CENTER FOR INFORMATION TECHNOLOGY SOCIETY AND LAW — ITSL

Volume 16

Samuel Mätzler

Das Recht auf Datenportabilität

Eine rechtsvergleichende Untersuchung von Art. 28 DSG anhand dreier Datenökosysteme

EIZ Publishing

Das Recht auf Datenportabilität

Eine rechtsvergleichende Untersuchung von Art. 28 DSG anhand dreier Datenökosysteme

Dissertation
der Rechtswissenschaftlichen Fakultät
der Universität Zürich

zur Erlangung der Würde eines Doktors der Rechtswissenschaft

vorgelegt von

Samuel Mätzler
von Berneck, SG

genehmigt auf Antrag von

Prof. Dr. Florent Thouvenin
und
Prof. Dr. Rolf H. Weber

Die Rechtswissenschaftliche Fakultät der Universität Zürich gestattet hierdurch die Drucklegung der vorliegenden Dissertation, ohne damit zu den darin ausgesprochenen Anschauungen Stellung zu nehmen.

Zürich, den 3. Dezember 2025

Der Dekan: Prof. Dr. Thomas Gächter

© 2026 – CC BY-NC-ND

Verlag: EIZ Publishing (eizpublishing.ch), Bellerivestrasse 49, 8008 Zürich,
eizpublishing@europa-institut.ch
Autor: Samuel Mätzler
ISBN:
978-3-03994-080-6 (Print – Softcover)
978-3-03994-081-3 (Print – Hardcover)
978-3-03994-082-0 (ePub)
DOI: https://doi.org/10.36862/74T3-4DSJ
Version: 1.00 – 20260302

Die Dissertation wurde publiziert mit Unterstützung des Schweizerischen Nationalfonds zur Förderung der wissenschaftlichen Forschung.

Die vorliegende Dissertation wurde von Samuel Mätzler eingereicht und am 3. Dezember 2025 von der Rechtswissenschaftlichen Fakultät der Universität Zürich auf Antrag von Herrn Professor Dr. Florent Thouvenin (erster Referent) und Herrn Professor Dr. Rolf H. Weber (zweiter Referent) genehmigt.

Dieses Werk ist als gedrucktes Buch sowie als E-Book (open access) in verschiedenen Formaten verfügbar. Weitere Informationen finden Sie unter der URL: https://eizpublishing.ch/publikationen/das-recht-auf-datenportabilitaet/.

Vorwort

Diese Arbeit untersucht das Recht auf Datenportabilität aus schweizerischer Perspektive. Entstanden ist sie hauptsächlich während meiner Tätigkeit am Center for Information Technology, Society, and Law (ITSL) der Universität Zürich, wo ich zugleich in der Forschungsgruppe Recht & Ethik des Universitären Forschungsschwerpunkts *Dynamics of Healthy Aging* mitwirkte. Des Weiteren verbrachte ich Forschungsaufenthalte an den Max-Planck-Instituten für Innovation und Wettbewerb (München) und für ausländisches und internationales Privatrecht (Hamburg). Dabei wurde ich durch ein UZH Doc.Mobility-Stipendium unterstützt. Eine fokussierte Schlussphase ermöglichte mir ein Stipendium der Janggen-Pöhn-Stiftung.

Mein besonderer Dank gilt meinem Doktorvater Prof. Dr. Florent Thouvenin für die umsichtige Betreuung und die lehrreiche Zeit am ITSL. Prof. Dr. Rolf H. Weber danke ich für die wertvollen Anregungen und die rasche Ausarbeitung des Zweitgutachtens. Beiden danke ich zudem für die Aufnahme in die ITSL-Schriftenreihe. Ein herzlicher Dank gebührt ferner allen meinen ehemaligen Kolleginnen und Kollegen am ITSL und am Lehrstuhl. Prof. Dr. Aurelia Tamò-Larrieux danke ich für die Unterstützung bei den Förderanträgen und dem Team von EIZ Publishing für den zügigen Publikationsprozess. Für ihr wertvolles Feedback zu dieser Arbeit danke ich Lara Blumer, Francesco Brenni, Sara Eberhart, Daniel Gnägi und Lena Hänni. Ein weiterer Dank gilt meinem Vater, Felix Mätzler, für das sorgfältige Lektorat.

Die Arbeit wurde von der Rechtswissenschaftlichen Fakultät der Universität Zürich am 3. Dezember 2025 als Dissertation abgenommen. Sie befindet sich grundsätzlich auf dem Stand von September 2025; spätere Entwicklungen wurden lediglich punktuell berücksichtigt, namentlich die bundesrätlichen Vorlagen zu Kommunikationsplattformen und Suchmaschinen sowie zum elektronischen Gesundheitsdossier. Soweit technisch möglich, sind Weblinks über Perma.cc dauerhaft abrufbar.

Widmen möchte ich diese Arbeit meinen Eltern, die mir stets den nötigen Rückhalt gegeben haben und mir meine Ausbildung ermöglichten.

Zürich, im Februar 2026 Samuel Mätzler

Inhaltsübersicht

Vorwort V

Inhaltsübersicht VII

Inhaltsverzeichnis X

Literatur XVII

Materialien und weitere amtliche Publikationen XLVIII

Abkürzungen LVIII

§ 1 Thematische Einführung 1

I. Einleitung 2

II. Gegenstand der Untersuchung 5

A. Ausgangslage 5

B. Stand der Forschung 5

C. Forschungsfrage und Vorgehensweise 6

D. Eingrenzung 8

III. Methode 10

A. Auslegungsmethoden 10

B. Auslegung in dieser Untersuchung 11

C. Rechtsvergleichung in dieser Untersuchung 12

D. Induktiver Ansatz dieser Untersuchung 13

IV. Grundbegriffe 15

A. Daten i.w.S. 15

B. Personendaten (Daten i.e.S.) 15

C. Sachdaten 16

D. Datenbearbeitung 16

E. Betroffene Person 17

F. Verantwortliche 17

G. Auftragsbearbeiter 17

H. Datenökosystem 18

I. Datenraum 19

J. Datenwirtschaft 20

K. Internetplattformen und soziale Netzwerke 21

V. Datenschutz als Rechtsgebiet 26

A. Anfänge und erste Gesetze 26

B. Deutsches Volkszählungsurteil 27

C. (K)ein Recht auf informationelle Selbstbestimmung in der EU 28

D. Entwicklung in der Schweiz 31

§ 2 Grundlagen 43

I. Chronologie des Rechts auf Datenportabilität 44

A. Ursprünge in der US-amerikanischen IT-Szene 44

B. In der EU 46

C. In der Schweiz 49

II. Technisch-organisatorische Aspekte 54
A. Allgemein 54
B. Perspektiven der Portabilität gemäss ISO 55
C. Interoperabilität als Wesenszug der Portabilität? 57
D. Personal Information Management Systems (PIMS) 58
E. Datensicherheit 60
III. Rechtlicher Rahmen 62
A. Art. 20 DSGVO 62
B. Art. 28 DSG 82
IV. Erkenntnisse 105

§ 3 Rechtsdogmatische Einordnung 109
I. Einleitung 110
II. Systematische Einordnung 112
III. Teleologische Einordnung 114
A. Datenschutzrechtliche Ziele 114
B. Wettbewerbsrechtliche Ziele 139
C. Konsumentenschutzrechtliche Ziele 165
IV. Abgrenzungen 167
A. Zum datenschutzrechtlichen Auskunftsrecht 167
B. Zu Datenzugang 171
C. Zu kartellrechtlichen Ansprüchen 174
D. Weitere mögliche Institute 176
V. Synthese 177
A. Vereinbarkeit von datenschutz- und wettbewerbsrechtlichen Zielen 177
B. Notwendigkeit der Regulierung 181
C. Einschränkungen der Wirtschaftsfreiheit 182
VI. Zwischenfazit: Datenschutzrechtliches Instrument mit wettbewerbsrechtlichem Einschlag 184

§ 4 Fallbeispiele: Drei Datenökosysteme 189
I. Methode 190
A. Auswahl der Sektoren 190
B. Untersuchung der Sektoren 193
II. Soziale Netzwerke 195
A. Strukturierung des Ökosystems 195
B. Kritische Würdigung der Datenportabilität 208
III. Gesundheitswesen 229
A. Strukturierung des Ökosystems 230
B. Kritische Würdigung der Datenportabilität 259
IV. Mobilität 273
A. Strukturierung des Ökosystems 275
B. Kritische Würdigung der Datenportabilität 301

§ 5 Erkenntnisse 317
I. Einleitung 318
II. Verhältnis zwischen sektorübergreifenden und sektorspezifischen Portabilitätsrechten 320
A. Vorteile sektorspezifischer Regelungen 320
B. Rechtfertigung der sektorübergreifenden Regelung 321
C. Folgerung 323
III. Mögliche Handlungsspielräume und deren Grenzen 325
A. Keine generelle Erweiterung des Anwendungsbereichs erforderlich 325
B. Präzisierung der technischen Vorgaben 326
C. Auf den modernen Datenverkehr angepasste Modalitäten 332
D. Keine Beschränkung auf spezifische Normadressatinnen 334
E. Vermehrter Einsatz von PIMS 335
F. Exkurs: Portierung von Sachdaten – eine Datenverordnung für die Schweiz? 338
IV. Fazit: Kaum sektorübergreifender Anpassungsbedarf 340
A. Mit Blick auf die datenschutzrechtlichen Ziele 340
B. Mit Blick auf die wettbewerbsrechtlichen Ziele 340
C. One size (rarely) fits all 341
D. Ausblick 343

Zusammenfassung der Erkenntnisse 345

Anhang 354

Curriculum Vitae 356

Inhaltsverzeichnis

Vorwort V

Inhaltsübersicht VII

Inhaltsverzeichnis X

Literatur XVII

Materialien und weitere amtliche Publikationen XLVIII

Abkürzungen LVIII

§ 1 Thematische Einführung 1

I. Einleitung 2

II. Gegenstand der Untersuchung 5

A. Ausgangslage 5

B. Stand der Forschung 5

C. Forschungsfrage und Vorgehensweise 6

D. Eingrenzung 8

III. Methode 10

A. Auslegungsmethoden 10

B. Auslegung in dieser Untersuchung 11

C. Rechtsvergleichung in dieser Untersuchung 12

D. Induktiver Ansatz dieser Untersuchung 13

IV. Grundbegriffe 15

A. Daten i.w.S. 15

B. Personendaten (Daten i.e.S.) 15

C. Sachdaten 16

D. Datenbearbeitung 16

E. Betroffene Person 17

F. Verantwortliche 17

G. Auftragsbearbeiter 17

H. Datenökosystem 18

I. Datenraum 19

J. Datenwirtschaft 20

K. Internetplattformen und soziale Netzwerke 21

1. Zweiseitige Märkte als Ausgangspunkt 21

2. Begriffsdefinition 21

3. Plattformisierung 23

V. Datenschutz als Rechtsgebiet 26

A. Anfänge und erste Gesetze 26

B. Deutsches Volkszählungsurteil 27

C. (K)ein Recht auf informationelle Selbstbestimmung in der EU 28

D. Entwicklung in der Schweiz 31

1. Erstes Datenschutzgesetz (DSG) 31

2. Verfassungsrechtlicher Datenschutz 32
a. Grundlagen 32
b. Unklarer Gehalt der informationellen Selbstbestimmung 34
c. Andere Ansätze 35
3. Revision des DSG 40
4. Zweck des DSG 41

§ 2 Grundlagen 43
I. Chronologie des Rechts auf Datenportabilität 44
A. Ursprünge in der US-amerikanischen IT-Szene 44
B. In der EU 46
C. In der Schweiz 49
II. Technisch-organisatorische Aspekte 54
A. Allgemein 54
B. Perspektiven der Portabilität gemäss ISO 55
1. Syntaktische Perspektive 55
2. Semantische Perspektive 56
3. Regulatorische Perspektive 56
C. Interoperabilität als Wesenszug der Portabilität? 57
D. Personal Information Management Systems (PIMS) 58
E. Datensicherheit 60
III. Rechtlicher Rahmen 62
A. Art. 20 DSGVO 62
1. Personenbezogene Daten der betroffenen Person 62
2. Betroffene Person hat die Daten dem Verantwortlichen bereitgestellt 64
3. Berechtigter Grund der Verarbeitung 66
a. Verarbeitung beruht auf einer Einwilligung 66
b. Verarbeitung beruht auf einem Vertrag 67
4. Verarbeitung erfolgt mithilfe automatisierter Verfahren 68
5. Rechtsfolge: Übertragung 68
a. Indirekte Übertragung 68
b. Direkte Übertragung 69
c. Form 72
aa. Strukturiertheit 72
bb. Gängigkeit 73
cc. Maschinenlesbarkeit 74
dd. Interoperabilität 76
d. Modalitäten 77
6. Unberührtheit des Rechts auf Löschung nach Art. 17 DSGVO 78
7. Nichtbeeinträchtigung der Rechte und Freiheiten anderer Personen 78
8. Weitere Einschränkungen 81
9. Folgen der Nichteinhaltung 82
B. Art. 28 DSG 82
1. Personendaten der betroffenen Person 83
a. Nicht Sachdaten 83
b. Datenumfang 83
2. Von betroffener Person bekanntgegeben 84

3. Personendaten Dritter 87
a. Allgemein 87
b. Pflichten in Bezug auf Dritte 89
c. Spezialfragen beim Doppelbezug 90
4. Mit Einwilligung oder in unmittelbarem Zusammenhang mit Vertragsabschluss erhoben 91
a. Allgemein 91
b. Datenbearbeitungen durch Bundesorgane 92
5. Automatisierte Bearbeitung durch den Verantwortlichen 93
6. Rechtsfolge: Portierung 94
a. An die betroffene Person (Datenherausgabe) 94
b. An die neue Verantwortliche (Datenübertragung) 95
c. In einem gängigen elektronischen Format 96
d. Modalitäten, Frist und Zuständigkeit 99
e. Keine Löschung beim alten Verantwortlichen 100
f. Folgen der Nichteinhaltung 101
7. Rechtsnatur 101
a. Allgemein 101
b. Keine Portierung nach dem Tod 102
8. Einschränkungen nach Art. 29 DSG 103
IV. Erkenntnisse 105

§ 3 Rechtsdogmatische Einordnung 109
I. Einleitung 110
II. Systematische Einordnung 112
III. Teleologische Einordnung 114
A. Datenschutzrechtliche Ziele 114
1. Europäische Konzeption: Teilhabesicherung an privater, sozialer und öffentlicher Kommunikation 114
a. Kritik an der herrschaftsrechtlichen Auslegung 114
b. Votum für ein erweitertes Datenschutzverständnis 115
2. Verwirklichung der informationellen Selbstbestimmung als Ausgangspunkt der Schweizer Konzeption 117
a. Allgemein 117
b. Selbstbestimmte Datendisposition als Ausfluss der informationellen Selbstbestimmung 117
c. Grundrechtsverwirklichung unter Privaten 118
d. Diskussion 119
3. Das Recht auf Datenportabilität als Folge grundlegend veränderter Rahmenbedingungen 121
a. Etablierung einer Datenwirtschaft als Ursprung 121
b. Selbstbestimmte Datendisposition als Reaktion 123
c. Einschränkungen als Resultat der auf Internetplattformen zugeschnittenen Zielsetzung 126
d. Einschränkungen als Resultat der Abwägung konfligierender Ziele 126
4. Neues Verständnis der informationellen Selbstbestimmung 127
a. Bisherige Konzeption kaum tragfähig 127

b. Neuer Ansatz nötig 129
c. Haltung der Lehre 130
aa. Europäische Literatur 130
bb. Schweizer Literatur 131
cc. Analogien zum sachenrechtlichen Eigentum 134
d. Alter Wein in neuen Schläuchen: Kommerzialisierung der Persönlichkeit 134
e. Folgerung 135
5. Allgemeiner Persönlichkeitsschutz als eigenständige Zielsetzung 137
6. Erkenntnisse 138
B. Wettbewerbsrechtliche Ziele 139
1. Ökonomische Einordnung 140
a. Daten als wirtschaftliche Güter 140
b. Ökonomische Relevanz des Rechts auf Datenportabilität 142
2. Wechselkosten senken und Lock-In-Effekt verhindern 143
a. Allgemein 143
b. Daten- oder userinduzierter Lock-In? 146
c. Kein Lock-In der beobachteten Daten? 148
3. Markteintrittsschranke für Konkurrenten verringern 149
4. Allgemeine Wettbewerbsförderung 150
a. Fehlende Einschränkungen – Bug or Feature? 150
b. Fokus auf andersartige Anbieter 153
c. Fokus auf ein Open Web 155
d. Datenschutz zur allgemeinen Wettbewerbsförderung 156
e. Innovationsförderung 157
5. Datenpolitische Strategie und freier Datenfluss 157
6. Erkenntnisse 162
C. Konsumentenschutzrechtliche Ziele 165
IV. Abgrenzungen 167
A. Zum datenschutzrechtlichen Auskunftsrecht 167
1. Unterschiede in der Zielsetzung 167
2. Unterschiede in der Ausgestaltung 170
B. Zu Datenzugang 171
C. Zu kartellrechtlichen Ansprüchen 174
D. Weitere mögliche Institute 176
V. Synthese 177
A. Vereinbarkeit von datenschutz- und wettbewerbsrechtlichen Zielen 177
B. Notwendigkeit der Regulierung 181
C. Einschränkungen der Wirtschaftsfreiheit 182
VI. Zwischenfazit: Datenschutzrechtliches Instrument mit wettbewerbsrechtlichem Einschlag 184

§ 4 Fallbeispiele: Drei Datenökosysteme 189
I. Methode 190
A. Auswahl der Sektoren 190
B. Untersuchung der Sektoren 193

II. Soziale Netzwerke 195
A. Strukturierung des Ökosystems 195
1. Akteure und deren Rollen 195
a. Private Nutzer 195
b. Betreiber 196
c. Kommerzielle Nutzer 197
2. Relevante Beziehungen 198
a. Private Nutzer und (mehrere) Betreiber 198
aa. Allgemein 198
bb. Data Transfer Initiative 200
cc. Europäischer Digital Markets Act (DMA) 202
dd. Rechtslage in der Schweiz 206
b. Private und kommerzielle Nutzer 207
3. Erkenntnisse und Überleitung 208
B. Kritische Würdigung der Datenportabilität 208
1. Datenschutzrechtliche Ziele: Die Krux mehrerer betroffener Personen 208
2. Wettbewerbsrechtliche Ziele 210
a. Netzwerkeffekte und Lock-In bei gleichartigen Betreibern 210
b. Weniger Netzwerkeffekte und Lock-In bei andersartigen Betreibern 212
c. Besondere Relevanz von «winner-takes-it-all»-Märkten 213
d. Allgemeine Wettbewerbs- und Innovationsförderung 214
e. In Bezug auf die Plattformisierung 216
f. Förderung des freien Datenflusses 218
3. Mögliche Handlungsspielräume 218
a. Fortentwicklung der datenschutzrechtlichen Portabilität in Richtung Interoperabilität 219
b. Spezifisches Portabilitätsrecht gegenüber einzelnen Betreibern 222
4. Erkenntnisse 226
III. Gesundheitswesen 229
A. Strukturierung des Ökosystems 230
1. Akteurinnen und deren Rollen 230
a. Natürliche Personen 230
b. Leistungserbringerinnen 230
c. Versicherungsunternehmen 231
d. Forschende 232
e. Staat 233
f. Herstellerinnen von Medizinprodukten 234
g. Anbieterinnen von gesundheitsrelevanten Anwendungen 235
2. Relevante Beziehungen 236
a. Natürliche Person (Patientin) und Leistungserbringerin 236
aa. Rechtsnatur des Behandlungsverhältnisses 236
bb. Dokumentationspflichten der Leistungserbringerin 237
cc. Datenbearbeitungen in dieser Beziehung 238
dd. Folgerungen 239
ee. Bundesorgane als Leistungserbringer 242
ff. Europäischer Raum für Gesundheitsdaten (EHDS) 243
gg. Rechtslage in der Schweiz 245

b. Natürliche Person (Versicherte) und Versicherungsunternehmen 248
c. Natürliche Person (Probandin) und Forschende 249
aa. Allgemein 249
bb. Sekundärnutzung für die Forschung 251
cc. Europäischer Raum für Gesundheitsdaten (EHDS) 252
dd. Rechtslage in der Schweiz 253
d. Natürliche Person und Anbieterinnen von gesundheitsrelevanten Anwendungen 257
3. Erkenntnisse und Überleitung 259
B. Kritische Würdigung der Datenportabilität 259
1. Allgemein 259
2. Datenschutzrechtliche Ziele 261
a. Im Regelfall mit Einschränkungen erreicht 261
b. Besondere Interessenlage in der Forschung 262
3. Wettbewerbsrechtliche Ziele 263
4. Spezialgesetzliche Vorgaben verdrängen das Portabilitätsrecht 265
5. PIMS als Bindeglied zwischen den Akteurinnen 266
6. Mögliche Handlungsspielräume 267
a. Partielle Anwendbarkeit auch für öffentliche Organe 267
b. Erweiterung des Portabilitätsrechts auf abgeleitete Daten 268
c. Interoperabilitätsvorgaben 269
7. Erkenntnisse 270
IV. Mobilität 273
A. Strukturierung des Ökosystems 275
1. Akteure und deren Rollen 275
a. Mobile Personen 275
b. Fahrzeughersteller 275
c. Anbieter von Dienstleistungen 276
d. Staat 277
e. Fahrzeughändler 278
2. Relevante Beziehungen 279
a. Mobile Personen und Fahrzeughersteller 279
aa. Allgemein 279
bb. Europäische Datenverordnung (DV) 282
(1) Grundlagen 282
(2) Weiter Datenbegriff 284
(3) Weiter sachlicher Anwendungsbereich 286
(4) Enger persönlicher Anwendungsbereich 287
(5) Erkenntnisse 288
b. Mobile Personen und Anbieter von Dienstleistungen 290
c. Mobile Personen und Staat 290
d. Mobile Personen und Fahrzeughändler 290
e. Fahrzeughersteller und Anbieter von Dienstleistungen 291
aa. Allgemein 291
bb. Europäische C-ITS-Initiative 294
cc. Europäische Datenverordnung (DV) 296
dd. Europäische TypgenehmigungsVO 297

ee. KFZ-Verordnung 299
3. Erkenntnisse und Überleitung 300
B. Kritische Würdigung der Datenportabilität 301
1. Datenschutzrechtliche Ziele 301
2. Wettbewerbsrechtliche Ziele beim Zugang zu Fahrzeugdaten für Anbieter von Dienstleistungen 302
a. Verringerung von Lock-In-Effekten und Markteintrittsschranken 302
b. Allgemeine Wettbewerbs- und Innovationsförderung sowie Förderung des freien Datenflusses 304
3. Einordnung unter Berücksichtigung der spezialgesetzlichen Datenzugangsregelungen 305
4. Mögliche Handlungsspielräume 308
a. Extensive Auslegung des Begriffs «bekanntgegeben» 308
b. Engere Orientierung an Normen und Standards 308
c. Erweiterung des Portabilitätsrechts auf Sachdaten 309
d. Erweiterung des Portabilitätsrechts auf eine Echtzeitübertragung 310
5. Erkenntnisse 314

§ 5 Erkenntnisse 317
I. Einleitung 318
II. Verhältnis zwischen sektorübergreifenden und sektorspezifischen Portabilitätsrechten 320
A. Vorteile sektorspezifischer Regelungen 320
B. Rechtfertigung der sektorübergreifenden Regelung 321
1. Datenschutzrechtliche Rechtfertigung 321
2. Wettbewerbsrechtliche Rechtfertigung 321
C. Folgerung 323
III. Mögliche Handlungsspielräume und deren Grenzen 325
A. Keine generelle Erweiterung des Anwendungsbereichs erforderlich 325
B. Präzisierung der technischen Vorgaben 326
1. Keine umfassende Interoperabilität erforderlich 326
2. Minimalvorgaben und Förderung von offenen Standards 327
3. Periodizität der Portierung 329
C. Auf den modernen Datenverkehr angepasste Modalitäten 332
D. Keine Beschränkung auf spezifische Normadressatinnen 334
E. Vermehrter Einsatz von PIMS 335
F. Exkurs: Portierung von Sachdaten – eine Datenverordnung für die Schweiz? 338
IV. Fazit: Kaum sektorübergreifender Anpassungsbedarf 340
A. Mit Blick auf die datenschutzrechtlichen Ziele 340
B. Mit Blick auf die wettbewerbsrechtlichen Ziele 340
C. One size (rarely) fits all 341
D. Ausblick 343

Zusammenfassung der Erkenntnisse 345

Anhang 354

Curriculum Vitae 356

Literatur

Die nachstehenden Werke werden, wenn nicht anders angegeben, mit Nachnamen der Autorin oder des Autors sowie mit Seitenzahl oder Randziffer zitiert. Zeitschriftenaufsätze werden mit Nachnamen und Fundstelle (Zeitschrift und Jahrgang) zitiert, Kommentarbeiträge mit einem Zusatz, der den Kommentar identifiziert. Werden mehrere Werke derselben Autorin oder desselben Autors zitiert, wird der Nachname jeweils mit einem identifizierenden Zusatz versehen, ausser die Identifizierung ist anderweitig möglich (bspw. bei Zeitschriftenaufsätzen). Nicht im Literaturverzeichnis aufgeführt sind amtlich in Auftrag gegebene und publizierte Gutachten. Sie werden in den Materialien und weiteren amtlichen Publikationen aufgeführt. Ebenfalls nicht aufgeführt sind Zeitungsartikel und sonstige Internetverweise, die als Vollzitat in der jeweiligen Fussnote angegeben werden.

