis, ZfA 2019, 18–39.

–, Das Verhältnis des Auskunftsanspruchs nach DS-GVO zu personalaktenrechtlichen Einsichtsrechten nach dem BetrVG, NZA 2020, 1593–1597.

Franzen, Martin/Gallner, Inken/Oetker, Hartmut (Hrsg.), Kommentar zum europäischen Arbeitsrecht, 4. Auflage, München 2022 (zitiert als: *Bearbeiter* in: Franzen/Gallner/Oetker, Europäisches Arbeitsrecht).

Friedewald, Michael/Bieker, Felix/Obersteller, Hannah/Nebel, Maxi/Martin, Nicholas/Rost, Martin/Hansen, Marit, White Paper Datenschutz-Folgenabschätzung: Ein Werkzeug für einen besseren Datenschutz, 2021, https://www.forum-privatheit.de/wp-content/uploads/Forum_Privatheit_White_Paper_DSFA-3.pdf [perma.cc/C6EV-5L8D].

Friel, Alan L./Fath, Kyle R., Data Counsel, California Voters Approve Reworking of Landmark Consumer Privacy Law – What CCPA 2.0 Will Mean for Businesses and Consumers, 2020, https://www.bakerdatacounsel.com/ccpa/california-voters-approve-reworking-of-landmark-consumer-privacy-law-what-ccpa-2-0-will-mean-for-businesses-and-consumers/ [perma.cc/3CPX-2APA].

Friel, Alan L./Loomis, Dennis C./Serrato, Jeewon/Wang, Catrina, Data Counsel, CCPA Compliance Meets Trade Secret Protection: A Peaceful Coexistence?, 2020, https://www.bakerdatacounsel.com/ccpa/ccpa-compliance-meets-trade-secret-protection-a-peaceful-coexistence/ [perma.cc/9B5W-6APF].

Frontier, Frontier Airlines, California Privacy Policy, https://www.flyfrontier.com/legal/california-privacy-policy [perma.cc/W5PR-L8KK].

FTC (Federal Trade Commission), Privacy Online: a Report to Congress, 1998, https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [perma.cc/KW63-5J3W].

–, Protecting Consumer Privacy in an Era of Rapid Change, 2012, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [perma.cc/B4AR-8Y9A] (zitiert als: *FTC,* Protecting Consumer Privacy).

–, Federal Trade Commission, Children's Online Privacy Protection Rule: Not Just for Kids' Sites, 2013, https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-not-just-kids-sites [perma.cc/68PY-547L].

–, Amicus Brief in support of neither party, U. S. Court of Appeals 9th Circuit, Batman v. Facebook, No. 13-16819, 2014, https://www.ftc.gov/system/files/documents/amicus_briefs/jo-batman-v.facebook-inc./140321batmanfacebookamicusbrief.pdf [perma.cc/Y2NS-CJBE] (zitiert als: *FTC,* Amicus Brief Batman v. Facebook).

–, Internet of Things: Privacy & Security in a Connected World, 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [perma.cc/2PRV-9X2Y].

–, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services: Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, 2016, https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf [perma.cc/PD7W-PB2R] (zitiert als: *FTC,* Comment: Privacy of Customers of Broadband and Other Telecommunications Services).

–, Consumer Information, National Do Not Call Registry, 2019, https://www.consumer.ftc.gov/articles/0108-national-do-not-call-registry [perma.cc/2B5A-4RZJ].

–, Data To Go: An FTC Workshop on Data Portability: Transcript, 2020, https://www.ftc.gov/system/files/documents/public_events/1568699/transcript-data-portability-workshop-final.pdf [perma.cc/4RLY-UHUV].
–, Consumer Sentinel Network Data Book 2020, 2021, https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf [perma.cc/S8PY-CJ3B].
–, Federal Trade Commission Fiscal Year 2022 Congressional Budget Justification, 2021, https://www.ftc.gov/system/files/documents/reports/fy-2022-congressional-budget-justification/fy22cbj.pdf [perma.cc/LG83-YFVV].
–, Do Not Call: Data Book 2021, 2021, https://www.ftc.gov/system/files/documents/reports/national-do-not-call-registry-data-book-fiscal-year-2021/dnc_data_book_2021.pdf [perma.cc/VQX4-CXYE].
Fuller, Thomas, N.Y. Times, The Pleasure and Pain of Being California, the World's 5th-Largest Economy, 07.05.2018, https://www.nytimes.com/2018/05/07/us/california-economy-growth.html [perma.cc/NKN3-AKXN].
Fung, Archon/Graham, Mary/Weil, David, Full disclosure: the perils and promise of transparency, New York City 2007.
Funke, Michael, Dogmatik und Voraussetzungen der datenschutzrechtlichen Einwilligung im Zivilrecht, Baden-Baden 2017.
Gaglione, Gregoy S., The Equifax Data Breach: An Opportunity to Improve Consumer Protection and Cybersecurity Efforts in America, 67 Buffalo L. Rev. 1133–1212.
Gallup News Service, Facebook, Google and Internet Privacy, 2018, https://news.gallup.com/file/poll/232418/180412FacebookGoogle.pdf [perma.cc/LRQ2-EUKG].
Gassner, Angela S., The Right to Delete: Protecting Consumer Autonomy in Direct-to-Consumer Genetic Testing, 12 U.C. Irvine L. Rev. 267–324.
Gemsa, Enrico, DSGVO: USA unter Druck, Internet World Business 14/2018 22–23.
Gersen, Jacob E., Overlapping and Underlapping Jurisdiction in Administrative Law, 2006 Sup. Ct. Rev. 201–246.
Gierschmann, Sibylle (Hrsg.), Kommentar Datenschutz-Grundverordnung, Köln 2018.
Glendon, Mary A., Rights talk, New York 1991.
Glicksman, Robert L./Earnhart, Dietrich H., The Comparative Effectiveness of Government Interventions on Environmental Performance in the Chemical Industry, 26 Stan. Envtl. L.J. 317–372.
Global Privacy Control, Take Control Of Your Privacy, 2020, https://globalprivacycontrol.org/ [perma.cc/T2WV-VZHF].
–, GPC Privacy Browser Signal Now Used by Millions and Honored By Major Publishers, 2021, https://globalprivacycontrol.org/press-release/20210128 [perma.cc/RF93-XM65].
Gola, Peter, Datenschutz-Grundverordnung, 2. Auflage, München 2018.
Goldman, Eric, Internet Law: Cases & Materials, Santa Clara 2021.
–, Technology & Marketing Law Blog, CCPA Definitions Confuse the Judge in a Data Breach Case-In re Blackbaud, 2021, https://blog.ericgoldman.org/archives/2021/08/ccpa-definitions-confuse-the-judge-in-a-data-breach-case-in-re-blackbaud.htm [perma.cc/HRY4-KTG7].
Golland, Alexander, Das Kopplungsverbot in der Datenschutz-Grundverordnung, MMR 2018, 130–135.
Google, CCPA Transparency Report, 2021, https://policies.google.com/privacy/ccpa-report?hl=en [perma.cc/JW53-KNRA].

–, Ersuchen um Entfernung von Inhalten gemäß europäischem Datenschutzrecht – Google Transparenzbericht, https://transparencyreport.google.com/eu-privacy/overview?requests_over_time=country:DE&lu=delisted_urls&delisted_urls=start:1401235200000;end:1401240200000;country:DE [perma.cc/L6UW-C7BY].

Gottlieb, Daniel F./Schreiber, Mark E., Inconsistent HIPAA and CCPA De-Identification Standards Create Compliance Challenges, 37 Computer & Internet Lawyer 6–9.

Gramlich, John, Pew Research Center, Only 2% of federal criminal defendants go to trial, and most who do are found guilty, 2019, https://www.pewresearch.org/fact-tank/2019/06/11/only-2-of-federal-criminal-defendants-go-to-trial-and-most-who-do-are-found-guilty/ [perma.cc/4YVF-XJWD].

Graziadei, Michele, Comparative Law, Transplants, and Receptions, in: Reimann, Mathias/Zimmermann, Reinhard (Hrsg.), The Oxford Handbook of Comparative Law, Oxford 2019, 443–473.

Greenleaf, Graham, California's CCPA 2.0: Does the US Finally Have a Data Privacy Act?, 2020, https://papers.ssrn.com/abstract=3793435 [perma.cc/KPG3-JK3R].

Gregg, Michael A., California's Consumer Privacy Act of 2018: Why its Ambigutities May Leave Businesses in a Quandary, 60 Orange County Lawyer 32–34.

Greig, Jonathan, TechRepublic, California voters back new data privacy law beefing up CCPA, 2020, https://www.techrepublic.com/article/california-voters-back-new-data-privacy-law-beefing-up-ccpa/ [perma.cc/2ZX2-V3G4].

Groeben, von der/Schwarze/Hatje (Hrsg.), Europäisches Unionsrecht: Vertrag über die Europäische Union, Vertrag über die Arbeitsweise der Europäischen Union, Charta der Grundrechte der Europäischen Union, 7. Auflage, Baden-Baden 2015.

Grossman, Lewis, Codification and the California Mentality, 45 Hastings L.J. 617–640.

Grove, Tara L., Which Textualism? The Supreme Court 2019 Term: Comments, 134 Harv. L. Rev. 265–307.

Gumusel, Ece, Preliminary Analysis of Data Subject Right Effectiveness and Blockages in Industry, 2021, https://papers.ssrn.com/abstract=3991237 [perma.cc/V98C-54BR].

Gunst, Simon/De Ville, Ferdi, The Brussels Effect: How the GDPR Conquered Silicon Valley, Eur. Foreign Aff. Rev. 26 (2021), 437–458.

Guzzetta, Joseph W., Beyond the Basics of the California Consumer Privacy Act: Unanticipated Challenges in Complying with the New Privacy Law, 61 Orange County Lawyer 28–33.

Guzzetta, Joseph W./Manukyan, Evelina, Feature: Attorney General's Regulations Leave Businesses in a Quandary, 62 Orange County Lawyer 40–45.

Haag, Nils, Direktmarketing mit Kundendaten aus Bonusprogrammen: datenschutzrechtliche Einwilligung als Nutzungslizenz?, Wiesbaden 2010.

Hacker, Philipp, Verhaltensökonomik und Normativität: die Grenzen des Informationsmodells im Privatrecht und seine Alternativen, Tübingen 2017 (zitiert als: *Hacker*, Verhaltensökonomik und Normativität).

–, Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht, ZfPW 2019, 148–197.

–, Datenprivatrecht, Tübingen 2020.

–, Regulating the Economic Impact of Data as Counter-Performance: From the Illegality Doctrine to the Unfair Contract Terms Directive, in: Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Data as Counter-Performance – Contract Law 2.0?, Baden-Baden 2020, 47–76.

Hadar, Mary, Washington Post, Think your credit card is safe in your wallet?, 11.09.2019, https://www.washingtonpost.com/business/think-your-credit-card-is-safe-in-your-wallet-think-again/2019/09/11/05e316e4-be0e-11e9-b873-63ace636af08_story.html [perma.cc/G9LT-WUXT].

Hagan, Hayes, How to Protect Consumer Data? Leave it to the Consumer Protection Agency: FTC Rulemaking as a Path to Federal Cybersecurity Regulation, 2019 Colum. Bus. L. Rev. 735–762.

Haggin, Patience, Wall Street Journal, Facebook Won't Change Web Tracking in Response to California Privacy Law, 12.12.2019, https://www.wsj.com/articles/facebook-wont-change-web-tracking-in-response-to-california-privacy-law-11576175345 [perma.cc/KQ9L-GVXZ].

Haley, Thomas D., Data Protection in Disarray, 95 Wash. L. Rev. 1193–1251.

Halim, Valentino/Klee, Ann-Kathrin, Aktuelle Entwicklungen in den USA – Risiken der Datenschutz Compliance bei M&A-Transaktionen nach dem neuen CPRA und der DSGVO, CCZ 2021, 300–305.

Hamilton, Isobel A., Business Insider, Microsoft CEO Satya Nadella Praises GDPR, Calls for Similar Laws Around the World, 2019, https://www.businessinsider.com/satya-nadella-on-gdpr-2019-1 [perma.cc/R7YZ-GZ4A].

Hammel, Thomas, Alliant Cybersecurity, Cybersecurity Risk: What does a „reasonable" posture entail?, 2019, https://www.alliantcybersecurity.com/cybersecurity-risk-what-does-a-reasonable-posture-entail-and-who-says-so/ [perma.cc/S2CG-J88J].

Harrell, Erika, U. S. Department of Justice: Victims of Identity Theft, 2016, 2016, www.bjs.gov/content/pub/pdf/vit16.pdf [perma.cc/9X75-PSCJ].

Harris, Rebecca, Forging a Path towards Meaningful Digital Privacy: Data Monetization and the CCPA Developments in the Law, 54 Loy. L.A. L. Rev. 197–234.

Härting, Niko, Legal Tribune Online, Trilog erfolgreich, Einwilligung tot: Datenschutzgrundverordnung als Instrument der Bevormundung, 2015, https://www.lto.de/recht/hintergruende/h/datenschutzgrund-vo-dsgvo-kritik/ [perma.cc/7PT9-6LEJ].

–, Datenschutz-Grundverordnung, Köln 2016.

–, „Dateneigentum" – Schutz durch Immaterialgüterrecht?, CR 2016, 646–649.

–, Digital Goods und Datenschutz – Daten sparen oder monetarisieren?, CR 2016, 735–740.

Hartzog, Woodrow, The Public Information Fallacy, 99 Boston L.Rev. 459–522.

Hartzog, Woodrow/Richards, Neil, Privacy's Constitutional Moment and the Limits of Data Protection, 61 B.C. L. Rev. 1687–1762.

Haustein, Berthold, Möglichkeiten und Grenzen von Dateneigentum, Baden-Baden 2021.

HBDI (Hessischer Beauftragter für Datenschutz und Informationsfreiheit), Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, Häufig gestellte Fragen, 2018, https://datenschutz.hessen.de/infothek/h%C3%A4ufig-gestellte-fragen-hgf [perma.cc/9FK5-R2UL].

–, Siebenundvierzigster Tätigkeitsbericht zum Datenschutz und Erster Bericht zur Informationsfreiheit, 2019, https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2018_47_TB.pdf [perma.cc/BQU7-BG8A] (zitiert als: *HBDI,* Tätigkeitsbericht 2018).

–, Datenschutzrechtliche Aspekte bei der Nutzung von Funkwasserzählern, 2020, https://datenschutz.hessen.de/datenschutz/verkehr-versorger/datenschutzrechtliche-aspekte-bei-der-nutzung-von-funkwasserz%C3%A4hlern [perma.cc/66S4-BNRE].

Heathcoat, Gayland O. II, Regulating Pharmaceutical Marketing after Sorrell v. IMS Health Inc., 15 Quinnipiac Health L. J. 187–208.

Heckmann, Dirk/Paschke, Anne, Juris-PraxisKommentar Internetrecht, 7. Auflage, Saarbrücken 2021.

Heinzke, Philippe/Lennart, Engel, Datenverarbeitung zur Vertragserfüllung – Anforderungen und Grenzen, ZD 2020, 189–194.

Heinzke, Philippe/Storkenmaier, Julia, Die kollektive Rechtsdurchsetzung bei Verletzungen des Datenschutzrechts, CR 2021, 299–307.

Henderson, Stephen E., Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search, 55 Cath. U. L. Rev. 373–438.

Henly, Burr, Penumbra: The Roots of a Legal Metaphor, 15 Hastings Const. L.Q. 81–100.

Hennemann, Moritz, Wettbewerb der Datenschutzrechtsordnungen, RabelsZ 84 (2020), 864–895.

Hense, Peter/Fischer, Celin, Kaliforniens neues Datenschutzgesetz: Der „California Consumer Privacy Act of 2018" (CCPA), DSB 2019, 26–27.

Hertzberg, Robert, Los Angeles Daily News, Give consumers back their power over data breaches, 28.10.2020, https://www.dailynews.com/give-consumers-back-their-power-over-data-breaches-bob-hertzberg [perma.cc/JHB4-HVSM].

Hess, Hannah M., Smart Grids Need Smart Privacy Laws: Reconciling the California Consumer Privacy Act with Decentralized Electricity Models, 47 Ecology L. Currents 233–253.

Hill, Kashmir, Jezebel, How a Woman Disappears from the History Books, 2018, https://jezebel.com/how-a-woman-disappears-from-the-history-books-1828393645 [perma.cc/BQH7-39LF].

–, N.Y. Times, Facial Recognition Start-Up Mounts a First Amendment Defense, 11.08.2020, https://www.nytimes.com/2020/08/11/technology/clearview-floyd-abrams.html [perma.cc/NN6T-LMUM].

Hintze, Mike, In Defense of the Long Privacy Statement, 76 Md. L. Rev. 1044–1084.

–, Science and Privacy: Data Protection Laws and Their Impact on Research, 14 Wash. J.L. Tech. & Arts 103–137.

Hoeren, Thomas, Information als Gegenstand des Rechtsverkehrs: Prolegomena zu einer Theorie des Informationsrechts, MMR-Beil. 1998, 6–11.

–, Dateneigentum: Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486–491.

–, Big Data und Datenqualität – ein Blick auf die DS-GVO, ZD 2016, 459–463.

–, Datenbesitz statt Dateneigentum: Erste Ansätze zur Neuausrichtung der Diskussion um die Zuordnung von Daten, MMR 2019, 5–8.

–, Dateneigentum und Besitz, in: Pertot, Tereza (Hrsg.), Rechte an Daten, Tübingen 2020, 37–47.

–, Staatliche Whistleblower?, ZD 2021, 497–501.

Hoeren, Thomas/Pinelli, Stefan, Das neue kalifornische Datenschutzrecht am Maßstab der DS-GVO, MMR 2018, 711–716.

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.), Handbuch Multimedia-Recht: Rechtsfragen des elektronischen Geschäftsverkehrs, München 2021.

Hofmann, Henning, Richtlinie Digitale Inhalte – Schuldrechtliche Kontexualisierung von Daten als Wirtschaftsgut, in: Stiftung Datenschutz (Hrsg.), Dateneigentum und Datenhandel, Berlin 2019, 161–175.

Hogan & Hartson/Analysys, Preparing the next steps in regulation of electronic communications: A contribution to the review of the electronic communications regulatory framework: Final Report For the European Commission, 2006, https://op.europa.eu/en/publication-detail/-/publication/7c7d08a2-bdf5-4835-8fb3-dd776bad47ca [perma.cc/9YRV-XQ45].

Hoofnagle, Chris, Comments on the CCPA, 2019, https://hoofnagle.berkeley.edu/2019/03/08/comments-on-the-ccpa/ [perma.cc/NXM6-79VZ].

Hoofnagle, Chris J., European Commission Directorate–General Justice-Freedom and Security: Comparative Study on Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments: Country Report: United States of America, 2010, https://papers.ssrn.com/abstract=1639161 [perma.cc/M7XJ-D6QJ] (zitiert als: *Hoofnagle*, Country Report U.S. for European Commission).

–, Federal trade commission: privacy law and policy, Cambridge, UK, 2016 (zitiert als: *Hoofnagle*, FTC).

–, 10 questions about the CCPA, answered by the American law scholar Chris Hoofnagle, 2020, https://www.privacycompany.eu/knowledge-base-en/10-questions-about-the-ccpa-answered-by-the-american-law-scholar-chris-hoofnagle [perma.cc/KJ9M-S7L2] (zitiert als: *Hoofnagle*, 10 questions about the CCPA).

Hoofnagle, Chris J./King, Jennifer, Research Report: What Californians Understand About Privacy Offline, 2008, https://papers.ssrn.com/abstract=1133075 [perma.cc/WM8U-TRM7].

Hoofnagle, Chris J./Whittington, Jan, Free: Accounting for the Costs of the Internet's Most Popular Price, 61 UCLA L. Rev. 606–671.

Hornung, Gerrit/Wagner, Bernd, Anonymisierung als datenschutzrelevante Verarbeitung?, ZD 2020, 223–228.

Humerick, Matthew, The Tortoise and the Hare of International Data Privacy Law: Can the United States Catch up to Rising Global Standards, 27 Cath. U. J. L. & Tech. 77–125.

IAPP (International Association of Privacy Professionals)/EY (Ernst & Young), IAPP-EY Annual Privacy Governance Report 2021, 2021, https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf [perma.cc/D5MD-UQPK].

ICO (Information Commissioner's Office; Vereinigtes Königreich), Update report into adtech and real time bidding, 2019, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf [perma.cc/PY57-3PSN].

–, What should we consider when responding to a request?, 2021, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/what-should-we-consider-when-responding-to-a-request/ [perma.cc/9L5Z-WYDG].

–, Right to erasure, 2021, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ [perma.cc/ZR2R-X9MX].

IHK Nürnberg für Mittelfranken, Fragen an das BayLDA zur Ausgestaltung der DSGVO in der Praxis, 2021, https://www.ihk-nuernberg.de/de/Geschaeftsbereiche/Innovation-Umwelt/IuK-E-Business/Datenschutz/eu-datenschutz-grundverordnung/fragen-an-das-baylda-zur-ausgestaltung-der-dsgvo-in-der-praxis/ [perma.cc/YA6F-KQD6].

Iliadis, Vassi/Maddigan, Michael, HL Chronicle of Data Protection, California Consumer Privacy Act: The Challenge Ahead – Consumer Litigation and the CCPA: What to Expect, 2018, https://www.hldataprotection.com/2018/09/articles/consumer-privacy/california-consumer-privacy-act-the-challenge-ahead-consumer-litigation-and-the-ccpa-what-to-expect/ [perma.cc/BF6M-Z9XX].

Illman, Erin/Temple, Paul, California Consumer Privacy Act: What Companies Need to Know, 75 Business Lawyer 1637–1646.

Incorporated Society of British Advertisers, Programmatic Supply Chain Transparency Study, 2020, https://www.isba.org.uk/media/2424/executive-summary-programmatic-supply-chain-transparency-study.pdf [perma.cc/MLP4-KQ6G].

Indenhuck, Moritz/Britz, Thomas, Vom Datenschutzrecht zum Datenschuldrecht – Neue Leitlinien zur Verarbeitung personenbezogener Daten bei Online-Dienstleistungen, BB 2019, 1091–1096.

Interactive Advertising Bureau, IAB CCPA Benchmark Survey: Summary, 2020, https://www.iab.com/wp-content/uploads/2020/11/IAB_CCPA_Benchmark_Survey_Summary_2020-11.pdf [perma.cc/FQS2-3N9X].

–, IAB Europe Transparency & Consent Framework Policies, 2020, https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/ [perma.cc/UQJ7-X7NW].

Ivers, Emily A., Using State-Based Adequacy Now, National Adequacy over Time to Anticipate and Defeat Schrems III 62 2573, 62 B.C. L. Rev. 2573–2617.

Jackson, Vicki, Oral History Project: Joan Z. Bernstein, 2007, https://dcchs.org/sb_pdf/complete-oral-history-bernstein/ [perma.cc/95UX-LVG8].

Jacobs, Sharon B., The Statutory Separation of Powers, 129 Yale L. J. 378–445.

Jahnel, Dietmar (Hrsg.), Kommentar zur Datenschutz-Grundverordnung: DSGVO, Wien 2021.

Jamison, Shaun G., Creating a National Data Privacy Law for the United States, 10 Cybaris Intell. Prop. L. Rev. 1–40.

Jandt, Silke/Steidle, Roland (Hrsg.), Datenschutz im Internet, Baden-Baden 2018.

Janeček, Václav/Malgieri, Gianclaudio, Data Extra Commercium, in: Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Data as Counter-Performance – Contract Law 2.0?, Baden-Baden 2020, 95–126.

Janofsky, Adam, Wall Street Journal, Compliance Costs for California Privacy Law Pegged at $55 Billion, 01.10.2019, https://www.wsj.com/articles/compliance-costs-for-california-privacy-law-pegged-at-55-billion-11569922202 [perma.cc/Y6D6-VN6M].

Jazzar, Helen, Bringing an End to the Wiretap Act as Data Privacy Legislation, 70 Case W. Res. L. Rev. 457–487.

Jeevanjee, Kiran K., Nice Thought, Poor Execution: Why the Dormant Commerce Clause Precludes California's CCPA from Setting National Privacy Law, 70 Am. U. L. Rev. 75–133.

Jeong, Sarah, The Verge, How the judge on Oracle v. Google taught himself to code, 2017, https://www.theverge.com/2017/10/19/16503076/oracle-vs-google-judge-william-alsup-interview-waymo-uber [perma.cc/K8PS-SKFA].

Jerome, Joseph, California Privacy Law Shows Data Protection Is on the March, 33 Antitrust ABA 96–101.

Jöns, Johanna, Daten als Handelsware: zur verfassungskonformen Ausgestaltung des Datenrechts nach dem Vorbild des Immaterialgüterrechts, Baden-Baden 2019.

Jordan, Scott, Strengths and Weaknesses of Notice and Consent Requirements under the GDPR, the CCPA/CPRA, and the FCC Broadband Privacy Order, 2021, https://papers.ssrn.com/abstract=3894553 [perma.cc/NM25-SZWZ].

Judicial Council of California, 2021 Court Statistics Report: Statewide Caseload Trends: 2010–11 Through 2019–20, 2021, https://www.courts.ca.gov/documents/2021-Court-Statistics-Report.pdf [perma.cc/DH9Y-VV4T].

Kagan, Robert A., Adversarial legalism: the American way of law, Cambridge, Massachusetts 2001.

Kaminski, Margot/Snow, Jacob/Wu, Felix/Hughes, Justin, Symposium: The California Consumer Privacy Act, 54 Loy. L.A. L. Rev. 157.

Kelso, J. Clark, California's Constitutional Right to Privacy, 19 Pepp. L. Rev. 327–484.

Kemp, Tom, A Closer Look at the CPRA's Privacy Protection Agency (Plus Some Fact Checking), 2020, https://tomkemp.blog/2020/07/22/a-closer-look-at-the-cpras-privacy-protection-agency-plus-some-fact-checking/ [perma.cc/H7TS-9VTU].

Kerr, Orin S., Katz Has Only One Step: The Irrelevance of Subjective Expectations, 82 U. Chi. L. Rev. 113–134.

Keslowitz, Steven, The Transformative Nature of Blogs and Their Effects on Legal Scholarship, 2009 Cardozo L. Rev. De Novo 252–272.

Kessler, Joanna, Data Protection in the Wake of the GDPR: California's Solution for Protecting „the World's most valuable Resource", 93 S. Cal. L. Rev. 99–128.

Kibler, Cornelia, Datenschutzaufsicht im europäischen Verbund: Unabhängigkeit, Effektivität, Rechtsschutz und Legitimation, Tübingen 2021.

Kilian, Wolfgang, Personenbezogene Daten als schuldrechtliche Gegenleistung, in: Stiftung Datenschutz (Hrsg.), Dateneigentum und Datenhandel, Berlin 2019, 191–207.

Leibold, Kevin, Übersicht über den Schadensersatzanspruch nach Art. 82 DS-GVO, 2022, https://content.beck.de/ZD/1_Uebersicht_Schadensersatzanspruch-linked.pdf [perma.cc/L9YJ-S2CG].

Kim, Tae W./Routledge, Bryan, Why a Right to an Explanation of Algorithmic Decision-Making Should Exist: A Trust-Based Approach, 2020, https://papers.ssrn.com/abstract=3742049 [perma.cc/QE7T-W2MZ].

King, Jennifer/Stephan, Adriana, Regulating Privacy Dark Patterns in Practice–Drawing Inspiration from California Privacy Rights Act, 5 Geo. L. Tech. Rev. 251–276.

Kischel, Uwe, Delegation of Legislative Power to Agencies: A Comparative Analysis of United States and German Law, 46 Admin. L. Rev. 213–256.

–, Rechtsvergleichung, München 2015.

Kohler, Christian, Zum Verbot des Geoblocking im europäischen Binnenmarkt: Angriff auf die Vertragsfreiheit und Schwächung des Verbraucherschutzes?, ZEuP 2020, 253–263.