Abegg Andreas/Bernauer Christof, Das Recht der Sharing Economy, Welchen Regulierungsbedarf schaffen Airbnb, Uber & Co?, Zürich 2018

ACEA, Access to vehicle data for third-party services, Position Paper vom Dezember 2016, <https://perma.cc/4QYW-JDJ7>

Aebi-Müller Regina E., Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes, Unter besonderer Berücksichtigung der Rechtslage in der Schweiz und in Deutschland, Bern 2005

Aebi-Müller Regina E., Patientendaten und Persönlichkeitsschutz, Aktuelle Fragestellungen aus der Sicht einer Zivilrechtlerin, Jusletter 27. April 2020

Aebi-Müller Regina E./Fellmann Walter/Gächter Thomas/Rütsche Bernhard/Tag Brigitte, Arztrecht, Bern 2016 (zit.: Arztrecht 2016)

Aebi-Müller Regina E./Fellmann Walter/Gächter Thomas/Rütsche Bernhard/Tag Brigitte, Arztrecht, 2. Aufl., Bern 2024 (zit.: Arztrecht 2024)

Alberini Adrien/Benhamou Yaniv, Data Portability and Interoperability: An issue that needs to be anticipated in today's IT-driven world, Expert Focus 2017, 518–522

Albers Marion, Neukonzeption des grundrechtlichen «Daten»schutzes, in: Haratsch Andreas (Hrsg.), Herausforderungen an das Recht der Informationsgesellschaft, 36. Tagung der Wissenschaftlichen Mitarbeiterinnen und Mitarbeiter der Fachrichtung «Öffentliches Recht», Stuttgart 1996, 113–139

Albers Marion, Information als neue Dimension im Recht, Rechtstheorie 2002, 61–89

Alpmann Klaus, Datenverarbeitung im Auto – Verratene Fahrer oder verhinderte Autoindustrie?, in: Stiftung Datenschutz (Hrsg.), Datenschutz im vernetzten Fahrzeug, Berlin 2020, 13–27

Anciaux Nicolas/Zolynski Célia/Chaudat Sébastien/Ladjel Riad, Empowerment and 'Big Personal Data': From Portability to Personal Agency, GPLR 2021, 16–30

Arioli Martina, Der EU Data Act: werden damit die «Datenschatztruhen» geöffnet?, iusNet DigR 2024

Arnold René/Schneider Anna/Lennartz Jonathan, Interoperability of interpersonal communications services – A consumer perspective, Telecommunications Policy 2020, 101927, 1–13

Bäcker Matthias, Kommentierung zu Art. 23 DSGVO, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung, BDSG: Kommentar, 4. Aufl., München 2024 (zit.: BeckKomm-Bäcker, Art. 23 DSGVO N …)

Baeriswyl Bruno, Big Data zwischen Anonymisierung und Re-Individualisierung, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014, 45–59 (zit.: Big Data)

Baeriswyl Bruno, § 12 Datenschutz als Instrument des Konsumentenschutzes, in: Heiss Helmut/Loacker Leander D. (Hrsg.), Grundfragen des Konsumentenrechts, Zürich 2020, 395–412 (zit.: Konsumentenschutz)

Baeriswyl Bruno, Die Einwilligung hilft (nicht) weiter, Das Dilemma der informationellen Selbstbestimmung bei der Verwendung von Gesundheitsdaten zu Forschungszwecken, digma 2020, 62–66

Baeriswyl Bruno, Vorbemerkungen zu Art. 25–29, Kommentierung zu Art. 28 und Art. 29, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz (DSG), 2. Aufl., Bern 2023 (zit.: SHK DSG-Baeriswyl, … N …)

Baeriswyl Bruno/Pärli Kurt, EMRK, ER-Konv 108+, Richtlinie (EU) 2016/680, DSGVO, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz (DSG), 2. Aufl., Bern 2023 (zit.: SHK DSG-Baeriswyl/Pärli, EMRK, ER-Konv 108+, Richtlinie (EU) 2016/680, DSGVO N …)

Béguin Nicolas, Kommentierung zu Art. 28, in: Benhamou Yaniv/Cottier Bertil (Hrsg.), Petit commentaire LPD, Loi sur la protection des données, Basel 2023 (zit.: PC LPD-Béguin, Art. 28 N …)

Belser Eva Maria, § 2 Entwicklung des Datenschutzes und § 6 Der grundrechtliche Rahmen des Datenschutzes, in: Belser Eva Maria/Epiney Astrid/Waldmann Bernhard (Hrsg.), Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, 33–51 (zit.: Datenschutzrecht, § …)

Belser Eva Maria, Zur rechtlichen Tragweite des Grundrechts auf Datenschutz: Missbrauchsschutz oder Schutz der informationellen Selbstbestimmung?, in: Epiney Astrid/Burkert Herbert (Hrsg.), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung = Instruments de mise en oeuvre du droit à l'autodétermination informationnelle, Zürich/Basel/Genf 2013, 19–45 (zit.: Rechtliche Tragweite)

Benhamou Yaniv, Kommentierung zu Art. 28 und Art. 29, in: Meier Philippe/Métille Sylvain (Hrsg.), Loi fédérale sur la protection des données, Commentaire Romand, Basel 2023 (zit.: CR LPD-Benhamou, Art. … N …)

Bergt Matthias, Kommentierung zu Art. 83 DSGVO, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung, BDSG, Kommentar, 4. Aufl., München 2024 (zit.: BeckKomm-Bergt, Art. 83 DSGVO N …)

Berlin Isaiah, Freiheit, Vier Versuche, Frankfurt am Main 2006

Berners-Lee Tim, Long Live the Web, Scientific American 2010, 80–85

BEUC, EU General Data Protection Framework, BEUC Answer to Consultation vom 31. Dezember 2009

Biaggini Giovanni, Orell Füssli Kommentar zur Bundesverfassung der Schweizerischen Eidgenossenschaft, 2. Aufl., Zürich 2017 (zit.: OFK BV-Biaggini, Art. … N …)

Bieri Adrian/Heymann Jaël/Odermatt Jacqueline, Kommentierung zu Art. 28 und Art. 29, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023 (zit.: OFK DSG-Bieri/Heymann/Odermatt, Art. … N …)

Bieri Adrian/Powell Julian, Die Totalrevision des Bundesgesetzes über den Datenschutz, Jusletter 16. November 2020

Bijok Alexander, Kommerzialisierungsfester Datenschutz, Rechtliche Problemlagen der Datennutzung in der Informationswirtschaft, Baden-Baden 2020

Birk Rasmus H./Samuel Gabrielle, Digital Phenotyping for Mental Health: Reviewing the Challenges of Using Data to Monitor and Predict Mental Health Problems, CPR 2022, 523–528

Bitter Philip/Straker Christian, Zugang zu Daten – technolegale Annäherung an eine Querschnittsmaterie, in: Taeger Jürgen/Deutsche Stiftung für Recht und Informatik (Hrsg.), Die Macht der Daten und der Algorithmen, Regulierung von IT, IoT und KI, Edewecht 2019, 743–755

Blatter Marc, Digitalisierung – Herausforderungen für die Wettbewerbspolitik, sic! 2016, 378–386

Blechta Gabor-Paul/Dal Molin Luca/Wesiak-Schmidt Kirsten, Kommentierung zu Art. 5, in: Vasella David/Blechta Gabor-Paul (Hrsg.), Basler Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, 4. Aufl., Basel 2024 (zit.: BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt, Art. 5 N …)

Blumer Lara, Telematik und Motorfahrzeugversicherung, Rahmenbedingungen und Vertragsgestaltung in der Schweiz, Zürich 2024

Bomhard David, Der Anwendungsbereich des Data Act, Offene Fragen rund um Art. 1 DA, MMR 2024, 71–75

Bondolfi Alberto, Zur «Privatsphäre» in sozialethischer Sicht: Einige Grundsatzüberlegungen zur ethischen Dimension des Datenschutzes, in: Baeriswyl Bruno/Rudin Beat (Hrsg.), Perspektive Datenschutz, Praxis und Entwicklungen in Recht und Technik, Zürich 2002, 127–141

Bosshardt Lorenz/Hermann Michael, Mobile Datennutzung in der Schweiz, Datenwachstum und Datenstau im mobilen Datennetz der Schweiz – 2010 bis 2021, Studie der Forschungsstelle Sotomo vom Mai 2021, <https://perma.cc/43BG-ABCZ>

Brall Caroline/Berlin Claudia/Zwahlen Marcel/Ormond Kelly E./Egger Matthias/Vayena Effy, Public willingness to participate in personalized health research and biobanking: A large-scale Swiss survey, PLoS ONE 2021, e0249141, 1–17

Brändli Sebastian, Gesundheitswesen, in: Historisches Lexikon der Schweiz <https://perma.cc/3874-XBAV>

Brandt Elena/Grewe Max, Datenportabilität 2.0, Neue Vorgaben im Zuge der EU-Digitalstrategie, MMR 2023, 928–932

Brauchbar Mathis, Nutzung von Gesundheitsdaten im digitalen Zeitalter, Bioethica Forum 2015, 54–55

Braun Binder Nadja/Thomas Burri/Lohmann Melinda Florina/Simmler Monika/Thouvenin Florent/Vokinger Kerstin Noëlle, Künstliche Intelligenz: Handlungsbedarf im Schweizer Recht, Jusletter 28. Juni 2021

Bräutigam Peter/Richter Diana, Vertragliche Aspekte der Social Media, in: Hornung Gerrit/Müller-Terpitz Ralf (Hrsg.), Rechtshandbuch Social Media, Berlin/Heidelberg 2021, 81–129

Breitenmoser Stephan, Kommentierung zu Art. 13, in: Ehrenzeller Bernhard/Schindler Benjamin/Schweizer Rainer J. (Hrsg.), St. Galler Kommentar zur schweizerischen Bundesverfassung, 4. Aufl., Zürich/St. Gallen 2023 (zit.: SGK BV-Breitenmoser, Art. 13 N …)

Brenner Tobias, Regulierung mithilfe des Kartellrechts? – Verpflichtungszusagen der Europäischen Kommission, EuR 2014, 671–698

Brink Stefan/von Ungern-Sternberg Antje, Einführung zum Data Act (DA), in: Wolff Heinrich Amadeus/Brink Stefan/von Ungern-Sternberg Antje (Hrsg.), BeckOK Datenschutzrecht, 53. Aufl., München 2025 (zit.: BeckOK DSR-Brink/von Ungern-Sternberg, Einführung zum Data Act (DA) N …)

Britz Gabriele, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Hoffmann-Riem Wolfgang (Hrsg.), Offene Rechtswissenschaft, Ausgewählte Schriften und begleitende Analysen, Tübingen 2010, 561–596

Brorsen Hans/Falk Richard, Die «Maschinenlesbarkeit» von Informationen, Unter der Haube der EU-Digitalregulierung, MMR 2025, 7–12

Brüggemann Sebastian, Das Recht auf Datenportabilität, in: Taeger Jürgen (Hrsg.), Recht 4.0 – Innovationen aus den rechtswissenschaftlichen Laboren, Tagungsband Herbstakademie 2017, Edewecht 2017, 1–13

Brüggemann Sebastian, Das Recht auf Datenportabilität, K&R 2018, 1–5

Büchler Andrea, Persönlichkeitsgüter als Vertragsgegenstand?, Von der Macht des Faktischen und der dogmatischen Ordnung, in: Honsell Heinrich/Rey Heinz (Hrsg.), Aktuelle Aspekte des Schuld- und Sachenrechts, Festschrift für Heinz Rey zum 60. Geburtstag, Zürich 2003, 177–195

Büchler Andrea, Die Kommerzialisierung von Persönlichkeitsgütern, Zur Dialektik von Ich und Mein, AcP 2–3/2006, 300–351

Buchner Benedikt, Wissen ist Macht?, Zum Verhältnis zwischen Datenschutz und Wettbewerb, DuD 2008, 724–728

Buchner Benedikt, Datenschutz und Kartellrecht, WRP 2019, 1243–1248

Bühler Gregor, § 4 Zivilrechtliche Rechtsdurchsetzung, in: Dal Molin Luca/Wesiak-Schmidt Kirsten (Hrsg.), Datenschutz im Unternehmen, Praxishandbuch mit Beispielen und Checklisten, Zürich 2023, 259–303

Cattaneo Gianni, Legge federale sulla protezione dei dati (nLPD) e Ordinanza sulla protezione dei dati (nOPDa): struttura, principi e obblighi nel settore privato, in: Bernasconi Giorgio A./Pasucci Paola (Hrsg.), Protezione dei dati personali: orizzonte 2023, Introduzione alle nuove norme di livello federale e cantonale, Basel 2024, 3–67

Chao Yongle/Xu Meihe/Tamò-Larrieux Aurelia/Kollnig Konrad, Data portability strategies in the EU: Moving beyond individual rights, CLSR 2025, 106135, 1–11

Charlet François, Protection des données en entreprise, Basel 2023

Cichocki Michal, Big Data und Datenschutz: Ausgewählte Aspekte, Jusletter IT 21. Mai 2015

Ciortuz Gabriela/Wiedekopf Joshua/Fudickar Sebastian, Integration von Wearables und Nutzung von digitalen Biomarkern zur Diagnostik und Therapie im Gesundheitswesen, in: Henke Viola/Hülsken Gregor/Schneider Henning/Varghese Julian (Hrsg.), Health Data Management, Wiesbaden 2024, 323–336

Clement Reiner/Schreiber Dirk/Bossauer Paul/Pakusch Christina, Internet-Ökonomie, Grundlagen und Fallbeispiele der digitalen und vernetzten Wirtschaft, Berlin/Heidelberg 2019

Copetti Cravo D., How to Make Data Portability Right More Meaningful for Data Subjects?, EDPL 2022, 52–60

Cornils Matthias, Der grundrechtliche Rahmen für ein (trans-)nationales Datenschutzrecht im digitalen Zeitalter, in: Stern Klaus/Pfeifer Karl-Nikolaus/Hain Karl-E. (Hrsg.), Datenschutz im digitalen Zeitalter – global, europäisch, national, Vortragsveranstaltung des Instituts für Rundfunkrecht an der Universität zu Köln vom 16. Mai 2014, München 2015, 11–50

Dal Molin Luca, § 1 Grundlagen des Datenschutzrechts in Unternehmen, in: Dal Molin Luca/Wesiak-Schmidt Kirsten (Hrsg.), Datenschutz im Unternehmen, Praxishandbuch mit Beispielen und Checklisten, Zürich 2023, 5–101

Daumke Philipp/Haverkamp Christian/Heckmann Simone/Kuper Marcus/Müller Annett/Oemig Frank/Ripperger Uta/Sabutsch Stefan/Sander André/Schulz Stefan, Kommunikationsfähigkeit und Interoperabilität von Gesundheitsdaten in einem vernetzten Gesundheitssystem, in: Henke Viola/Hülsken Gregor/Schneider Henning/Varghese Julian (Hrsg.), Health Data Management, Wiesbaden 2024, 457–496

De Hert Paul/Papakonstantinou Vagelis/Malgieri Gianclaudio/Beslay Laurent/Sanchez Ignacio, The right to data portability in the GDPR: Towards user-centric interoperability of digital services, CSLR 2018, 193–203

De La Mano Miguel/Padilla Jorge, Big Tech Banking, JCLE 2018, 494–526

Denoth Seraina/Kaufmann Oliver, Kartellrechtliches Erfassen von Wettbewerbswirkungen grosser Datenbestände (Big Data), sic! 2016, 501–516

Deuring Simon, Datenmacht, Zugang als Herausforderung, Baden-Baden 2021

Dewenter Ralf/Bernhardt Lea, Ökonomische Grundlagen, in: Künstner Kim Manuel/Louven Sebastian (Hrsg.), Plattform-Governance und Recht, Berlin 2024, 19–61

Di Porto Fabiana/Ghidini Gustavo, «I Access Your Data, You Access Mine»: Requiring Data Reciprocity in Payment Services, IIC 2020, 307–329

Dierks Christian, Health Data: Datenschutzrechtlicher Rahmen und Nutzungsmöglichkeiten im Krankenhaus, Verbesserte Datennutzung durch Kenntnis des Rechtsrahmens, in: Henke Viola/Hülsken Gregor/Schneider Henning/Varghese Julian (Hrsg.), Health Data Management, Wiesbaden 2024, 225–239

Diggelmann Oliver, Kommentierung zu Art. 13, in: Waldmann Bernhard/Belser Eva Maria/Epiney Astrid (Hrsg.), Basler Kommentar zur Bundesverfassung, Basel 2015 (zit.: BSK BV-Diggelmann, Art. 13 N …)

Dix Alexander, Kommentierung zu Art. 20 DSGVO, in: Simitis Spiros/Hornung Gerrit/Spiecker genannt Döhmann Indra (Hrsg.), Nomos Kommentar zum Datenschutzrecht, DSGVO/BDSG, 2. Aufl., Baden-Baden 2024 (zit.: NomosKomm-Dix, Art. 20 DSGVO N …)

Drepper Johannes/Schlünder Irene/Buckow Karoline, Praktische Umsetzbarkeit der Datenportabilität im Bereich der medizinischen Forschung, in: Stiftung Datenschutz, Praktische Umsetzung des Rechts auf Datenübertragbarkeit, Rechtliche, technische und verbraucherbezogene Implikationen, 3. Aufl., Leipzig 2018, 178–196

Drexl Josef, Designing Competitive Markets for Industrial Data – Between Propertisation and Access, 2016, <https://perma.cc/7M3X-VUVQ> (zit.: Competitive Markets)

Drexl Josef, Data Access and Control in the Era of Connected Devices, Study on Behalf of the European Consumer Organisation BEUC, 2018 (zit.: Data Access)

Drexl Josef, Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy, in: De Franceschi Alberto/Schulze Reiner (Hrsg.), Digital Revolution – new challenges for law: data protection, artificial intelligence, smart products, blockchain technology and virtual currencies, München/Baden-Baden 2019, 19–41 (zit.: Challenges)

Drexl Josef, Connected devices – An unfair competition law approach to data access rights of users, in: German Federal Ministry of Justice and Consumer Protection/Max Planck Institute for Innovation and Competition (Hrsg.), Data Access, Consumer Interests and Public Welfare, Baden-Baden 2021, 477–527 (zit.: Connected Devices)

Drexl Josef/Banda Carolina/González Otero Begoña/Hoffmann Jörg/Kim Daria/Kulhari Shraddha/Moscon Valentina/Richter Heiko/Wiedemann Klaus, Position Statement of the Max Planck Institute for Innovation and Competition on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act) vom 25. Mai 2022, <https://perma.cc/J9EU-62YM>

Drexl Josef/Hilty Reto/Desaunettes Luc/Greiner Franziska/Kim Daria/Richter Heiko/Surblyte Gintare/Wiedemann Klaus, Data Ownership and Access to Data – Position Statement of the Max Planck Institute for Innovation and Competition on the Current European Debate vom 16. August 2016, <https://perma.cc/3RBS-UG4T> (zit.: Data Ownership)

Drexl Josef/Hilty Reto/Globocnik Jure/Greiner Franziska/Kim Daria/Richter Heiko/Slowinski Peter R./Surblyte Gintare/Walz Axel/Wiedemann Klaus, Position Statement of the Max Planck Institute for Innovation and Competition on the European Commissions «Public consultation on Building the European Data Economy» vom 26. April 2017, <https://perma.cc/8UPQ-QYAB> (zit.: European Data Economy)

Duller Yannic, Data access and portability, Diss. Wien 2024

Dumauthioz Michel/Löhrer Tobias/Singler Sebastian, Shape the Future of Mobility – Für ein zukunftsfähiges Schweizer Mobilitätssystem, Barrieren, Stossrichtungen und Handlungsempfehlungen für ein Mobilitätsökosystem, 2019, <https://perma.cc/4QCR-6379>

Dumermuth Martin, Grundrechtskollisionen auf Social Media, in: Brunner Arthur/Josuran-Binder Anja Martina/Zumsteg Patrice Martin (Hrsg.), Der Mensch als Massstab des Rechts, Liber amicorum für Regina Kiener, Zürich 2025, 129–161

Durchholz Sebastian, Datenübertragbarkeit und Interoperabilität in der DSGVO und den neuen EU-Digitalgesetzen, PinG 2024, 209–216

Durmus Erdem/Kaplan Nadya, Das Recht auf Datenübertragbarkeit – Anwendungsbeispiele jenseits von Social Networks, DSB 2023, 203–206

Durner Wolfgang, Kommentierung zu Art. 10, in: Dürig Günter/Herzog Roman/Scholz Rupert/Herdegen Matthias/Klein Hans H./Maunz Theodor (Hrsg.), Grundgesetz: Kommentar, Band II, 107. Aufl., München 2025 (zit.: GG Komm-Durner, Art. 10 N …)

Ebersberger Bernd/Dachs Bernhard, Die Ökonomik digitaler multinationaler Unternehmen, in: Staffler Lukas/Ebersberger Bernd/Jobin Anna (Hrsg.), Digitalwirtschaft, Technische, wirtschaftliche und gesellschaftliche Grundlagen, Wiesbaden 2024, 69–85

Eckardt Martina/Kerber Wolfgang, Property rights theory, bundles of rights on IoT data, and the EU Data Act, EJLE 2024, 113–143

Eckardt Martina/Kerber Wolfgang, Designing the Bundle of Rights on IoT Data: The EU Data Act, in: Sattler Andreas/Zech Herbert (Hrsg.), The Data Act: First Assessments, Trier 2024, 1–22

Eckert Martin, Digitale Daten als Wirtschaftsgut: digitale Daten als Sache, SJZ 2016, 245–249

Eggen Mirjam/Toneatti Michael, Zahlen mit Daten, Eine schuldrechtliche Einordnung von Daten als Entgelt, Jusletter 18. November 2024

Elfering Stephanie, Unlocking the right to data portability, An analysis of the interface with the sui generis database right, Baden-Baden 2019

Engels Barbara, Data portability among online platforms, Internet Policy Review 2/2016, 1–17

Ensthaler Jürgen/Üge Duygu, Wem gehören die durch die Nutzung von Maschinen generierten Daten?, BB 2022, 2051–2055

Epiney Astrid, Big Data und Datenschutzrecht: Gibt es einen gesetzgeberischen Handlungsbedarf?, Jusletter IT 21. Mai 2015

Epiney Astrid/Nüesch Daniela/Rovelli Sophia, Datenschutzrecht in der Schweiz, Eine Einführung in das Datenschutzgesetz des Bundes, mit besonderem Akzent auf den für Bundesorgane relevanten Vorgaben, Bern 2023

Epiney Astrid/Zlatescu Petru Emanuel, Kommentierung zu Art. 1, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023 (zit.: OFK DSG-Epiney/Zlatescu, Art. 1 N …)

Erard Frédéric/di Tria Livio, Consentement aux traitements de données en cabinet médical, Ni libre, ni éclairé, ni nécessaire ?, Jusletter 23. September 2024

Ernst Stefan, Kommentierung zu Art. 1 DSGVO, in: Paal Boris P./Pauly Daniel A. (Hrsg.), Beck'scher Kompakt-Kommentar zur Datenschutzgrundverordnung und zum Bundesdatenschutzgesetz, 3. Aufl., München 2021 (zit.: BeckKompaktKomm-Ernst, Art. 1 DSGVO N …)

Evers Hans Ulrich, Privatsphäre und Ämter für Verfassungsschutz, Berlin/Boston 1960

EY/FIA Region I, Expert study on: 'GDPR application in the context of car connectivity', Final Report vom November 2021, <https://perma.cc/PJ4Q-AF2G>

Fankhauser Roland, Kommentierung zu Art. 19c, in: Geiser Thomas/Fountoulakis Christina (Hrsg.), Basler Kommentar zum Zivilgesetzbuch I. Art. 1–456 ZGB, 7. Aufl., Basel 2022 (zit.: BSK ZGB I-Fankhauser, Art. 19c N …)

Fasnacht Tobias, Die Einwilligung im Datenschutzrecht, Vorgaben einer völker- und verfassungsrechtlich konformen Ausgestaltung der datenschutzrechtlichen Einwilligung im schweizerischen Recht, Genf/Zürich/Basel 2017

Fast Victoria/Schnurr Daniel/Wohlfarth Michael, Marktmacht durch Daten: Eine Analyse aus ökonomischer Perspektive, in: Specht-Riemenschneider Louisa/Werry Nikola/Werry Susanne (Hrsg.), Datenrecht in der Digitalisierung, Berlin 2020, 745–778

Fellmann Walter, Arzt und das Rechtsverhältnis zum Patienten, in: Kuhn Moritz W./Poledna Tomas (Hrsg.), Arztrecht in der Praxis, 2. Aufl., Zürich/Basel/Genf 2007, 103–231

FIA Region I, Policy Position on Car Connectivity vom April 2016, <https://perma.cc/R5F6-X4PA>

Fix Alexander Daniel, Das Recht auf Datenportabilität, Art. 20 DSGVO als Schnittstelle zwischen Wettbewerbsförderung und Datenschutz, Berlin 2022

Flückiger Alexandre, L'autodétermination en matière de données personnelles: un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété?, AJP 2013, 837–863

Flügge Barbara, Ecosystems Thinking, Gestaltungsrahmen für intelligente Mobilitätskonzepte, in: Flügge Barbara (Hrsg.), Smart Mobility, Trends, Konzepte, Best Practices für die intelligente Mobilität, 2. Aufl., Wiesbaden 2020, 53–76

Forstmoser Peter/Vogt Hans-Ueli, Einführung in das Recht, 5. Aufl., Bern 2012

Frei Nula, Die Revision des Datenschutzgesetzes aus europarechtlicher Sicht, Jusletter 17. September 2018

Früh Alfred, Zum Bedarf nach Datenzugangsrechten, Jusletter IT Flash 11. Dezember 2017

Früh Alfred, Datenzugangsrechte, Rechtsrahmen für einen neuen Interessenausgleich in der Datenwirtschaft, sic! 2018, 521–539

Früh Alfred, Datenzuordnung und Datenzugang, Eine Übersicht über Stand und Entwicklungspotenziale zweier komplementärer Aspekte der Datenpolitik, digma 2019, 172–176

Früh Alfred/Braun Binder Nadja/Schibli Robert, Data Governance für Smart Mobility aus rechtlicher Perspektive, sui generis 2022, 15–23

Früh Alfred/Schibli Robert/Braun Binder Nadja, Sekundärnutzung von Mobilitätsdaten: Infrastruktur und Governance bei Mobility-as-a-Service, SZW 2023, 69–79

Füllsack Anna Lena/Kirschke-Biller Jonathan, Kapitel 5: Datenschutz, in: Gerecke Martin (Hrsg.), Handbuch Social-Media-Recht, München 2023, 229–298

Funk Axel, Das Prinzip der Nutzerzentriertheit des Data Act – ein gravierender Strukturfehler, Untersuchung und Bewertung der zentralen Rolle des Nutzers in der Datenökonomie nach der Konzeption des Data Act, CR 2023, 421–427

Gächter Thomas/Egli Philipp, Informationsaustausch im Umfeld der Sozialhilfe, Jusletter 6. September 2010

Gächter Thomas/Werder Gregori, Einbettung ausgewählter Konzepte in das schweizerische Datenschutzrecht, in: Epiney Astrid/Burkert Herbert (Hrsg.), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung = Instruments de mise en oeuvre du droit à l'autodétermination informationnelle, Zürich/Basel/Genf 2013, 87–111

Gal Michal S./Rubinfeld Daniel L., Data Standardization, New York University Law Review 2019, 737–770

Garstka Hansjürgen, Selbstdatenschutz, in: Baeriswyl Bruno/Rudin Beat (Hrsg.), Perspektive Datenschutz, Praxis und Entwicklungen in Recht und Technik, Zürich/Baden-Baden 2002, 159–175

Gasser Urs, Perspectives on the Future of Digital Privacy, ZSR II/2015, 335–448

Gatti Stefano, Dalla portabilità alle «portabilità»: l'evoluzione al plurale di un diritto (e concetto) chiave nella disciplina europea dei dati, EJPLT 2024, 157–177

Gehring Kaspar, Neues DSG / Auswirkungen auf die Sozialversicherungen, HAVE 2023, 224–227

Geminn Christian/Rossnagel Alexander, Datenschutz-Grundverordnung verbessern, Änderungsvorschläge aus Verbrauchersicht, Baden-Baden 2020

Genecand Téo, Kommentierung zu Art. 31, in: Benhamou Yaniv/Cottier Bertil (Hrsg.), Petit commentaire LPD, Loi sur la protection des données, Basel 2023 (zit.: PC LPD-Genecand, Art. 31 N …)

George Damian, Prinzipien und Rechtmässigkeitsbedingungen im privaten Datenschutzrecht, Kritische Betrachtungen zu Geschichte und Gegenwart eines Schutzkonzepts in der Schweiz und der Europäischen Union, Zürich/Basel/Genf 2021 (zit.: Prinzipien)

George Damian, § 17: Datenschutz im Gesundheitswesen und Heilmittelbereich (E-Health), in: MLL Legal (Hrsg.), Praxishandbuch Produktregulierung, Genf/Zürich/Basel 2023, 635–689 (zit.: Gesundheitswesen)

Gerber Felix, Kosteneinsparung durch Datenaustausch, Nutzung von Einsparpotentialen durch Austausch von Daten über Patienten und Versicherte im schweizerischen Gesundheitswesen, Muri 1991

Gill Daniel/Kerber Wolfgang, Data Portability Rights: Limits, Opportunities, and the Need for Going Beyond the Portability of Personal Data, CPI Antitrust Chronicle 2020, 54–59

Gill Daniel/Metzger Jakob, Data Access through Data Portability: Economic and Legal Analysis of the Applicability of Art. 20 GDPR to the Data Access Problem in the Ecosystem of Connected Cars, EDPL 2022, 221–237

Glass Philip, Die rechtsstaatliche Bearbeitung von Personendaten in der Schweiz, Regelungs- und Begründungsstrategien des Datenschutzrechts mit Hinweisen zu den Bereichen Polizei, Staatsschutz, Sozialhilfe und elektronische Informationsverarbeitung, Zürich/St. Gallen 2017

Glatthaar Matthias, Prompts für eine Optimierung des Datenschutzrechts, in: Datenschutz-Forum Schweiz (Hrsg.), Persönlichkeitsschutz zwischen Mensch und Maschine, 25 Jahre Datenschutz-Forum Schweiz, Zürich/Genf 2024, 19–30

Gohari Ramin Silvan, Die Essential Facilities-Doktrin, sic! 2019, 533–549

Golder Lukas/Keller Tobias/Schena Corina/Rellstab Sara, Swiss eHealth Barometer 2024: Mit KI in die Zukunft vom 22. März 2024, <https://perma.cc/U7GJ-HTWN>

Golland Alexander, Datenverarbeitung in sozialen Netzwerken, Frankfurt am Main 2019

Gonin Luc, Droit constitutionnel suisse, Genf 2021

Gordon Clara-Ann, Daten aus Selbstvermessung, Eine Analyse der datenschutzrechtlichen Rahmenbedingungen von Quantified Self in der Schweiz, digma 2016, 70–75

Götzinger Lena/Vasella David, Datenportabilität und ihre Umsetzung, SZW 2021, 40–51

Graef Inge, Mandating portability and interoperability in online social networks: Regulatory and competition law issues in the European Union, Telecommunications Policy 2015, 502–514

Graef Inge, EU competition law, data protection and online platforms, Data as essential facility, Alphen aan den Rijn 2016

Graef Inge, The Opportunities and Limits of Data Portability for stimulating Competition and Innovation, CPI Antitrust Chronicle 2020, 34–41

Graef Inge/Gellert Raphaël/Husovec Martin, Towards a holistic regulatory approach for the European data economy: Why the illusive notion of non-personal data is counterproductive to data innovation, European Law Review 2019, 605–621

Graef Inge/Husovec Martin/Purtova Nadezhda, Data Portability and Data Control: Lessons for an Emerging Concept in EU Law, GLJ 2018, 1359–1398

Graef Inge/Husovec Martin/Van den Boom Jasper, Spill-Overs in Data Governance: Uncovering the Uneasy Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes, EuCML 2020, 3–16

Graef Inge/Verschakelen Jeroen/Valcke Peggy, Putting the Right to Data Portability into a Competition Law Perspective, LJHSE 2013, 53–63

Gramigna Ralph, Kommentierung zu Art. 25, in: Vasella David/Blechta Gabor-Paul (Hrsg.), Basler Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, 4. Aufl., Basel 2024 (zit.: BSK DSG-Gramigna, Art. 25 N …)

Grünig Shirin, Die Haftung nach Humanforschungsgesetz, Genf/Zürich/Basel 2020

Guillod Olivier, Droit médical, Basel 2020

Gusy Christoph/Eichenhofer Johannes, Kommentierung zu § 1 BDSG, in: Wolff Heinrich Amadeus/Brink Stefan/von Ungern-Sternberg Antje (Hrsg.), BeckOK Datenschutzrecht, 53. Aufl., München 2025 (zit.: BeckOK DSR-Gusy/Eichenhofer, § 1 BDSG N …)

Häfelin Ulrich/Haller Walter/Keller Helen/Thurnherr Daniela, Schweizerisches Bundesstaatsrecht, 11. Aufl., Zürich/Genf 2024

Hanloser Stefan, EuGH: FIN kann personenbezogenes Datum sein, ZD 2024, 173–176

Hartmann Bernd/McGuire Mary-Rose/Schulte-Nölke Hans, Datenzugang bei smarten Produkten nach dem Entwurf für ein Datengesetz (Data Act), Rechtliche Rahmenbedingungen für die Vertragsgestaltung, RDi 2023, 49–59

Haucap Justus/Kruse Jörn, Ex-Ante-Regulierung oder Ex-Post-Aufsicht für netzgebundene Industrien?, Diskussionspapier Nr. 25 der Universität der Bundeswehr Hamburg vom November 2003, <https://www.econstor.eu/bitstream/10419/23541/1/paperno25.pdf>

Hawker Norman W., Automotive Aftermarkets: A Case Study in Systems Competition, The Antitrust Bulletin 2011, 57–79

Heinemann Andreas, Das Kartell- und Regulierungsrecht der Netzindustrien aus Schweizer Perspektive, in: Bien Florian/Ludwigs Markus (Hrsg.), Das europäische Kartell- und Regulierungsrecht der Netzindustrien, Baden-Baden 2015, 205–239

Heinemann Andreas, 25 Jahre Kartellgesetz, ius.full 2021, 166–178

Heinemann Andreas, Plattformregulierung und allgemeines Kartellrecht – aus Sicht der Schweiz, ZWeR 2022, 308–319

Heinemann Andreas/Meier Giulia Mara, Der Digital Markets Act (DMA): Neues «Plattformrecht» für mehr Wettbewerb in der digitalen Wirtschaft, EuZ 2021, 86–101

Helmond Anne, The Platformization of the Web: Making Web Data Platform Ready, SM+S 2/2015, 1–11

Hempel Gunnar/Schmid Karl, Expertise zur Datenportabilität vom 4. Oktober 2017, in: Stiftung Datenschutz, Praktische Umsetzung des Rechts auf Datenübertragbarkeit, Rechtliche, technische und verbraucherbezogene Implikationen, 3. Aufl., Leipzig 2018, 226–245

Hennemann Moritz, Datenportabilität, PinG 2017, 5–8

Hennemann Moritz/Steinrötter Björn, Der Data Act, Neue Instrumente, alte Friktionen, strukturelle Weichenstellungen, NJW 2024, 1–8

Herbst Tobias, Kommentierung zu Art. 20 DSGVO, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung, BDSG: Kommentar, 4. Aufl., München 2024 (zit.: BeckKomm-Herbst, Art. 20 DSGVO N …)

Hermonies Felix, VII. Rechte der Betroffenen, 7. Datenübertragbarkeit, in: Jandt, Silke/Steidle, Roland (Hrsg.), Datenschutz und Internet, DS-GVO, BDSG, TDDDG, KI-VO, DMA, DSA, 2. Aufl., Baden-Baden 2025, Rz. 73–83

Hettich Peter, § 1: Konsumentenschutz als Verfassungsaufgabe, in: Heiss Helmut/Loacker Leander D. (Hrsg.), Grundfragen des Konsumentenrechts, Zürich 2020, 9–26

Hijmans Hielke, Kommentierung zu Art. 1, in: Kuner Christopher/Bygrave Lee A./Docksey Christopher/Drechsler Laura (Hrsg.), The EU General Data Protection Regulation (GDPR): a commentary, Oxford 2020 (zit.: GDPR-Comm-Hijmans, Art. 1, …)

Hildebrand Volker G., Kundenbindung mit Online Marketing, in: Link Jörg (Hrsg.), Wettbewerbsvorteile durch Online Marketing, Die strategischen Perspektiven elektronischer Märkte, 2. Aufl., Berlin/Heidelberg 2000, 55–75

Hoffmann Raphael/Schmidt Dominik, Facebook-Profiling zu Marketingzwecken – datenschutzkonform?, GRUR 2021, 679–685

Hofstetter David, Das Verhältnismässigkeitsprinzip als Grundsatz rechtsstaatlichen Handelns (Art. 5 Abs. 2 BV), Ausgewählte Aspekte, Zürich/Basel/Genf 2014

Höhn Ernst, Wie grau ist die Theorie?, AJP 1994, 411–424

Hommen Nils, Mashups und weborientierte Architekturen als Technologie-Trends des Web 2.0, in: Kollmann Tobias/Häsel Matthias (Hrsg.), Web 2.0: Trends und Technologien im Kontext der Net Economy, Wiesbaden 2007, 103–120

Honsell Heinrich, Kommentierung zu Art. 1, in: Geiser Thomas/Fountoulakis Christina (Hrsg.), Basler Kommentar zum Zivilgesetzbuch I. Art. 1–456 ZGB, 7. Aufl., Basel 2022 (zit.: BSK ZGB I-Honsell, Art. 1 N …)

Hooke Mary C./Gilchrist Laura/Tanner Lynn/Hart Nicole/Withycombe Janice S., Use of a Fitness Tracker to Promote Physical Activity in Children With Acute Lymphoblastic Leukemia, Pediatric Blood & Cancer 2016, 684–689

Hübener Fabian/Lutz Benedikt, Zugang zu Fahrzeugreparatur- und -wartungsinformationen: Welche Rolle spielt das Kartellrecht?, ZWeR 2024, 130–152

Huber Felix, Das BAG soll keine weiteren Kompetenzen mehr erhalten, SÄZ 2022, 174–175

Husi-Stämpfli Sandra, Entstehungsgeschichte, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz (DSG), 2. Aufl., Bern 2023 (zit.: SHK DSG-Husi-Stämpfli, Entstehungsgeschichte N …)

Husi-Stämpfli Sandra, Kommentierung zu Art. 1, in: Steiner Thomas/Morand Anne-Sophie/Hürlimann Daniel (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz, Version vom 31. Juli 2023 (zit.: OK DSG-Husi-Stämpfli, Art. 1 N …)

Husi-Stämpfli Sandra/Morand Anne-Sophie, Datenschutzrecht, 2. Aufl., Zürich/Genf 2024

Ichihashi Shota, Competing data intermediaries, RJE 2021, 515–537

Irion Kristina/Luchetta Giacomo, Online Personal Data Processing and EU Data Protection Reform, Brüssel 2013

Isler Michael, Lifestyle- oder Medizinprodukt?, Datengetriebene Dienste zur Vermessung des eigenen Körpers betreten mitunter auch reguliertes Terrain, digma 2016, 64–69

Isler Michael, Die Rollenverteilung in klinischen Versuchen, digma 2020, 68–72

ISO, Information technology — Cloud computing — Interoperability and portability (ISO/IEC 19941) vom Dezember 2017 (zit.: ISO/IEC 19941)

ISO, Road Vehicles — Extended vehicle (ExVe) methodology — Part 1: General information (ISO 20077-1:2017) vom Dezember 2017 (zit.: ISO 20077-1:2017)

Janal Ruth, Data Portability – A Tale of Two Concepts, JIPITEC 2017, 59–59

Janal Ruth, Data portability under the GDPR: A blueprint for access rights?, in: German Federal Ministry of Justice and Consumer Protection/Max Planck Institute for Innovation and Competition (Hrsg.), Data Access, Consumer Interests and Public Welfare, Baden-Baden 2021, 319–342

Jandt Silke/Rossnagel Alexander, Datenschutz in Social Networks, Kollektive Verantwortlichkeit für die Datenverarbeitung, ZD 2011, 160–166

Jentzsch Nicole, Die persönliche Datenökonomie: Plattformen, Datentresore und persönliche Clouds, Ökonomische Rahmenbedingungen innovativer Lösungen zu Einwilligungen im Datenschutz, Berlin 2017

Jotterand Alexandre, Contrats cloud : qualification, gestion des données et sortie de la relation, in: Métille Sylvain (Hrsg.), L'informatique en nuage, Bern 2022, 1–33

Jotterand Alexandre, (Non-Personal) Data Sharing in Switzerland, sic! 2025, 441–454

Jülicher Tim/Röttgen Charlotte/v. Schönfeld Max, Das Recht auf Datenübertragbarkeit, Ein datenschutzrechtliches Novum, ZD 2016, 358–362

Kamann Hans-Georg/Braun Martin, Kommentierung zu Art. 20, in: Ehmann Eugen/Selmayr Martin (Hrsg.), Beck'scher Kurz-Kommentar zur Datenschutz-Grundverordnung, 3. Aufl., München 2024 (zit.: KUKO DSGVO-Kamann/Braun, Art. 20 N …)

Kamlah Ruprecht, Right of privacy, Das allgemeine Persönlichkeitsrecht in Amerikanischer Sicht unter Berücksichtigung neuer technologischer Entwicklungen, Köln 1969

Karasoy Özlem/Turgut Gülcan/Degeling Martin, Datenübertragbarkeit – Zwischen Abwarten und Umsetzen, in: Friedewald Michael/Kreutzer Michael/Hansen Marit (Hrsg.), Selbstbestimmung, Privatheit und Datenschutz, Wiesbaden 2022, 327–342

Karikari Bernard A., Big Data in der Automobilindustrie, Die Erhebung von Fahrzeugfunktionsdaten als Rechtsproblem, Frankfurt am Main 2018

Katz Michael L./Shapiro Carl, Systems Competition and Network Effects, JEP 1994, 93–115

Kerber Wolfgang, Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data, JIPITEC 2018, 310–331

Kerber Wolfgang, Data Sharing in IoT Ecosystems and Competition Law: The Example of connected Cars, JCLE 2019, 381–426

Kerber Wolfgang, From (horizontal and sectoral) data access solutions towards data governance systems, in: German Federal Ministry of Justice and Consumer Protection/Max Planck Institute for Innovation and Competition (Hrsg.), Data Access, Consumer Interests and Public Welfare, Baden-Baden 2021, 441–476

Kerber Wolfgang, Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives, GRUR Int. 2023, 120–135

Kerber Wolfgang/Frank Jonas Severin, Data Governance Regimes in the Digital Economy: The Example of Connected Cars, 2017, <https://perma.cc/3LDH-6G2G>

Kerber Wolfgang/Gill Daniel, Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation, JIPITEC 2019, 244–256

Kerber Wolfgang/Gill Daniel, Datenzugang und Datenschutz im vernetzten Fahrzeug: eine ökonomische Perspektive, in: Stiftung Datenschutz (Hrsg.), Datenschutz im vernetzten Fahrzeug, Berlin 2020, 85–99

Kerber Wolfgang/Schweitzer Heike, Interoperability in the Digital Economy, JIPITEC 2017, 39–58

Kerber Wolfgang/Specht-Riemenschneider Louisa, Synergies between Data Protection Law and Competition Law, Gutachten im Auftrag der Verbraucherzentrale Bundesverband vom 30. September 2021

Kindler Thomas, Händlerverträge in der Schweizer Automobilbranche, Unter besonderer Berücksichtigung vertriebs- und wettbewerbsrechtlicher Gesichtspunkte, Bern 2000

Klar Manuel/Kühling Jürgen, Kommentierung zu Art. 4 Ziff. 1 DSGVO, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung, BDSG: Kommentar, 4. Aufl., München 2024 (zit.: BeckKomm-Klar/Kühling, Art. 4 Ziff. 1 DSGVO N …)

Klaus Samuel/Thomann Kenzo, Kommentierung zu Art. 6, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023 (zit.: OFK DSG-Klaus/Thomann, Art. 6 N …)

Klement Jan Henrik, Kommentierung zu Art. 8 DSGVO, in: Simitis Spiros/Hornung Gerrit/Spiecker genannt Döhmann Indra (Hrsg.), Nomos Kommentar zum Datenschutzrecht, DSGVO/BDSG, 2. Aufl., Baden-Baden 2024 (zit.: Nomos-Komm-Klement, Art. 8 DSGVO N …)

Klemperer Paul, Markets with Consumer Switching Costs, The Quarterly Journal of Economics 1987, 375–394

Klink-Straub Judith/Straub Tobias, Vernetzte Fahrzeuge – portable Daten, Das Recht auf Datenübertragbarkeit gem. Art. 20 DS-GVO, ZD 2018, 459–463

Kokolakis Spyros, Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon, Computers & Security 2017, 122–134

Kollmann Tobias, Einführung in die E-Community, in: Kollmann Tobias (Hrsg.), Handbuch Digitale Wirtschaft, Wiesbaden 2018, 1–36

Kortus-Schultes Doris, Konvergenz der Ökosysteme, Indirekte Netzwerkeffekte und Monetarisierungsmodelle auf digitalen Plattformen für Mobilität, in: Proff Heike (Hrsg.), Mobilität in Zeiten der Veränderung: Technische und betriebswirtschaftliche Aspekte, Wiesbaden 2019, 93–107

Kramer Ernst A./Arnet Ruth, Juristische Methodenlehre, 7. Aufl., Bern 2024

Krämer Jan, Personal Data Portability In The Platform Economy: Economic Implications And Policy Recommendations, JCLE 2021, 263–308

Krämer Jan/Schnurr Daniel, Big Data and Digital Markets Contestability: Theory of Harm and Data Access Remedies, JCLE 2022, 255–322

Krämer Jan/Schnurr Daniel/Broughton Micova Sally, The role of data for digital markets contestability, case studies and data access remedies vom September 2020, <https://perma.cc/4V5T-PLHQ>

Krämer Jan/Senellart Pierre/De Streel Alexandre, Making Data Portability More Effective for the Digital Economy, Economic Implications and Regulatory Challenges vom Juni 2020, <https://perma.cc/4BUS-RK8X>

Kranz Johann/Kuebler-Wachendorff Sophie/Syrmoudis Emmanuel/Grossklags Jens/Mager Stefan/Luzsa Robert/Mayr Susanne, Data Portability, BISE 2023, 597–607

Kratz Alexander, Datenportabilität und «Walled Gardens», InTeR 2019, 26–31

Krause Peter, Datenportabilität, Anwendungsbereich des Rechts auf Datenübertragbarkeit (Teil 1), PinG 2018, 239–243

Krause Peter, Datenportabilität, Pflichten für Verantwortliche im Rahmen des Rechts auf Datenübertragbarkeit (Teil 2), PinG 2019, 13–20

Kuebler-Wachendorff Sophie/Luzsa Robert/Kranz Johann/Mager Stefan/Syrmoudis Emmanuel/Mayr Susanne/Grossklags Jens, The Right to Data Portability: conception, status quo, and future directions, Informatik Spektrum 2021, 264–272

Kühling Jürgen/Hildebrandt Christian/Bulowski Stefan, Die Zukunft der Interoperabilitätsregulierung für OTT-Kommunikationsdienste, K&R 2022, 670–677

Kühling Jürgen/Martini Mario, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, 448–454

Külling-Knecht Céline/Waller Gregor/Willemse Isabel/Deda-Bröchin Svenja/Suter Lilian/Streule Pascal/Settegrana Nicolò/Jochim Mirjam/Bernath Jael/Süss Daniel, JAMES – Jugend, Aktivitäten, Medien – Erhebung Schweiz, Zürich 2024

Lam Wing Man Wynne/Liu Xingyi, Does data portability facilitate entry?, IJIO 2020, 102564, 1–24

Landolt Robin, Datenkooperationen, Der unternehmensübergreifende Zugang zu Daten im Spannungsfeld zwischen Datenschutz und Wettbewerbsförderung, Zürich 2024

Laux Christian, Das Recht auf Datenportabilität, digma 2019, 166–170

Laux Christian/Steiner Thomas, Kommentierung zu Art. 28 und Art. 29, in: Vasella David/Blechta Gabor-Paul (Hrsg.), Basler Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, 4. Aufl., Basel 2024 (zit.: BSK DSG-Laux/Steiner, Art. … N …)

Lazarotto Bárbara da Rosa, The Right to Data Portability: A Holistic Analysis of GDPR, DMA and the Data Act, EJLT 1/2024, 1–15

Leins-Zurmühle Sarah, Mobile Applikationen als Medizinprodukte, Qualifikation und Pflichten nach der revidierten Schweizer Medizinprodukteverordnung, LSR 2021, 137–147

Li Wenkai/Quinn Paul, The European Health Data Space: An expanded right to data portability?, CLSR 2024, 105913, 1–13

Li Wenlong, Data Portability as a New Means of Data Protection? Examining the Right to Data Portability in the EU General Data Protection Regulation, Diss. Edinburgh 2019

Lichtnecker Florian, Die Werbung in sozialen Netzwerken und mögliche hierbei auftretende Probleme, GRUR 2013, 135–140

Lippert André/Schreyer-Bestmann Sylle, Mobilitätsdaten – Treibstoff der Zukunft, BB 2024, 328–335

Louven Sebastian, Datenzugangsverhältnis, FRAND und Wettbewerbsrecht, K&R 2018, 230–236

Louven Sebastian, Braucht es mehr materielles Kartellrecht für digitale Plattformen?, ZWeR 2019, 154–191

Luzsa Robert/Mayr Susanne, Effekte von Datenportabilität auf die Nutzungs- und Zahlungsbereitschaft für Online-Services, Eine Conjoint-Analyse am Beispiel E-Mail-Dienste, 2022, <https://perma.cc/98ZF-DKS5>

Luzsa Robert/Mayr Susanne/Syrmoudis Emmanuel/Grossklags Jens/Kübler-Wachendorff Sophie/Kranz Johann, Datenportabilität zwischen Online-Diensten: Nutzeranforderungen und Gestaltungsempfehlungen, Ergebnisse einer bevölkerungsrepräsentativen Befragung, 2022, <https://perma.cc/SSD3-MXEV>

Lynskey Orla, Aligning data protection rights with competition law remedies? The GDPR right to data portability, European Law Review 2017, 793–814

Lynskey Orla, Kommentierung zu Art. 20, in: Kuner Christopher/Bygrave Lee A./Docksey Christopher/Drechsler Laura (Hrsg.), The EU General Data Protection Regulation (GDPR): a commentary, Oxford 2020 (zit.: GDPR-Comm-Lynskey, Art. 20, …)

Magnin Josianne, Wettbewerbsrecht und Entflechtung im Infrastrukturbereich, Zürich/Genf 2024

Mahon Pascal, Le droit à l'intégrité numérique : réelle innovation ou simple évolution du droit ? Le point de vue du droit constitutionnel, in: Guillaume Florence/Mahon Pascal (Hrsg.), Le droit à l'intégrité numérique, Basel 2021, 43–63

Marsch Nikolaus, Das europäische Datenschutzgrundrecht, Grundlagen, Dimensionen, Verflechtungen, Tübingen 2018

Martens Bertin, An economic perspective on data and platform market power, JRC Digital Economy Working Paper 2020-09, Sevilla 2020 (zit.: Economic Perspective)

Martens Bertin, Data access, consumer interests and social welfare – An economic perspective on data, in: German Federal Ministry of Justice and Consumer Protection/Max Planck Institute for Innovation and Competition (Hrsg.), Data Access, Consumer Interests and Public Welfare, Baden-Baden 2021, 69–102 (zit.: Data Access)

Martens Bertin/Mueller-Langer Frank, Access to digital car data and competition in aftersales services, JRC Digital Economy Working Paper 2018-06, Sevilla 2018

Martens Bertin/Mueller-Langer Frank, Access to Digital Car Data and Competition in Aftermarket Maintenance Services, JCLE 2020, 116–141

Martinelli Silvia, Sharing Data and Privacy in the Platform Economy: The Right to Data Portability and «Porting Rights», in: Reins Leonie (Hrsg.), Regulating New Technologies in Uncertain Times, Den Haag 2019, 133–152

Meier Philippe, Protection des données, Fondements, principes généraux et droit privé, Bern 2010

Mendelsohn Juliane/Budzinski Oliver, § 2: Hintergrund, Ziele und wettbewerbspolitische Einordnung des DMA, in: Schmidt Jens-Peter/Hübener Fabian (Hrsg.), Das neue Recht der digitalen Märkte: Digital Markets Act (DMA), Baden-Baden 2023, 43–65

Menz Monika, Kapitel 7: Sonstige Betroffenenrechte, in: Katko Peter (Hrsg.), Checklisten zur Datenschutz-Grundverordnung (DS-GVO): implementieren, mitigieren, auditieren, München 2020, 155–170

Metere Roberto/Pourmirza Zoya/Walker Sara/Neaimeh Myriam, An Overview of Cyber Security and Privacy on the Electric Vehicle Charging Infrastructure, ArXiv 2022, 1–12

Métille Sylvain, La (nouvelle) Loi fédérale sur la protection des données du 25 septembre 2020 : des principes, des droits et des obligations, in: Epiney Astrid/Moser Sophie/Rovelli Sophia (Hrsg.), Die Revision des Datenschutzgesetzes des Bundes = La révision de la Loi fédérale sur la protection des données, Zürich/Basel/Genf 2022, 1–45 (zit.: Obligations)

Métille Sylvain, Loi fédérale sur la protection des données révisée : principes généraux et nouveautés, in: Défago Valérie/Dunand Jean-Philippe/Mahon Pascal/Posse-Ousmane Samah/Raedler David (Hrsg.), La protection des données dans les relations de travail à la lumière de la nouvelle loi fédérale sur la protection des données, Genf/Zürich 2024, 3–47 (zit.: Nouveautés)

Metzger Axel, Allgemeine Rechtsgrundsätze im Europäischen Privatrecht: Ansätze für eine einheitliche Methodenlehre im europäischen Mehrebenensystem, Rechtstheorie 2009, 313–335

Metzger Axel, Digitale Mobilität – Verträge über Nutzerdaten, GRUR 2019, 129–136

Metzger Axel, Contracts under the Data Act: Review of standard terms and FRAND conditions, in: Sattler Andreas/Zech Herbert (Hrsg.), The Data Act: First Assessments, Trier 2024, 67–81

Metzger Axel/Schweitzer Heike, Shaping Markets: A Critical Evaluation of the Draft Data Act, ZEuP 2023, 42–82

Metzger Axel/Schweitzer Heike/Wagner Gerhard, Datenschutz und Datenmarkt: Grundzüge einer Marktordnung für die europäische Datenwirtschaft, ZfPW 2023, 228–266

Meyer Caroline B., Privatrechtliche Persönlichkeitsrechte im kommerziellen Rechtsverkehr, Eine rechtsvergleichende Untersuchung zur tatsächlichen und rechtlichen Kommerzialisierung von Persönlichkeitsrechten, Basel 2008

Michl Walther, Das Verhältnis zwischen Art. 7 und Art. 8 GRCh – zur Bestimmung der Grundlage des Datenschutzgrundrechts im EU Recht, DuD 2017, 349–353

Müller Jörg Paul, Verwirklichung der Grundrechte nach Art. 35 BV, Der Freiheit Chancen geben, Bern 2018

Müller Jörg Paul/Schefer Markus, Grundrechte in der Schweiz, Im Rahmen der Bundesverfassung, der EMRK und der UNO-Pakte, 4. Aufl., Bern 2008

Munz Martin, Kommentierung zu Art. 20 DSGVO, in: Taeger Jürgen/Gabel Detlev (Hrsg.), Kommunikation & Recht Kommentar zu DSGVO/BDSG/TDDDG, 4. Aufl., Frankfurt am Main 2022 (zit.: KRKomm-Munz, Art. 20 DSGVO N …)

Nagel Lars/Lycklama Douwe, Design Principles for Data Spaces – Position Paper Version 1.0, Berlin 2021, <https://perma.cc/635E-23JT>

Nebel Maxi, Datenportabilität in Social Networks im «Schnellcheck», ZD-Aktuell 2019, 04380

Nebel Maxi/Richter Philipp, Datenschutz bei Internetdiensten nach der DS-GVO, Vergleich der deutschen Rechtslage mit dem Kommissionsentwurf, ZD 2012, 407–413

Nicholas Gabriel, Taking It With You: Platform Barriers to Entry and the Limits of Data Portability, Michigan Technology Law Review 2021, 263–298

Nicholas Gabriel/Weinberg Michael, Data Portability and Platform Competition, Is User Data Exported From Facebook Actually Useful to Competitors?, 2019, <https://perma.cc/97WX-72MF>

Oliveira Marcelo Iury S./Lóscio Bernadette Farias, What is a data ecosystem?, dg.o 2018, 1–9, <https://dl.acm.org/doi/10.1145/3209281.3209335>

Otto Boris/Burmann Anja, Europäische Dateninfrastrukturen, Ansätze und Werkzeuge zur Nutzung von Daten zum Wohl von Individuum und Gemeinschaft, Informatik Spektrum 2021, 283–291

Paal Boris, Marktmacht im Daten(schutz)recht, ZWeR 2020, 215–245

Paal Boris P., Kommentierung zu Art. 20 und Art. 83 DSGVO, in: Paal Boris P./Pauly Daniel A. (Hrsg.), Beck'scher Kompakt-Kommentar zur Datenschutzgrundverordnung und zum Bundesdatenschutzgesetz, 3. Aufl., München 2021 (zit.: BeckKompaktKomm-Paal, Art. … DSGVO N …)

Paal Boris P./Götz Matthias, Aktuelle Rechtsfragen zur Datenübertragbarkeit aus Art. 20 DS-GVO – Voraussetzungen – Verantwortlichkeit – Anspruchsinhalt und -grenzen, ZD 2023, 67–72

Palfrey John G./Gasser Urs, Interop, The promise and perils of highly interconnected systems, New York 2012

Pärli Kurt/Flück Nathalie, Kommentierung zu Art. 25, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz (DSG), 2. Aufl., Bern 2023 (zit.: SHK DSG-Pärli/Flück, Art. 25 N …)

Pautke Stephanie/Oest Isabel, 2. Teil § 3 P.: Automatisiertes Fahren – Kartell- und Wettbewerbsrecht, in: Chibanguza Kuuya/Kuß Christian/Steege Hans (Hrsg.), Künstliche Intelligenz, Recht und Praxis automatisierter und autonomer Systeme, Baden-Baden 2022, 421–430

Payllier Pascal, Rechtsprobleme der ärztlichen Aufklärung, Unter besonderer Berücksichtigung der spitalärztlichen Aufklärung, Zürich 1999

Pfaffinger Monika, Kommentierung zu Art. 1, in: Büchler Andrea/Jakob Dominique (Hrsg.), Kurzkommentar ZGB, 2. Aufl., Basel 2018 (zit.: KUKO ZGB-Pfaffinger, Art. 1 N …)

Pflaum Alexander/Klötzer Christoph, Von der Pipeline zur Plattform – Strategische Implikationen für das Unternehmen, in: Becker Wolfgang/Eierle Brigitte/Fliaster Alexander/Ivens Björn/Leischnig Alexander/Pflaum Alexander/Sucky Eric (Hrsg.), Geschäftsmodelle in der digitalen Welt, Strategien, Prozesse und Praxiserfahrungen, Wiesbaden 2019, 57–73

Picht Peter Georg, Dateneigentum und Datenzugang, Schutz von Geschäftsgeheimnissen als Alternative?, Jusletter IT Flash 11. Dezember 2017

Picht Peter Georg, Towards an Access Regime for Mobility Data, IIC 2020, 940–976

Picht Peter Georg/Nenadic Luka/Barnes Octavia/Eschenbaum Nicolas/Kuster Yannick, Schweizer DMA-Brussels-Effect? Wie Gatekeeper den DMA in der Schweiz (nicht) umsetzen, sic! 2025, 3–14

Pieper Stefan Ulrich, § 6 Rechtsquellen, in: Dauses Manfred A./Ludwigs Markus (Hrsg.), Handbuch des EU-Wirtschaftsrechts, Band I, 64. Aufl., München 2025

Piltz Carlo, Kommentierung zu Art. 20 DSGVO, in: Gola Peter/Heckmann Dirk (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, Kommentar, 3. Aufl., München 2022 (zit.: GK-Piltz, Art. 20 DSGVO N …)

Pletscher Flurina/Mändli Lerch Karin/Glinz Dominik, Willingness to share anonymised routinely collected clinical health data in Switzerland: a cross-sectional survey, SMW 2022, w30182, 1–10

Podszun Rupprecht, Handwerk in der digitalen Ökonomie, Rechtlicher Rahmen für den Zugang zu Daten, Software und Plattformen, Baden-Baden 2021

Podszun Rupprecht, From Competition Law to Platform Regulation – Regulatory Choices for the Digital Markets Act, Economics 1/2023, 20220037, 1–12

Polański Paul Przemysław, Some thoughts on data portability in the aftermath of the Cambridge Analytica scandal, EuCML 2018, 141–146

Putnings Markus, Datenökosystem, in: Putnings Markus/Neuroth Heike/Neumann Janna (Hrsg.), Praxishandbuch Forschungsdatenmanagement, Berlin 2021, 7–10

Rajendra-Nicolucci Chand, Implementing «Continuous and Real-time» Data Portability with Webhooks, in: Data Transfer Initiative (Hrsg.), The Present and Future of Data Portability, A Collected Volume of Independent Scholarly Research, 2024, 51–61

Reich Andreas/Krämer Nicolai A./Lenninger Ralf, Fahrzeugdaten-Management, Standardisierter Zugang als Basis für neue Geschäftsmodelle, ATZelektronik 2018, 42–47

Reichlin Jeremy, Le droit à la portabilité des données sous le RGPD, in: Dal Molin-Kränzlin Alexandra/Schneuwly Anne Mirjam/Stojanovic Jasna (Hrsg.), Digitalisierung – Gesellschaft – Recht, Zürich 2019, 401–415

Reimsbach-Kounatze Christian/Molnar Andras, The impact of data portability on user empowerment, innovation, and competition, OECD Going Digital Toolkit Note, 2024

Reinert Mani/Wälchli Barbara, Kommentierung zu Art. 4 Abs. 2, in: Amstutz Marc/Reinert Mani (Hrsg.), Basler Kommentar zum Kartellgesetz, 2. Aufl., Basel 2021 (zit.: BSK KG-Reinert/Wälchli, Art. 4 Abs. 2 N …)

Reitze Christophe Peter, Kommentierung zu Art. 27, in: Geiser Thomas/Fountoulakis Christiana (Hrsg.), Basler Kommentar zum Zivilgesetzbuch I, Art. 1–456 ZGB, 7. Aufl., Basel 2022 (zit.: BSK ZGB I-Reitze, Art. 27 N …)

Rochet Jean-Charles/Tirole Jean, Platform Competition in Two-Sided Markets, JEEA 2003, 990–1029

Rochet Jean-Charles/Tirole Jean, Two-Sided Markets: An Overview, 2004

Rochet Jean-Charles/Tirole Jean, Two-sided markets: a progress report, The RAND Journal of Economics 2006, 645–667

Rodríguez de las Heras Ballell Teresa, The New Digital Architecture of the Urban Space: Typology and Legal Anatomy of Mobility Platforms, EBLR 2023, 11–21

Rohner Tristan, Datenherrschaft: Property Rights im Data Act, EuDIR 2025, 10–16

Rosenthal David, Kommentierung zu Art. 3, in: Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008 (zit.: HK DSG-Rosenthal, Art. 3 N …)

Rosenthal David, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, Jusletter 17. Juni 2019

Rosenthal David, Das neue Datenschutzgesetz, Jusletter 16. November 2020

Rossnagel Alexander, Einleitung, in: Roßnagel Alexander (Hrsg.), Hessisches Datenschutz- und InformationsfreiheitsG, Handkommentar, Baden-Baden 2021 (zit.: HK HDSIG-Rossnagel, Einleitung N …)