Kohne, Natasha/Reed, Michelle/Kurzweil, Rachel, Law360, Calif. Privacy Law Resembles, Transcends EU Data Regulation, 2020, https://www.law360.com/articles/1327949/calif-privacy-law-resembles-transcends-eu-data-regulation [perma.cc/8F95-QGQB].

Koloßa, Stephan, The GDPR's Extra-Territorial Scope, ZaöRV 2020, 791–818.

Korch, Stefan, Vertragsrecht in der Datenökonomie Datenprivatrecht zwischen europäischem Datenschutz und technischer Realität, ZEuP 2021, 792–820.

Korch, Stefan/Chatard, Yannick, Der datenschutzrechtliche Auskunftsanspruch in Geschäftsleiterhaftungsfällen, NZG 2020, 893–898.

Koreng, Ansgar/Lachenmann, Matthias, Formularhandbuch Datenschutzrecht, 3. Auflage, München 2021.

Kosseff, Jeff, Technology & Marketing Law Blog, Ten Reasons Why California's New Data Protection Law is Unworkable, Burdensome, and Possibly Unconstitutional, 2018, https://blog.ericgoldman.org/archives/2018/07/ten-reasons-why-californias-new-data-protection-law-is-unworkable-burdensome-and-possibly-unconstitutional-guest-blog-post.htm [perma.cc/9KQV-PVT8].

Kraft, Mary, Big Data, Little Privacy: Protecting Consumers' Data While Promoting Economic Growth Comments, 45 U. Dayton L. Rev. 97–126.

Kremer, Michael J./Conrady, Jan/Penners, Anja, Data Privacy Litigation, ZD 2021, 128–134.

Kremer, Sascha, Das Auskunftsrecht der betroffenen Person in der DSGVO, CR 2018, 560–569.

Kress, Lindsey/Trifon, Tara, JD Supra, The Murky Waters of the CCPA's Private Right of Action: Real and Perceived Ambiguities Complicating Litigation, 2020, https://www.jdsupra.com/legalnews/the-murky-waters-of-the-ccpa-s-private-56783/ [perma.cc/SFS6-89SM].

Kretschmer, Tobias, Innovation und Datenschutz – von datenbasierten Geschäftsmodellen und deren Chancen und Gefahren, Wirtschaftsdienst 2018, 459–462.

Krishnamurthy, Vivek, A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy, 114 AJIL Unbound 26–30.

Krohm, Niclas/Müller-Peltzer, Philipp, Auswirkungen des Kopplungsverbots auf die Praxistauglichkeit der Einwilligung, ZD 2017, 551–556.

Krönke, Christoph, Datenpaternalismus: Staatliche Interventionen im Online-Datenverkehr zwischen Privaten, dargestellt am Beispiel der Datenschutz-Grundverordnung, Der Staat 55 (2019), 319–351.

Krusche, Jan, Kumulation von Rechtsgrundlagen zur Datenverarbeitung, ZD 2020, 232–237.

Kühling, Jürgen/Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung/BDSG: Kommentar, 3. Auflage, München 2020.

Kühling, Jürgen/Martini, Mario, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, 448–454.

Kühling, Jürgen/Sackmann, Florian, Irrweg „Dateneigentum", ZD 2020, 24–30.
Kühling, Jürgen/Sackmann, Florian/Schneider, Hilmar, Forschungsbericht 550: Datenschutzrechtliche Dimensionen Datentreuhänder: Kurzexpertise, 2020, https://www.bmas.de/SharedDocs/Downloads/DE/Publikationen/Forschungsberichte/fb-550-pdf-datenschutzrechtliche-dimensionen-datentreuhaender.pdf [perma.cc/CZ9Y-F3S4].
Kuiu, Financial Incentives Terms, https://www.kuiu.com/pages/financial-incentives-terms [perma.cc/J34M-G2JW].
Kumar, Vineet, Making "Freemium" Work, 2014, https://hbr.org/2014/05/making-freemium-work [perma.cc/HF3U-65VU].
Kwoka, Margaret B., First-Person FOIA, 127 Yale L. J. 2204–2269.
Lalji, Nur, Featurization and the Myth of Data Empowerment, 15 Wash. J.L. Tech. & Arts 1–35.
Lancieri, Filippo, Narrowing Data Protection's Enforcement Gap, 2021, https://papers.ssrn.com/abstract=3806880 [perma.cc/TNC9-8G94].
Langhanke, Carmen, Daten als Leistung: Eine rechtsvergleichende Untersuchung zu Deutschland, Österreich und der Schweiz, Tübingen 2018.
Lapowsky, Issie, Bill Could Give Californians Unprecedented Control Over Data, 2018, https://www.wired.com/story/new-privacy-bill-could-give-californians-unprecedented-control-over-data/ [perma.cc/F9BT-UKXZ].
–, Protocol, Inside the closed-door campaigns to rewrite California privacy law, again, 2020, https://www.protocol.com/inside-california-privacy-law-redo [perma.cc/S67T-RMSQ].
Larson, Robert G. III, Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to Be Forgotten Are Incompatible with Free Speech, 18 Comm. L. & Pol'y 91–120.
Latham & Watkins, DSGVO-Schadensersatztabelle, 2022, https://de.lw.com/thoughtLeadership/Latham-DSGVO-Schadensersatztabelle [perma.cc/TSM3-P28T].
Lauricella, Alexis R./Cingel, Drew P./Beaudoin-Ryan, Leanne/Robb, Michael B./Saphir, Melissa/Wartella, Ellen, The Common Sense Census: Plugged-In Parents of Tweens and Teens, 2016, https://www.commonsensemedia.org/sites/default/files/uploads/research/common-sense-parent-census_whitepaper_new-for-web.pdf [perma.cc/5GT2-ZRTQ].
LDI NRW (Landesbeauftragte für den Datenschutz und die Informationsfreheit Nordrhein-Westfalen), 25. Datenschutzbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen für die Zeit vom 1. Januar 2019 bis zum 31. Dezember 2019, 2020, https://www.ldi.nrw.de/mainmenu_Service/submenu_Berichte/Inhalt/25_-Datenschutzbericht/25-Datenschutzbericht-LDI-NRW.pdf [perma.cc/J3TC-TJMB].
Leinemann, Franziska, Personenbezogene Daten als Entgelt: eine Untersuchung anhand schuldvertrags-, datenschutz- und kartellrechtlicher Fragestellungen, Berlin/Bern/Wien 2020.
Leistner, Matthias/Antoine, Lucie/Sagstetter, Thomas, Big Data: Rahmenbedingungen im europäischen Datenschutz- und Immaterialgüterrecht und übergreifende Reformperspektive, Tübingen 2021.
Lejeune, Mathias, California Consumer Privacy Act 2018 – erste Ansätze einer Annäherung zu Prinzipien der DSGVO in den USA, CR 2018, 569–576.
–, Die Angemessenheit drittstaatlichen Datenschutzniveaus nach dem BVerfG und die „unangemessenen" Vorgaben nach EuGH „Schrems II", CR 2020, 716–726.
–, California Privacy Rights Act (CPRA), ITRB 2021, 13–19.
–, Der California Privacy Rights Act (CPRA), PinG 2021, 25–27.
Lembke, Mark, Der datenschutzrechtliche Auskunftsanspruch im Anstellungsverhältnis, NJW 2020, 1841–1846.
Leupold, Andreas/Wiebe, Andreas/Glossner, Silke (Hrsg.), Münchener Anwaltshandbuch IT-Recht: Recht, Wirtschaft und Technik der digitalen Transformation, 4. Auflage, München 2021 (zitiert als: *Bearbeiter* in: Leupold/Wiebe/Glossner, IT-Recht).

Levi, Stuart D./Healow, Daniel, California Consumer Privacy Act: A Compliance Guide, 2019, https://iapp.org/media/pdf/resource_center/CCPA_Comliance_Guide_skadden_2019.pdf [perma.cc/WYQ7-RTP5].

Lewinski, Kai von, Die Matrix des Datenschutzes: Besichtigung und Ordnung eines Begriffsfeldes, Tübingen 2014.

LfD Niedersachsen (Landesbeauftragte für den Datenschutz Niedersachsen), 24. Tätigkeitsbericht 2017–2018, 2019, https://www.zaftda.de/tb-bundeslaender/niedersachsen/711-24-tb-lfd-niedersachsen-2017-18-3840-vom-06-06-2019/file [perma.cc/R6KZ-PKRC].

–, 25. Tätigkeitsbericht 2019, 2020, https://www.zaftda.de/tb-bundeslaender/niedersachsen/748-25-tb-lfd-niedersachen-2019-0-drs-nr-vom-03-09-2020/file [perma.cc/A5YX-PU9W].

–, LfD Niedersachsen verhängt Bußgeld über 10,4 Millionen Euro gegen notebooksbilliger.de, 2021, https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/lfd-niedersachsen-verhangt-bussgeld-uber-10-4-millionen-euro-gegen-notebooksbilliger-de-196019.html [perma.cc/XNA5-LYHQ].

–, Beschwerden zu Datenschutzverstößen und Komplexität von Verarbeitungsprozessen nehmen weiter zu, 2021, https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/taetigkeitsbericht-2020-200726.html [perma.cc/4QYU-MPV6].

LfD Sachsen-Anhalt (Landesbeauftragter für den Datenschutz Sachsen-Anhalt), XVI. Tätigkeitsbericht, 2020, https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Veroeffentlichungen/Taetigkeitsberichte/TB_16/16._Taetigkeitsbericht_Datenschutz.pdf [perma.cc/8KH7-GLLD].

LfDI Baden-Württemberg (Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg), Tätigkeitsbericht Datenschutz 2019, 2020, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/01/35.-T%C3%A4tigkeitsbericht-f%C3%BCr-den-Datenschutz-Web.pdf [perma.cc/4KHZ-4SFA].

LfDI Bremen (Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen), 3. Jahresbericht der Landesbeauftragten für Datenschutz nach der Europäischen Datenschutzgrundverordnung, 2021, https://www.datenschutz.bremen.de/sixcms/media.php/13/3.%20Jahresbericht%20Datenschutz.pdf [perma.cc/U33F-AVAZ].

LfDI Rheinland-Pfalz (Landesbeauftragter für Datenschutz und Informationsfreiheit Rheinland-Pfalz), Tätigkeitsbericht zum Datenschutz 2019, 2020, https://www.datenschutz.rlp.de/fileadmin/lfdi/Taetigkeitsberichte/ds_tb28.pdf [perma.cc/F34C-QS84].

LfDI Saarland (Landesbeauftragte für Datenschutz und Informationsfreiheit Saarland), 28. Tätigkeitsbericht Datenschutz 2019, 2020, https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/tberichte/tb28_2019.pdf [perma.cc/MJ3P-DD93].

Li, Carol, A Repeated Call for Omnibus Federal Cybersecurity Law, 94 Notre Dame L. Rev. 2211–2242.

Li, Yunge, The California Consumer Privacy Act of 2018: Toughest U.S. Data Privacy Law with Teeth, 32 Loy. Consumer L. Rev. 177–192.

Liebert, L. Tobe, Researching California Ballot Measures, 90 Law Libr. J. 27–50.

Linnea, Doan/Gomboa, Marin, The Privacy Advisor, Are there joint controllers under the CCPA?, 2019, https://iapp.org/news/a/are-there-joint-controllers-under-the-ccpa/ [perma.cc/8H2D-JW6R].

Linxweiler, Jan A., Von Goldstandards und sicheren Häfen, rescriptum 2012, 28–30.

Lissner, Britta Iris, Auftragsdatenverarbeitung nach der DSGVO – Was kommt, was bleibt?, DSRITB 2016, 401–416.

Lode, Sarah, „You Have the Data".The Writ of Habeas Data and Other Data Protection Rights: Is the United States Falling Behind?, 94 Ind. L. Rev. Supp. 41–63.

Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Data as Counter-Performance – Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V, Baden-Baden 2020.

Loosen, Maximilian, Die Rückabwicklung des Vertrages Daten gegen Leistung, Baden-Baden 2022

Los Angeles Times Editorial Board, Endorsement: Yes on Prop. 24. It's not perfect, but it would improve online privacy, 15.09.2020, https://www.latimes.com/opinion/story/2020-09-15/yes-on-proposition-24 [perma.cc/MD2Z-6KVS].

LRDP Kantor/Centre for Public Reform, Europäische Kommission: Generaldirektion Justiz, Freiheit und Sicherheit: Vergleichende Studie über verschiedene Ansätze zur Bewältigung neuer Herausforderungen für den Schutz der Privatsphäre, insbesondere aufgrund technologischer Entwicklungen, 2010, https://op.europa.eu/de/publication-detail/-/publication/9c7a02b9-ecba-405e-8d93-a1a8989f128b [perma.cc/SY7P-ZZS9].

Lucy Burns Institute, Ballotpedia, Number of ballot propositions per decade in California, 2021, https://ballotpedia.org/Number_of_ballot_propositions_per_decade_in_California [perma.cc/PL94-YKWE].

Luthi, Susannah, Politico PRO, „Functionally useless": California privacy law's big reveal falls short, 2021, https://www.politico.com/states/california/story/2021/08/05/functionally-useless-california-privacy-laws-big-reveal-falls-short-1389429 [perma.cc/A4WD-5PP7].

Lyon, Christine/Moerel, Lokke, Privacy Perspectives, Why placing a price tag on personal data may harm consumer privacy, 2020, https://iapp.org/news/a/why-placing-a-price-tag-on-personal-data-may-harm-consumer-privacy/ [perma.cc/R9PD-NK5L].

Madison, James, Federalist No. 47, 1788, https://guides.loc.gov/federalist-papers/text-41-50 [perma.cc/NFD7-SK5A].

–, Federalist No. 48, 1788, https://guides.loc.gov/federalist-papers/text-41-50 [perma.cc/LBA5-TVDV].

–, Letter to W. T. Barry. Mad. Mss., 1822, https://www.loc.gov/resource/mjm.20_0155_0159/?sp=1&st=text [perma.cc/UPX8-ATCW].

Mahieu, René, The right of access to personal data: A genealogy, 2021 TechReg 62–75.