Roth David, «Open Banking» in der Schweiz – Herausforderungen an den Schnittstellen von Finanzmarkt-, Datenschutz- und Kartellrecht, SZW 2020, 669–685

Rubinstein Ira S., Big Data: The End of Privacy or a New Beginning?, IDPL 2013, 74–87

Rudin Beat, Die Erosion der informationellen Privatheit – oder: Rechtsetzung als Risiko?, in: Sutter-Somm Thomas/Hafner Felix/Schmid Gerhard/Seelmann Kurt (Hrsg.), Risiko und Recht, Festgabe zum Schweizerischen Juristentag 2004, Basel/Genf/München 2004, 415–440

Rudin Beat, Kommentierung zu § 3, in: Rudin Beat/Baeriswyl Bruno (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt (IDG), Zürich 2014 (zit.: PK IDG/BS-Rudin, § 3 N …)

Rudin Beat, Kommentierung zu Art. 2, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz (DSG), 2. Aufl., Bern 2023 (zit.: SHK DSG-Rudin, Art. 2 N …)

Rütsche Bernhard, Datenschutzaufsicht über Spitäler, digma 2012, 176–181

Rütsche Bernhard, Datenschutzrechtliche Aufsicht über Spitäler = Surveillance de la protection des données dans les hôspitaux, Zürich/Basel/Genf 2012

Rütsche Bernhard, Mehr Wettbewerb im Gesundheitswesen?, SZKW 2025, 45–46

Rysman Marc, The Economics of Two-Sided Markets, JEP 2009, 125–143

Sackmann Florian, Datenschutz bei der Digitalisierung der Mobilität, Eine sektorspezifische Analyse der Leistungsfähigkeit und des Weiterentwicklungsbedarfs der Datenschutzordnung, Baden-Baden 2020

Sadowski Jathan, When data is capital: Datafication, accumulation, and extraction, Big Data & Society 2019, 1–12

Sattler Andreas, Personenbezug als Hindernis des Datenhandels, in: Pertot Tereza (Hrsg.), Rechte an Daten, Tübingen 2020, 49–85 (zit.: Personenbezug)

Sattler Andreas, Data Act and Data Protection Law, in: Sattler Andreas/Zech Herbert (Hrsg.), The Data Act: First Assessments, Trier 2024, 103–135 (zit.: Data Act)

Savary Fiona, Regulierung dominanter Internetplattformen, Eigenheiten, Herausforderungen und Lösungsansätze im Licht von Ökonomie, Innovation und Recht, Zürich/St. Gallen 2017

Schantz Peter, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841–1847

Schätzle Daniel, Ein Recht auf die Fahrzeugdaten, Das Recht auf Datenportabilität aus der DS-GVO, PinG 2016, 71–75

Schiess Daniel/Schaller Olivier, Online-Plattformen – Chancen und Herausforderungen im Wettbewerbsrecht, in: Thouvenin Florent/Weber Rolf H. (Hrsg.), Werbung – Online, Zürich 2017, 109–130

Schild Hans Hermann, Kommentierung zu Art. 4 DSGVO, in: Wolff Heinrich Amadeus/Brink Stefan/von Ungern-Sternberg Antje (Hrsg.), BeckOK Datenschutzrecht, 53. Aufl., München 2025 (zit.: BeckOK DSR-Schild, Art. 4 DSGVO N …)

Schindler Benjamin, Kommentierung zu Art. 5, in: Ehrenzeller Bernhard/Schindler Benjamin/Schweizer Rainer J. (Hrsg.), St. Galler Kommentar zur schweizerischen Bundesverfassung, 4. Aufl., Zürich/St. Gallen 2023 (zit.: SGK BV-Schindler, Art. 5 N …)

Schmid Alain/Schmidt Kirsten Johanna/Zech Herbert, Rechte an Daten – zum Stand der Diskussion, sic! 2018, 627–639

Schmidt Kirsten Johanna, Datenmärkte ohne «Dateneigentum», Wie der Handel mit Personendaten durch Anpassungen des Datenschutzrechts gefördert werden könnte, digma 2019, 178–182

Schmidt Kirsten Johanna, Datenschutz als Vermögensrecht, Datenschutzrecht als Instrument des Datenhandels, Wiesbaden 2020

Schmidt-Kessel Martin, Heraus- und Weitergabe von IoT-Gerätedaten, MMR 2024, 75–82

Schneble Christophe Olivier/Elger Bernice Simone/Shaw David Martin, All Our Data Will Be Health Data One Day: The Need for Universal Data Protection and Comprehensive Consent, JMIR 5/2020, e16879, 1–8

Schneider Adrian, § 15: Datenschutz in der Informationstechnik, in: Specht Louisa/Mantz Reto (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, Bereichsspezifischer Datenschutz in Privatwirtschaft und öffentlichem Sektor, München 2019, 418–449

Schönbächler Matthias R./Maurer-Lambrou Urs/Kunz Simon, Kommentierung zu Art. 1, in: Vasella David/Blechta Gabor-Paul (Hrsg.), Basler Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, 4. Aufl., Basel 2024 (zit.: BSK DSG-Schönbächler/Maurer-Lambrou/Kunz, Art. 1 N …)

Schrader Leonie Felicia, Datenschutz im Gesundheitswesen unter der Europäischen Datenschutz-Grundverordnung, Berlin 2022

Schürmann Kathrin, Kommentierung zu Art. 20 DSGVO, in: Eßer Martin/Kramer Philipp/von Lewinski Kai (Hrsg.), DSGVO, BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze: Kommentar, 8. Aufl., Köln 2024 (zit.: AuernhammerKomm-Schürmann, Art. 20 DSGVO N …)

Schweitzer Heike, Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung, GRUR 2019, 569–579

Schweitzer Heike/Metzger Axel, Data Access Under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Competition and Innovation?, GRUR Int. 2023, 337–357

Schweitzer Heike/Metzger Axel/Blind Knut/Richter Heiko/Niebel Crispin/Gutmann Frederik, Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy, A legal, economic and competition policy angle, Final Report vom 8. Juli 2022

Schweitzer Heike/Peitz Martin, Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf?, ZEW Discussion Paper Nr. 17-043, Mannheim 2017

Schweitzer Heike/Peitz Martin, Ein neuer europäischer Ordnungsrahmen für Datenmärkte?, NJW 2018, 275–280

Schweitzer Heike/Welker Robert, A legal framework for access to data – A competition policy perspective, in: German Federal Ministry of Justice and Consumer Protection/Max Planck Institute for Innovation and Competition (Hrsg.), Data Access, Consumer Interests and Public Welfare, Baden-Baden 2021, 103–153

Schweizer Rainer J., Digitalisierung im Gesundheitswesen, digma 2020, 204–213

Schweizer Rainer J./Bongiovanni Jérémie, Kommentierung zu Art. 10, in: Ehrenzeller Bernhard/Schindler Benjamin/Schweizer Rainer J. (Hrsg.), St. Galler Kommentar zur schweizerischen Bundesverfassung, 4. Aufl., Zürich/St. Gallen 2023 (zit.: SGK BV-Schweizer/Bongiovanni, Art. 10 N …)

Schweizer Rainer J./Krebs Alina, Kommentierung zu Art. 36, in: Ehrenzeller Bernhard/Schindler Benjamin/Schweizer Rainer J. (Hrsg.), St. Galler Kommentar zur schweizerischen Bundesverfassung, 4. Aufl., Zürich/St. Gallen 2023 (zit.: SGK BV-Schweizer/Krebs, Art. 36 N …)

Schweizer Rainer J./Striegel Lea S., Kommentierung zu Art. 13, in: Ehrenzeller Bernhard/Schindler Benjamin/Schweizer Rainer J. (Hrsg.), St. Galler Kommentar zur schweizerischen Bundesverfassung, 4. Aufl., Zürich/St. Gallen 2023 (zit.: SGK BV-Schweizer/Striegel, Art. 13 N …)

Seemann Bruno, Persönlichkeitsvermarktung und virtuelle Realität – Unsterblichkeit im Recht und Rechner, sic! 1997, 259–266

Sénécal Sylvain/Fredette Marc/Léger Pierre-Majorique/Courtemanche Francois/Riedl René, Consumers' Cognitive Lock-in on Websites: Evidence from a Neurophysiological Study, Journal of Internet Commerce 2015, 277–293

Siglmüller Jonas, Standardisierungsbestrebungen für das Rückgrat der europäischen Digitalwirtschaft, Erste Einordnung von Begrifflichkeiten, Systematik und praktischen Herausforderungen, MMR 2024, 112–116

Specht-Riemenschneider Louisa/Kerber Wolfgang, Designing Data Trustees – A Purpose-Based Approach, Berlin 2022

Sperlich Tim, Das Recht auf Datenübertragbarkeit, DuD 2017, 377

Sperlich Tim, Informationelle Selbstbestimmung zwischen Wettbewerbs- und Datenschutzrecht, Eine Analyse und Beurteilung der Wechselwirkungen zwischen dem Wettbewerbs- und Datenschutzrecht, Berlin 2021

Spiecker genannt Döhmann Indra, Wissensverarbeitung im Öffentlichen Recht, RW 2010, 247–282

Spiecker genannt Döhmann Indra, The legal framework for access to data from a data protection viewpoint – especially under the GDPR, in: German Federal Ministry of Justice and Consumer Protection/Max Planck Institute for Innovation and Competition (Hrsg.), Data Access, Consumer Interests and Public Welfare, Baden-Baden 2021, 175–208

Spindler Gerald/Dalby Lukas, Kommentierung zu Art. 20 DSGVO, in: Spindler Gerald/Schuster Fabian (Hrsg.), Kommentar zum Recht der elektronischen Medien, 4. Aufl., München 2019 (zit.: ReMKomm-Spindler/Dalby, Art. 20 DSGVO N …)

Sprecher Franziska, Datenschutz und Big Data im Allgemeinen und im Gesundheitsrecht im Besonderen Teil 1, ZBJV 2018, 482–519 (zit.: Teil 1)

Sprecher Franziska, Datenschutz und Big Data im Allgemeinen und im Gesundheitsrecht im Besonderen Teil 2, ZBJV 2018, 519–552 (zit.: Teil 2)

Sprecher Franziska, Regulierung von Gesundheitsdaten und Gesundheitsdatenräumen, MedR 2022, 829–838

Sprecher Franziska, Digitalisierung im Gesundheitswesen – Zum Umgang mit Gesundheitsdaten und zur Schaffung von Gesundheitsdatenräumen, in: Epiney Astrid/Havalda Stefanie/Zlatescu Petru Emanuel (Hrsg.), Datenschutz und Gesundheitsschutz = Protection des données et protection de la santé, Zürich/Genf 2023, 29–44 (zit.: Digitalisierung)

Sprecher Franziska/Hofer Aline, Das elektronische Patientendossier, in: Epiney Astrid/Sangsue Déborah (Hrsg.), Datenschutz und Gesundheitsrecht = Protection des données et droit de la santé, Genf/Zürich/Basel 2019, 43–78

Staffelbach Oliver, Social-Media-Auftritte einrichten, in: Keller Claudia/Staffelbach Oliver (Hrsg.), Social Media und Recht für Unternehmen, Zürich 2015, 1–42

Staffler Lukas/Ebersberger Bernd, Digitalwirtschaft, in: Staffler Lukas/Ebersberger Bernd/Jobin Anna (Hrsg.), Digitalwirtschaft, Technische, wirtschaftliche und gesellschaftliche Grundlagen, Wiesbaden 2024, 1–17

Steffen Nico/Wieworra Lukas/Kroon Peter, Wettbewerb und Regulierung in der Plattform- und Datenökonomie, Bad Honnef 2021

Steiger Martin, Kommentierung zu Art. 25, in: Steiner Thomas/Morand Anne-Sophie/Hürlimann Daniel (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz, Version vom 28. August 2023 (zit.: OK DSG-Steiger, Art. 25 N …)

Steiner Thomas, Zwischen Autonomie und Angleichung, Eine Analyse zur Anwendung des neuen DSG im Lichte der DSGVO, in: Widmer Michael (Hrsg.), Datenschutz, Rechtliche Schnittstellen, Zürich 2023, 51–138

Steinrötter Björn, Kommentierung zu Art. 20 DSGVO, in: Borges Georg/Hilber Marc (Hrsg.), Beck'scher Online-Kommentar zum IT-Recht, 19. Aufl., München 2025 (zit.: BeckOK IT-Recht-Steinrötter, Art. 20 DSGVO N …)

Stiftung Datenschutz, Datenportabilität: Transparenz unter Ausschluss der Öffentlichkeit?, Politikbrief August 2018, <https://perma.cc/CCA7-Z269> (zit.: Politikbrief)

Stiftung Datenschutz, Praktische Umsetzung des Rechts auf Datenübertragbarkeit, Rechtliche, technische und verbraucherbezogene Implikationen = Practical Implementation of the Right to Data Portability Legal, Technical and Consumer-Related Implications, 3. Aufl., Leipzig 2018 (zit.: Praktische Umsetzung)

Stiftung Datenschutz, Praktische Umsetzung des Rechts auf Datenübertragbarkeit: Rechtliche, technische und verbraucherbezogene Implikationen – Zusammenfassung und Handlungsempfehlungen, Leipzig 2018, <https://perma.cc/9XR4-VT22> (zit.: Zusammenfassung)

Störing Marc, What EU legislation says about car data, Legal Memorandum to FIA on connected vehicles and data vom 16. Mai 2017, <https://perma.cc/J2XE-YP8N>

Strubel Michael, Anwendungsbereich des Rechts auf Datenübertragbarkeit, Auslegung des Art. 20 DS-GVO unter Berücksichtigung der Guidelines der Art. 29-Datenschutzgruppe, ZD 2017, 355–361

Swire Peter P./Lagos Yianni, Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, Maryland Law Review 2013, 335–380

Swiss Data Alliance, Leitlinie zur Umsetzung der Datenübertragbarkeit in der Schweiz, Version 1.0 vom 20. August 2020 (zit.: Leitlinien Datenportabilität)

Swiss Data Alliance, Der europäische Datenraum aus Schweizer Sicht, Whitepaper Version 1.2 vom 25. Januar 2023 (zit.: Whitepaper Datenraum)

Sydow Gernot/Wilhelm-Robertson Maria, Kommentierung zu Art. 20, in: Sydow Gernot/Marsch Nikolaus (Hrsg.), Nomos Handkommentar zu DS-GVO/BDSG, 3. Aufl., Baden-Baden 2022 (zit.: HK DSGVO-Sydow/Wilhelm-Robertson, Art. 20 N …)

Taeger Jürgen/Schmidt Bernd, Einführung, in: Taeger Jürgen/Gabel Detlev (Hrsg.), Kommunikation & Recht Kommentar zu DSGVO/BDSG/TDDDG, 4. Aufl., Frankfurt am Main 2022 (zit.: KRKomm-Taeger/Schmidt, Einführung N …)

Thouvenin Florent, Forschung im Spannungsfeld von Big Data und Datenschutzrecht: eine Problemskizze, in: Boehme-Neßler Volker/Rehbinder Manfred (Hrsg.), Big Data: Ende des Datenschutzes?, Gedächtnisschrift für Martin Usteri, Bern 2017, 27–53 (zit.: Big Data)

Thouvenin Florent, Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs, SJZ 2017, 21–32

Thouvenin Florent, Datenschutz auf der Intensivstation, digma 2019, 206–213

Thouvenin Florent, Informational Self-Determination: A Convincing Rationale for Data Protection Law?, JIPITEC 2021, 246–256

Thouvenin Florent, Informationelle Selbstbestimmung: Intuition, Illusion, Implosion, ZSR Beiheft 2023

Thouvenin Florent, Immaterialgüterrecht, Zürich 2025 (zit.: Immaterialgüterrecht)

Thouvenin Florent/De Werra Jacques/Benhamou Yaniv/Bernstein Abraham/Gille Felix/Kuonen Diego/Lovis Christian/Volz Stephanie/Von Wyl Viktor, Governance Mechanisms for Access and Use of Data in Public Health Crises: Call for Action, Jusletter 17. Oktober 2022

Thouvenin Florent/Weber Rolf H./Früh Alfred, Elemente einer Datenpolitik, Zürich/Basel/Genf 2019

Tombal Thomas, Les droits de la personne concernée dans le RGPD, in: de Terwangne Cécile/Rosier Karen (Hrsg.), Le Règlement général sur la protection des données (RGPD / GDPR), Analyse approfondie, Brüssel 2018, 407–554

Tombal Thomas/Graef Inge, The Regulation of Access to Personal and Non-Personal Data in the EU: From Bits and Pieces to a System?, in: Van Der Sloot Bart/Van Schendel Sascha (Hrsg.), The Boundaries of Data, Amsterdam 2024, 195–226

Toren Naomi, Drei wesentliche Veränderungen im Datenschutzrecht der Schweiz, Jusletter IT 5. Dezember 2019

Torous John/Kiang Mathew V/Lorme Jeanette/Onnela Jukka-Pekka, New Tools for New Research in Psychiatry: A Scalable and Customizable Platform to Empower Data Driven Smartphone Research, JMIR Mental Health 2/2016, e16, 1–17

Troiano Stefano, Potential and Limitations of the Right to Data Portability Eight Years after the Adoption of the GDPR, in: Anzenberger Philipp/Schwaighofer Klaus (Hrsg.), Recht der Digitalisierung II, Tübingen 2025, 159–178

Tschentscher Axel, Kommentierung zu Art. 10, in: Waldmann Bernhard/Belser Eva Maria/Epiney Astrid (Hrsg.), Basler Kommentar zur Bundesverfassung, Basel 2015 (zit.: BSK BV-Tschentscher, Art. 10 N …)

Van den Boom Freyja, Regulating Telematics Insurance – Enabling Car Data-Driven Innovations, EBLR 2023, 157–167

Van Der Auwermeulen Barbara, How to attribute the right to data portability in Europe: A comparative analysis of legislations, CLSR 2017, 57–72

Van Der Vlist Fernando N./Helmond Anne/Burkhardt Marcus/Seitz Tatjana, API Governance: The Case of Facebook's Evolution, SM+S 2/2022, 205630512210862, 1–24

van Spyk Benedikt, Das Recht auf Selbstbestimmung in der Humanforschung, Zugleich eine Untersuchung der Grundlagen und Grenzen des «informed consent» im Handlungsbereich der Forschung am Menschen, Zürich/St. Gallen 2011

van Spyk Benedikt, Kommentierung zu Art. 2, in: Rütsche Bernhard/D'Amico Nadja (Hrsg.), Humanforschungsgesetz (HFG), Bundesgesetz vom 30. September 2011 über die Forschung am Menschen, Bern 2015 (zit.: SHK HFG-van Spyk, Art. 2 N …)

Vasella David, Einleitung, in: Vasella David/Blechta Gabor-Paul (Hrsg.), Basler Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, 4. Aufl., Basel 2024 (zit.: BSK DSG-Vasella, Einleitung N …)

Vasella David/Ziegler Noémi, Krankenversicherung und DSG-Revision, Überlegungen zu datenschutzrechtlichen Herausforderungen im Bereich der sozialen Krankenversicherung, digma 2020, 80–87

Veil Winfried, Kommentierung zu Art. 1 DA, in: Wolff Heinrich Amadeus/Brink Stefan/von Ungern-Sternberg Antje (Hrsg.), BeckOK Datenschutzrecht, 53. Aufl., München 2025 (zit.: BeckOK DSR-Veil, Art. 1 DA N …)

von Lewinski Kai, Geschichte des Datenschutzrechts von 1600 bis 1977, in: Arndt Felix/Betz Nicole/Farahat Anuscheh/Goldmann Matthias/Huber Matthias/Keil Rainer/Láncos Petra Lea/Schaefer Jan/Smrkolj Maja/Sucker Franziska/Valta Stefanie (Hrsg.), Freiheit – Sicherheit – Öffentlichkeit, Baden-Baden 2009, 196–220 (zit.: Geschichte)

von Lewinski Kai, Die Matrix des Datenschutzes, Besichtigung und Ordnung eines Begriffsfeldes, Tübingen 2014 (zit.: Matrix)

von Lewinski Kai, Kommentierung zu Art. 1 DSGVO, in: Eßer Martin/Kramer Philipp/von Lewinski Kai (Hrsg.), DSGVO, BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze: Kommentar, 8. Aufl., Köln 2024 (zit.: AuernhammerKomm-von Lewinski, Art. 1 DSGVO N …)

von Lewinski Kai, Kommentierung zu Art. 20 DSGVO, in: Wolff Heinrich Amadeus/Brink Stefan/von Ungern-Sternberg Antje (Hrsg.), BeckOK Datenschutzrecht, 53. Aufl., München 2025 (zit.: BeckOK DSR-von Lewinski, Art. 20 DSGVO N …)

Wagner Christian/Karagkouni Evangelia, Genehmigung und Marktüberwachung von Kraftfahrzeugen, Neue Kompetenzen für die Kommission nach der TypgenehmigungsVO, EuZW 2019, 108–114

Waldmeier Stefanie-Daniela, Informationelle Selbstbestimmung – ein Grundrecht im Wandel?, Diss. Zürich 2015

Wasilewski Luisa, Die Digital-Health-Strategien der Tech-Giganten im Überblick, in: Matusiewicz David (Hrsg.), Plattformen und Tech-Giganten, Die neuen Player im Gesundheitswesen, Berlin 2023, 42–47

Weber Rolf H., Information und Schutz Privater, ZSR 1999 II, 1–86

Weber Rolf H., Neue Grundrechtskonzeptionen zum Schutz der Privatheit, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Neuer Regulierungsschub im Datenschutzrecht?, Zürich/Basel/Genf 2012, 7–29 (zit.: Grundrechtskonzeptionen)

Weber Rolf H., Big Data: Sprengkörper des Datenschutzrechts?, Jusletter IT 11. Dezember 2013

Weber Rolf H., Big Data: Rechtliche Perspektive, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014, 17–29 (zit.: Rechtliche Perspektive)

Weber Rolf H., Information at the crossroads of competition and data protection law, ZWeR 2014, 169–183

Weber Rolf H., From competition law to sector-specific regulation in internet markets? A critical assessment of a possible structural chance, in: Drexl Josef/Di Porto Fabiana (Hrsg.), Competition law as regulation, Cheltenham 2015, 239–267 (zit.: Sector-specific Regulation)

Weber Rolf H., Big Data: Herausforderungen für das Datenschutzrecht, in: Epiney Astrid/Nüesch Daniela (Hrsg.), Big Data und Datenschutzrecht = Big Data et droit de la protection des données, Genf/Zürich/Basel 2016, 1–22 (zit.: Herausforderungen)

Weber Rolf H., Synchronisierung von Technologie und Regulierung zur Schaffung sachgerechter Datenschutzstandards, in: Boehme-Nessler Volker/Rehbinder Manfred (Hrsg.), Big Data: Ende des Datenschutzes?, Genf/Zürich/Basel 2017, 55–72 (zit.: Synchronisierung)

Weber Rolf H./Henseler Simon, Daten als Entgelt, SZW 2019, 335–345

Weber Rolf H./Thouvenin Florent, Dateneigentum und Datenzugangsrechte – Bausteine der Informationsgesellschaft?, ZSR 2018, 43–74

Weber Rolf H./Volz Stephanie, Fachhandbuch Wettbewerbsrecht, 2. Aufl., Zürich/Genf 2023

Weller David, Personenbezug der Fahrzeugidentifikationsnummer (FIN), GRUR-Prax 2023, 761

Wendehorst Christiane/Schwamberger Sebastian, Zugang zu Kfz-Nutzerdaten im (zukünftigen) europäischen Datenrecht, DAR 2022, 541–545

Werkmeister Christoph/Brandt Elena, Datenschutzrechtliche Herausforderungen für Big Data, CR 2016, 233–238

Westphal Miriam/Wichtermann Marco, Datenportierung nach Art. 20 DS-GVO, Ausgewählte Ausschlussgründe, ZD 2019, 191–194

Widmer Michael/Egli Philipp, J. Datenschutz im Gesundheitsrecht, in: Rumetsch, Virgilia/Poledna, Tomas (Hrsg.), Gesundheitsrecht, SBVR Band VIII/2, Basel 2025, 551–668

Wiebe Andreas, Der Data Act – Innovation oder Illusion?, GRUR 2023, 1569–1578

Wielsch Dan, Medienregulierung durch Persönlichkeits- und Datenschutzrechte, JZ 2020, 105–114

Willard Brian/Chavez Jessie/Fair Greg/Levine Kyle/Lange Ali/Dickerson Joyce, Data Transfer Project: From Theory to Practice, 2018, <https://perma.cc/FJK2-J7SM>

Wohlfarth Michael, Data Portability on the Internet: An Economic Analysis, BISE 2019, 551–574

Wolter Stefan, Smart Mobility – Intelligente Vernetzung der Verkehrsangebote in Großstädten, in: Proff Heike/Schönharting Jörg/Schramm Dieter/Ziegler Jürgen (Hrsg.), Zukünftige Entwicklungen in der Mobilität: betriebswirtschaftliche und technische Aspekte, Wiesbaden 2012, 527–548

Wunner Katharina, Zugang ist gut, Kontrolle ist besser!, ZUM 2024, 424–434

Yan Xingyu/He Huaiwen, Fine-tuning the Ex Ante Approach to Regulating Data Combination Practices, JCLE 2022, 881–904

Yildiz Okan, Kopplungsgeschäfte in der digitalen Wirtschaft, Marktabgrenzung und Marktmissbrauch in der Plattformökonomie, Zürich 2024

Zäch Roger/Heizmann Reto, Schweizerisches Kartellrecht, 3. Aufl., Bern 2023

Zanfir Gabriela, The right to Data portability in the context of the EU data protection reform, IDPL 2012, 149–162

Zech Herbert, Information als Schutzgegenstand, Tübingen 2012

Zhang Jiawei, The Paradox of Data Portability and Lock-In Effects, HJLT 2023, 658–683

Ziegler Noémi/Vasella David, Informationelle Selbstbestimmung, Was leistet das Datenschutzrecht für die Selbstbestimmung der Betroffenen?, digma 2019, 158–164

Zschoch Claudia, Soziale Netzwerke im Kartellrecht, Eine Untersuchung zum Wettbewerb im Umfeld internetbasierter Netzwerkmärkte unter Berücksichtigung der Auswirkungen von Datensammlungen und des Einflusses des Datenschutzrechts im kartellrechtlichen Kontext, Köln 2018

Zuboff Shoshana, Big other: Surveillance Capitalism and the Prospects of an Information Civilization, JIT 2015, 75–89

Zufall Frederike/Zingg Raphael, Data Portability in a Data-Driven World, in: Peng Shin-yi/Lin Ching-Fu/Streinz Thomas (Hrsg.), Artificial Intelligence and International Economic Law, Cambridge 2021, 215–234

Zweifel-Keegan Cobun, Portable Trust, Fostering Both Autonomy and Privacy in Data Portability Mechanisms, in: Data Transfer Initiative (Hrsg.), The Present and Future of Data Portability, A Collected Volume of Independent Scholarly Research, 2024, 4–16

Materialien und weitere amtliche Publikationen

Soweit Materialien und weitere amtliche Publikationen auf Deutsch verfügbar sind, ist die deutsche Fundstelle angegeben. Sind sie nur in englischer Sprache verfügbar, wird die Autorenschaft dennoch auf Deutsch bezeichnet, wenn von der gleichen Autorenschaft auch deutschsprachige Publikationen aufgeführt sind.

Schweiz

Bolliger Christian/Féraud Marius/Epiney Astrid/Hänni Julia, Evaluation des Bundesgesetzes über den Datenschutz, Schlussbericht vom 10. März 2011

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988, BBl 1988 II 413 ff. (zit.: Botschaft DSG 1988)

Botschaft über eine neue Bundesverfassung vom 20. November 1996, BBl 1997 I 1 ff. (zit.: Botschaft BV)

Botschaft zum Bundesgesetz über das elektronische Patientendossier (EPDG) vom 29. Mai 2013, BBl 2013 5321 (zit.: Botschaft EPDG)

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941 ff. (zit.: Botschaft DSG 2017)

Botschaft zur Änderung des Personenbeförderungsgesetzes vom 4. Juni 2021, BBl 2021 1485 (zit.: Botschaft PBG)

Botschaft zum Verpflichtungskredit für ein Programm zur Förderung der digitalen Transformation im Gesundheitswesen für die Jahre 2025–2034, BBl 2023 2908 (zit.: Botschaft Verpflichtungskredit)

Botschaft zum Bundesgesetz über die Mobilitätsdateninfrastruktur vom 14. Mai 2025, BBl 2025 1805 (zit.: Botschaft MODIG)

Botschaft zum Bundesgesetz über das elektronische Gesundheitsdossier vom 5. November 2025, BBl 2025 3398 (zit.: Botschaft EGDG)

Bundesamt für Justiz, Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016 (zit.: BJ, Erläuternder Bericht VE-DSG)

Bundesamt für Justiz, Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens vom 10. August 2017 (zit.: BJ, Zusammenfassung Vernehmlassungsverfahren)

Bundesamt für Justiz, Erläuternder Bericht Verordnung über den Datenschutz (Datenschutzverordnung, DSV) vom 31. August 2022 (zit.: BJ, Erläuternder Bericht DSV)

Bundesamt für Kommunikation, «Auf dem Weg zu einer Datenpolitik des Bundes», Medienmitteilung vom 22. März 2017, <https://perma.cc/7GEL-C7L7> (zit.: BAKOM, Medienmitteilung vom 22. März 2017)

Bundesamt für Kommunikation, «Massnahmen für eine zukunftsorientierte Datenpolitik der Schweiz», Medienmitteilung vom 9. Mai 2018, <https://perma.cc/VJE24KLZ> (zit.: BAKOM, Medienmitteilung vom 9. Mai 2018)

Bundesamt für Kommunikation, Vorentwurf des Bundesgesetzes über Kommunikationsplattformen und Suchmaschinen (VE-KomPG), Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens vom 29. Oktober 2025 (zit.: BAKOM, Bericht Vernehmlassung VE-KomPG)

Bundesamt für Strassen, Faktenblatt eCall in der Schweiz vom 9. Mai 2018, <https://perma.cc/B25M-N33N> (zit.: ASTRA)

Bundesrat, Rechtliche Basis für Social Media, Bericht des Bundesrates in Erfüllung des Postulats Amherd 11.3912 vom 29. September 2011 (zit.: Bericht Social Media)

Bundesrat, Bericht über die Evaluation des Bundesgesetzes über den Datenschutz vom 9. Dezember 2011, BBl 2012 335 ff. (zit.: Bericht Evaluation DSG)

Bundesrat, Open-Government-Data-Strategie Schweiz 2014–2018 vom Bundesrat am 16. April 2014 genehmigt, BBl 2014 3493 ff. (zit.: Open-Government-Data-Strategie)

Bundesrat, Patientenrechte und Patientenpartizipation in der Schweiz, Bericht in Erfüllung der Postulate 12.3100 Kessler, 12.3124 Gilli und 12.3207 Steiert vom 24. Juni 2015 (zit.: Bericht Patientenrechte)

Bundesrat, «Auf dem Weg zu einer Datenpolitik des Bundes», Medienmitteilung vom 22. März 2017, <https://perma.cc/7GEL-C7L7> (zit.: Medienmitteilung vom 22. März 2017)

Bundesrat, Rechtliche Basis für Social Media: Erneute Standortbestimmung, Nachfolgebericht des Bundesrates zum Postulatsbericht Amherd 11.3912 «Rechtliche Basis für Social Media» vom 10. Mai 2017 (zit.: Nachfolgebericht Social Media)

Bundesrat, Strategie «Digitale Schweiz» vom 5. September 2018, BBl 2018 5961 ff. (zit.: Strategie «Digitale Schweiz» 2018)

Bundesrat, Abbau von Regulierungskosten. Lockerung von Dokumentations- und Archivierungsvorschriften, Bericht des Bundesrates in Erfüllung des Postulates 15.3122 de Courten vom 27. September 2019 (zit.: Bericht Regulierungskosten)

Bundesrat, Die gesundheitspolitische Strategie des Bundesrates 2020–2030 vom Dezember 2019 (zit.: Bericht Gesundheit2030)

Bundesrat, Strategie «Digitale Schweiz» vom September 2020, BBl 2020 7593 ff. (zit.: Strategie «Digitale Schweiz» 2020)

Bundesrat, Bessere Nutzung von Gesundheitsdaten für eine qualitativ hochstehende und effiziente Gesundheitsversorgung Bericht des Bundesrates in Erfüllung des Postulates 15.4225 Humbel vom 4. Mai 2022 (zit.: Bericht Nutzung von Gesundheitsdaten)

Bundesrat, Digitalisierung – Handlungsfelder der Wirtschaftspolitik, Bericht vom 9. Dezember 2022 (zit.: Bericht Handlungsfelder)

Bundesrat, «Grosse Kommunikationsplattformen: Bundesrat strebt Regulierung an», Medienmitteilung vom 5. April 2023, <https://perma.cc/7NWT-58VL> (zit.: Medienmitteilung vom 5. April 2023)

Bundesrat, Änderung des Bundesgesetzes über das elektronische Patientendossier (EPDG), Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens vom 21. Juni 2023 (zit.: Bericht Vernehmlassung EPDG)

Bundesrat, «Bundesrat schafft Grundlagen für Schweizer Datenökosystem», Medienmitteilung vom 8. Dezember 2023, <https://perma.cc/AVH4-VHFZ> (zit.: Medienmitteilung vom 8. Dezember 2023)

Bundesrat, Kohärente Datenstrategie für das Gesundheitswesen, Bericht des Bundesrates in Erfüllung des Postulats 18.4102 der Kommission für soziale Sicherheit und Gesundheit des Ständerates vom 8. Dezember 2023 (zit.: Bericht Kohärente Datenstrategie für das Gesundheitswesen)

Bundesrat, «Datenökosystem Schweiz: Anlaufstelle hat Betrieb aufgenommen», Medienmitteilung vom 15. Januar 2025, <https://perma.cc/7Z7E-9RG3> (zit.: Medienmitteilung vom 15. Januar 2025)

Bundesrat, «Bundesrat präsentiert seine Ziele für das Jahr 2026», Medienmitteilung Rohstoff vom 8. September 2025, <https://perma.cc/9K3G-XZBC> (zit.: Medienmitteilung vom 8. September 2025)

Bundesrat, «Neues Gesetz über Kommunikationsplattformen und Suchmaschinen: Start der Vernehmlassung», Medienmitteilung vom 29. Oktober 2025, <https://perma.cc/RV3Y-M5M4> (zit.: Medienmitteilung vom 29. Oktober 2025)

Bundesrat, «Bundesrat beschliesst Neuausrichtung: Elektronisches Gesundheitsdossier E-GD löst EPD ab», Medienmitteilung vom 5. November 2025, <https://perma.cc/65BY-WX8S> (zit.: Medienmitteilung vom 5. November 2025)

Collovà Patrizio/Marti Michael/Schwarz Daniel/Wäspi Flurina/Wenger Nicolai, Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung, Studie zu zentralen Herausforderungen, Grundprinzipien und Voraussetzungen, konkreten Beispielen sowie Kernelementen eines Modells vertrauenswürdiger Datenräume im Auftrag des BAKOM vom 22. Juli 2021

eHealth Suisse, Strategie eHealth Schweiz 2.0, 2018–2024, Ziele und Massnahmen von Bund und Kantonen zur Verbreitung des elektronischen Patientendossiers sowie zur Koordination der Digitalisierung rund um das elektronische Patientendossier vom 14. Dezember 2018 (zit.: Strategie)

eHealth Suisse, Grundlagen für interoperable Prozesse im Gesundheitswesen, Input für strategische Arbeiten von Bund und Kantonen vom 8. April 2021 (zit.: Interoperabilität)

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Das neue Datenschutzgesetz aus Sicht des EDÖB vom 9. Februar 2021 (zit.: EDÖB, Das neue DSG)

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, «Schweiz ratifiziert Konvention 108+», Medienmitteilung vom 8. September 2023, <https://perma.cc/K4FC-HMFV> (zit.: EDÖB, Medienmitteilung vom 8. September 2023)

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes (TOM) vom 15. Januar 2024 (zit.: EDÖB, Leitfaden TOM)

Eidgenössisches Departement für auswärtige Angelegenheiten, Strategie Digitalaussenpolitik 2021–2024 vom 4. November 2020 (zit.: EDA)

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation, Bericht zu den Empfehlungen der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit: Kenntnisnahme und weiteres Vorgehen vom 15. Oktober 2019 (zit.: UVEK)

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation/Eidgenössisches Departement für auswärtige Angelegenheiten, Schaffung von vertrauenswürdigen Datenräumen basierend auf der digitalen Selbstbestimmung, Bericht an den Bundesrat vom 30. März 2022 (zit.: UVEK/EDA)

Eidgenössisches Institut für Geistiges Eigentum, Zugang zu Sachdaten in der Privatwirtschaft vom 1. März 2021 (zit.: IGE)

Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit, Bericht vom 17. August 2018, <https://perma.cc/YB65-ECG9> (zit.: Expertengruppe Zukunft)

Fahne 17.059, Datenschutzgesetz, Teilrevision und Änderung weiterer Erlasse zum Datenschutz, Entwurf 3 Herbstsession 2019, Beschluss Nationalrat, <https://perma.cc/JQL2-XP5J> (zit. Fahne DSG, Entwurf 3 Herbstsession 2019)

Interdepartementale Koordinationsgruppe EU-Digitalpolitik, Die Schweiz und die Digitalpolitik der Europäischen Union vom 13. Februar 2025 (zit.: IK-EUDP)

Interpellation Dittli 20.3220, «Standortbestimmung zum regulierten Wettbewerb im schweizerischen Gesundheitswesen» vom 4. Mai 2020, <https://perma.cc/62KL-J2A2> (zit.: Interpellation Dittli 20.3220)

Interpellation Hässig 25.3836, «Datenschutz-Regeln in Spitälern vereinheitlichen/harmonisieren, um Innovation zu fördern» vom 20. Juni 2025, <https://perma.cc/K9WL-X5EL> (zit.: Interpellation Hässig 25.3836)

Lovis Christian, Transparenzstrategie im Bereich der Gesundheitskosten und -leistungen, Bericht gemäss Mandat 18.0130531500.0000-586/1 des Bundesamts für Gesundheit vom Dezember 2019

Motion Bussey 10 898, «Gesetzgebung über Computer» vom 17. März 1971, AB 1972 N 2127 ff. (zit.: Motion Bussey 10 898)

Motion WBK-S 22.3890, «Rahmengesetz für die Sekundärnutzung von Daten» vom 22. August 2022, <https://perma.cc/VN7Y-Q5R6> (zit.: Motion WBK-S 22.3890)

Motion Marti 23.3069, «Digital Markets Act für die Schweiz» vom 8. März 2023, Stellungnahme des Bundesrates vom 17. Mai 2023, <https://perma.cc/WA33-FGU9> (zit.: Motion Marti 23.3069, Stellungnahme Bundesrat)

Parlamentarische Initiative Gerwig 77.223, «Persönlichkeits- und Datenschutz. Bundesverfassung» vom 22. März 1977, <https://perma.cc/64CF-BUJF> (zit.: Pa.Iv. Gerwig 77.223)

Parlamentarische Initiative Gerwig 77.224, «Persönlichkeits- und Datenschutzgesetz» vom 22. März 1977, <https://perma.cc/V893-9K2G> (zit.: Pa.Iv. Gerwig 77.224)

Postulat Derder 15.4045, «Recht auf Nutzung der persönlichen Daten. Recht auf Kopie» vom 25. September 2015, <https://perma.cc/K3P6-PVNQ> (zit.: Postulat Derder 15.4045)

Postulat Wyss 24.3013, «Mindeststandards für Primärsysteme im Gesundheitswesen» vom 22. Februar 2024, <https://perma.cc/NL2E-SYCM> (zit.: Postulat Wyss 24.3013)

PricewaterhouseCoopers AG, Regulierungsfolgenabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG) vom 11. Juli 2016

Rütsche Bernhard/D'Amico Nadja/Schläpfer Lea, Stärkung der Patientenrechte: internationales Soft Law und nationale Gesetze im Vergleich, Studie zuhanden des Bundesamts für Gesundheit BAG vom 30. Oktober 2013

Schweizerisches Institut für Rechtsvergleichung, Gutachten zur Datenportabilität sowie zu Regelungen betreffend die Wiederverwendung von Daten, Lausanne 2018 (zit.: SIR)

Swissmedic, Merkblatt Medizinprodukte-Software, Version 3.0 gültig ab 10. April 2024

Verhaltenskodex für den Betrieb von vertrauenswürdigen Datenräumen basierend auf der digitalen Selbstbestimmung, vom Bundesrat gutgeheissen am 8. Dezember 2023 (zit.: Verhaltenskodex Datenräume)

Weber Rolf H./Thouvenin Florent, Gutachten zur Möglichkeit der Einführung eines Datenportabilitätsrechts im schweizerischen Recht und zur Rechtslage bei Personal Information Management Systems (PIMS) vom 22. Dezember 2017

Wettbewerbskommission, Jahresbericht 2018 an den Bundesrat (zit.: WEKO, Jahresbericht 2018)

Wettbewerbskommission, Jahresbericht 2019 an den Bundesrat (zit.: WEKO, Jahresbericht 2019)

Wettbewerbskommission, Jahresbericht 2021 an den Bundesrat (zit.: WEKO, Jahresbericht 2021)

Wettbewerbskommission, Schlussbericht des Sekretariats in Sachen «22-0502 Vertriebssystem von Yamaha-Produkten» vom 10. Mai 2022 (zit.: WEKO, Yamaha)

Wettbewerbskommission, Erläuterungen der Wettbewerbskommission zur Verordnung über die wettbewerbsrechtliche Behandlung von vertikalen Abreden im Kraftfahrzeugsektor vom 4. Dezember 2023 (zit.: WEKO, Erläuterungen KFZV)

International

Artikel 29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen «für die Verarbeitung Verantwortlicher» und «Auftragsverarbeiter», WP 169, angenommen am 16. Februar 2010 (zit.: Stellungnahme Verantwortlicher/Auftragsverarbeiter)

Artikel 29-Datenschutzgruppe, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP 217, angenommen am 9. April 2014 (zit.: Stellungnahme Berechtigtes Interesse)

Artikel 29-Datenschutzgruppe, Guidelines on the right to data portability, WP 242 rev.01, zuletzt überarbeitet und angenommen am 5. April 2017 (zit.: Guidelines Data Portability)

Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, zuletzt überarbeitet und angenommen am 5. April 2017 (zit.: Leitlinien Datenübertragbarkeit)

Bundeskartellamt, Arbeitspapier Marktmacht von Plattformen und Netzwerken vom Juni 2016 (zit.: BKartA, Plattformen)

Bundeskartellamt, Sektoruntersuchung Messenger- und Video-Dienste, Zwischenbericht «Branchenüberblick und Stimmungsbild Interoperabilität» vom November 2021 (zit.: BKartA, Sektoruntersuchung)

Bundesministerium für Verkehr und digitale Infrastruktur, «Eigentumsordnung» für Mobilitätsdaten?, Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive vom März 2017

C-ITS Platform, Final Report vom Januar 2016, <https://perma.cc/AYM3-L32Z>

Crémer Jacques/De Montjoye Yves-Alexandre/Schweitzer Heike, Competition policy for the digital era, Luxemburg 2019, <https://perma.cc/T59C-XUB8>

Datenschutzkonferenz/Verband der Automobilindustrie, Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge, Berlin/Schwerin 2016, <https://perma.cc/Y95U-K9WG> (zit.: DSK/VDA)

Europäische Kommission, Commission Staff Working Document, Europe 2020 – public consultation, Overview of responses, SEC(2010) 246 final vom 4. März 2010 (zit.: Europe 2020)

Europäische Kommission, Eine Digitale Agenda für Europa, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, KOM(2010)245 endg. vom 19. Mai 2010 (zit.: Digitale Agenda)

Europäische Kommission, Gesamtkonzept für den Datenschutz in der Europäischen Union, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, KOM(2010) 609 endg. vom 4. November 2010 (zit.: Gesamtkonzept)

Europäische Kommission, Impact Assessment, Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, SEC(2012) 72 final vom 25. Januar 2012 (zit.: Impact Assessment)

Europäische Kommission, Für eine florierende datengesteuerte Wirtschaft, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, COM(2014) 442 final vom 2. Juli 2014 (zit.: Datengesteuerte Wirtschaft)

Europäische Kommission, Strategie für einen digitalen Binnenmarkt für Europa, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, COM(2015) 192 final vom 6. Mai 2015 (zit.: Strategie digitaler Binnenmarkt)

Europäische Kommission, Eine europäische Strategie für Kooperative Intelligente Verkehrssysteme – ein Meilenstein auf dem Weg zu einer kooperativen, vernetzten und automatisierten Mobilität, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, COM(2016) 766 final vom 30. November 2016 (zit.: Intelligente Verkehrssysteme)

Europäische Kommission, Bericht der Kommission an das Europäische Parlament und den Rat über das Funktionieren der Regelung für den Zugang zu Reparatur- und Wartungsinformationen für Fahrzeuge, eingerichtet durch die Verordnung (EG) Nr. 715/2007 über die Typgenehmigung von Kraftfahrzeugen hinsichtlich der Emissionen von leichten Personenkraftwagen und Nutzfahrzeugen (Euro 5 und Euro 6) und über den Zugang zu Reparatur- und Wartungsinformationen für Fahrzeuge, COM(2016) 782 final vom 19. Dezember 2016 (zit.: Evaluation)

Europäische Kommission, Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Accompanying the document Communication, Building a European data economy, SWD(2017) 2 final vom 10. Januar 2017 (zit.: Free Flow)

Europäische Kommission, Aufbau einer Europäischen Datenwirtschaft, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, COM(2017) 9 final vom 10. Januar 2017 (zit.: Aufbau Datenwirtschaft)

Europäische Kommission, Aufbau eines gemeinsamen europäischen Datenraums, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, COM(2018) 232 final vom 25. April 2018 (zit.: Aufbau Datenraum)

Europäische Kommission, Eine europäische Datenstrategie, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, COM(2020) 66 final vom 19. Februar 2020 (zit.: Datenstrategie)

Europäische Kommission, Datenschutz als Grundpfeiler der Teilhabe der Bürgerinnen und Bürger und des Ansatzes der EU für den digitalen Wandel – zwei Jahre Anwendung der Datenschutz- Grundverordnung, Mitteilung der Kommission an das Europäische Parlament und den Rat, COM(2020) 264 final vom 24. Juni 2020 (zit.: Zwei Jahre DSGVO)

Europäische Kommission, Impact Assessment Report, Commission Staff Working Document accompanying the document Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), SWD(2020) 363 final vom 15. Dezember 2020 (zit.: DMA Impact Assessment Report)

Europäische Kommission, «Fusionskontrolle: Kommission genehmigt Übernahme von Fitbit durch Google unter Auflagen», Medienmitteilung vom 17. Dezember 2020, <https://perma.cc/AJ62-PP77> (zit.: Medienmitteilung vom 17. Dezember 2020)

Europäische Kommission, Zugang zu Fahrzeugdaten, -funktionen und -ressourcen, Aufforderung zur Stellungnahme für eine Folgenabschätzung, Ares(2022)2302201 vom 29. März 2022 (zit.: Aufforderung zur Stellungnahme)

Europäische Kommission, Vorschlag für eine Verordnung der Europäischen Parlaments und des Rates über den europäischen Raum für Gesundheitsdaten, COM(2022) 197 final vom 3. Mai 2022 (zit.: Vorschlag EHDS)

Europäischer Datenschutzausschuss, Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht, Version 2.1, angenommen am 28. März 2023 (zit.: EDSA)

Europäischer Datenschutzausschuss/Europäischer Datenschutzbeauftragter, Gemeinsame Stellungnahme 3/2022 zum Vorschlag für eine Verordnung über den europäischen Raum für Gesundheitsdaten vom 12. Juli 2022 (zit.: EDSA/EDSB)

Europäischer Datenschutzbeauftragter, Stellungnahme 9/2016 des EDSB zu Systemen für das Personal Information Management (PIM), Hin zu einer intensiveren Einbindung der Nutzer in das Management und die Verarbeitung personenbezogener Daten vom 20. Oktober 2016 (zit.: EDSB)

Europäisches Parlament, Entschließung des Europäischen Parlaments zum Gesamtkonzept für den Datenschutz in der Europäischen Union (2011/2025(INI)) vom 6. Juli 2011 (zit.: Gesamtkonzept Datenschutz)

Europäisches Parlament, Bericht über den 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)) vom 21. November 2013 (zit.: Bericht Albrecht)

Furman Jason/Coyle Diane/Fletcher Amelia/McAuley Derek/Marsden Philip, Unlocking digital competition, Report of the Digital Competition Expert Panel vom März 2019

Hustinx Peter, Stellungnahme des Europäischen Datenschutzbeauftragten zum Datenschutzreformpaket, Brüssel 2012, <https://perma.cc/9ZX2-8QWA>

International Working Group on Data Protection in Technology, The Case for Data Portability as a Privacy Protection in the Digital Age, Working Paper, Written procedure prior to 67th (virtual) meeting on 24 April 2021

McCarthy Mike/Seidl M./Mohan S./Hopkin J./Stevens A./Ognissanto F., Access to In-vehicle Data and Resources, Final Report CPR2419, Luxemburg 2017

Monopolkommission, Empfehlungen für einen effektiven und effizienten Digital Markets Act, Sondergutachten 82, Bonn 2021

Organisation for Economic Co-operation and Development (OECD), Data-Driven Innovation, Big Data for Growth and Well-Being, Paris 2015 (zit.: OECD, Data-Driven Innovation)

Organisation for Economic Co-operation and Development (OECD), Enhancing Access to and Sharing of Data, Reconciling Risks and Benefits for Data Re-use across Societies, Paris 2019 (zit.: OECD, Enhancing Access)

Organisation for Economic Co-operation and Development (OECD), Data portability, interoperability and digital platform competition, Paris 2021 (zit.: OECD, Data Portability)

Organisation for Economic Co-operation and Development (OECD), Mapping data portability initiatives, opportunities and challenges, Paris 2021 (zit.: OECD, Mapping Initiatives)

OECD Committee on Digital Economy Policy, Working Party on Security and Privacy in the Digital Economy, Summary of the OECD Privacy Expert Roundtable, Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking, DSTI/ICCP/REG(2014)3 vom 20. Mai 2014 (zit.: OECD Committee, Expert Roundtable)

Rat der Europäischen Union, Ratsdokument zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), 11013/13 vom 21. Juni 2013 (zit.: Ratsdokument 11013/13 vom 21. Juni 2013)

Rat der Europäischen Union, Ratsdokument zum Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 8835/15 vom 12. Mai 2015 (zit.: Ratsdokument 8835/15 vom 12. Mai 2015)

Rat der Europäischen Union, Ratsdokument zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), 9565/15 vom 11. Juni 2015 (zit.: Ratsdokument 9565/15 vom 11. Juni 2015)

Rat der Europäischen Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Preparation for trilogue – whole Regulation, 14481/15 vom 27. November 2015 (zit.: Ratsdokument 14481/15 vom 27. November 2015)

Schallbruch Martin/Schweitzer Heike/Wambach Achim/Kirchhoff Wolfgang/Langeheine Bernd/Schneider Jens-Peter/Schnitzer Monika/Seeliger Daniela/Wagner Gerhard/Durz Hansjörg/Heider Matthias/Mohrs Falko, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft: Bericht der Kommission Wettbewerbsrecht 4.0, Berlin 2019

Steinmüller Wilhelm/Lutterbeck Bernd/Mallmann Christoph/Harbort U./Kolb G./Schneider J., Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, Deutscher Bundestag, 6. Wahlperiode, Drucksache VI/3826, Anlage 1, Bonn 1972, <https://perma.cc/39AR-XHXB>

Abkürzungen

a.A.	anderer Ansicht
a.a.O.	am angeführten Ort
AB	Amtliches Bulletin
ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
aBV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 29. Mai 1874 (ausser Kraft)
ACEA	Association des Constructeurs Européens d'Automobiles
ADAC	Allgemeiner Deutscher Automobil-Club
aDSG	Bundesgesetz über den Datenschutz vom 19. Juni 1992 (ausser Kraft)
AEUV	Vertrag über die Arbeitsweise der Europäischen Union (konsolidierte Fassung)
AG	Aktiengesellschaft
AJP	Aktuelle Juristische Praxis (Zeitschrift)
API	Application programming interface (= Programmierschnittstelle)
Art.	Artikel
ASTRA	Bundesamt für Strassen
Aufl.	Auflage
aVDSG	Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (ausser Kraft)
B2B	Business to Business
BAG	Bundesamt für Gesundheit
BAKOM	Bundesamt für Kommunikation
BB	Betriebs-Berater (Zeitschrift)
BBl	Bundesblatt
BDSG	Bundesdatenschutzgesetz vom 30. Juni 2017 (Deutschland)
BEUC	Bureau Européen des Unions de Consommateurs
BFS	Bundesamt für Statistik

BGE	Entscheid des Schweizerischen Bundesgerichts, Amtliche Sammlung
BGer	Bundesgericht
BISE	Business & Information Systems Engineering (Zeitschrift)
BJ	Bundesamt für Justiz
BKartA	Bundeskartellamt (Deutschland)
BR	Bundesrätin/Bundesrat
BSK	Basler Kommentar
bspw.	beispielsweise
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (SR 101)
BVerfG	Bundesverfassungsgericht (Deutschland)
BVerfGE	Entscheidung des Bundesverfassungsgerichts, Amtliche Sammlung
BVGer	Bundesverwaltungsgericht
bzw.	beziehungsweise
C-ITS	Cooperative Intelligent Transport Systems
CHF	Schweizer Franken
CLSR	Computer Law & Security Review
Comm	Commentary
CPI	Competition Policy International (Zeitschrift)
CPR	Current Psychiatry Reports (Zeitschrift)
CR	Computer und Recht (Zeitschrift)
CRi	Computer Law Review International
CR LPD	Loi fédérale sur la protection des données, Commentaire Romand
CSV	Comma-separated values (Dateiformat)
d.h.	das heisst
DA	Data Act (siehe DV)
DAR	Deutsches Autorecht (Zeitschrift)
dcm	DICOM (Dateiformat; siehe DICOM)
dg.o	Annual International Conference on Digital Government Research

DGA	Data Governance Act = 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 (Daten-Governance-Rechtsakt)
DICOM	Digital Imaging and Communications in Medicine (Standard)
DIRL	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
DMA	Digital Markets Act = Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte)
DS-GVO	Siehe DSGVO
DSA	Digital Services Act = Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste)
DSB	Datenschutz-Berater (Zeitschrift)
DSG	Bundesgesetz über den Datenschutz vom 25. September 2020 (SR 235.1)
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)
DSK	Datenschutzkonferenz (Konferenz der unabhängigen Datenschutzbehörden des [deutschen] Bundes und der Länder)
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
DSV	Verordnung über den Datenschutz vom 31. August 2022 (SR 235.11)
DuD	Datenschutz und Datensicherheit (Zeitschrift)

DV	Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (= Data Act)
E-DSG	Entwurf des Bundesgesetzes über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl 2017 7193 ff.)
E-DSGVO	Vorschlag für die Verordnung des Europäischen Parlaments und des Rates vom 25. Januar 2012 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endgültig
E-EGDG	Entwurf des Bundesgesetzes über das elektronische Gesundheitsdossier (BBl 2025 3399)
E-EHDS-VO	Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates vom 3. Mai 2022 über den europäischen Raum für Gesundheitsdaten, COM(2022) 197 final
E.	Erwägung(en)
e.g.	exempli gratia (= zum Beispiel)
E2EE	End-to-end encryption = Ende-zu-Ende-Verschlüsselung
EBLR	European Business Law Review
eCallVO	Verordnung (EU) 2015/758 des Europäischen Parlaments und des Rates vom 29. April 2015 über Anforderungen für die Typgenehmigung zur Einführung des auf dem 112-Notruf basierenden bordeigenen eCall-Systems in Fahrzeugen und zur Änderung der Richtlinie 2007/46/EG
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDI	Eidgenössisches Departement des Innern
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDPL	European Data Protection Law Review
EDSA	Europäischer Datenschutzausschuss
EDSB	Europäischer Datenschutzbeauftragter
EFD	Eidgenössisches Finanzdepartement
EG	Europäische Gemeinschaft

E-GD	Siehe EGD
EGD	Elektronisches Gesundheitsdossier
EGDG	Bundesgesetz über das elektronische Gesundheitsdossier (BBl 2025 3399; noch nicht in Kraft)
EGMR	Europäischer Gerichtshof für Menschenrechte
EHDS	European Health Data Space (= Europäischer Raum für Gesundheitsdaten)
EHDS-VO	Verordnung (EU) 2025/327 des Europäischen Parlaments und des Rates vom 11. Februar 2025 über den europäischen Gesundheitsdatenraum sowie zur Änderung der Richtlinie 2011/24/EU und der Verordnung (EU) 2024/2847
EHR	Electronic Health Record (= elektronische Gesundheitsaufzeichnung)
eidg.	eidgenössisch
EJLE	European Journal of Law and Economics
EJLT	European Journal of Law and Technology
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EJPLT	European Journal of Privacy Law & Technologies
eml	Electronic Mail (Dateiformat)
Empfehlung 2003/361/EG	Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, 2003/361/EG
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950 (SR 0.101)
endg.	endgültig
EPD	Elektronisches Patientendossier
EPDG	Bundesgesetz über das elektronische Patientendossier vom 19. Juni 2015 (SR 816.1)
EPDV	Verordnung über das elektronische Patientendossier vom 22. März 2017 (SR 816.11)
EPDV-EDI	Verordnung des EDI über das elektronische Patientendossier vom 22. März 2017 (SR 816.111)
EpG	Bundesgesetz über die Bekämpfung übertragbarer Krankheiten des Menschen vom 28. September 2012 (SR 818.101)

ER-Konv 108+	Modernisierte Europaratskonvention zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 10. Oktober 2018 (BBl 2020 599 ff.; noch nicht in Kraft)
Erw.G	Erwägungsgrund/Erwägungsgründe
et al.	et alii (= und andere)
ETH	Eidgenössische Technische Hochschulen
EU	Europäische Union
EuCML	Journal of European Consumer and Market Law
EuDIR	Zeitschrift für Europäisches Daten- und Informationsrecht
EuGH	Gerichtshof der Europäischen Union
EUR	Euro
EuR	Europarecht (Zeitschrift)
EuZ	Zeitschrift für Europarecht
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EWR	Europäischer Wirtschaftsraum
EY	Ernst & Young
f. / ff.	folgend(e)
FDV	Verordnung über Fernmeldedienste vom 9. März 2007 (SR 784.101.1)
FHIR	Fast Healthcare Interoperability Resources (Standard)
FIA	Fédération Internationale de l'Automobile
FIFG	Bundesgesetz über die Förderung der Forschung und der Innovation vom 14. Dezember 2012 (SR 420.1)
FIN	Fahrzeugidentifikationsnummer
FMG	Fernmeldegesetz vom 30. April 1997 (SR 784.10)
Fn.	Fussnote
FRAND	Fair, Reasonable and Non-Discriminatory
G	Gesetz
GDPR	General Data Protection Regulation (= DSGVO)
gem.	gemäss
GesG/BS	Gesundheitsgesetz des Kantons Basel-Stadt vom 21. September 2011 (SG 300.100)