Mahoney, Maureen, Privacy Perspectives, CPRA promises short-term consumer benefits, long-term uncertainty, 2020, https://iapp.org/news/a/cpra-promises-short-term-consumer-benefits-long-term-uncertainty/ [perma.cc/DN7B-M2ZZ].

Mahoney, Maureen/Fahs, Ginny/Marti, Don, The State of Authorized Agent Opt Outs Under the California Consumer Privacy Act, 2021, https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_AuthorizedAgentCCPA_022021_VF_.pdf [perma.cc/9ESN-3T7T].

Majetek, Michael/Mäusezahl, Steffen, Gewöhnliche vs. sensible personenbezogene Daten, ZD 2019, 551–556.

Manacourt, Vincent, Twitter, Twitter-Beitrag vom 27.10.2020, 2020, https://twitter.com/vmanancourt/status/1321120178617417728 [perma.cc/X8L3-FWSL].

–, Politico, EU privacy chief bashes lack of GDPR enforcement against Big Tech, 2022, https://www.politico.eu/article/gdpr-europe-wojciech-wiewiorowski-privacy-chief-lack-enforcement-big-tech/ [perma.cc/MTF2-SJNN].

Manheim, Karl/Kaplan, Lyric, Artifical Intelligence: Risks to Privacy and Democracy, 21 Yale J. L. & Tech. 106–188.

Mann, Kenneth, Punitive Civil Sanctions: The Middleground between Criminal and Civil Law, 101 Yale L.J. 1795–1874.

Manning, John F., The New Purposivism, 2011 Sup. Ct. Rev. 113–182.

Marcus, Daniel J., The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information, 68 Duke L.J. 555–594.

Marini, Alice/Kateifides, Alexis/Bates, Joel/Zanfir-Fortuna, Gabriela/Bae, Michelle/Gray, Stacey/Gargi, Sen/Greenberg, Jeremy/Papageorgiou, Nikolaos, Comparing privacy laws: GDPR v. CCPA, 2019, https://fpf.org/wp-content/uploads/2019/12/ComparingPrivacyLaws_GDPR_CCPA.pdf [perma.cc/EN3J-XK63].

Marotta, Veronica/Abhishek, Vibhanshu/Acquisti, Alessandro, Online Tracking and Publishers' Revenues: An Empirical Analysis, 2019, https://weis2017.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf [perma.cc/PY37-MMH7].

Marsch, Nikolaus, Das europäische Datenschutzgrundrecht, Tübingen 2018.

Martin, Brittany A., The Unregulated Underground Market for Your Data: Providing Adquate Protectons for Consumer Privacy in The Modern Era, 105 Iowa L. Rev. 865–900.

Mayer, Jonathan/Narayanan, Arvind/Stamm, Sid, Do Not Track: A Universal Third-Party Web Tracking Opt Out, 2011, https://tools.ietf.org/html/draft-mayer-do-not-track-00 [perma.cc/M5KL-ZSBZ].

McDonald, Aleecia M./Cranor, Lorrie Faith, The Cost of Reading Privacy Policies, 4 ISJLP 543–568.

McGruer, Jonathan, Emerging Privacy Legislation in the International Landscape: Strategy and Analysis for Compliance, 15 Wash. J. L. Tech. & Arts 120–159.

Meglio, Max, Embracing Insecurity: Harm Reduction through a No-Fault Approach to Consumer Data Breach Litigation Notes, 61 B.C. L. Rev. 1223–1269.

Meller-Hannich, Caroline, Sammelklagen, Gruppenklagen, Verbandsklagen – bedarf es neuer Instrumente des kollektiven Rechtsschutzes im Zivilprozess? Gutachten A zum 72. Deutschen Juristentag, München 2018.

Metzger, Axel, A Market Model for Personal Data: State of Play under the New Directive on Digital Content and Digital Services, in: Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Data as Counter-Performance – Contract Law 2.0?, Baden-Baden 2020, 23–46.

Michaels, Ralf, The Functional Method of Comparative Law, in: Reimann, Mathias/Zimmermann, Reinhard (Hrsg.), The Oxford Handbook of Comparative Law, Oxford 2019, 339–382.

Michaud, Teresa/Davis, Alexander, Privacy Perspectives, Will private litigants be able to enforce the CCPA compliance provisions?, 2020, https://iapp.org/news/a/will-private-litigants-be-able-to-enforce-the-ccpa-compliance-provisions/ [perma.cc/4W55-2Z4Z].

Michel, Saskia, Gerichtsverwaltung und Court Management in Deutschland und in den USA, Tübingen 2020.

Michl, Walther, Das Verhältnis zwischen Art. 7 und Art. 8 GRCh – zur Bestimmung der Grundlage des Datenschutzgrundrechts im EU-Recht, DuD 2017, 349–353.

Microsoft, Windows Insider, Microsoft Windows Insider Program Agreement, 2020, https://insider.windows.com [perma.cc/MAD8-878V].

Miller, Akiva, Is the California Consumer Privacy Act the Answer to Price Discrimination?, 2018, https://papers.ssrn.com/abstract=3245548 [perma.cc/KD97-BGUW].

Minzner, Max, Why Agencies Punish, 53 Wm. & Mary L. Rev. 853–917.

Miron, Jeffrey/Zwiebel, Jeffrey, Alcohol Consumption During Prohibition, 1991, https://econpapers.repec.org/paper/nbrnberwo/3675.htm [perma.cc/E3NC-7TV7].

Mischau, Lena, Daten als „Gegenleistung" im neuen Verbrauchervertragsrecht, ZEuP 2020, 335–365.

Möllers, Christoph, Gewaltengliederung, Tübingen 2005.

Monnin, Paul, A New Wave of Privacy and Consumer Laws: Should the California Consumer Privacy Act Be Implemented in North Dakota? Notes, 95 N.D. L. Rev. 345–372.

Monreal, Manfred, Der europarechtliche Rahmen für das mitgliedstaatliche Beschäftigtendatenschutzrecht: Die optionale Spezifizierungsklausel des Art. 88 DS-GVO, ZD 2022, 359–364.

Monticollo, Allaire/Reckell, Chelsea/Cividanes, Emilio, California Privacy Landscape Changes Again with Approval of New Ballot Initiative, 35 Antitrust ABA 32–37.

Mork, Marisol/Baig, Zarish/Garavaglia, Aaron, Consumer Privacy World, The California Consumer Privacy Act ("CCPA") – 2020 Year in Review, 2020, https://www.consumerprivacyworld.com/2020/12/the-california-consumer-privacy-act-ccpa-2020-year-in-review/ [perma.cc/UW44-8STJ].

MükoBGB: *Säcker, Franz Jürgen/Riexecker, Roland/Oetker, Hartmut/Limperg, Bettina (Hrsg.)*, Münchner Kommentar zum Bürgerlichen Gesetzbuch, 8. Auflage, München 2018–2020 (zitiert als: *Bearbeiter* in: MükoBGB).

Murray, Patrick J, The Adequacy Standard Under Directive 95/46/EC: Does U. S. Data Protection Meet This Standard?, 21 Fordham Int'l L. J. 932–1018.

Musielak, Hans-Joachim (Hrsg.), Zivilprozessordnung mit Gerichtsverfassungsgesetz: Kommentar, 18. Auflage, München 2021.

N. Y. Times, Privacy Policy, 2021, https://www.nytimes.com/privacy/privacy-policy [perma.cc/CXA5-EHKM].

Nägele, Thomas/Apel, Simon (Hrsg.), Beck'sche Online-Formulare IT- und Datenrecht, 8. Auflage, München 2021.

Nastasi, Gabriela, Where Vicitims of Data Breach Stand: Why the Breach of Personally Identifying Information Should Be Federally Codified as Sufficient Standing for Data Breach Cause of Action, 38 Cardozo Arts & Ent. L.J. 257–288.

National Conference of State Legislatures, Security Breach Notification Laws, 2021, https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [perma.cc/4Z54-KJ5T].

National Commission for Computing and Liberties (Frankreich), Cookie walls : la CNIL publie des premiers critères d'évaluation, 2022, https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookie-walls/la-cnil-publie-des-premiers-criteres-devaluation {perma.cc/PDL7-DXBJ.

Network Advertising Iniative, Considerations for NAI Members Regarding the Classification of Ad-tech Data Flows as "Sales" Under the CCPA: An NAI Analysis, 2019, https://www.privacysecurityacademy.com/wp-content/uploads/2019/06/NAI-Analysis-CCPA-Sales.pdf [perma.cc/MM9U-HZT8].

Neuerer, Dietmar, Handelsblatt, Datenschützer Ulrich Kelber bringt neue EU-Behörde ins Spiel, 28.01.2020, https://www.handelsblatt.com/politik/deutschland/datenschutz-verstoesse-datenschuetzer-kelber-bringt-neue-eu-behoerde-gegen-facebook-und-co-ins-spiel/25479302.html [perma.cc/N94Y-JN26].

Nguyen, David/Paczos, Marta, Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective, OECD Digital Economy Papers No. 297, 2020, https://www.oecd-ilibrary.org/science-and-technology/measuring-the-economic-value-of-data-and-cross-border-data-flows_6345995e-en [perma.cc/QFE3-K8RQ].

Nicola, Fernanda/Pollicino, Oreste, The Balkanization of Data Privacy Regulation, 2020, https://papers.ssrn.com/abstract=3824143 [perma.cc/PK4F-SQZF].

Niedersächsisches Finanzministerium, Vorbericht zum Haushaltsplan für die Haushaltsjahre 2022 und 2023, 2021, https://www.mf.niedersachsen.de/download/173919/Vorbericht.pdf [perma.cc/LXT2-YDXE].

Nietsch, Michael/Osmanovic, Daniel, Zurechnung von DSGVO-Verstößen im Unternehmensbereich, BB 2021, 1858–1865.

Nimmer, Melville B., The Right of Publicity Literary and Artistic Products and Copyright Problems, 19 Law & Contemp. Probs. 203–223.

Nizer, Louis, Right of Privacy – A Half Century's Developments, 39 Mich. L. Rev. 526–596.

noyb, News Sites: Readers need to „buy back" their own data at an exorbitant price?!, 2021, https://noyb.eu/en/news-sites-readers-need-buy-back-their-own-data-exorbitant-price [perma.cc/9H4M-RLLW].

Obama, Barack, Presidential Policy Directive -- Signals Intelligence Activities, 2014, https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [perma.cc/CP8X-6ZJ2].

Obar, Jonathan A./Oeldorf-Hirsch, Anne, The biggest lie on the Internet ignoring the privacy policies and terms of service policies of social networking services, 23 Inf. Commun. Soc. 128–147.

Oberlin, Jutta S., California Consumer Privacy Act – ein neues Datenschutzniveau für die USA? Oder gar eine »Mini-DSGVO«?, BvD-NEWS 2/2019, 47–53.

OECD (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung), Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, 2013, https://www.oecd-ilibrary.org/docserver/5k486qtxldmq-en.pdf?expires=1639755487&id=id&accname=guest&checksum=271DC11620F23A11EAB3146327B72CE2 [perma.cc/E8MF-46LE].

Ohly, Ansgar, „Volenti non fit iniuria": die Einwilligung im Privatrecht, Tübingen 2002.

Ohm, Paul, The Many Revolutions of Carpenter, 32 Harv. J.L. & Tech. 357–416.

Olsen, Robert K./Davis, John M., The California Consumer Privacy Act for Financial Institutions: Understanding the GLBA Exemption, 38 Banking & Financial Services Policy Report 1–3.

Ormerod, Peter C., A Private Enforcement Remedy for Information Misuse, 60 B.C. L. Rev. 1893–1948.

–, Privacy Qui Tam, 2022, https://papers.ssrn.com/abstract=4159932 [perma.cc/FB3J-WWSV].

Paal, Boris P./Pauly, Daniel A. (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 3. Auflage, München 2021.

Packer, Jason, Quantable, How Many of Your Users Set „Do Not Track"?, 2015, https://www.quantable.com/analytics/how-many-do-not-track/ [perma.cc/WW6C-HLXM].

Palmieri, Nicolas F. III, Who Should Regulate Data?: An Analysis of the Californa Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws, 11 Hastings Sci. & Tech. L.J. 37–59.

Pardau, Stuart L., The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States, 23 J. Tech. L. & Pol'y 68–114.

Park, Grace, The Changing Wind of Data Privacy Law: A Comparative Study of the European Union's General Data Protection Regulation and the 2018 California Consumer Privacy Act Note, 10 UC Irvine L. Rev. 1455–1490.

Parks, Andrew, Unfair Collection: Reclaiming Control of Publicly Available Personal Information from Internet Data Scrapers, 2021, https://papers.ssrn.com/abstract=3866297 [perma.cc/9AWP-H2ZS].

Partsch, Christoph/Rump, Lauritz, Auslegung der „angemessenen Geheimhaltungsmaßnahme" im Geschäftsgeheimnis-Schutzgesetz, NJW 2020, 118–121.

Pavur, James/Knerr, Casey, GDPArrrrr: Using Privacy Laws to Steal Identities, 2019, https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf [perma.cc/W67N-HT4C].

Peel, Edwin, The law of contract, 14. Auflage, New York City 2015.

Peifer, Karl-Nikolaus, Individualität im Zivilrecht: der Schutz persönlicher, gegenständlicher und wettbewerblicher Individualität im Persönlichkeitsrecht, Immaterialgüterrecht und Recht der Unternehmen, Tübingen 2001.

Perkins Coie, CCPA Litigation Tracker, 2021, https://infogram.com/1pw2wrxnyvxd6kfv27wzwxv6zgt990m23vl [perma.cc/ZD2U-UQLG].

Perlingeri, Carolina, Data as the object of a contract and contract epistemology, in: Pertot, Tereza (Hrsg.), Rechte an Daten, Tübingen 2020, 207–225.

Pernot-Leplay, Emmanuel, EU Influence on Data Privacy Laws: Is the US Approach Converging with the EU Model?, 18 Colo. Tech. L.J. 25–48.

Peukert, Christian/Bechtold, Stefan/Batikas, Michail/Kretschmer, Tobias, Working Paper: European Privacy Law and Global Markets for Data, 2020, https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/406601/CLE_WP_2020_01.pdf [perma.cc/FRV6-GJL5].