GesG/ZH	Gesundheitsgesetz des Kantons Zürich vom 2. April 2007 (Ordnungsnummer 810.1)
GG	Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949
ggf.	gegebenenfalls
GK	Gelber Kommentar
GLJ	German Law Journal
GPS	Global Positioning System
GRCh	Charta der Grundrechte der Europäischen Union (ABl. C 83/389 vom 30. März 2010)
GRUR	Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)
GRUR Int.	GRUR International (Zeitschrift)
GRUR-Prax	Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter- und Wettbewerbsrecht (Zeitschrift)
HAVE	Haftung und Versicherung (Zeitschrift)
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz vom 3. Mai 2018
Hess. GVBl.	Gesetz- und Verordnungsblatt für das (deutsche Bundes-)Land Hessen
HFG	Bundesgesetz über die Forschung am Menschen vom 30. September 2011 (SR 810.30)
HJLT	Harvard Journal of Law & Technology
HK	Handkommentar
HL7	Health Level 7 (Standard)
HMG	Bundesgesetz über Arzneimittel und Medizinprodukte vom 15. Dezember 2000 (SR 812.21)
Hrsg.	Herausgeberin/Herausgeber
HTML	Hypertext Markup Language
HTTP/S	Hypertext Transfer Protocol/Hypertext Transfer Protocol Secure
i.d.R.	in der Regel
i.E.	im Ergebnis
i.e.S.	im engeren Sinn
i.S.d.	im Sinne des/der

i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
i.w.S.	im weiteren Sinn
ICD	International Statistical Classification of Diseases and Related Health Problems
IDG/BS	Informations- und Datenschutzgesetz des Kantons Basel-Stadt vom 9. Juni 2010 (SG 153.260)
IDG/ZH	Gesetz über die Information und den Datenschutz des Kantons Zürich vom 12. Februar 2007 (Ordnungsnummer 170.4)
IDPL	International Data Privacy Law (Zeitschrift)
IGE	Eidgenössisches Institut für Geistiges Eigentum
IIC	International Review of Intellectual Property and Competition Law
IJIO	International Journal of Industrial Organization
IK-EUDP	Interdepartementale Koordinationsgruppe EU-Digitalpolitik
Inc.	Incorporated
insb.	insbesondere
InTeR	Zeitschrift zum Innovations- und Technikrecht
IoT	Internet of Things = Internet der Dinge
IP	Internetprotokoll
ISO	Internationale Organisation für Normung
IT	Informationstechnologie
IV	Invalidenversicherung
JCLE	Journal of Competition Law & Economics
JEEA	Journal of the European Economic Association
JEP	Journal of Economic Perspectives
JIPITEC	Journal of Intellectual Property, Information Technology and E-Commerce Law
JIT	Journal of Information Technology
JMIR	Journal of Medical Internet Research
JRC	Joint Research Centre
JSON	JavaScript Object Notation (Dateiformat)
JZ	JuristenZeitung

K&R	Kommunikation & Recht (Zeitschrift)
Kfz	Kraftfahrzeug
KFZV	Verordnung über die wettbewerbsrechtliche Behandlung von vertikalen Abreden im Kraftfahrzeugsektor (KFZ-Verordnung, SR 251.6)
KG	Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen vom 6. Oktober 1995 (SR 251)
KI	Künstliche Intelligenz
KI-VO	Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz)
KMU	Kleine und mittlere Unternehmen
Komm	Kommentar
Konvention 108	Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (SR 0.235.1)
Konvention 108+	Siehe ER-Konv 108+
KRKomm	Kommunikation & Recht Kommentar zu DSGVO/BDSG/TDDDG
KUKO	Kurzkommentar
KVAG	Bundesgesetz betreffend die Aufsicht über die soziale Krankenversicherung vom 26. September 2014 (SR 832.12)
KVG	Bundesgesetz über die Krankenversicherung vom 18. März 1994 (SR 832.10)
lit.	litera
LJHSE	Law Journal of the Higher School of Economics
LSR	Life Science Recht – Juristische Zeitschrift für Pharma, Biotech und Medtech
m.a.W.	mit anderen Worten
m.E.	meines Erachtens
m.H.a.	mit Hinweis auf
m.w.H.	mit weiterem/weiteren Hinweis(en)

m.w.N.	mit weiterem/weiteren Nachweis(en)
MedR	Medizinrecht (Zeitschrift)
MepV	Medizinprodukteverordnung vom 1. Juli 2020 (SR 812.213)
MG	Bundesgesetz über die Armee und die Militärverwaltung vom 3. Februar 1995 (SR 510.10)
Mia.	Milliarde(n)
Mio.	Million(en)
MMR	Multimedia und Recht (Zeitschrift)
MODIG	Bundesgesetz über die Mobilitätsdateninfrastruktur (BBl 2025 1806; noch nicht in Kraft)
msg	Message File (Dateiformat)
MTLR	Michigan Technology Law Review
N	Note (bei Quellen aus Gesetzeskommentaren) Nationalrat (bei Quellen des AB)
NDKS	Nationale Datenkoordinationsstelle
NJW	Neue Juristische Wochenschrift
NR	Nationalrat
Nr.	Nummer
o.ä.	oder ähnlich
OASIS	Organization for the Advancement of Structured Information Standards
OAuth	Open Authorization (Protokoll)
OBD	On-Board-Diagnose
OCR	Optical Character Recognition
OECD	Organisation for Economic Co-operation and Development = Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OEM	Original Equipment Manufacturer = Erstausrüster
OFK	Orell Füssli Kommentar
OK	Onlinekommentar
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911 (SR 220)
OVF	Open Virtualization Format (Dateiformat)

OWL	Web Ontology Language
Pa.Iv.	Parlamentarische Initiative
PatG/ZH	Patientinnen- und Patientengesetz des Kantons Zürich vom 5. April 2004 (Ordnungsnummer 813.13)
PBG	Personenbeförderungsgesetz vom 20. März 2009 (SR 745.1)
PC LPD	Petit commentaire, Loi sur la protection des données
PCM	Puls-Code-Modulation (Dateiformat)
PDF	Portable Document Format (Dateiformat)
PIMS	Personal Information Management System
PinG	Privacy in Germany (Zeitschrift)
PLoS	Public Library of Science
PoPETs	Proceedings on Privacy Enhancing Technologies
PR	Public Relations
PSD2	Payment Services Directive 2 = Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG
PublG	Bundesgesetz über die Sammlungen des Bundesrechts und das Bundesblatt vom 18. Juni 2004 (SR 170.512)
RDi	Recht Digital (Zeitschrift)
ReMKomm	Kommentar zum Recht der elektronischen Medien
REST	Representational State Transfer (Architekturstil)
RGPD	Règlement Général sur la Protection des Données (siehe DSGVO)
RJE	The RAND Journal of Economics
RL	Richtlinie
RL 2007/46/EG	Richtlinie 2007/46/EG des Europäischen Parlaments und des Rates vom 5. September 2007 zur Schaffung eines Rahmens für die Genehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge (Rahmenrichtlinie) (ausser Kraft)

RL 2011/24/EU	Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung
RL 2019/1024	Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (Neufassung)
Rs.	Rechtssache
RW	Rechtswissenschaft (Zeitschrift)
Rz.	Randziffer
S	Ständerat
SÄZ	Schweizerische Ärztezeitung
SBB	Schweizerische Bundesbahnen
SBVR	Schweizerisches Bundesverwaltungsrecht
SDA	Schweizerische Depeschenagentur
SG	Systematische Gesetzessammlung
SGK	St. Galler Kommentar
SHK	Stämpflis Handkommentar
sic!	Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht
SIR	Schweizerisches Institut für Rechtsvergleichung
SJZ	Schweizerische Juristen-Zeitung
SM+S	Social Media + Society (Zeitschrift)
SMW	Swiss Medical Weekly (Zeitschrift)
SNOMED CT	Systematized Nomenclature of Medicine – Clinical Terms (Standard)
sog.	sogenannt
Solid	Social Linked Data
SPK-N	Staatspolitische Kommission des Nationalrats
SR	Systematische Rechtssammlung des Bundesrechts (bei Gesetzestexten) Ständerätin (bei Quellen des AB)
SRF	Schweizer Radio und Fernsehen

StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR 311.0)
Suva	Schweizerische Unfallversicherungsanstalt
SwissHDS	Swiss Health Data Space
SZKW	Schweizerische Zeitschrift für Kartellrecht- und Wettbewerbsrecht
SZW	Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht
TCS	Touring Club Schweiz
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (Deutschland)
TOM	Technische und organisatorische Massnahme(n)
Typgenehmigungs-ErgänzungsVO	Verordnung (EU) 2017/1151 der Kommission vom 1. Juni 2017 zur Ergänzung der Verordnung (EG) Nr. 715/2007 des Europäischen Parlaments und des Rates über die Typgenehmigung von Kraftfahrzeugen hinsichtlich der Emissionen von leichten Personenkraftwagen und Nutzfahrzeugen (Euro 5 und Euro 6) und über den Zugang zu Fahrzeugreparatur- und -wartungsinformationen, zur Änderung der Richtlinie 2007/46/EG des Europäischen Parlaments und des Rates, der Verordnung (EG) Nr. 692/2008 der Kommission sowie der Verordnung (EU) Nr. 1230/2012 der Kommission und zur Aufhebung der Verordnung (EG) Nr. 692/2008 der Kommission
Typgenehmigungs-VO	Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates vom 30. Mai 2018 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge, zur Änderung der Verordnungen (EG) Nr. 715/2007 und (EG) Nr. 595/2009 und zur Aufhebung der Richtlinie 2007/46/EG
u.a.	unter anderem
u.U.	unter Umständen
UAbs.	Unterabsatz
URL	Uniform Resource Locator
US	United States (of America)
usw.	und so weiter

UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
UVG	Bundesgesetz über die Unfallversicherung vom 20. März 1981 (SR 832.20)
UWG	Bundesgesetz gegen den unlauteren Wettbewerb vom 19. Dezember 1986 (SR 241)
v.	von
VDA	Verband der Automobilindustrie (Deutschland)
VE-DSG	Vorentwurf zum Bundesgesetz über den Datenschutz vom 21. Dezember 2016
VE-EPDG	Vorentwurf zum Bundesgesetz über das elektronische Patientendossier vom 28. Juni 2023
VE-KomPG	Vorentwurf zum Bundesgesetz über Kommunikationsplattformen und Suchmaschinen vom 29. Oktober 2025
VG	Verwaltungsgericht (Deutschland)
VO	Verordnung (EU)
VO 2018/1807	Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union
VTS	Verordnung über die technischen Anforderungen an Strassenfahrzeuge vom 19. Juni 1995 (SR 741.41)
VVG	Bundesgesetz über den Versicherungsvertrag vom 2. April 1908 (SR 221.229.1)
WBK-S	Kommission für Wissenschaft, Bildung und Kultur des Ständerats
WEKO	Wettbewerbskommission
WLAN	Wireless Local Area Network
WuW	Wirtschaft und Wettbewerb (Zeitschrift)
WWAN	Wireless Wide Area Network
XML	Extensible Markup Language (Dateiformat)
z.B.	zum Beispiel
ZBJV	Zeitschrift des Bernischen Juristenvereins
ZD	Zeitschrift für Datenschutz

ZEuP	Zeitschrift für Europäisches Privatrecht
ZEuS	Zeitschrift für europarechtliche Studien
ZEW	Leibniz-Zentrum für Europäische Wirtschaftsforschung
ZfPW	Zeitschrift für die gesamte Privatrechtswissenschaft
ZGB	Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907 (SR 210)
Ziff.	Ziffer
zit.	zitiert
ZSR	Zeitschrift für Schweizerisches Recht
ZUM	Zeitschrift für Urheber- und Medienrecht
ZWeR	Zeitschrift für Wettbewerbsrecht

§ 1 Thematische Einführung

I. Einleitung

1 Digitalisierung hat die Welt verändert. Innert weniger Jahrzehnte ist eine Wissensgesellschaft entstanden und mit ihr eine Wirtschaft, in der Daten ein zentraler Rohstoff sind.[1] Dies wirkt sich auf sämtliche Tätigkeitsbereiche und das tägliche Leben aller Menschen aus.[2] Länder weltweit versuchen deshalb, die neuartigen Phänomene zu erfassen, indem sie Gesetze erlassen oder bestehende revidieren. Im Fokus gesetzgeberischer Aktivitäten standen in den letzten Jahren unter anderem die Datenschutzgesetze: Sie sollen den von Datenbearbeitungen betroffenen Personen mehr Befugnisse einräumen und gleichzeitig die Regulierung und Kontrolle privater Akteurinnen sicherstellen.[3] Im Zuge dessen haben verschiedene Rechtsordnungen Datenportabilitätsrechte gesetzlich verankert.

2 Als Vorreiterin hierfür gilt die EU. In ihrer seit 2018 geltenden DSGVO ist mit dem «Recht auf Datenübertragbarkeit»[4] ein Datenportabilitätsrecht enthalten. Dieses wird in der juristischen Lehre allerdings vielfach kritisch rezipiert. Auch in der Praxis lässt eine Wirkung noch immer auf sich warten: Die Möglichkeit zur Portierung von Daten ist in der Bevölkerung kaum bekannt[5] und wird nur selten wahrgenommen.[6] So wurde das Recht auf Datenportabilität schon als «normatives Luftschloss»[7] bezeichnet. Dies kontrastiert mit den im Vorfeld geäusserten grossen Hoffnungen, die auf dem Datenportabilitätsrecht ruhten.

3 Das Portabilitätsrecht hat ausserhalb der EU zahlreiche Nachahmerinnen gefunden; eine davon ist die Schweiz.[8] Mit der Totalrevision des DSG fand das

---

1 Bundesrat, Strategie «Digitale Schweiz» 2020, 7620.

2 Europäische Kommission, Datenstrategie, 1.

3 Für die Schweiz etwa Botschaft DSG 2017, 6956.

4 Sowohl diese Bezeichnung als auch die Bezeichnung «Recht auf Datenherausgabe oder -übertragung» werden nachfolgend synonym zum Recht auf Datenportabilität verwendet.

5 Gerade im Vergleich zu anderen Betroffenenrechten ist das Portabilitätsrecht unbekannt, siehe Luzsa et al., 15; Kuebler-Wachendorff et al., Informatik Spektrum 2021, 266.

6 Siehe etwa die empirische Untersuchung von Karasoy/Turgut/Degeling, 335, wonach vom Recht auf Datenübertragbarkeit «so gut wie nie Gebrauch gemacht» wird; am Beispiel eines Musikstreamingdiensts auch Stiftung Datenschutz, Politikbrief, 4.

7 Kühling/Martini, EuZW 2016, 451; diese Bezeichnung wurde in der Literatur zahlreich übernommen, etwa durch Götzinger/Vasella, SZW 2021, 51; Hennemann, PinG 2017, 8; BSK DSG-Laux/Steiner, Art. 28 N 70; Sattler, Personenbezug, 81.

8 Zudem existieren in Brasilien, Singapur und im Vereinigten Königreich ähnliche Regelungen. Auf subnationaler Ebene gibt es in den US-Bundesstaaten Colorado und Kalifornien und in der kanadischen Provinz Québec Portabilitätsrechte. Diese Liste ist nicht abschliessend, siehe dazu Reimsbach-Kounatze/Molnar, 30 ff.; Zweifel-Keegan, 9 f.

Institut per 1. September 2023 Eingang in das eidgenössische Datenschutzgesetz. Art. 28 DSG sieht nunmehr ein «Recht auf Datenherausgabe oder -übertragung» vor, also das Recht einer Betroffenen, «vom Verantwortlichen die Herausgabe ihrer Personendaten, die sie ihm bekanntgegeben hat, in einem gängigen elektronischen Format» zu verlangen (Abs. 1). Nach Abs. 2 kann eine Betroffene zudem verlangen, dass der Verantwortliche die Daten einem anderen Verantwortlichen überträgt, soweit dies keinen unverhältnismässigen Aufwand erfordert. Diese Möglichkeit einer direkten Übertragung war dem Schweizer Recht zwar bereits davor nicht völlig fremd: Das FMG schreibt etwa seit längerem die Portierung von Telefonnummern vor,[9] und es existieren weitere Bestimmungen, die spezifisch die Pflicht zur Übertragung von Daten regeln.[10] Dennoch handelt es sich beim Portabilitätsrecht um ein grundlegend neuartiges Institut.

Dessen Einführung ist eng verbunden mit dem Aufkommen der grossen Internetplattformen und sozialen Netzwerke und lässt sich auf die damit einhergehende Veränderung der zwischenmenschlichen Kommunikation zurückführen.[11] In diesem Zeitgeist der 2010er-Jahre entstanden das Bedürfnis und die Notwendigkeit, den Umgang mit (Personen-)Daten neu zu verhandeln. Dabei stand nicht von vornherein fest, dass ein Portabilitätsrecht geschaffen werden muss. Tatsächlich liegen die Ursprünge der Datenportabilität denn auch nicht in der DSGVO, sondern reichen weiter zurück in die US-amerikanische IT-Szene – jene Szene also, die die Geburtsstätte der heute populären und erfolgreichen Internetplattformen ist. Entsprechend war sowohl in der EU als auch in der Schweiz lange umstritten, ob ein Portabilitätsrecht überhaupt gesetzlich verankert werden sollte, und wenn ja, in welchem Erlass und in welcher Form. 4

Als Folge davon ist sich die Schweizer Literatur bis heute uneinig darüber, welches Ziel das Portabilitätsrecht verfolgt. Dieses ist im DSG verankert und erfasst somit (nur) Personendaten. In dieser Ausgestaltung als Betroffenenrecht wird einerseits eine Nähe zum Datenschutz gesehen. Andererseits wird argumentiert, dass das Institut dem Wettbewerbs- oder Konsumentenschutzrecht zuzuordnen sei, weil es darauf ausgerichtet ist, Betroffenen die Wiederver- 5

[9] Siehe Art. 28 Abs. 5 lit. e FMG und gestützt darauf Art. 34*a* Abs. 1 FDV. Dies ermöglicht Kundinnen von Fernmeldediensten ihre Mobil- oder Festnetznummer zu behalten, wenn sie eine Anbieterin wechseln.

[10] Dazu Rz. 345 ff. sowie verschiedene Portabilitätsrechte in der sektoriellen Untersuchung.

[11] Das Portabilitätsrecht wurde daher schon als *lex social media* bezeichnet, siehe zu diesem Begriff Irion/Luchetta, 68; in dieselbe Richtung Thouvenin/Weber/Früh, 183; ebenso Graef/Verschakelen/Valcke, LJHSE 2013, 9; Kratz, InTeR 2019, 27.

wendung ihrer Daten zu ermöglichen, um den Wettbewerb spielen zu lassen.[12] Die Zielsetzung wird somit regelmässig nicht (nur) im Datenschutz-, sondern (auch) im Wettbewerbs-, Kartell-, oder Konsumentenschutzrecht verortet.

6 Der Nebel hat sich seit dem Inkrafttreten des DSG kaum gelichtet. Nicht anders ist die Situation in der EU, wo seit 2018 zahlreiche weitere Portabilitätsrechte hinzugekommen sind. Die genaue Tragweite des Rechts auf Datenportabilität ist damit bis heute weitgehend unklar geblieben – und bildet den Anlass für die vorliegende Untersuchung.

[12] Botschaft DSG 2017, 6984. Das Wettbewerbsrecht im weiteren Sinn umfasst das Kartellrecht (KG) und das Lauterkeitsrecht (UWG), siehe Weber/Volz, Rz. 1.20. Wenngleich im Zusammenhang mit dem Recht auf Datenportabilität meist pauschal vom «Wettbewerbsrecht» die Rede ist, so meint man damit zumeist das Kartellrecht. Ebenso Fix, 37.

II. Gegenstand der Untersuchung

A. Ausgangslage

Die Konturlosigkeit eines neu in ein Rechtssystem eingeführten Rechtsinstituts ist nicht überraschend, aber gleichwohl problematisch. Dies gilt besonders, wenn das Institut zunehmend als Grundlage für ähnliche Instrumente in anderen Bereichen diskutiert wird. Daher erscheint es erforderlich, das neuartige Rechtsinstitut grundlegend aufzuarbeiten. Das bedeutet, dass eine dogmatische Annäherung an das Recht auf Datenportabilität zu erfolgen hat, indem das Institut umfassend untersucht wird. Konkret sollen Gehalt und Zielsetzung des Rechts auf Datenportabilität ergründet, Unzulänglichkeiten erkannt und darauf gestützt Handlungsspielräume aufgezeigt werden.[13] 7

B. Stand der Forschung

Da das Recht auf Datenportabilität in der EU seit 2018 gilt, war es auch bereits Gegenstand von Forschungsarbeiten. Zum einen liegt eine deutsche Dissertation aus dem Jahr 2022 vor, die Zielsetzung und technische Aspekte des Rechts auf Datenportabilität beleuchtet.[14] Zum anderen existiert eine an der *University of Edinburgh* eingereichte Dissertation.[15] Ferner wurde und wird an der Universität Wien zum Recht auf Datenportabilität unter der DSGVO geforscht.[16] Diese Arbeiten betrachten das Portabilitätsrecht allerdings ausschliesslich aus Sicht der DSGVO und haben keinen induktiven Ansatz, mit welchem einzelne relevante Sektoren beleuchtet und daraus mit Blick auf die Zielsetzung des Instituts sektorspezifische (auch: sektorielle) Probleme untersucht werden können. 8

Relevante Rechtsprechung existiert, soweit ersichtlich, für das Institut bislang nicht. Dies gilt auch für die Schweiz. Allerdings sind hierzulande ebenfalls zahlreiche Abhandlungen erschienen, die das Schweizer Recht auf Datenportabilität thematisieren. Vereinzelt wurde das Institut zudem vertieft wissen- 9

---

13 Dazu sogleich Rz. 10 ff.

14 FIX, 35 ff., 275 ff. und *passim*.

15 LI, *passim*.

16 DULLER, *passim*. Unter dem Arbeitstitel «The Right to Data Portability under the GDPR: Implementation and Enforcement» entsteht zudem eine weitere Dissertation, siehe https://perma.cc/V9PD-HPVN.

schaftlich untersucht, namentlich in einem Gutachten[17] und in einer Untersuchung von Datenkooperationen[18]. Diese Arbeiten verbinden das Institut jeweils stark mit den sozialen Netzwerken. Dies drängt sich aufgrund der Entstehungsgeschichte auch auf. Allerdings ist das Rechtsinstitut nicht nur sektoriell, sondern grundsätzlich sektorübergreifend anwendbar.[19] Eine vertiefte Auseinandersetzung mit den Zielen, die das Recht auf Datenportabilität verfolgt, fand in der Schweizer Lehre bislang nicht statt. Daher ist es notwendig, das Institut für die Schweizer Rechtslage umfassend zu analysieren, freilich unter Einbezug der Überlegungen und Entwicklungen in der EU.

C. Forschungsfrage und Vorgehensweise

10 Mit dieser Untersuchung soll das Recht auf Datenportabilität an Kontur gewinnen. Das genaue Ziel oder die genauen Ziele sollen erkannt, und es sollen hinsichtlich dieses Ziels bzw. dieser Ziele Verbesserungsvorschläge gemacht werden. Dabei soll, ausgehend von den Zielen, eine inhaltliche Anpassung des bestehenden Datenportabilitätsrechts nach Art. 28 DSG erwogen und allenfalls die Notwendigkeit weiterer Portabilitätsrechte angestossen werden. Die Forschungsfrage lautet:

> Welches Ziel oder welche Ziele verfolgt das Recht auf Datenportabilität im Schweizer Recht und welche Eigenschaften sollte es umfassen, um das Ziel oder die Ziele (besser) erreichen zu können?

11 Weil das Schweizer Recht bislang einzig im DSG ein umfassendes Datenportabilitätsrecht kennt, knüpft die Untersuchung an diesem an. Entsprechend soll in einem ersten Teil eine Annäherung an das Rechtsinstitut erfolgen, indem die historischen, technisch-organisatorischen und rechtlichen Grundlagen aus Schweizer und europäischer Perspektive dargelegt werden (§ 2). Ausgehend davon ist sodann auf dem Weg der systematischen und teleologischen Auslegung festzustellen, was das Ziel oder die Ziele dieses Portabilitätsrechts ist resp. sind (§ 3). Im Fokus der Untersuchung stehen, aufbauend auf der existierenden Literatur, neben dem persönlichkeitsrechtlich gelagerten Ziel der datenschutzrechtlichen Selbstbestimmung und Autonomie der betroffenen Person auch wettbewerbsrechtliche Ziele. Dabei werden, wo erforderlich,

---

17 WEBER/THOUVENIN, *passim*. Dieses bezieht sich allerdings noch auf die Rechtslage unter dem aDSG. Siehe auch THOUVENIN/WEBER/FRÜH, 141 ff.

18 LANDOLT, 149 ff. und *passim*.

19 Eine Einschränkung wurde durch die eidgenössischen Räte nicht vorgenommen. Ausführlich zu den parlamentarischen Beratungen Rz. 97 ff.

politische und rechtliche Entwicklungen berücksichtigt, die teils über das klassische Datenschutzrecht hinausgehen.

Anschliessend befasst sich der zweite Teil der Untersuchung mit der Frage, ob mit Art. 28 DSG die Grundlagen geschaffen wurden, um das beabsichtigte Ziel oder die Ziele erreichen zu können. Angesichts des breiten Anwendungsbereichs der Regelung sind dafür induktiv drei Sektoren näher zu untersuchen (§ 4). Dabei handelt es sich um die sozialen Netzwerke, das Gesundheitswesen und den Mobilitätssektor.[20] Sie sind zunächst zu strukturieren, indem die jeweiligen Akteure eines Sektors und deren Beziehungen untereinander festgelegt und die möglichen Anwendungsfälle des Datenportabilitätsrechts ausgelotet und dargelegt werden. Daneben sind in den Sektoren zahlreiche spezifische Regelungen zu berücksichtigen. Für die einzelnen Sektoren ist daher individuell zu prüfen, ob das Portabilitätsrecht die Grundlagen für eine Zielerreichung schafft. Entsprechend werden sektorielle Probleme, Unzulänglichkeiten und resultierend daraus mögliche Handlungsspielräume je für die einzelnen Sektoren untersucht und kritisch diskutiert. 12

Die Sektoren sind in rechtlicher und tatsächlicher Hinsicht vielschichtig und lassen sich in dieser Untersuchung nicht in ihrer ganzen Breite darstellen. Sie sind daher nur so weit zu behandeln, als das Portabilitätsrecht und dessen Zielsetzungen in relevanter Weise berührt sind. Dabei lässt sich nicht vermeiden, dass Schwerpunkte gesetzt und somit eine gewisse Auswahl des Untersuchungsgegenstands getroffen wird. Im Zuge dessen werden auch andere existierende, aktuell diskutierte oder mögliche zukünftige (spezialgesetzliche) Portabilitätsrechte – jeweils mit Blick auf die Ziele – dargestellt, wenn diese für das datenschutzrechtliche Portabilitätsrecht relevant sind und dieses bspw. ergänzen oder verdrängen können. Angesichts des bisherigen Gleichlaufs der Jurisdiktionen wird hierbei ebenfalls von einer hohen Relevanz des europäischen Rechts für die Schweiz ausgegangen. Daher wird die Entwicklung in der EU dargelegt und aus Schweizer Perspektive berücksichtigt. Auf den zahlreichen spezialgesetzlichen Portabilitätsrechten liegt aber nicht der Schwerpunkt dieser Untersuchung. 13

Abschliessend sollen für das Rechtsinstitut als Ganzes Vorschläge entwickelt werden, wie die Grundlagen geschaffen werden könnten, damit das beabsichtigte Ziel oder die beabsichtigten Ziele (besser) erreicht und die genannten Probleme und Unzulänglichkeiten gelöst werden können (§ 5). Aufgrund der induktiven Methode ist dabei zu berücksichtigen, dass sich die sektoriellen Er- 14

[20] Zur Auswahl der Sektoren Rz. 392 ff.

kenntnisse nicht zwingend ohne Weiteres auf die zahlreichen Lebenssachverhalte ummünzen lassen, auf die das datenschutzrechtliche Portabilitätsrecht anwendbar ist.[21] Insofern konterkariert der breite Anwendungsbereich des Rechts auf Datenportabilität damit, dass einzelne Sektoren induktiv und notwendigerweise isoliert betrachtet werden müssen. Nur so lassen sich Erkenntnisse über das Rechtsinstitut als Ganzes gewinnen.

D. Eingrenzung

15 Was unter dem Recht auf Datenportabilität verstanden wird, hat sich jüngst, besonders unter dem Einfluss der europäischen Diskussion, gewandelt. Während der Begriff ursprünglich ausschliesslich mit Bezug auf Personendaten verstanden wurde,[22] hat sich dieses Verständnis nunmehr ausgeweitet, etwa auf Sachdaten.[23] Da sich nicht sämtliche Portabilitätsrechte, die in den einzelnen Sektoren mit Blick auf die Zielsetzungen denkbar sind, untersuchen lassen, muss das Thema eingegrenzt werden. Im Zentrum dieser Untersuchung sollen das datenschutzrechtliche Portabilitätsrecht und mit ihm die betroffene, portabilitätsberechtigte Person stehen. Einzig sie darf das Recht gemäss Art. 28 DSG ausüben. Weitere Portabilitätsrechte, etwa solche, die von juristischen Personen und damit B2B geltend gemacht, oder allein gestützt auf wettbewerbs- oder kartellrechtliche Überlegungen hergeleitet werden, sind daher nur dann anzusprechen, wenn es für das Verständnis des (datenschutzrechtlichen) Portabilitätsrechts hilfreich ist. Dies gilt namentlich in den einzelnen zu untersuchenden Sektoren. Folglich werden auch Anpassungsvorschläge für nur sektoriell anwendbare Portabilitätsrechte so weit wie möglich ausgeklammert oder nur am Rand thematisiert. Einzugehen ist indes auf das Verhältnis zwischen dem datenschutzrechtlichen Portabilitätsrecht und bestehenden sektoriellen Portabilitätsrechten.

16 Nicht Teil der Untersuchung ist ferner die Frage, ob das Datenportabilitätsrecht in der Praxis tragfähig ist, d.h. ob die Ziele tatsächlich erreicht werden. Dies wäre empirisch zu untersuchen, etwa durch eine Evaluation. Es findet damit einzig eine Annäherung aus rechtswissenschaftlicher Sicht statt, welche Denkanstösse vermittelt, die als Ausgangspunkt für künftige Untersuchungen dienen können.

---

21 Ähnlich Podszun, 95.

22 So etwa noch Thouvenin/Weber/Früh, 2.

23 Statt vieler Drexl, Challenges, 38; Jotterand, sic! 2025, 454.

Mit Blick auf die Forschungsfrage ist somit nicht zu untersuchen, *welche Vorgehensweisen* existieren, um die Grundlagen zu schaffen, um die mit dem Recht auf Datenportabilität verfolgten Ziele zu erreichen. Vielmehr soll erkannt werden, *wie das datenschutzrechtliche Portabilitätsrecht ausgestaltet werden müsste*, um die Grundlagen für die Zielerreichung zu schaffen. Das Datenportabilitätsrecht in Art. 28 DSG bildet Ausgangspunkt und zugleich Grenze des Untersuchungsgegenstands. 17

III. Methode

18 In der Schweiz legen die Bestimmungen in Art. 28 f. DSG und Art. 20 ff. DSV den Rechtsrahmen des Rechts auf Datenportabilität fest. Sie wurden im Wesentlichen aus Art. 20 DSGVO übernommen. Methodisch geht diese Untersuchung daher einerseits durch Auslegung dieser Rechtsnormen vor.[24] Andererseits ist rechtsvergleichend die Situation in der EU heranzuziehen, um die Forschungsfrage zu beantworten.[25] Für den zweiten Teil der Forschungsfrage wird zudem ein induktiver Ansatz verfolgt.[26]

A. Auslegungsmethoden

19 Rechtsnormen werden sprachlich-grammatikalisch, systematisch, historisch und teleologisch ausgelegt.[27] Gefolgt wird dabei dem sog. pragmatischen Methodenpluralismus, wonach den einzelnen Auslegungselementen keine hierarchische Prioritätsordnung zukommt.[28] Im Einzelfall soll eine sachlich richtige Entscheidung im normativen Gefüge resultieren, die auf ein befriedigendes Ergebnis der *ratio legis* ausgerichtet ist.[29]

20 Ausgangspunkt jeder Auslegung ist gemäss dem pragmatischen Methodenpluralismus der Wortlaut einer Bestimmung.[30] Sind aufgrund des blossen Wortlauts verschiedene Interpretationen möglich, ist nach der wahren Tragweite der Bestimmung zu suchen.[31] Dabei sind sämtliche Auslegungselemente zu berücksichtigen, namentlich der Zweck der Regelung, die dem Text zugrunde liegenden Wertungen sowie der Sinnzusammenhang, in dem die Norm steht.[32] Bei der Auslegung neuerer Bestimmungen kommt den Materialien eine besondere Stellung zu, weil die veränderten Umstände oder ein gewandeltes

---

24 Dazu sogleich Rz. 19 ff.
25 Dazu Rz. 23 ff.
26 Dazu Rz. 26.
27 Ausführlich KRAMER/ARNET, 66; für eine inhaltliche Abhandlung unter Einbezug der «realistischen» Auslegung siehe KUKO ZGB-PFAFFINGER, Art. 1 N 4.
28 So die ständige Rechtsprechung des BGer, siehe exemplarisch BGE 142 III 557 E. 8.3; BGE 141 III 195 E. 2.4; für das DSG ebenso BSK DSG-VASELLA, Einleitung N 84.
29 BGE 141 III 195 E. 2.4.
30 BGE 137 III 470 E. 6.4.
31 BGE 138 II 440 E. 13.
32 BGE 138 II 440 E. 13. Damit bekennt sich das BGer ebenfalls zu den vier Auslegungsmethoden.

Rechtsverständnis eine andere Lösung weniger nahelegen.[33] Bei jüngeren Gesetzen wird deshalb verstärkt auf die Materialien abgestellt.[34] Wenn unterschiedliche Auslegungen möglich sind, ist jene zu wählen, die der Verfassung am besten entspricht.[35] Wurde eine Norm im Kontext eines Staatsvertrags erlassen, ist zudem ein besonderes Augenmerk auf deren völkerrechtskonforme Auslegung zu legen.[36] Die drei Amtssprachen sind bei der Auslegung gleichwertig und entsprechend als Gesamtgefüge auszulegen (siehe Art. 14 Abs. 1 PublG).[37] Diese Methodik stammt zwar aus der juristischen Praxis, ist jedoch in der juristischen Doktrin ebenfalls anwendbar.[38]

Auf europäischer Ebene wird das Unionsrecht nach ständiger Rechtsprechung des EuGH nicht nur nach dem Wortlaut, sondern auch unter Berücksichtigung des Zusammenhangs und der Ziele einer Unionsvorschrift ausgelegt.[39] Zudem kann die Entstehungsgeschichte einer Norm relevante Anhaltspunkte für die Auslegung liefern.[40] Dem Wortlaut wird dabei jedoch ein gewisser Vorrang gegenüber den anderen Auslegungsmethoden eingeräumt.[41] Ist dieser eindeutig, bildet er die Grenze der Auslegung und der EuGH wendet weitere Auslegungsmethoden nicht mehr an.[42] Aus diesem Grund ist eine «Korrektur» einer Norm anhand von Sinn und Zweck selten.[43] Ist ein Wortlaut zweideutig oder führen die unterschiedlichen, jedoch allesamt verbindlichen Sprachfassungen zu unterschiedlichen Ergebnissen, muss auf die weiteren Auslegungsmethoden zurückgegriffen werden.[44] 21

B. Auslegung in dieser Untersuchung

Zur besseren Kontextualisierung werden noch vor der grammatikalischen Auslegung zunächst die historischen Grundlagen des Rechts auf Datenporta- 22

33 BGE 140 III 206 E. 3.5.4; BGE 139 III 98 E. 3.1; BGE 133 III 497 E. 4.1.
34 So das BGer wörtlich in BGE 138 II 440 E. 15.
35 BGE 138 II 440 E. 13. Auch diese Auslegung findet ihre Grenze jedoch im klaren Wortlaut und dem Sinn einer Bestimmung, siehe BGE 137 III 217 E. 2.4.1; BGE 131 II 697 E. 4.1.
36 BGE 141 II 436 E. 4.1.
37 Dies gilt insb. wenn die drei Versionen sprachlich nicht übereinstimmen, siehe BSK ZGB I-Honsell, Art. 1 N 9.
38 Höhn, AJP 1994, 419; ebenso Kramer/Arnet, 39.
39 EuGH C-127/14 vom 2. September 2015, Rz. 28.
40 EuGH C-127/14 vom 2. September 2015, Rz. 28.
41 Pieper, Rz. 12.
42 Pieper, Rz. 12.
43 Pieper, Rz. 15 m.w.N.
44 Pieper, Rz. 15.

bilität aufgearbeitet. Da es sich um ein junges Institut handelt, kommt der historischen Auslegung anhand der Materialien besonderes Gewicht zu.[45] Anschliessend sind für ein besseres Verständnis einige technische Grundlagen kurz zu skizzieren, ehe Art. 28 DSG im Einklang mit der bundesgerichtlichen Rechtsprechung anhand seines Wortlauts (sprachlich-grammatikalisch) ausgelegt wird.[46] Da das Rechtsinstitut gemäss Forschungsfrage ausdrücklich auf seine Zielsetzung untersucht werden soll und dies einen eigentlichen Kernbereich der Untersuchung darstellt, wird Art. 28 DSG sodann vertieft teleologisch ausgelegt.[47] Nach der Systematik ist vorliegend ebenfalls auszulegen, diese Methode steht jedoch nicht im Vordergrund.[48] Ebenfalls nicht vertieft wird die völkerrechtskonforme Auslegung, weil für das Recht auf Datenportabilität keine völkerrechtlichen Vorgaben existieren: Art. 8 EMRK geht kaum weiter als der verfassungsrechtliche Schutz durch Art. 13 BV.[49] Auch der zweite potenziell relevante Staatsvertrag, die von der Schweiz ratifizierte Konvention 108 des Europarats, ist als völkerrechtliche Vorgabe nicht einschlägig; ein Portabilitätsrecht ist darin nicht vorgesehen.

C. Rechtsvergleichung in dieser Untersuchung

23 Die Regelungen der EU haben die schweizerische Ausgestaltung des Datenportabilitätsrechts massgeblich beeinflusst. Namentlich im Gesetzgebungsprozess verwiesen die Räte explizit darauf.[50] Da die Bestimmungen der DSGVO aber nicht aufgrund einer völkerrechtlichen Verbindlichkeit, sondern primär aus praktischen und politischen Gründen übernommen wurden, sind sie nicht Gegenstand einer völkerrechtlichen Auslegung.[51]

24 Allerdings hat der Schweizer Gesetzgeber das Recht auf Datenportabilität im Wesentlichen autonom nachvollzogen,[52] weshalb sich die DSGVO als Auslegungshilfe heranziehen lässt.[53] Dies entspricht der konstanten Praxis des BGer, welches EU-Recht berücksichtigt, wenn die Schweiz eine materielle Re-

45 Dazu Rz. 86 ff. und für die Schweiz im Besonderen Rz. 97 ff.
46 Für die Schweiz Rz. 173 ff. und für die EU Rz. 123 ff.
47 Dazu Rz. 245 ff.
48 Dazu Rz. 241 ff.
49 BSK DSG-Vasella, Einleitung N 88.
50 Dazu Rz. 97 ff.
51 BSK DSG-Vasella, Einleitung N 91.
52 Mit eingehender Begründung Steiner, 126; ebenso SHK DSG-Baeriswyl/Pärli, EMRK, ER-Konv 108+, Richtlinie (EU) 2016/680, DSGVO N 49; BJ, Erläuternder Bericht DSV, 44; BSK DSG-Laux/Steiner, Art. 28 N 22.
53 Generell BSK DSG-Vasella, Einleitung N 92.

gelung der EU übernahm und damit eine Angleichung des Schweizer Rechts an das EU-Recht beabsichtigte.[54] Es tut dies im Rahmen seiner teleologischen und historischen Auslegung.[55] Neben dem Wortlaut des Rechts auf Datenportabilität in der DSGVO, von dem ausgehend allfällige Unterschiede aufzuzeigen sind, sind die teleologische und historische Auslegung die rechtsvergleichenden Anknüpfungspunkte dieser Untersuchung. Dabei wird die Regelung der DSGVO immer dann herangezogen, wenn sich daraus für die Schweiz Gemeinsamkeiten oder Unterschiede ergeben, aus welchen für die Schweiz relevante Schlüsse gezogen werden können. Darüber hinaus sind generell die datenpolitischen Entwicklungen in der EU zu berücksichtigen, namentlich im Kontext eines Aufbaus einer europäischen Datenwirtschaft.[56]

Soweit rechtsvergleichend vorgegangen wird, werden die Regelungen in der DSGVO oder anderen Erlassen der EU und des EWR und die dazugehörige Literatur der Einfachheit halber als «europäisch» bezeichnet, während als Gegenstück dazu von Schweizer Regelungen oder Literatur die Rede ist. 25

D. Induktiver Ansatz dieser Untersuchung

Im Fall der Rechtsanwendung ist die juristische Logik i.d.R. deduktiv, d.h. es wird vom Allgemeinen (einem Rechtssatz) auf das Besondere (einen Sachverhalt) geschlossen.[57] Umgekehrt ist es möglich, induktiv von einzelnen, beobachteten Beispielen auf allgemeine Regeln oder Gesetze zu schliessen.[58] Dieser sog. Induktionsschluss wird besonders in den empirischen Naturwissenschaften angewendet, findet sich aber auch in der juristischen Methodenlehre.[59] Der zweite Teil dieser Arbeit folgt einem solchen induktiven Ansatz, weil sich Anpassungen des Portabilitätsrechts nur anhand konkreter Anwendungsbeispiele herleiten lassen. 26

Mit dem induktiven Ansatz lassen sich aus Einzelfällen allgemeine Regeln oder Fallgruppen bilden.[60] Einzelne Problemlagen können mithilfe der verfügbaren Literatur beschrieben und anschliessend zu allgemeinen Fallgruppen «ver- 27

54 BGE 144 III 285 E. 2.2.2.

55 BGE 144 III 285 E. 2.2.2.

56 Europäische Kommission, Aufbau Datenwirtschaft, *passim*; aus Schweizer Sicht IK-EUDP, *passim*.

57 Forstmoser/Vogt, 2.

58 Forstmoser/Vogt, 4; Metzger, Rechtstheorie 2009, 317.

59 Forstmoser/Vogt, 4; Metzger, Rechtstheorie 2009, 317 m.w.N., im Kontext der Herleitung allgemeiner Rechtsgrundsätze.

60 Forstmoser/Vogt, 4.

dichtet» werden.[61] So kann sich aus der Analyse verschiedener Einzelfälle ein genereller Handlungsbedarf herausbilden. Gleichwohl ist festzuhalten, dass bei einem induktiven Ansatz die Problemlagen nicht abschliessend erfassbar sind.[62] Induktionsschlüsse basieren nicht allein auf den herangezogenen Einzelfällen, sondern stets auch auf der Prämisse, dass künftige Fälle gleichbehandelt werden wie die bereits herangezogenen Fälle.[63] Induktionsschlüsse können daher keine absolute, ausnahmslose Geltung beanspruchen.[64]

28 Vorliegend wird das Portabilitätsrecht in spezifischen Sektoren und Anwendungsbeispielen betrachtet, um zu erkennen, ob dessen Ziele erreichbar sind. Über die sektorielle Betrachtung von Einzelfällen lassen sich Erkenntnisse über das Rechtsinstitut als Ganzes gewinnen.[65] Damit die Erkenntnisse nicht einzig auf den Umständen eines spezifischen Sektors basieren und dadurch an abstrakter Aussagekraft einbüssen, sind drei Sektoren und in diesen die sektoriell auftretenden Probleme und Unzulänglichkeiten zu untersuchen. Die gewählten Sektoren sollen möglichst heterogen sein, unterschiedliche Nutzer tangieren und (nur) teilweise über sektorspezifische Regelungen verfügen.[66] Damit wird eine möglichst grosse Erkenntnistiefe angestrebt. In den Sektoren sollen Muster und Regelmässigkeiten erkannt, und so über einen spezifischen Sektor hinaus verallgemeinerungsfähige Aussagen zum Recht auf Datenportabilität gemacht werden können.[67] Die Untersuchung mehrerer Sektoren soll dabei sicherstellen, dass die Anpassungen sektorübergreifend tragfähig sind.

29 Mit dieser Methode lassen sich Anpassungsvorschläge herausbilden, die potenziell für das Portabilitätsrecht als Ganzes belastbar sind. Nach dem Gesagten ist allerdings nicht auszuschliessen, dass sich die Tragfähigkeit der Anpassungen in anderen Sektoren widerlegen liesse. Wie bereits aufgeführt, könnten auch andere Sektoren für diese Untersuchung gewählt werden, solange in ihnen das Portabilitätsrecht grundsätzlich anwendbar ist. Daraus liessen sich andere, womöglich sogar konträre Schlüsse ziehen als in den vorliegend gewählten Sektoren. Eine Auswahl ist allerdings unumgänglich und wird letztlich dadurch relativiert, dass bei den gewählten Sektoren darauf geachtet wird, dass sie praktisch relevant sind.

---

61 Ähnlich das Vorgehen bei Früh, sic! 2018, 523; Thouvenin/Weber/Früh, 97.

62 Früh, sic! 2018, 523; wohl auch Metzger, Rechtstheorie 2009, 318; Thouvenin/Weber/Früh, 97.

63 Metzger, Rechtstheorie 2009, 318.

64 Metzger, Rechtstheorie 2009, 318.

65 Ähnlich für Datenzugangsrechte im Allgemeinen Früh, sic! 2018, 522 f.

66 Zur Methodik der Auswahl der Sektoren Rz. 392 ff.

67 Schallbruch et al., 44; ähnlich das Vorgehen auch bei Thouvenin/Weber/Früh, 97.

IV. Grundbegriffe

Nachfolgend werden einige Grundbegriffe erläutert, die in dieser Untersuchung relevant sind. 30

A. Daten i.w.S.

Ein Datum (im Plural: Daten) ist eine besondere Art der Information, die sich dadurch kennzeichnet, dass sie maschinenlesbar codiert ist.[68] Der Begriff der Information wiederum lässt sich in dreierlei Hinsicht abgrenzen: Als semantische, syntaktische und strukturelle Information.[69] Bei Daten müssen Informationen als physikalische Struktur vorliegen, damit sie von einer Maschine verarbeitet werden können (strukturelle Komponente).[70] Dabei muss es sich auf syntaktischer Ebene um maschinenlesbare Zeichen handeln (syntaktische Komponente).[71] Es ist möglich, dass diese Zeichen auf semantischer Ebene eine Bedeutung haben, für eine Qualifikation als Datum i.w.S. ist dies aber nicht notwendig (semantische Komponente).[72] Folglich müssen einzig die strukturelle und syntaktische Komponente erfüllt sein, damit von Daten i.w.S. ausgegangen werden kann.[73] 31

B. Personendaten (Daten i.e.S.)

Anders als der Datenbegriff i.w.S.[74] setzt der Begriff der Personendaten auf der semantischen Ebene an: Ein Personendatum konstituiert sich durch die personenbezogene Bedeutung, die der Information zukommt.[75] Diese semantische Ebene ist massgebend für die gängige Definition in den Datenschutzgesetzen. Nach Art. 5 lit. a DSG sind Personendaten «alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen». Mit Angabe ist ebenfalls 32

---

68 Zech, 32, dazu auch Eckert, SJZ 2016, 246.

69 Zech, 45.

70 Spiecker genannt Döhmann, RW 2010, 253; Zech, 32 m.w.N.

71 Zech, 32 m.w.N.

72 Zech, 32 f. Anders bei den sogleich zu behandelnden Personendaten.

73 Eckert, SJZ 2016, 247; Zech, 32 f.; siehe auch Spiecker genannt Döhmann, RW 2010, 253, die primär an der Körperlichkeit des Datums ansetzt.

74 Dazu Rz. 31.

75 Eckert, SJZ 2016, 247; Zech, 33.

Information gemeint.[76] Bestimmt ist eine Person dann, wenn sich aus einer Information selbst ergibt, dass es sich um diese Person handelt.[77] Bestimmbarkeit liegt demgegenüber vor, wenn auf die Person aufgrund zusätzlicher Informationen geschlossen werden kann.[78] Der Struktur und der Syntax eines Personendatums kommt dabei keine konstitutive Bedeutung zu.[79]

33 Die europäische Konzeption von «personenbezogenen Daten» in Art. 4 Ziff. 1 DSGVO entspricht im Wesentlichen der Schweizer Regelung; die Schweiz hat mit der DSG-Revision den Begriff an die DSGVO angeglichen.[80] In dieser Untersuchung sind, wo nicht ausdrücklich anders festgehalten, die Begriffe «Personendaten», «personenbezogene Daten» und «Daten» synonym zu verstehen.

C. Sachdaten

34 Sachdaten setzen ebenfalls auf der semantischen Ebene an, allerdings ohne Bezug der Daten zu einer natürlichen Person. Der Umgang mit ihnen ist daher nicht vom DSG erfasst.[81] Sie können in der Schweiz unbeschränkt bearbeitet werden, ohne dass die Vorgaben des Datenschutzrechts anwendbar sind. Auch in der EU fallen Sachdaten nicht unter die DSGVO.[82] Dort können allerdings bei Daten ohne Personenbezug andere gesetzliche Vorgaben gelten, etwa die DV.[83]

D. Datenbearbeitung

35 Eine Datenbearbeitung ist jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren (Art. 5 lit. d DSG). Das Gesetz nennt

76 HK DSG-Rosenthal, Art. 3 N 8.

77 Bspw. Standortdaten, Identifikationsnummer oder ein Personalausweis, siehe BGE 136 II 508 E. 3.2; Botschaft DSG 2017, 7019; bereits Botschaft DSG 1988, 444.

78 BGE 136 II 508 E. 3.2.

79 Eckert, SJZ 2016, 247. Auch menschliche Gedanken, die nicht aufgezeichnet wurden und sich damit nicht «materialisiert» haben, fallen unter den Datenbegriff, siehe HK DSG-Rosenthal, Art. 3 N 3. Dazu ebenfalls BGE 147 III 139 E. 3.4.6; a.A. in Bezug auf das diesbezüglich deckungsgleiche IDG/BS jedoch PK IDG/BS-Rudin, § 3 N 13 f.

80 Rosenthal, Jusletter 2020, Rz. 19.

81 BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt, Art. 5 N 101; Götzinger/Vasella, SZW 2021, 42.

82 BeckOK DSR-Schild, Art. 4 DSGVO N 22 ff.; BeckKomm-Klar/Kühling, Art. 4 Ziff. 1 DSGVO N 12 ff.

83 Dazu Rz. 611 ff.

einige Beispiele, die ein Bearbeiten darstellen, namentlich das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten. Unter der DSGVO ist mit dem Begriff der «Verarbeitung» im Wesentlich dasselbe gemeint (Art. 4 Ziff. 2 DSGVO).

E. Betroffene Person

Die betroffene Person (auch: der oder die Betroffene) ist gemäss Art. 5 lit. b DSG diejenige natürliche Person, über die Daten bearbeitet werden. Im Kontext der Datenportabilität kann die betroffene Person die Herausgabe «ihrer» Personendaten verlangen. Diese Definition deckt sich mit derjenigen unter der DSGVO (Art. 4 Ziff. 1 DSGVO). 36

F. Verantwortliche

Als der oder die Verantwortliche wird diejenige private Person oder dasjenige Bundesorgan verstanden, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet (Art. 5 lit. j DSG; ebenso Art. 4 Ziff. 7 DSGVO). 37

Beim Recht auf Datenportabilität sind u.U. mehrere Verantwortliche beteiligt. Vorliegend wird der durch das Recht auf Datenportabilität Verpflichtete als *alter* Verantwortlicher bezeichnet. Dieser muss die Daten herausgeben oder übertragen. Als *neue* Verantwortliche wird demgegenüber diejenige Partei bezeichnet, der die portierten Daten übertragen werden, sodass die Betroffene sie weiter nutzen kann. 38

G. Auftragsbearbeiter

Als Auftragsbearbeiter wird gemäss Art. 5 lit. k DSG die private Person oder das Bundesorgan bezeichnet, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet. Unter der DSGVO existiert mit dem Auftragsverarbeiter ein im Wesentlichen deckungsgleiches Konstrukt (Art. 4 Ziff. 8 DSGVO). 39

H. Datenökosystem

40 Der Begriff des Ökosystems stammt ursprünglich aus der Biologie, wird heute jedoch im Kontext von Daten auch in der betriebswirtschaftlichen[84] und juristischen Lehre[85] oder in der IT-Literatur[86] verwendet. Charakteristisch an einem Ökosystem ist der alles umspannende Funktionsraum, der durch die Interaktion von Lebewesen untereinander geprägt ist.[87] Auf Daten bezogen umfasst es «das prägende, ganzheitliche Umfeld, in dem verschiedene Akteure zusammenkommen, um Daten zu produzieren, anzubieten, zu finden und zu ‹konsumieren›».[88] Demnach wirken die Einflüsse des Datenökosystems in alle Phasen der Datenlebenszyklen hinein, dieses «schafft die entsprechenden Rahmen-, Netzwerk- und regulativen Bedingungen für die (Zusammen-)Arbeit mit Daten bzw. stellt diese konkret dar».[89] Auch andere Autoren diskutieren den Begriff vorwiegend im Kontext der Interaktionen von Beteiligten, die ein Datenökosystem ausmachen.[90] Die Artikel 29-Datenschutzgruppe und die Swiss Data Alliance verbinden den Begriff explizit mit dem Recht auf Datenportabilität.[91]

41 Kernbestandteil von Datenökosystemen sind vier Aspekte: Akteure, Rollen, Beziehungen und Ressourcen.[92] Damit diese gemeinsam ein Datenökosystem bilden, müssen zusätzlich zwei Eigenschaften vorliegen: Vernetzung und Selbstorganisation.[93] Diese Eigenschaften werden für das Recht auf Datenportabilität angenommen, da das Portabilitätsrecht eine Vernetzung bewirken kann und diese selbstorganisiert durch die Akteurinnen – primär die betroffenen Personen

84 Flügge, 53 ff.; Schweitzer/Peitz, 11 f.; Steffen/Wieworra/Kroon, 37.

85 Gasser, ZSR 2015, 349; Graef/Husovec/Van den Boom, EuCML 2020, 16; BSK DSG-Laux/Steiner, Art. 28 N 71.

86 Metere et al., ArXiv 2022, *passim*.

87 Flügge, 54.

88 Putnings, 7.

89 Putnings, 7.

90 OECD, Data-Driven Innovation, 91.

91 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 4; Swiss Data Alliance, Leitlinien Datenportabilität, 7.

92 Oliveira/Lóscio, dg.o 2018, 3 ff., die nach Auswertung zahlreicher Studien zu diesem Schluss gelangen und eine Definition von Datenökosystem vorschlagen als «a set of networks composed by autonomous actors that directly or indirectly consume, produce or provide data and other related resources (e.g., software, services and infrastructure). Each actor performs one or more roles and is connected to other actors through relationships, in such a way that actors collaboration and competition promotes Data Ecosystem self-regulation».

93 Oliveira/Lóscio, dg.o 2018, 6.

– erfolgt. Im zweiten Teil der Untersuchung werden drei Sektoren als Fallbeispiele gewählt. Um diese vertieft und vergleichend untersuchen zu können, werden sie ausgehend von diesem Verständnis als Datenökosysteme strukturiert.[94]

I. Datenraum

Der Gesetzgeber knüpft nicht an den Begriff des Datenökosystems, sondern zumeist an denjenigen des Datenraums an.[95] Ein Datenraum ist eine dezentralisierte Infrastruktur für den vertrauenswürdigen Austausch von Daten in Datenökosystemen auf der Grundlage gemeinsam vereinbarter Grundsätze.[96] Diese Infrastruktur stellt für einen bestimmten Gesellschaftsbereich oder für eine ganze Volkswirtschaft Daten, Datendienste und Regeln für die Datennutzung bereit.[97] Die Nutzung einer solchen Dateninfrastruktur besteht dabei aus den verschiedenen Interaktions- und Austauschbeziehungen der Teilnehmenden (Datengeber, Datennutzer, Intermediäre); sie machen das Datenökosystem aus.[98] Es handelt sich somit bei Datenräumen und Datenökosystemen um zwei Seiten derselben Medaille: Während das Datenökosystem die reale Welt und deren (Daten-)Beziehungen beschreibt, bezieht sich der Datenraum als digitales Abbild dieses Ökosystems (sog. *shared digital twin*[99]) auf die Datenobjekte. Die Datenobjekte beschreiben ihrerseits das Datenökosystem. 42

Ähnlich, wenngleich weniger ausführlich, definieren die EU und die Schweiz Datenräume. Nach der EU-Kommission besteht ein Datenraum aus einem echten Binnenmarkt für Daten, der für Daten aus aller Welt offensteht, in dem sowohl personenbezogene als auch nicht personenbezogene Daten sicher sind und in dem Unternehmen leicht Zugang zu einer nahezu unbegrenzten Menge hochwertiger industrieller Daten erhalten.[100] Nach schweizerischem Verständnis ist ein Datenraum hingegen die technische und organisatorische Struktur, welche Bereitstellung, Austausch und Bezug von Daten aus verschie- 43

94 Dazu unten § 4 und insb. Rz. 392 ff.

95 Bundesrat, Strategie «Digitale Schweiz» 2020, 7624; Europäische Kommission, Datenstrategie, 5; Swiss Data Alliance, Whitepaper Datenraum, *passim*; UVEK/EDA, *passim*.

96 Eigene Übersetzung des Wortlauts «a decentralised infrastructure for trust-worthy data sharing and exchange in data ecosystems based on commonly agreed principles» nach Nagel/Lycklama, 23. Auf diese Definition verweist auch die Swiss Data Alliance, Whitepaper Datenraum, 12.

97 Otto/Burmann, Informatik Spektrum 2021, 284.

98 Otto/Burmann, Informatik Spektrum 2021, 284.

99 In diesem Sinn Otto/Burmann, Informatik Spektrum 2021, 285; ebenso am Beispiel des Mobilitätsdatenökosystems Nagel/Lycklama, 23.

100 Europäische Kommission, Datenstrategie, 5.

denen Quellen und von verschiedenen Akteuren ermöglicht und regelt.[101] Datenräume sind oft sektorspezifisch organisiert, durch Zweck, klare Regeln und Standards definiert, und werden von einem Betreiber verwaltet.[102] Ausgehend von solchen Datenräumen werden in § 4 die einzelnen zu untersuchenden Datenökosysteme bzw. Sektoren ausgewählt.

J. Datenwirtschaft

44 Das Recht auf Datenportabilität ist ein auf den digitalen Verkehr und besonders auf den Datenverkehr im Internet zugeschnittenes Institut.[103] Entsprechend ist das Institut eng mit der Funktionsweise der Datenwirtschaft verknüpft. Darunter versteht man ein Ökosystem von unterschiedlichen Marktteilnehmenden, deren Zusammenarbeit dafür sorgt, dass Daten zugänglich und nutzbar sind.[104] Dabei steht die Frage der ökonomischen Verwertung der Daten im Vordergrund. Die Marktteilnehmenden sollen einen Wert aus den Daten schöpfen, indem sie Anwendungen hervorbringen, die zur Verbesserung des Lebensalltags der Bevölkerung beitragen.[105] Der Begriff beschreibt mithin die Gesamtheit der wirtschaftlichen Aktivitäten, die auf digitalen Technologien zur Verarbeitung von Informationen und Datenübertragung basiert.[106] Diese Datenwirtschaft ist durch besondere Marktmechanismen und -strukturen geprägt[107] sowie durch die spezifischen Eigenschaften von Daten[108].