Pew Research Center, Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information, 2019, https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf [perma.cc/EDQ9-3LLQ].

Piltz, Carlo/Zwerschke, Johannes, Das Verhältnis von Art. 15 DSGVO zu 630g BGB, MedR 2021, 1070–1075.

Pimentel, Amy C./Mooney, Austin/Zhang, Wendy, A Sale, or Not a Sale? The Digital Advertising Debate, 2020, https://www.mwe.com/insights/a-sale-or-not-a-sale-the-digital-advertising-debate/ [perma.cc/FT8Z-UR4G].

Pincus, Andrew J./Nemetz, Miriam R./Volokh, Eugene, Memorandum: Invalidity Under The First Amendment Of The Restrictions On Dissemination Of Accurate, Publicly Available Information Contained In The California Consumer Privacy Act of 2018, 2019, https://fisd.net/wp-content/uploads/2021/06/Memo-re-CCPA-FINAL.pdf [perma.cc/3PEM-WNS4].

Pink, Scott, California Consumer Privacy Act Annotated, 2. Auflage, New York City 2022.

Plath, Kai-Uwe (Hrsg.), DSGVO/BDSG, 3. Auflage, Köln 2018.

Pohl, Dirk, Durchsetzungsdefizite der DSGVO? – Der schmale Grat zwischen Flexibilität und Unbestimmtheit, PinG 2017, 85–91.

Polanco, Kassandra, Trimming the Fat: The GDPR as a Model for Cleaning up Our Data Usage, 36 Touro L. Rev. 603–636.

Popova, Aleksandra, The Fine Line between Identifiers Capable of Identifying and Identifiable Information Notes, 24 Suffolk J. Trial & App. Advoc. 255–277.

Porta, Rafael La/Lopez-de-Silanes, Florencio/Shleifer, Andrei/Vishny, Robert W., Law and Finance, 106 Journal of Political Economy 1113–1155.

Privacy and Civil Liberties Oversight Board, Chairman's White Paper: Oversight of Foreign Intelligence Surveillance, 2021, https://documents.pclob.gov/prod/Documents/EventsAndPress/ec2bfc95-f111-4123-87d5-8a7827bf2fdd/Chairman's%20FISA%20White%20Paper.pdf [perma.cc/J2GX-MEEU].

Propp, Kenneth/Swire, Peter, Lawfare, After Schrems II: A Proposal to Meet the Individual Redress Challenge, 2020, https://www.lawfareblog.com/after-schrems-ii-proposal-meet-individual-redress-challenge [perma.cc/2GJU-YZ72].

Prosser, William L., Privacy, 48 Cal. L. Rev. 383–423.

PwC (Pricewaterhouse Coopers), Global Top 100 companies by market capitalisation: May 2021, https://www.pwc.com/gx/en/audit-services/publications/assets/pwc-global-top-100-companies-2021.pdf [perma.cc/2UYH-MRJZ].

RA Sushi, Notice of Financial Incentive, https://rasushi.com/privacy-statement/notice-of-financial-incentive/ [perma.cc/2UYH-MRJZ].

Radtke, Tristan, Gemeinsame Verantwortlichkeit unter der DSGVO: Unter besonderer Berücksichtigung von Internetsachverhalten, Baden-Baden 2021.

Ramirez, Edith, Letter From Chairwoman Edith Ramirez To Vera Jourova, Commissioner for Justice, Consumers and Gender Equality of the European Commission, Describing Federal Trade Commission Enforcement of the New EU-U.S. Privacy Shield Framework,

2016, https://www.ftc.gov/system/files/documents/public_statements/927423/160229ftc_privacyshieldletter.pdf [perma.cc/KS3C-FUH3].

Rauda, Christian, Gemeinsamkeiten von US Children Online Privacy Protection Act (COPPA) und DS-GVO, MMR 15–19.

Reader, Ruth, Fast Company, California's Proposition 24 is an ambitious – but controversial – privacy overhaul, 2020, https://www.fastcompany.com/90568584/california-privacy-rights-act-proposition-24 [perma.cc/KNH8-DSC8].

Redfield & Wilton Strategies, Redfield & Wilton Strategies, California Presidential, Proposition 22, and Proposition 24 Voting Intentions (19-21 September), 2020, https://redfieldandwiltonstrategies.com/california-presidential-proposition-22-and-proposition-24-voting-intentions-19-21-september/ [perma.cc/79C3-NVE2].

Regan, Priscilla M., Legislating privacy: technology, social values, and public policy, Chapel Hill, North Carolina 1995.

Reidenberg, Joel R., Privacy in the Information Economy: A Fortress or Frontier for Individual Rights, 44 Fed. Comm. L.J. 195–244.

–, Setting Standards for Fair Information Practice in the U. S. Private Sector, 80 Iowa L. Rev. 497–552.

Reimann, Mathias/Zimmermann, Reinhard (Hrsg.), The Oxford Handbook of Comparative Law, Oxford 2019.

Reinholtsen, Dale A., The Role of California's Attorney General and District Attorneys in Protecting the Consumer, 4 U.C. Davis L. Rev. 35–56.

Resnick, Scott, Easing the Burdens of a Patchwork Approach to Data Privacy Regulation in Favor of a Singular Comprehensive International Solution – The International Data Privacy Agreement Notes, 46 Brook. J. Int'l L. 277–310.

Richards, Neil M., Why Data Privacy Law Is (Mostly) Constitutional, 56 Wm. & Mary L. Rev. 1501–1534.

Richards, Neil M./Hartzog, Woodrow, Taking Trust Seriously in Privacy Law, 19 Stan. Tech. L. Rev. 431–472.

Richards, Neil M./Solove, Daniel J., Prosser's Privacy Law: A Mixed Legacy Prosser's Privacy at 50, 98 Cal. L. Rev. 1887–1924.

Richter, Heiko, Europäisches Datenprivatrecht: Lehren aus dem Kommissionsvorschlag für eine „Verordnung über europäische Daten-Governance", ZEuP 2021, 634–667.

Richter, Heiko/Hilty, Reto M., Die Hydra des Dateneigentums – eine methodische Betrachtung, in: Stiftung Datenschutz (Hrsg.), Dateneigentum und Datenhandel, Berlin 2019, 241–259.

Riechert, Anne, Data as a Counter-Performance, in: Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Data as Counter-Performance – Contract Law 2.0?, Baden-Baden 2020, 267–278.

Riesenhuber, Karl (Hrsg.), Europäische Methodenlehre, 4. Auflage, Boston 2021.

Rinehart, Liz Clark, Clapper v. Amnesty International USA: Allowing the FISA Amendments Act of 2008 to Turn Incidentally into Certainly, 73 Md. L. Rev. 1018–1048.

Rippy, Sarah, The Privacy Advisor, Top-10 operational impacts of the CPRA: Part 5 – Notice obligations and right to opt out, 2021, https://iapp.org/news/a/top-10-operational-impacts-of-the-cpra-notice-obligations-and-the-right-to-opt-out/ [perma.cc/UD5N-CP67].

Rix, Ashley, How Data Privacy Regulations Affect Public Corporations That Profit From Consumers' Data During an Ongoing Pandemic, 2021, https://papers.ssrn.com/abstract=3896785 [perma.cc/DGF2-LYBH].

Robinson, Dallin, Click Here to Sue Everybody: Cutting the Gordian Knot of the Internet of Things with Class Action Litigation, 26 Rich. J.L. & Tech. 1–83.

Rogers, Kaleigh/Paul, Kari, Vice, There's a Problem in the Silk Road Trial: the Jury Doesn't Get the Internet, 2015, https://www.vice.com/en/article/xyw77q/theres-a-problem-in-the-silk-road-trial-the-jury-doesnt-get-the-internet [perma.cc/PU3M-4Z2P].

Rogosch, Patricia, Die Einwilligung im Datenschutzrecht, Baden-Baden 2013.

Roland-Holst, David/Evans, Samuel/Behnke, Drew/Neal, Samuel/Frölund, Liam/Xiao, Yao, Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations, 2019, https://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf [perma.cc/6UVV-3RB3].

Romanosky, Sasha/Hoffman, David/Acquisti, Alessandro, Empirical Analysis of Data Breach Litigation, 11 Empirical Legal Stud. 74–104.

Romm, Tony, Washington Post, California adopted the country's first major consumer privacy law. Now, Silicon Valley is trying to rewrite it., 03.09.2019, https://www.washingtonpost.com/technology/2019/09/02/california-adopted-countrys-first-major-consumer-privacy-law-now-silicon-valley-is-trying-rewrite-it/ [perma.cc/SHB4-XTZG].

Rose, Blaire, The Commodification of Personal Data and the Road to Consumer Autonomy Through the CCPA, 15 Brook. J. Corp. Fin. & Com. L. 521–542.

Rosen, Jeffrey, The Right to Be Forgotten, 64 Stan. L. Rev. Online 88–92.

Rosenberg, Matthew/Confessore, Nicholas/Cadwalladr, Carole, N.Y. Times, How Trump Consultants Exploited the Facebook Data of Millions, 17.03.2018, https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html [perma.cc/Q4WD-6NBM].

Rosenkranz, Frank, Spezifische Vorschriften zu Verträgen über die Bereitstellung digitaler Produkte im BGB Kommentar zum Regierungsentwurf des BMJV zu einem Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, ZUM 2021, 195–210.

Ross, Mary S., Privacy Perspectives, The CCPA needs clarification, 2019, https://iapp.org/news/a/mary-stone-ross-the-ccpa-needs-clarification/ [perma.cc/XP48-2DAQ].

Roßnagel, Alexander, Kein „Verbotsprinzip" und kein „Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht, NJW 2019, 1–5.

–, Datenlöschung und Anonymisierung, ZD 2021, 188–192.

Roßnagel, Alexander/Geminn, Christian, Datenschutz-Grundverordnung verbessern: Änderungsvorschläge aus Verbrauchersicht, Baden-Baden 2020.

Rothchild, John A., Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else), 66 Clev. St. L. Rev. 559–648.

Röthemeyer, Ltd MinR Peter, Die neue Verbandsklagen-Richtlinie, VuR 2021, 43–53.

Röthemeyer, Peter, Befugnis zur Musterfeststellungsklage: Der Narrativ der Klageindustrie, seine Folgen und Überlegungen zur Überwindung, VuR 2020, 130–142.

Rubinstein, Ira S./Hartzog, Woodrow, Anonymization and Risk, 91 Wash. L. Rev. 703–760.

Rubinstein, Jacob, The Privacy Advisor, A close-up on deidentified data under CCPA, 2019, https://iapp.org/news/a/a-close-up-on-de-identified-data-under-the-ccpa/ [perma.cc/PT23-YP5J].

Rustad, Michael L./Koenig, Thomas H., Towards a Global Data Privacy Standard, 71 Fla. L. Rev. 365–454.

Ryle, Patrick/Bueltel, Brett/Walker, A. Kelly/Gabrini, Carl/McKnight, Mark, The Impact of the Facebook Court Order & CCPA 2020: Helping Businesses and Accountants Meet the Challenge of the New Era of Privacy Compliance, 21 Journal of Accounting, Ethics & Public Policy 247–262.

SächsDSB (Sächsischer Datenschutzbeauftragter), Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten: Berichtszeitraum: 1. Januar 2019 bis 31. Dezember 2019, 2020, https://

www.saechsdsb.de/images/stories/sdb_inhalt/oeb/taetigkeitsberichte/Ttigkeitsbericht_2019_final.pdf [perma.cc/6V4A-PMQY] (zitiert als: *SächsDSB,* Tätigkeitsbericht 2019).

–, Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten: Berichtszeitraum: 1. Januar bis 31. Dezember 2020, 2021, https://www.saechsdsb.de/images/stories/sdb_inhalt/oeb/taetigkeitsberichte/SDB_Ttigkeitsbericht_2020.pdf [perma.cc/4SME-VKUK] (zitiert als: *SächsDSB,* Tätigkeitsbericht 2020).

Salzmann, Miriam/Schindler, Stephan, Der internationale Siegeszug der größten Katastrophe des 21. Jahrhunderts?, ZD-Aktuell 06293.

San Francisco Chronicle Editorial Board, San Francisco Chronicle, Chronicle recommends: Vote no on Prop. 24, a flawed privacy initiative, 26.09.2020, https://www.sfchronicle.com/opinion/editorials/article/Chronicle-recommends-Vote-no-on-Prop-24-a-15598736.php [perma.cc/J386-P4W9].

Sattler, Andreas, From Personality to Property?, in: Bakhoum, Mor/Conde Gallego, Beatriz/Mackenrodt, Mark-Oliver/Surblytė-Namavičienė, Gintarė (Hrsg.), Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?, Berlin/Heidelberg 2018, 27–54.

–, Personenbezug als Hindernis des Datenhandels, in: Pertot, Tereza (Hrsg.), Rechte an Daten, Tübingen 2020, 49–85.

–, Neues EU-Vertragsrecht für digitale Güter, CR 2020, 145–154.

–, Urheber- und datenschutzrechtliche Konflikte im neuen Vertragsrecht für digitale Produkte, NJW 2020, 3623–3629.

–, Autonomy or Heteronomy – Proposal for a Two-Tier Interpretation of Art 6 GDPR, in: Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Data as Counter-Performance – Contract Law 2.0?, Baden-Baden 2020, 225–252.

Schaffland, Hans-Jürgen/Wiltfang, Noeme (Hrsg.), Datenschutz-Grundverordnung (DS-GVO)/Bundesdatenschutzgesetz (BDSG): Kommentar, Stand: EL 12/2021, Berlin .

Schantz, Peter, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841–1847.

Schantz, Peter/Wolff, Heinrich Amadeus, Das neue Datenschutzrecht: Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, München 2017.

Schapiro, Zachary, Data Protection in the Digital Economy: Legislating in Light of Sorrell v. IMS Health Inc., 63 Boston College Law Review 2007–2050.

Schmedt, Michael, Telematikinfrastruktur: Zugang mit Identitätsdiebstahl, DÄ 2020, 7.

Schmidt, Kirsten J., Datenschutz als Vermögensrecht, Wiesbaden 2020.

Schmidt-Kessel, Martin, Right to Withdraw Consent to Data Processing – The Effect on the Contract, in: Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Data as Counter-Performance – Contract Law 2.0?, Baden-Baden 2020, 129–146.

Schneider, Jana/Schindler, Stephan, Videoüberwachung als Verarbeitung besonderer Kategorien personenbezogener Daten, ZD 2018, 463–469.

Schneider, Jochen, Schließt Art. 9 DS-GVO die Zulässigkeit der Verarbeitung bei Big Data aus?, ZD 2017, 303–308.

Schrader, Julius, Datenschutz Minderjähriger: Geschäftsfähigkeit als Grundlage der Einwilligungsfähigkeit im Datenrecht, Tübingen 2021.

Schreiner, Pirmin E., Die Vermessung des Mietrechts, Tübingen 2021.

Schröder, Markus, „Sale of Data" nach dem California Consumer Privacy Act, DSB 2021, 15–17.

Schubert, Christoph, Deutscher AnwaltSpiegel, Drohen amerikanische Verhältnisse? Im Blickpunkt: Die EU-Verbandsklage kommt, 2020, https://www.deutscheranwaltspiegel.de/anwaltspiegel/verbandssanktionengesetz/drohen-amerikanische-verhaeltnisse-20605/ [perma.cc/S2VM-RATN].

Schur, Nico B., Die Lizenzierung von Daten: Einordnung, Grenzen und Möglichkeiten von vertraglichen Zugangs- und Datennutzungsrechten in der digitalen Ökonomie, Tübingen 2020.

Schwartmann, Rolf/Jaspers, Andreas/Thüsing, Gregor/Kugelmann, Dieter (Hrsg.), DS-GVO/BDSG: Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2. Auflage, Heidelberg 2020.

Schwartz, Adam/Crocker, Andrew/Lynch, Jennifer, ACLU v. Clearview: Brief of Amicus Electronic Frontier Foundatin in Opposition to Defendant's Motion to Dismiss, 2020, https://www.eff.org/files/2020/11/05/2020-11-02_-_aclu_v_clearview_il_-_effs_amicus_brief_-_w_file_stamp.pdf [perma.cc/VBZ5-UE6L].

Schwartz, Adam/Tien, Lee/McSherry, Corynne, Electronic Frontier Foundation, How to Improve the California Consumer Privacy Act of 2018, 2018, https://www.eff.org/deeplinks/2018/08/how-improve-california-consumer-privacy-act-2018 [perma.cc/ND5U-R2LP].

Schwartz, Paul M., The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination, 37 Am. J. Comp. L. 675.

–, Preemption and Privacy, 118 Yale L. J. 902–947.

–, Global Data Privacy: The EU Way, 94 N.Y.U. L. Rev. 771–818.

Schwartz, Paul M./Peifer, Karl-Nikolaus, Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?, 98 Cal. L. Rev. 1925–1988.

Scott, Alexandra/Canter, Elizabeth/Tonsager, Lindsey, The Privacy Advisor, „Sale" under CCPA may not be as scary as you think, 2019, https://iapp.org/news/a/sale-under-the-ccpa-may-not-be-as-scary-as-you-think/ [perma.cc/MLF3-PUTJ].

Selmayr, Martin, Europa wagt die digitale Selbstbehauptung, ZD 2018, 197–198.

Shah, Bastian, Commercial Free Speech Constraints on Data Privacy Statutes after Sorrell v. IMS Health, 54 Colum. J.L. & Soc. Probs. 93–130.

Shatz, Sanford/Chylik, Susan E., The California Consumer Privacy Act of 2018: A Sea Change in the Protection of California Consumers' Personal Information, 75 Bus. Law. 1917–1924.

Shelton Leipzig, Dominique, Implementing the CCPA: A Guide for Global Business, Portsmouth 2019.

Sheppard, Stephen, The Wolters Kluwer Bouvier Law Dictionary: Desk Edition, New York City 2012.

Short, James E/Todd, Steve, Many businesses don't yet know the answer to that question. But going forward, companies will need to develop greater expertise at valuing their data assets., MITSloan 17–19.

Shubet, Aaron, Not All Those Who Wander Are Lost: The Pathway towards American Data Privacy Law, 48 Hofstra L. Rev. 835–872.

Siems, Mathias, Statistische Rechtsvergleichung, RabelsZ (72) 2008, 354–390.

Silvers, Robert P./Decker, Danielle D./Dayanim, Behnam/Smith, Sherrese M./Philips, John P., Steps You Can Take Now To Reduce The Risk Of Litigation Under The New California Consumer Privacy Act, 2019, http://www.paulhastings.com/publications-items/details/?id=8c332e6d-2334-6428-811c-ff00004cbded [perma.cc/BK5Q-MDV2].

Simitis, Spiros, Datenschutz – Rückschritt oder Neubeginn?, NJW 1998, 2473–2479.

Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hrsg.), Datenschutzrecht: DSGVO mit BDSG, Baden-Baden 2019.

Simon, Amy/Whaley, John, Summary of Key Findings from California Privacy Survey, 2019, https://assets-global.website-files.com/5aa18a452485b60001c301de/5da7a66278dd751306184114_MEMO%3A%20Key%20Findings%20CA%20Privacy%20Online%20Survey%20October%202019.pdf [perma.cc/E98Q-B58J].

Slicktext, One Year After Cambridge Analytica, Survey Reveals Strong Consumer Privacy Fears Remain, 2019, https://www.slicktext.com/blog/2019/02/survey-consumer-privacy-fears-after-cambridge-analytica/ [perma.cc/H3LJ-VA6S].

Smith, Nicole, Protecting Consumers in the Age of the Internet of Things Notes, 93 St. John's L. Rev. 851–882.

Snow, Jacob/Conley, Chris, ACLU Northern California, Californians Should Vote No on Prop 24, 2020, https://www.aclunc.org/blog/californians-should-vote-no-prop-24 [perma.cc/7ZYG-T68M].

Solove, Daniel J., A Taxonomy of Privacy, 154 U. Pa. L. Rev. 477–564.

–, Introduction: Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880–1903.

–, The Myth of the Privacy Paradox, 89 Geo. Wash. L. Rev. 1–51.

Solove, Daniel J./Antonipillai, Justin, CPRA and Its Potential Effects A Talk with Alastair Mactaggart, Justin Antonipillai, and Daniel Solove, 2020, https://www.youtube.com/watch?v=PqY472vCeM4 [perma.cc/BH3Z-49EG].

Solove, Daniel J./Citron, Danielle K., Risk and Anxiety: A Theory of Data-Breach Harms, 96 Tex. L. Rev. 737–786.

–, Standing and Privacy Harms: A Critique of TransUnion v. Ramirez, 101 B. U. L. Rev. Online 62–71.

Solove, Daniel J./Hartzog, Woodrow, The FTC and the New Common Law of Privacy, 114 Colum. L. Rev. 583–676.

Solove, Daniel J./Schwartz, Paul M., Information privacy law, 6. Auflage, New York City 2018.

–, ALI Data Privacy: Overview and Black Letter Text, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3457563 [perma.cc/N63V-RDMF].

Soltani, Ashkan, Twitter, Twitter-Beitrag vom 24.07.2020, 2020, https://twitter.com/ashk4n/status/1286687231101423616 [perma.cc/TSU2-XQS7].

Solum, Lawrence B., Blogging and the Transformation of Legal Scholarship Bloggership: How Blogs Are Transforming Legal Scholarship, 84 Wash. U. L. Rev. 1071–1088.

Soubouti, Fara, Data Privacy and the Financial Services Industry: A Federal Approach to Consumer Protection, 24 N.C. Banking Inst. 527–551.

Southwell, Alexander H./Bergsieker, Ryan T./Gaedt-Sheckter, Cassandra L./Waldmann, Frances A., Virginia Passes Comprehensive Privacy Law, 2021, https://www.gibsondunn.com/wp-content/uploads/2021/03/virginia-passes-comprehensive-privacy-law.pdf [perma.cc/T3U9-5EZU].

SPD/Bündnis 90/Die Grünen/FDP, Koalitionsvertrag 2021–2025: Mehr Fortschritt wagen: Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, 2021, https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf [perma.cc/27X7-SP68].

Specht, Louisa (damaliger Name von: *Specht-Riemenschneider, Louisa),* Konsequenzen der Ökonomisierung informationeller Selbstbestimmung: die zivilrechtliche Erfassung des Datenhandels, Köln 2012 (zitiert als: *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung).

–, Daten als Gegenleistung – Verlangt die Digitalisierung nach einem neuen Vertragstypus?, JZ 2017, 763–770.

Specht, Louisa/Mantz, Reto (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht: Bereichsspezifischer Datenschutz in Privatwirtschaft und öffentlichem Sektor, München 2019.

Specht-Riemenschneider, Louisa, Data access rights – A comparative perspective, in: Bundesministerium der Justiz und für Verbraucherschutz/Max-Planck-Institut für Innovation und Wettbewerb (Hrsg.), Data access, consumer interests and public welfare, Baden-Baden 2021, 401–438.

Specht-Riemenschneider, Louisa/Blankertz, Aline/Sierek, Pascal/Schneider, Ruben/Knapp, Jakob/Henne, Theresa, Die Datentreuhand, MMR-Beil. 2021, 25–48.

Specht-Riemenschneider, Louisa/Werry, Nikola/Werry, Susanne (Hrsg.), Datenrecht in der Digitalisierung, Berlin 2020.

Spiekermann, Sarah/Korunovska, Jana, Towards a value theory for personal data, Journal of Information Technology 72 (2017), 62–84.

Spies, Axel, Die DS-GVO – mit einem Blick von außen, ZD 2018, 501–502.

–, USA: Neues kalifornisches Datenschutzgesetz CCPA als Vorreiter, ZD-Aktuell 2018, 04318.

Spindler, Gerald, Ausgewählte Rechtsfragen der Umsetzung der digitalen Inhalte-Richtlinie in das BGB, MMR 2021, 528–533.

–, Umsetzung der Richtlinie über digitale Inhalte in das BGB, MMR 2021, 451–457.

Spindler, Gerald/Schuster, Fabian, Recht der elektronischen Medien: Kommentar, 4. Auflage, München 2019.

Spivak, Russell, Too Big a Fish in the Digital Pond? The California Consumer Privacy Act and the Dormant Commerce Clause, 88 U. Cin. L. Rev. 475–513.

Stadler, Astrid, Kollektiver Rechtsschutz – Chancen und Risiken, ZHR 2018, 623–656.

Statistisches Bundesamt, Bevölkerung mit Migrationshintergrund – Ergebnisse des Mikrozensus 2020 – Fachserie 1 Reihe 2.2 - 2020 (Erstergebnisse), 2020, https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bevoelkerung/Migration-Integration/Publikationen/Downloads-Migration/migrationshintergrund-2010220207004.html [perma.cc/JLU5-NZ52].

Statt, Nick, The Verge, Apple updates Safari's anti-tracking tech with full third-party cookie blocking, 2020, https://www.theverge.com/2020/3/24/21192830/apple-safari-intelligent-tracking-privacy-full-third-party-cookie-blocking [perma.cc/HD9P-WF3M].

Staudenmayer, Dirk, Die Richtlinien zu den digitalen Verträgen, ZEuP 2019, 663–694.

Stein, Eric, Uses, Misuses--and Nonuses of Comparative Law, 72 Nw. U. L. Rev. 198–216.

Stein, Matthew/Lisy, Christopher, Privacy & Data Security Law News, Figuring Out if You Are 'Doing Business' in California Under the CCPA, 2020, https://news.bloomberglaw.com/privacy-and-data-security/insight-figuring-out-if-you-are-doing-business-in-california-under-the-ccpa [perma.cc/7E8R-RSL2].

Stenbeck, Magnus/Fält, Sonja E./Reichel, Jane, Swedish Law on Personal Data in Biobank Research: Permissible But Complex, in: Slokenberga, Santa/Tzortzatou, Olga/Reichel, Jane (Hrsg.), GDPR and Biobanking: Individual Rights, Public Interest and Research Regulation across Europe, Cham 2021, 379–394.

Stiftung Datenschutz (Hrsg.), Dateneigentum und Datenhandel, Berlin 2019.

Stine, Molly McGinnis/Kilian, Sean, Deletion Completion Under the CCPA, 37 Computer & Internet Lawyer 3–5.

Streinz, Rudolf/Michl, Walther, Die Drittwirkung des europäischen Datenschutzgrundrechts (Art. 8 GRCh) im deutschen Privatrecht, EuZW 2011, 384–388.

Streinz, Thomas, The Evolution of European Data Law, in: Craig, Paul/Búrca, Gráinne de (Hrsg.), The Evolution of EU Law, 3. Auflage, Oxford 2021, 902–936.

Stroock, California's Unfair Competition Law and Consumers Legal Remedies Act 2021 Annual Overview, 2021, https://www.stroock.com/uploads/2021-UCL-Article.pdf [perma.cc/6LTX-5TUN].

Stuenkel, Brian, Personal Information and Artificial Intelligence: Website Scraping and the California Consumer Privacy Act Notes, 19 Colo. Tech. L.J. 429–460.

Stürmer, Verena, Löschen durch Anonymisieren?, ZD 2020, 626–631.

Stürner, Rolf, Privatautonomie und Wettbewerb unter der Hegemonie der angloamerikanischen Rechtskultur?, AcP 210 (2010), 105–155.

Sweeney, Latanya, Simple Demographics Often Identify People Uniquely, 2000, https://dataprivacylab.org/projects/identifiability/paper1.pdf [perma.cc/C8NT-P6HL].

Swisher, Kara, Vox Recode, Interview with Nancy Pelosi, 2019, https://www.vox.com/2019/4/12/18307957/nancy-pelosi-donald-trump-twitter-tweet-cheap-freak-presidency-kara-swisher-decode-podcast-interview [perma.cc/S9EM-JMV6].

Sydow, Gernot (Hrsg.), Europäische Datenschutzgrundverordnung, 2. Auflage, Baden-Baden 2018.

Taeger, Jürgen/Gabel, Detlev (Hrsg.), DSGVO – BDSG, 4. Auflage, Frankfurt am Main 2022.

Tam, Jonathan, Law.com, Experts Weigh in on California Privacy Rights Act Changes, 08.12.2021, www.law.com/therecorder/2021/12/08/experts-weigh-in-on-california-privacy-rights-act-changes/ [perma.cc/3EP6-DYG7].

Tavanti, Pascal, Datenverarbeitung zu Werbezwecken nach der Datenschutz-Grundverordnung (Teil 2), RDV 2016, 13.

Taylor, Charlie, The Irish Times, Data Protection Commission 'disappointed' at budget allocation, 09.10.2019, https://www.irishtimes.com/business/technology/data-protection-commission-disappointed-at-budget-allocation-1.4045248 [perma.cc/YTD3-Y3BH].

Teme, Omar, Privacy Perspectives, With Ramirez, FTC became the Federal Technology Commission, 2017, https://iapp.org/news/a/with-ramirez-ftc-became-the-federal-technology-commission/ [perma.cc/4XS5-WEE9].

Terry, Jana, Texas Businesses Take Heed: Five Misconceptions about the California Consumer Privacy Act Debunked, 83 Tex. B. J 148–148.

Thiel, Barbara, Zusammenarbeit der Datenschutzaufsicht auf europäischer Ebene, ZD 2021, 467–470.

Thomas, Lauren/Hoofnagle, Chris Jay, Exploring Information Sharing through California's „Shine the Light" Law, 2009, https://papers.ssrn.com/abstract=1448365 [perma.cc/E757-X4TJ].

Thomson, Hunter B., Whither Central Hudson – Commercial Speech in the Wake of Sorrell v. IMS Health, 47 Colum. J.L. & Soc. Probs. 171–207.

Thüsing, Gregor/Rombey, Sebastian, Anonymisierung an sich ist keine rechtfertigungsbedürftige Datenverarbeitung, ZD 2021, 548–553.

Tien, Lee/Schwartz, Adam/Tskukayama, Hayley, Electronic Frontier Foundation, Why EFF Doesn't Support California Proposition 24, 2020, https://www.eff.org/de/deeplinks/2020/07/why-eff-doesnt-support-cal-prop-24 [perma.cc/9VJP-78DU].

TLfDI (Thüringer Landesbeauftragter für Datenschutz und Informationsfreiheit), 2. Tätigkeitsbericht zum Datenschutz nach der DS-GVO 2019, 2020, https://www.zaftda.de/tb-bundeslaender/thueringen/landesdatenschutzbeauftragter-9/749-2-tb-dsgvo-lfd-thueringen-2019-0-ds-nr-vom-22-10-2020/file [perma.cc/XP5P-63CV].

Tokson, Matthew, The Emerging Principles of Fourth Amendment Privacy, 88 Geo. Wash. L. Rev. 1–75.

Tönnesmann, Von Jens, Die Zeit Nr. 37/2016, Das Produkt bist du, 01.09.2016, https://www.zeit.de/2016/37/whatsapp-facebook-daten-individualisierte-werbung-schutz [perma.cc/5EU4-862F].

Tsukayama, Hayley, Electronic Frontier Foundation, Why Getting Paid for Your Data Is a Bad Deal, 2020, https://www.eff.org/de/deeplinks/2020/10/why-getting-paid-your-data-bad-deal [perma.cc/7QED-MPUN].

Tutt, Andrew, On the Invalidation of Terms in Contracts of Adhesion, 30 Yale J. on Reg. 439–474.

Udeshi, Nadia, Saving Small Business from the Big Impact of Data Breach: A Tiered Federal Approach to Data Protection Law Notes, 14 Brook. J. Corp. Fin. & Com. L. 389–414.

Uniform Law Commission, Uniform Personal Data Protection Act, 2021, https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=009e3927-eafa-3851-1c02-3a05f5891947&forceDialog=0 [perma.cc/P9SL-SLR2].

Unseld, Florian, Die Kommerzialisierung personenbezogener Daten, München 2010.

Urgoiti, Lucas, The Video Privacy Protection Act and Consumer Data: Are You Pflugged In?, 53 U.C. Davis L. Rev. 1689–1737.

Urness, Devin, The Standing of Article III Standing for Data Breach Litigants: Proposing a Judicial and a Legislative Solution, 73 Vand. L. Rev. 1517–1560.

Ursul, Mallory, The States' Role in Data Privacy: California Consumer Privacy Act versus Dormant Commerce Clause, 52 Suffolk U. L. Rev. 577–602.

U. S. Census Bureau, 2017 SUSB Annual Datasets by Establishment Industry, 2020, https://www.census.gov/data/datasets/2017/econ/susb/2017-susb.html [perma.cc/3QJL-WXSR].

–, The United States Census Bureau, 2020 Census Apportionment Results, 2021, https://www.census.gov/data/tables/2020/dec/2020-apportionment-data.html [perma.cc/VVP2-VFD7].

–, 2020 American Community Survey 1-Year Experimental Data Tables: Table XK201601. Household Language, 2021, https://www.census.gov/programs-surveys/acs/data/experimental-data/1-year.html [perma.cc/Z6RG-QU5D] (zitiert als: *U. S. Census Bureau*, 2020 American Community Survey Household Language Table).

U. S. Chamber Institute for Legal Reform, 2019 Lawsuit Climate Survey: Ranking the States: A Survey of the Fairness and Reasonableness of State Liability Systems, 2019, https://instituteforlegalreform.com/wp-content/uploads/2020/10/2019_Harris_Poll_State_Lawsuit_Climate_Ranking_the_States.pdf [perma.cc/YJ6P-ZRFC].

U. S. Department of Commerce, Information on U. S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U. S. Data Transfers after Schrems II: White Paper, 2019, https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF [perma.cc/7KYN-637N].

U. S. Department of Health, Education & Welfare, Records, Computers and the Rights of Citizens, 1973, https://www.justice.gov/opcl/docs/rec-com-rights.pdf [perma.cc/R8ZM-44P7].

U. S. Senate, Committee on Government Operations/U. S. House of Representatives, Committee on Government Operations, Legislative History of the Privacy Act of 1974, 1974, https://www.loc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf [perma.cc/J9ES-B8VV].

Vagts, Detlev, Comparative company law – The new wave, in: Schweizer, Rainer J./Druey, Jean Nicolas (Hrsg.), Festschrift für Jean Nicolas Druey zum 65. Geburtstag, Zürich 2002, 595–605.

Valdetero, Jena/Zetoony, David/Maciejewski, Andrea, Data Breach Litigation Report: 2019 Edition, 2019, https://www.bclplaw.com/images/content/1/6/v6/163774/2019-Litigation-Report.pdf [perma.cc/NY4Q-U2LL].

Veil, Winfried, Die Datenschutz-Grundverordnung: des Kaisers neue Kleider, NVwZ 2018, 686–696.

–, Einwilligung oder berechtigtes Interesse? – Datenverarbeitung zwischen Skylla und Charybdis, NJW 2018, 3337–3344.

Verbraucherzentrale Bundesverband, Jahresbericht 2019, 2020, https://www.vzbv.de/publikationen/vzbv-legt-jahresbericht-2019-vor [perma.cc/A8CP-RX8X].

Vibbert, Jami Mills/Perkins, Nancy L./Samson, Anthony J./Raylesberg, Jason T., Arnold & Porter, Voters Overhaul California Consumer Privacy Act Via Ballot Initiative, 2020, https://www.arnoldporter.com/en/perspectives/publications/2020/11/voters-overhaul-cpa-via-ballot-initiative [perma.cc/WT6Y-SNE4].

Vogel, David, Trading up: consumer and environmental regulation in a global economy, Cambridge, Massachusetts 1995.

Voigt, Marlene, Die datenschutzrechtliche Einwilligung: zum Spannungsfeld von informationeller Selbstbestimmung und ökonomischer Verwertung personenbezogener Daten, Baden-Baden 2020.

Voit, Moritz, Sammelklagen und ihre Finanzierung: Ein Vorschlag zur Ablösung der Musterfeststellungsklage unter Berücksichtigung der Verbandsklagenrichtlinie sowie der Class Action des australischen Bundesrechts, Baden-Baden 2021.

Volokh, Eugene, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You, 52 Stan. L. Rev. 1049–1124.

–, Tort Law vs. Privacy, 114 Colum. L. Rev. 879–948.

Voss, Gregory, Obstacles to Transatlantic Harmonization: Privacy Law in Context, 2019 U. III. J. L. Tech & Pol'y 405–463.

Voss, Gregory/Houser, Kimberly A., Personal Data and the GDPR: Providing a Competitive Advantage for U. S. Companies, 56 Am. Bus. L.J. 287–344.

Wächter, Michael, Datenschutz im Unternehmen, 6. Auflage, München 2021.

Waldman, Ari Ezra, Privacy Law's False Promise, 97 Wash. U. L. Rev. 773–834.

–, Privacy, Practice, and Performance, 2021, https://papers.ssrn.com/abstract=3784667 [perma.cc/RT3N-5NZT].

Warren, Samuel D./Brandeis, Louis D., Right to Privacy, 4 Harv. L. Rev. 193–220.

Washington Post, Washington Post, Privacy Policy, 2021, https://www.washingtonpost.com/discussions/2021/01/01/privacy-policy/ [perma.cc/L3F6-WKV9].

Watson, Alan, Legal transplants, 2. Auflage, Athens, Georgia 1993.

Weber, Alexa Lynn, Who Really Controls the Privacy Conversation? The Need for a Fundamental Right to Privacy in the United States Comment, 2 Corp. & Bus. L.J. 188–202.

Weber, Marc Philipp/Dehnert, Henning, Das Kooperations- und Kohärenzverfahren vor dem EDSA, ZD 2021, 63–68.

Weckler, Adrian, Independent, Will the appointment of more Data Protection Commissioners be enough to silence Ireland's critics?, 22.10.2021, https://www.independent.ie/business/technology/will-the-appointment-of-more-data-protection-commissioners-be-enough-to-silence-irelands-critics-40972937.html [perma.cc/FDF5-H8A2].

Weichert, Thilo, Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, NJW 2001, 1463–1469.

–, Die DSGVO, ein – ganz guter – Anfang, DuD 2020, 293–296.

–, Überlegungen anlässlich der Evaluation der DSGVO und des Beginns der deutschen Präsidentschaft im Europäischen Rat, 2020, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2020_dsgvoevaluation2.pdf [perma.cc/HUE5-QNN5] (zitiert als: *Weichert*, Überlegungen Evaluation DSGVO).

Wendehorst, Christiane/Westphalen, Friedrich Graf von, Das Verhältnis zwischen Datenschutz-Grundverordnung und AGB-Recht, NJW 2016, 3745–3750.

Whitman, James Q., The Two Western Cultures of Privacy: Dignity versus Liberty, 113 Yale L.J. 1151–1222.

Whitney, Tyler, Heavyweight Privacy Battle: California Legislators vs. Tech & Telecom Giants, 96 Denv. L. Rev. Online 176–180.

Williams, Sahara, CCPA Tipping the Scales: Balancing Individual Privacy with Corporate Innovation for a Comprehensive Federal Data Protection Law Notes, 53 Ind. L. Rev. 217–243.

Wilson, Christine S., A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation, 2020, https://www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf [perma.cc/7DJC-YTK5]

Winkler, Adam, Fatal in Theory and Strict in Fact: An Empirical Analysis of Strict Scrutiny in the Federal Courts, 59 Vand. L. Rev. 793–872.

Wybitul, Tim/Brams, Isabelle, Welche Reichweite hat das Recht auf Auskunft und auf eine Kopie nach Art. 15 I DS-GVO?, NZA 2019, 672–677.

Yallen, Jordan, Untangling the Privacy Law Web: Why the California Consumer Privacy Act Furthers the Need for Federal Preemptive Legislation, 53 Loy. L.A. L. Rev. 787–826.

Yannella, Philip, Cyber Litigation: Data Breach, Data Privacy & Digital Rights, New York City 2021.

Ziegenhorn, Gero/Fokken, Martin, Rechtsdienstleister: Verantwortliche oder Auftragsverarbeiter?, ZD 2019, 194–199.

Zikesch, Philipp/Sörup, Thorsten, Der Auskunftsanspruch nach Art. 15 DS-GVO, ZD 2019, 239–245.

Zipursky, Benjamin C., Reasonableness in and out of Negligence Law, 163 U. Pa. L. Rev. 2131–2170.

Zittrain, Jonathan/Albert, Kendra/Lessig, Lawrence, Perma: Scoping and Addressing the Problem of Link and Reference Rot in Legal Citations, 127 Harv. L. Rev. 176–199.

Zweigert, Konrad/Kötz, Hein, Einführung in die Rechtsvergleichung, 3. Auflage, Tübingen 1996.

Sachregister

administrative law judge 192
AGB-Recht 221, 251, 263
Angemessenheitsbeschluss
– Kein angemessenes Schutzniveau in Kalifornien 233–241
– Maßstab der Angemessenheit 233–235
– Motiv für Änderung des CCPA 64, 170, 175, 231, 236
anti-avoidance, *siehe* Umgehungsverbot
Anwendungsbereich
– Bereichsausnahmen, *siehe* Bereichsausnahmen
– persönlich, *siehe* Dienstleister, Unternehmen, Verbraucher: innen
– räumlich 71–74
– sachlich, *siehe* persönliche Informationen
Attorney General, *siehe* California Attorney General
Aufbau 41
Aufsichtsbehörden 181–204, 232
– *siehe* California Attorney General, California Privacy Protection Agency, city attorney, district attorney
– Vergleich mit Aufsichtsbehörden der DSGVO 200–204
Auskunftsrecht, *siehe* Recht auf Auskunft
authorized agent, *siehe* Datenschutzagenturen

Barrierefreiheit 164
berechtigte Erwartung von Privatheit 8, 50
berechtigte Interessen, *siehe* Rechtsgrundlage der Interessenabwägung
Bereichsausnahmen 74–76
Berichtigungsrecht, *siehe* Recht auf Berichtigung
Besondere Kategorien personenbezogener Daten 112–114, 271
Betriebsprüfungen durch California Privacy Protection Agency 190–191
Biometric Information Privacy Act 109
Branchenspezifischer Ansatz 19–24, 27, 62, 78, 238
business, *siehe* Unternehmen
Bußgelder 191–194, 202

California Attorney General 27, 194–198
California effect, *siehe* Kalifornien-Effekt
California Privacy Protection Agency 182–194
– Abhilfemaßnahmen 193
– Budget 186
– Bußgeldkompetenz 191–194
– Öffentlichkeitsarbeit 194
– Rolle der Kommission 184
California Privacy Rights Act, *siehe* Proposition 24
chain of custody 173
Children's Online Privacy Protection Act 23–24, 27, 78, 98–100
city attorneys 198–200
civil penalties 196–198
class actions, *siehe* Sammelklagen
common law 17–19, 83
consideration 83
Constitution of the State of California 15–17
Constitution of the United States 7–15
consumer, *siehe* Verbraucher:innen
Consumer Privacy Fund 186 f.
contractor, *siehe* Dienstleister
counties 198
cybersecurity audits, *siehe* Datensicherheit-Audit

Dateneigentum 254
Datenhandelsdefinition 59, 82–86

Datenlokalisierung 174
Datenminimierung 169–171
– Vergleich mit Art. 5 DSGVO 171
– Vorläufer im sonstigen U. S.-Datenschutzrecht 169
– Zielkonflikte 226
Datenpannenmeldepflicht 28, 242
Datenschutzagenturen 91–93, 97 f., 130
Datenschutz als Grundrecht 105, 223–225, 243–245
Datenschutzbeauftragte 180, 239
Datenschutz durch Technikgestaltung 180
Datenschutzgesetze anderer Bundesstaaten 28, 285
– Biometric Information Privacy Act (Illinois) 109
Datenschutzgesetze des Bundes 19–24, *siehe auch* umfassendes Datenschutzgesetz des Bundes
Datensicherheit 171–173, 210
– Vorläufer im sonstigen U. S.-Datenschutzrecht 172 f.
Datensicherheit-Audit 177–180
Datensparsamkeit, *siehe* Datenminimierung
Datentreuhand 97–98, 255
Datenüberlassungsverträge 241–277
– angemessenes Alternativangebot 265
– Definition 262–264
– Informationsasymmetrie 265–267
– keine AGB-rechtliche Inhaltskontrolle 251
– Kommerzialisierung des Persönlichkeitskerns 271
– Regelungsalternativen *de lege ferenda* 254–256
– Regelungsvorschlag 256–277
– Skepsis aus grundrechtsorientierter Sicht 243–245
– unzureichende bisherige Regelung 245–254
deliktsrechtlicher Privatsphäreschutz 17, 51
Dienstleister 65–70
– Vergleich mit Definition des Auftragsverarbeiters (Art. 4 Nr. 8 DSGVO) 68–70
Dienstleistervertrag 173–176
– Vergleich mit Auftragsverarbeitungsvertrag (Art. 28 DSGVO) 176
Digitale-Inhalte-RL 108, 250 f., 259, 264
direkte Demokratie, *siehe* Volksbegehren
Direktwerbung 95
district attorneys 198–200
doing business, *siehe* Anwendungsbereich: räumlich
Dokumentationspflichten 177
Do-Not-Track-Signal 90
Dormant Commerce Clause 13–15, 73 f., 175, 240
Dritter 71
Durchführungsverordnung 35, 42, 187–190

Einfluss der DSGVO auf den CCPA 230–233
Einfluss des CCPA auf andere U. S.-Datenschutzgesetze 284–285
Einfluss des CCPA auf Europa 2, *siehe auch* Datenüberlassungsverträge: Regelungsvorschlag
Einfluss des U. S.-Datenschutzrechts auf die DSGVO 23, 242
ePrivacy-RL 97, 114, 249
ePrivacy-VO 97, 250, 273

Fair Credit Reporting Act (FCRA) 77, 169
fair information practice principles 232
Federal Trade Commission (FTC) 24–27, 48, 222
financial incentives, *siehe* finanzielle Anreize
finanzielle Anreize 101–108
– Auswirkungen der Regelung auf Datenwirtschaft 104–106
– Informationspflicht 103
– Regelungsvorschlag einer Rechtsübernahme 241–277
– Vergleich mit europäischem Datenschuldrecht 108
– Vergleich mit europäischen Datenschutzrecht 107–108
First Amendment 10–15
– *commercial speech* 10, 12
– *compelled speech* 11
– Einfluss auf CCPA 51–55, 79, 82, 134 f., 140, 226–228
– Verhältnis zu Recht auf Vergessenwerden 140
Forschung 137
Fourteenth Amendment 9
Fourth Amendment 8 f., 50

Freemium 263

gemeinsame Verantwortung 57
Gesetzesauslegung in den U.S.A. 45, 63, 229
Gesetzgebungsgeschichte 30–41
Gewaltenteilung 181 f.
Global Privacy Control 91
Gramm-Leach-Bliley Act (GLBA) 22, 77, 82

Haushaltsausnahme 60
haushaltsbezogene Informationen 122
Health Insurance Portability and Accountability Act (HIPAA) 22 f., 49, 77, 146, 174
Humanarzneimittel-Prüf-VO 271

Identitätsdiebstahl 110–112, 113, 118, 124, 127, 209
Informationelle Selbstbestimmung 224
Informationsasymmetrie 225, 265–267
Informationspflichten 150–166
– Effektivität 154–155, 159
– Form und Sprache 163–166
– kurzer Datenschutzhinweis 151–155
– umfassende Datenschutzerklärung 155–160
– Verbraucherrechte-Statistik 157–159
– Vergleich mit Art. 13, 14 DSGVO 160–162, 164
Instruktionspflichten, *siehe* Trainingspflichten
Insurance Code 78
intermediate scrutiny 11, 52

Kalifornien als multilingualer Bundesstaat 163
Kalifornien-Effekt 28–29, 242, 285
kalifornischer Verwaltungsaufbau 181
kalifornisches Datenschutzrecht 27–29
Klausel-RL 252–254, 259
Kollisionsregeln 76–79
Kommerzialisierung des Persönlichkeitskerns 271
Kontrolle über die eigenen Daten 223
Koppelungsverbot (Art. 7 Abs. 4 DSGVO) 107, 245–249
Kundenkarten 28, 101, 262

Lebenswichtige Interessen als Bereichsausnahme 75
Leistung gegen Daten, *siehe* Datenüberlassungsverträge
– Unschärfe des Begriffs 262 f.
Löschung, *siehe* Recht auf Löschung

marketplace of ideas 10, 134, 149, 226–228
Massenüberwachung, *siehe* Überwachung durch den Staat
Maßregelungsverbot 100–108
– bei Recht auf Einschränkung sensibler Informationen 115
– bei Recht auf Löschung 142
– bei Widerspruchsrecht gegen Datenhandel 100–108
– Finanzielle Anreize als Grenze 101–106, *siehe auch* finanzielle Anreize
– Mögliche Rechtsübernahme 257
Medienprivileg 55
Meinungsfreiheit, *siehe* First Amendment
Minderjährigenschutz 23, 98–100
Mittelbare Drittwirkung von Grundrechten 223–225
Musterfeststellungsklage 217

notice-and-choice-Modell 25–27, 222
notice at collection, *siehe* Informationspflichten: kurzer Datenschutzhinweis
notice of financial incentive, *siehe* finanzielle Anreize: Informationspflichten
notice of right to opt out, *siehe* Widerspruchsrecht gegen Datenhandel: Informationspflichten

Öffnungsklauseln der DSGVO 78
One-Stop-Shop-System 203–204
opt-out-Gesetz *vs*. *opt-in*-Gesetz 96
opt-out preference signal, *siehe* Widerspruchsrecht gegen Datenhandel: Widerspruchssignal

personal information, *siehe* persönliche Informationen
Personal Information Management Systems 97 f.
personenbezogene Daten, *siehe* persönliche Informationen

persönliche Informationen 43–55
– aggregierte 47–50
– als Wirtschaftsgut 105, 243–245
– Definition 43–55
– öffentliche 50
– Vergleich mit Definition der personenbezogenen Daten (Art. 4 Nr. 1 DSGVO) 45–47
– Wert 101, 267–270
politische Meinungen 113
Prinzip der Rechtmäßigkeit (Art. 6 DSGVO) 95, 237, 260
privacy by design, *siehe* Datenschutz durch Technikgestaltung
privacy policy, *siehe* Informationspflichten: umfassende Datenschutzerklärung
privacy self-management, *siehe* Selbstdatenschutz
Privatautonomie 26, 100, 244, 256
Privatklagerecht wegen Datenpannen 204–219
– Abhilfefrist 210
– kein weitergehendes Privatklagerecht 214–215
– Schadensersatzhöhe 211 f.
– Tatbestand 208–211
– Verfahren 212–214
– Vergleich mit Privatklagerechten des Art. 79, 82 DSGVO 216–219
– Zuständigkeit 213
Proposition 24
– Gesetzgebungsgeschichte 35–38
– wesentliche Änderungen 42, 49, 59, 85, 145, 170, 177, 182
Pur-Abos 249

reasonable expectation of privacy, *siehe* berechtigte Erwartung von Privatheit
Reasonableness 45, 171
Recht auf Auskunft 116–134
– Ausnahmen 120–122
– Ausübung 125–133
– Datenportabilität 133 f.
– Frist für Antwort 130
– Identifizierung 127–131
– Reichweite 118
– Vergleich mit Ausübung des Art. 15 DSGVO 131–133
– Vergleich mit Reichweite des Art. 15 DSGVO 122–125
– Vorläufer im sonstigen U. S.-Datenschutzrecht 117
Recht auf Berichtigung 145–147
– Vergleich mit Art. 16 DSGVO 146 f.
– Vorläufer im sonstigen U. S.-Datenschutzrecht 145
Recht auf Beschränkung sensibler Informationen 109–116
– Ausübung 114
– Reichweite 114–116
– *sensible Informationen* 109–114
– Vergleich mit Art. 9, 10 DSGVO 112–114, 115 f.
Recht auf Datenportabilität 133 f.
Recht auf Löschung 134–144
– Ausnahmen 135–139
– Ausübung 141
– Durchführung 144
– Recht auf Vergessenwerden 140
– Vergleich mit Ausübung des Art. 17 DSGVO 143
– Vergleich mit Durchführung des Art. 17 DSGVO 144
– Vergleich mit Reichweite des Art. 17 DSGVO 139–144
– Vorläufer im sonstigen U. S.-Datenschutzrecht 135
Recht auf Privatsphäre in U. S. Constitution 7–9
Rechtsgrundlage der Interessenabwägung 95, 99, 116, 237
Rechtsübernahmen 241
Rechtsvergleichungsmethode 4
Redaktionsfehler 229
Regelungstechnik 45–47, 228–230
regulatory capture 183
Rezeption 2, 221–233
right to correct, *siehe* Recht auf Berichtigung
right to delete, *siehe* Recht auf Löschung
right to know, *siehe* Recht auf Auskunft
right to limit use and disclosure of sensitive personal information, *siehe* Recht auf Beschränkung sensibler Informationen
right to no retaliation, *siehe* Maßregelungsverbot

right to opt-in, *siehe* Widerspruchsrecht gegen Datenhandel: Einwilligungsvorbehalt für Minderjährige
right to opt-out, *siehe* Widerspruchsrecht gegen Datenhandel
Risikoanalyse 177–180
risk assessment, *siehe* Risikoanalyse
Rückwirkung 208

Sammelklagen 204–208, 212
Schadensersatz wegen Datenpannen, *siehe* Privatklagerecht wegen Datenpannen
Schrems-II-Urteil 239
sectoral approach, *siehe* Branchenspezifischer Ansatz
Selbstdatenschutz 106, 223, 225 f.
selling, *siehe* Datenhandelsdefinition
sensible Informationen 109–114
sensitive personal information, *siehe* sensible Informationen
service provider, *siehe* Dienstleister
sharing, *siehe* Datenhandelsdefinition
Speicherfristbegrenzung 169–171
Standarddatenschutzklauseln 175
standing 205
Standortdaten 111, 113
Strafverfolgung 74
strict scrutiny 11, 51
Supremacy Clause 76
Systematik, *siehe* Aufbau

Third Amendment 9
third party, *siehe* Dritter
torts law, *siehe* deliktsrechtlicher Privatsphäreschutz
Trainingspflichten 176
Transparenz 52, 55, 117, 201, 226–228
– Grundprinzip des U. S.-Rechts 150
Treuprogramme, *siehe* Kundenkarten
Treu und Glauben 107
TTDSG 97, 114, 249 f.

Überwachung durch den Staat 9, 239–240
umfassendes Datenschutzgesetz des Bundes 19–21, 284 f.
Umgehungsverbot 85
Unfair Competition Law 27, 168, 199
Unklarheiten 228
Unternehmen 56–65
– bestimmender Einfluss 56–58
– Gewinnerzielungsabsicht 58
– Konzerngesellschaften 62
– Schwellenwerte 58–62
– Vergleich mit Definition des Verantwortlichen 57, 60–62, 64
Unternehmensgröße 62, 176
Unternehmenskauf 85

Verbandsklagen-RL 218
Verbraucher:innen 56
Verfassungsmäßigkeit des CCPA 13, 15, 51
Verjährung von Verstößen 193
Verordnungsermächtigung 187–190
Vertraulichkeit der Verarbeitung, *siehe* Datensicherheit
Verwertungsgesellschaft für personenbezogene Daten 256
Verzeichnis der Verarbeitungstätigkeiten 180
Video Privacy Protection Act 21, 169
Videoüberwachung 71
Volksbegehren 30–32, 35–38

Weiterübermittlungsvertrag 173–176
Widerspruchsrecht gegen Datenhandel 81–108
– Ausübung 86–93
– Einwilligungsvorbehalt für Minderjährige 98
– Folgen eines Widerspruchs 93 f.
– Informationspflicht 87–89
– Reichweite 82
– Vergleich mit § 25 TTDSG 97
– Vergleich mit Art. 6 DSGVO 95 f.
– Vergleich mit Art. 21 DSGVO 94 f.
– Widerspruchslink 87–89
– Widerspruchslogo 89
– Widerspruchssignal 89

Zweckbindung 166–168
– Vergleich mit Art. 5 DSGVO 168
– Vorläufer im sonstigen U. S.-Datenschutzrecht 166