45 In der Literatur zum Recht auf Datenportabilität werden unterschiedliche Begriffe benutzt, um diese Funktionsweise zu beschreiben, etwa «digitale Wirtschaft», «Digitalwirtschaft», «Datenökonomie», «Plattformökonomie», «Datengesellschaft», «datenbasierter Markt» und viele mehr. Im Kern und soweit vorliegend relevant ist damit jeweils die eben geschilderte ökonomische Verwertung von Daten gemeint, weshalb einheitlich der Begriff der «Datenwirtschaft» verwendet wird.

---

101 UVEK/EDA, 46. Dabei wohl zurückgehend auf Collovà et al., 57.
102 UVEK/EDA, 46. Dabei wohl zurückgehend auf Collovà et al., 57.
103 Dazu Rz. 198.
104 Europäische Kommission, Aufbau Datenwirtschaft, 2.
105 Europäische Kommission, Aufbau Datenwirtschaft, 2.
106 Staffler/Ebersberger, 2.
107 Etwa global auftretende Unternehmen, für welche digitale Technologien geradezu die Basis ihrer Geschäftsmodelle bilden. Sie sind oft als Plattformen ausgestaltet und können von starken Netzwerkeffekten profitieren. Siehe ausführlich Ebersberger/Dachs, 69, 75 ff. und *passim*. Dazu auch Rz. 46 ff.
108 Dazu Rz. 295.

K. Internetplattformen und soziale Netzwerke

1. Zweiseitige Märkte als Ausgangspunkt

In der Untersuchung wird wiederholt auf Internetplattformen und soziale Netzwerke verwiesen. Damit sind sog. *Big Tech*-Unternehmen gemeint. Sie dienten bereits im Gesetzgebungsprozess als Anwendungsbeispiel für das Portabilitätsrecht und werden daher in der Literatur regelmässig aufgeführt. Dies liegt daran, dass gerade plattformbasierte Geschäftsmodelle von den Marktmechanismen der Datenwirtschaft geprägt sind: Sie beruhen auf zweiseitigen Märkten und damit darauf, zwei unterschiedliche Akteure zur Teilnahme an einer Plattform zu bewegen.[109] Die Plattform übernimmt dabei die Rolle des Intermediärs. Ein Beispiel sind die sozialen Netzwerke, welche ihre Nutzer mit Werbetreibenden auf der Plattform verbinden. Damit unterscheidet sich die Funktionsweise der Plattformen von einseitigen Märkten, auf welchen die Akteure unmittelbar in einer Beziehung zueinanderstehen, etwa wenn ein Käufer ein Buch in einer Buchhandlung erwirbt. 46

2. Begriffsdefinition

Der Begriff der (Internet-)Plattform wird je nach Disziplin unterschiedlich verwendet und lässt sich kaum einheitlich definieren.[110] Im Kern geht es jedoch immer um Dienstleistungen, die zwei Gruppen von Nutzern verbinden.[111] Der DMA, auf den zurückzukommen sein wird, verwendet den Begriff der «zentralen Plattformdienste» und meint damit Online-Vermittlungsdienste, Online-Suchmaschinen, Onlinedienste sozialer Netzwerke, Video-Sharing-Plattform-Dienste und weitere (Art. 2 Ziff. 2 DMA). Inhaltlich wird der Begriff jedoch nicht erläutert. Allerdings verweist Erw.G 2 DMA auf einige Marktmechanismen und -eigenschaften, welche zentrale Plattformdienste zu ihrem eigenen Vorteil nutzen könnten. Beispielhaft werden extreme Grössenvorteile genannt, die in vielen Fällen darauf zurückzuführen seien, dass für die Bedienung weiterer gewerblicher Nutzer oder Endnutzer fast keine Grenzkosten entstünden. Weitere Beispiele gemäss Erw.G 2 DMA sind Netzwerkeffekte, Lock-In-Effekte, fehlende Multi-Homing-Möglichkeiten der Endnutzer, vertikale Integration sowie Datenvorteile. Die Onlinedienste eines sozialen Netzwerks oder im Fol- 47

109 Blatter, sic! 2016, 379; Louven, ZWeR 2019, 156.
110 Steffen/Wieworra/Kroon, 7.
111 Ebersberger/Dachs, 75.

genden schlicht die «sozialen Netzwerke» sind gemäss Art. 2 Ziff. 7 DMA diejenigen Plattformen, auf denen Endnutzer mit unterschiedlichen Geräten, insb. durch Unterhaltungen, Beiträge, Videos und Empfehlungen, miteinander in Kontakt treten und kommunizieren sowie Inhalte teilen und andere Nutzer und Inhalte entdecken können.

48 Im Kontext des Rechts auf Datenportabilität werden sowohl die Plattformen als auch die sozialen Netzwerke stets genannt, jedoch begrifflich nicht näher erläutert. Entsprechend wird in dieser Untersuchung auf das ökonomische Verständnis abgestellt, auf welchem das Verständnis im DMA gründet: Plattformen werden vorwiegend durch ihre vermittelnde Funktion in zweiseitigen Märkten charakterisiert,[112] zuweilen wird auch von zweiseitigen Plattformen gesprochen.[113] Eine Plattform ist nach diesem Verständnis also diejenige Akteurin, die eine potenziell gewinnbringende Interaktion zwischen zwei anderen Akteuren ermöglicht oder erleichtert.[114] Die Plattform handelt als vermittelnde oder intermediäre Akteurin, bspw. zwischen Verkäufer und Käufer.[115] An der eigentlichen Transaktion ist sie dagegen nicht beteiligt. Sie kann als Aufmerksamkeitsplattform (auch: Werbeplattform) einer Nutzergruppe die Aufmerksamkeit der anderen Nutzergruppe ermöglichen oder als Vermittlungsplattform eine auf individuelle Präferenzen abgestimmte und von allen Nutzergruppen angestrebte Vermittlung zwischen unterschiedlichen Nutzergruppen ermöglichen.[116]

49 Im Fokus des Handelns der Plattform liegen meist sog. Netzwerkeffekte.[117] Sind diese direkt, besteht eine positive Abhängigkeit der Wertschätzung eines Nutzers von der Anzahl der Akteure auf der eigenen Marktseite.[118] Dies gilt besonders in denjenigen digitalen Märkten, in denen Konsumenten auch als Produzenten auftreten, etwa in den sozialen Netzwerken: Dort steigt der Nutzen eines sozialen Netzwerks mit einer zunehmenden Anzahl anderer erreichbarer Nutzer.[119]

50 Bei indirekten Netzwerkeffekten erhöht sich hingegen der Wert des Produkts für die eine Marktseite mit der Anzahl der Teilnehmenden auf der anderen

112 Steffen/Wieworra/Kroon, 7; BSK KG-Reinert/Wälchli, Art. 4 Abs. 2 N 202 ff.; Rochet/Tirole, *passim*; Rochet/Tirole, JEEA 2003, *passim*; Rysman, JEP 2009, *passim*.
113 Blatter, sic! 2016, 379; Rochet/Tirole, RJE 2006, 648 f.
114 Rochet/Tirole, RJE 2006, 646.
115 Steffen/Wieworra/Kroon, 7.
116 Schallbruch et al., 15.
117 Steffen/Wieworra/Kroon, 7.
118 Fast/Schnurr/Wohlfarth, 764.
119 Fast/Schnurr/Wohlfarth, 764.

Marktseite.[120] Die Nachfrage nach einem Gut hängt in diesem Fall also von der Bereitstellung eines ergänzenden Gutes ab, das wiederum von der Nachfrage nach dem ursprünglichen Gut abhängt.[121]

Dies trifft für soziale Netzwerke ebenfalls zu, welche für Werbetreibende umso attraktiver sind, je mehr Nutzer sich darauf befinden. Zwar findet auf sozialen Netzwerken eine Interaktion gegen aussen ausschliesslich innerhalb einer einzigen Nutzergruppe (der User) statt, was sie zunächst zu einer einseitigen Plattform macht.[122] Da Plattformen jedoch regelmässig werbebasiert sind, tritt mit den Werbetreibenden eine zweite Nutzergruppe hinzu, welche das soziale Netzwerk zu einer zweiseitigen Plattform macht.[123] 51

Aufgrund dieser Netzwerkeffekte reicht es für neue oder bereits existierende Wettbewerber nicht aus, wenn sie eine bessere Qualität oder bessere Konditionen anbieten.[124] Der Intermediär hingegen kann in einem zweiseitigen Markt regelmässig den Preis von Null festsetzen, um die auf diese Weise gewonnenen Nutzer auf der anderen Marktseite zu monetarisieren.[125] Die Plattform verlangt also von anderen Akteuren ein Entgelt und maximiert dabei ihren Gewinn mit Hilfe von Netzwerk- und Skaleneffekten.[126] 52

3. Plattformisierung

Ein ökonomisches Verständnis legt auch HELMOND ihren Überlegungen zugrunde. Auf sie geht der Begriff der «Plattformisierung» zurück. Darunter versteht sie den Aufstieg der Plattform zum dominanten Infrastruktur- und Wirtschaftsmodell des *Social Web*[127] und die Folgen der Ausweitung von sozialen 53

120 RYSMAN, JEP 2009, 125; BSK KG-REINERT/WÄLCHLI, Art. 4 Abs. 2 N 202.

121 RYSMAN, JEP 2009, 127.

122 SCHALLBRUCH et al., 16.

123 SCHALLBRUCH et al., 16.

124 Monopolkommission, 43.

125 FAST/SCHNURR/WOHLFARTH, 764. Zu nennen sind etwa soziale Netzwerke, die für Nutzerinnen kostenlos sind, aber durch die Schaltung von Werbung finanziert werden.

126 Dieser Preis kann unterschiedlich ausgestaltet sein und etwa aus Transaktionsgebühren oder Registrationsgebühren bestehen, siehe ROCHET/TIROLE, RJE 2006, 647 ff.; ROCHET/TIROLE, JEEA 2003, 994 m.w.N. Das Angebot kann auch für den Enduser kostenlos sein und sich durch Werbeeinblendungen (beim Enduser) finanzieren, so etwa die Musikanbieterin Spotify, siehe BKartA, Plattformen, 27. Für die kostenpflichtige und werbefreie Variante ist in Spotify gemäss BKartA hingegen keine Plattform zu sehen, da es keinen zweiten (oder je nach Sichtweise dritten) Akteur gibt.

127 Das *Social Web* wird auch *Web 2.0* oder heute primär *Social Media* genannt. Darunter verstanden wird die Möglichkeit der Nutzer des *World Wide Web*, aktiv am Web zu partizipie-

Medienplattformen auf andere Online-Räume.[128] Nach ihr geht eine soziale Medien*seite* zu einer sozialen Medien*plattform* über, wenn sie eine oder mehrere Programmierschnittstellen anbietet und damit ein Interface, das die (Re-)Programmierbarkeit der Plattform ermöglicht (sog. APIs).[129] Die API ist dabei nicht eine Datenbank oder ein Server, sondern ein Satz von Befehlen, Funktionen, Protokollen und Objekten, der verwendet werden kann, um eine Software zu erstellen oder mit einem externen System zu interagieren.[130] Sie ermöglicht unterschiedlichen Anwendungen, miteinander zu kommunizieren.[131]

54 Eine Plattform gibt also Teile der Gestaltungsmöglichkeit über ihre Plattform in fremde Hände und ermöglicht damit, dass eine andere Partei als Akteurin die Grundlagen für eine potenziell gewinnbringende Interaktion mit einer dritten Person *auf ihrer Plattform* schafft. Die sozialen Netzwerke als Plattformen bieten dabei das dafür erforderliche infrastrukturelle Modell an, indem sie den technologischen Rahmen bereitstellen, auf dem andere aufbauen können, und der darauf ausgerichtet ist, sich mit anderen Websites, Apps und deren Daten zu verbinden.[132] Damit wird auf das Fundament der Plattform ein weiteres Angebot, gewissermassen als Erweiterung, gebaut.[133]

55 Dies kann sinnvoll sein, etwa wenn offene, im Internet zugängliche Inhalte oder Anwendungen verknüpft werden, um ein neues Angebot zu schaffen (sog. API-Mashup).[134] Denn auf solche Weise können neuartige, innovative Angebote entstehen, was ein Anliegen der frühen Befürworter des Datenportabilitätsrechts und des *Open Web* war.[135] Beispielhaft zu nennen ist die Datingapp Tinder, auf welcher sich User via sozialem Netzwerk einloggen können, sodass dort hinterlegte Daten wie «Likes» oder Angaben über «Freunde» genutzt werden, um potenzielle Partner zu finden.[136] Allerdings kann dieses Vorgehen gerade bei sozia-

ren, Inhalte zu erstellen, teilen und kommentieren und nicht bloss passiv in der Rolle des Konsumenten zu sein, siehe etwa https://perma.cc/A4KW-KY3S.

128 Helmond, SM+S 2015, 5.

129 Helmond, SM+S 2015, 4.

130 BKartA, Sektoruntersuchung, 39.

131 BKartA, Sektoruntersuchung, 39.

132 Helmond, SM+S 2015, 8.

133 Ähnlich auch BKartA, Beschluss B6-22/16 vom 6. Februar 2019, Rz. 227, wonach ein solches Produkt dem sozialen Netzwerk als Aufmerksamkeitsplattform «aufgesetzt» werde.

134 Hommen, 104 ff.; dazu auch Palfrey/Gasser, 116 ff.

135 Dazu Rz. 86 f.

136 Helmond, SM+S 2015, 4. Siehe auch die Datenschutzerklärung von Tinder: «Sie können uns Daten über Ihre Konten auf anderen Plattformen (z.B. Facebook, Instagram, Spotify, Apple) weitergeben, z.B. wenn Sie ein Konto erstellen und sich über diese Plattformen bei Ihrem Konto anmelden oder wenn Sie Daten wie Fotos oder Playlists von diesen Plattformen auf unseren Dienst hochladen.», abrufbar unter: https://perma.cc/8B4G-79NG.

len Netzwerken auch heikel sein, da es die Abhängigkeit von der Plattform drastisch erhöht, wenn der Zugang zum neuen Dienst (stets) via Plattform erfolgt. Entscheidend ist hierbei die konkrete Ausgestaltung: Möglich ist, dass auf diese Weise die Marktmacht einer Plattform konsolidiert wird, während diese in immer neue Bereiche des Webs expandiert. Die Plattform profitiert von einer steigenden Bekanntheit, weil sie prominent bei Drittanbietern angezeigt wird und sich ihr eigener Datenbestand ohne grossen Aufwand vergrössert.[137] Sie erfährt, dass eine Person einen bestimmten Drittanbieter nutzt, kann deren Verhalten beobachten und dieses Wissen u.U. zu eigenen Zwecken verwerten, etwa um zielgerichtete(re) Werbung zu schalten oder eigene Angebote zu lancieren, die aufgrund der Drittdaten besser auf die Bedürfnisse der Kundschaft zugeschnitten sind.[138] Sie kann somit zusätzlich zu ihrem eigenen Angebot mit bereits vorhandenen Inhalten weitere Einnahmen generieren.[139] Die Datenproduktion wird ausgelagert und «dezentralisiert», die Datensammlung hingegen zugunsten der Plattform «zentralisiert».[140] Dazu kommt, dass die Plattform die API-Anbindung jederzeit aussetzen, einstellen oder so abändern kann, dass das Angebot der Dritten nicht länger funktioniert.[141]

Die Plattform kann ein direktes oder indirektes Erlösmodell verfolgen, indem sie die API-Anbindung entweder nur gegen eine Nutzungsgebühr oder durch Einbindung von Werbung zulässt.[142] Darüber hinaus kann die Plattform das durch die API-Anbindung erworbene Wissen nutzen, um ähnliche Angebote oder «Klone» zu erstellen und den bisherigen Anbieter so vom Markt zu verdrängen.[143] 56

137 Kollmann, 11. Siehe beispielhaft das Anmeldefenster eines Schweizer Versandhändlers, bei welchem ein Login mit den Accounts von Google, Facebook und Apple möglich ist, abrufbar unter: https://perma.cc/UA4M-854R.

138 Ähnlich auch Krämer/Schnurr, JCLE 2022, 263 f.; Nicholas, MTLR 2021, 271, der diese Form der Datenübertragung einer Einmalübertragung gegenüberstellt.

139 Kollmann, 10.

140 Helmond, SM+S 2015, 5 m.w.N.

141 Nicholas, MTLR 2021, 282 f.; Nicholas/Weinberg, 19 und 21. Siehe ferner die Plattform-Nutzungsbedingungen von Meta: «Wir können die Verfügbarkeit der Plattform jederzeit ändern, aussetzen oder einstellen. Darüber hinaus können wir ohne Ankündigung oder Haftung bestimmte Funktionen und Dienste beschränken oder deinen Zugriff auf alle unsere APIs oder Websites oder Teile davon einschränken.» (Ziff. 11 lit. e), abrufbar unter: https://developers.facebook.com/terms/.

142 Hommen, 112.

143 Bspw. kreierte Facebook mit LASSO, Slingshot und Bonfire verschiedene Klone von beliebten Angeboten ihrer Konkurrenten, namentlich TikTok, Snapchat und Houseparty, siehe Nicholas/Weinberg, 21. Siehe ferner die Plattform-Nutzungsbedingen von Meta, das sich ausdrücklich vorbehält, «Apps, Produkte, Features oder Dienste [zu entwickeln oder entwickelt zu haben], die deiner App ähnlich sind oder mit deiner App im Wettbewerb stehen.», abrufbar unter: https://developers.facebook.com/terms/.

V. Datenschutz als Rechtsgebiet

57 Das Recht auf Datenportabilität ist eingebettet in das normative Gefüge des Datenschutzrechts. Bereits daraus lassen sich gewisse Tendenzen betreffend die Zielsetzung des Rechtsinstituts ableiten. Daher ist es notwendig, das Rechtsgebiet als Ganzes und dessen Entstehung kurz näher zu betrachten.

A. Anfänge und erste Gesetze

58 Als Ausgangspunkt für den Datenschutz als Rechtsgebiet wird regelmässig auf das Hessische Datenschutzgesetz aus dem Jahr 1970 verwiesen, das als erstes Datenschutzgesetz der Welt gilt.[144] In diese Zeit reihen sich auch akademische Diskussionen rund um «Datenschutz» ein, die vorwiegend aus den USA nach Deutschland und etwas später in die Schweiz getragen und mit den Entwicklungen der automatisierten Datenverarbeitung verbunden wurden.[145] Der Begriff «Datenschutz» wurde damals freilich noch anders verstanden und bezweckte «Unterlagen, Daten und Ergebnisse […] so zu ermitteln, weiterzuleiten und aufzubewahren, daß sie nicht durch Unbefugte eingesehen, verändert, abgerufen oder vernichtet werden können».[146] Im Laufe der Zeit fand jedoch eine Begriffsverschiebung hin zum Persönlichkeitsschutz statt. Das ursprünglich mit «Datenschutz» gemeinte wird heute eher als «Datensicherheit» oder «Datensicherung» bezeichnet.[147] Umgekehrt schützt der Datenschutz heute nicht mehr Daten an sich, sondern die von einer Datenbearbeitung betroffenen Personen und namentlich deren Persönlichkeit und Grundrechte.[148]

59 Ein 1971 vorgelegtes Gutachten im Auftrag des deutschen Bundesministeriums des Innern gab diese Stossrichtung vor und ebnete den Weg für das erste BDSG. Demnach hinterlasse eine Handlung auch nach ihrer zeitlichen Beendigung noch Spuren in der Umwelt, die mit der Persönlichkeitsentfaltung in Be-

---

144 Hess. GVBl. I, 625 ff., abrufbar unter: https://perma.cc/34U4-GKBV; SHK DSG-Husi-Stämpfli, Entstehungsgeschichte N 3; weiterführend HK HDSIG-Rossnagel, Einleitung N 2 ff.

145 KRKomm-Taeger/Schmidt, Einführung N 1; grundlegend dazu etwa Kamlah, *passim*; noch grundlegender bereits 1960, dabei allerdings noch ohne Bezug zur Automatisierung dafür zum Schutz vor staatlicher Ausforschung verstanden als «Privatsphäre» Evers, 7 ff.

146 So der «Inhalt des Datenschutzes» gemäss § 2 des Hessischen Datenschutzgesetzes.

147 von Lewinski, Geschichte, 197 f.

148 Meier, Rz. 326; BSK DSG-Vasella, Einleitung N 1; dazu ferner Rz. 73 ff.

ziehung gebracht werden könnten.[149] Daraus wurde gefolgert, dass die Persönlichkeitsbildung von der Reaktion der Umwelt abhänge.[150] Diese Reaktion setze voraus, dass sie Individualinformationen über den einzelnen besitzt, welche die Art der Reaktion beeinflussen.[151] In der Folge wurde aus dem Recht auf freie Entfaltung der Persönlichkeit nach Art. 2 Abs. 1 GG abgeleitet, dass der Handelnde auch hinsichtlich der Handlungsfolgen durch Art. 2 Abs. 1 GG geschützt werden soll.[152] Zur Freiheit der Entfaltung der Persönlichkeit sei daher das Recht zu zählen, den Umfang, in dem die Umwelt von Denken und Handeln einer Person Kenntnis nehmen soll, selbst zu bestimmen.[153] Das «regelungsbedürftige Problem» bestehe darin, dass in dieses aus Art. 2 Abs. 1 GG abgeleitete Selbstbestimmungsrecht die moderne Informationsverarbeitung mittels Informationssystem massiv eingreifen könne und dadurch das «Informationsgleichgewicht» empfindlich zuungunsten des Staatsbürgers – und ebenso der Gruppierungen – gestärkt werde.[154] Durch die Transparenz der Individualinformation im Informationssystem werde der Verhaltensspielraum des Einzelnen eingeschränkt.[155] Die Folgerung war, dass nur – aber alle – Individualinformationen von Art. 2 GG im Rahmen der Schranken dieses Artikels geschützt sein müssten.[156] Das auf diesen Gedanken aufbauende BDSG trat 1977 in Kraft. Bereits 1973 hatte Schweden ein Datenschutzgesetz geschaffen, Österreich und Frankreich folgten 1978.[157]

B. Deutsches Volkszählungsurteil

Wegweisend für das Datenschutzrecht war das sog. Volkszählungsurteil von 1983. Das deutsche BVerfG anerkannte darin ein Recht auf informationelle Selbstbestimmung als Ausprägung des in Art. 1 und 2 GG verankerten allgemeinen Persönlichkeitsrechts und vor dem Hintergrund der «heutigen und 60

149 Steinmüller et al., 86.
150 Steinmüller et al., 87.
151 Steinmüller et al., 87. Die Autoren sind sich der Lückenhaftigkeit ihres Ansatzes bewusst und erwähnen dies auch explizit.
152 Steinmüller et al., 87. Die Schweiz hat das Konzept einer derart weitgehenden, allgemeinen Handlungsfreiheit nicht übernommen. Namentlich hat das BGer das Grundrecht der persönlichen Freiheit nicht dergestalt erweitert, siehe Belser, Datenschutzrecht, § 6 Rz. 10; siehe auch BGE 102 Ia 321 E. 3.a).
153 Steinmüller et al., 87 m.w.H.
154 Steinmüller et al., 88.
155 Steinmüller et al., 88.
156 Steinmüller et al., 89.
157 SHK DSG-Husi-Stämpfli, Entstehungsgeschichte N 3 m.w.H.

künftigen Bedingungen der automatisierten Datenverarbeitung».[158] Demnach umfasse das Persönlichkeitsrecht «auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden».[159] Ferner: «Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.»[160] Bereits in diesem Urteil – darauf wird zurückzukommen sein – hielt das BVerfG indes ebenfalls fest, dass die Betroffene nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über ihre Daten habe; vielmehr sei sie eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit.[161] Insgesamt nahm das BVerfG aber die Gedanken aus dem Gutachten von Steinmüller et al. auf[162] und mass dem Datenschutz Verfassungsrang bei.[163]

C. (K)ein Recht auf informationelle Selbstbestimmung in der EU

61 Auf europäischer Ebene stützt sich der Datenschutz auf Art. 8 Abs. 1 GRCh und Art. 16 Abs. 1 AEUV.[164] Parallel dazu wendet der EuGH Art. 7 GRCh an.[165] Art. 8 Abs. 2 GRCh gibt zwar einige Aspekte des Grundrechts wieder und konkretisiert dieses dadurch vermeintlich. Es verfällt dabei aber in einen Zirkelschluss, weil lediglich auf gesetzlich vorgesehene Prinzipien verwiesen wird.[166] Auf europäischer Ebene ist der Gehalt des Grundrechts weitgehend unklar und daher seit jeher Anlass für rege Diskussionen. Herangezogen wird in der Literatur oft das Recht auf informationelle Selbstbestimmung nach dem deutschen Verständnis. Auch die Kritik bezieht sich oft auf ein aus dieser informationellen Selbstbestimmung fliessendes eigentumsähnliches Verständnis des Daten-

158 BVerfGE 65, 1, 144 ff.; GG Komm-Durner, Art. 10 N 74.
159 BVerfGE 65, 1, 144.
160 BVerfGE 65, 1, 146.
161 BVerfGE 65, 1, 148.
162 Dazu Rz. 59.
163 BeckOK DSR-Gusy/Eichenhofer, § 1 BDSG N 17.
164 So ausdrücklich Erw.G 1 DSGVO.
165 BeckKompaktKomm-Ernst, Art. 1 DSGVO N 6; AuernhammerKomm-von Lewinski, Art. 1 DSGVO N 5; grundlegend dazu Michl, DuD 2017, *passim*.
166 Thouvenin, digma 2019, 208 f. Verwiesen wird etwa auf das Recht auf Auskunft, den Grundsatz der Zweckbindung und die Einwilligung.

schutzgrundrechts.[167] Eine individuelle Herrschaft über die Daten als geradezu «allein bestimmendes Dogma» wird denn auch von einem Teil der Lehre abgelehnt.[168] Diese Haltung wurde ebenfalls vom BVerfG vertreten, das in seiner 2019 ergangenen Entscheidung *Recht auf Vergessen I* klarstellte, dass das (deutsche) Recht auf informationelle Selbstbestimmung kein «allgemeines oder gar umfassendes Selbstbestimmungsrecht über die Nutzung der eigenen Daten» enthält.[169]

Die Kritik in der Literatur basiert im Wesentlichen auf der Unterscheidung zwischen Daten i.w.S. und Informationen.[170] Dabei wird vorgebracht, dass ein grundrechtlicher Schutz von Daten i.w.S. nicht erforderlich sei. Denn erst die Verwendungskontexte, in denen die Bildung von Informationen erfolgt, führten zu Gefährdungen und «Schutzbedürfnissen» der Einzelnen und erst diese machten einen grundrechtlichen Schutz erforderlich.[171] Ein blosses Herrschaftsrecht an Daten i.w.S. würde demnach sein Ziel verfehlen, da von einem solchen Datum selbst keine Gefährdungen ausgingen.[172] Aber auch ein «Informationsbeherrschungsrecht» verspräche Unmögliches, weil sich die subjektiven Beobachtungen und Sinnkonstruktionen anderer schlicht nicht beherrschen liessen.[173] Folglich wäre eine Herrschaft über Daten i.w.S. selbst nutzlos und umgekehrt die Herrschaft über die Interpretation der Daten (d.h. der Information) unmöglich, weil sich dies nicht kontrollieren lässt.[174] 62

Entsprechend plädieren unterschiedliche Stimmen für eine Differenzierung des grundrechtlichen Schutzes: Nach einer Meinung muss etwa zwischen der grundrechtstheoretischen Konzeption und der rechtstechnischen Konstruktion des Grundrechts streng unterschieden werden.[175] Nach einer anderen Ansicht fallen «Schutzgegenstand» und «Schutzziele» auseinander.[176] Die informationelle Selbstbestimmung sei Schutzgegenstand des Grundrechts, dieses erlange aber seine grundrechtliche Schutzwürdigkeit nicht aus sich selbst, sondern erst mit Blick auf die Gefahren, die von Informationshandlungen für grundrechtlich schon anderweitig gewährleistete Privatheits- und Verhaltens- 63

167 Albers, Rechtstheorie 2002, 81; Cornils, 31.
168 Fix, 49; Marsch, 105 ff.; Wielsch, JZ 2020, 111, der für ein Teilnahmerecht am Kommunikationsprozess plädiert.
169 BVerfGE 152, 152, 87.
170 Grundlegend dazu Albers, 121 ff.; dazu auch Rz. 31.
171 Marsch, 100.
172 Britz, 567; Marsch, 100 f.
173 Britz, 567; Marsch, 100.
174 Britz, 567; Fix, 51.
175 Marsch, 101 f.
176 Cornils, 32 f.

freiheitsinteressen ausgehen könnten.[177] Damit gewährleiste das Recht auf informationelle Selbstbestimmung einen Schutz im Vorfeld anderer Freiheitsrechte und leiste «grundrechtliche Risikovorsorge».[178] Eine andere Autorin sieht im Recht auf informationelle Selbstbestimmung einen konstruierten Schutzgegenstand in Form einer Datenverfügungsbefugnis, der zwar nicht unmittelbar das grundrechtliche Schutzgut abbilde und damit nicht um seiner selbst willen geschützt werde, dessen abwehrrechtlicher Schutz aber einen Mechanismus zur Sicherung des eigentlichen Schutzguts biete.[179]

64 Nach dem Gesagten lässt sich festhalten, dass die europarechtliche Auslegung das nationale, vom deutschen BVerfG geprägte Recht auf informationelle Selbstbestimmung, das aus Art. 2 Abs. 1 GG abgeleitet wird, nicht miteinzubeziehen hat. Es stellt aus europäischer Sicht einen «dogmatischen Sonderweg» dar.[180] Entsprechend weist Fix zurecht darauf hin, dass der Begriff der informationellen Selbstbestimmung in der deutschsprachigen Literatur oft unreflektiert auch für die europäische Ebene verwendet werde, was die Gefahr berge, zu sehr auf den deutschen Massstab zurückzufallen, obwohl dieser namentlich für das Recht auf Datenportabilität nicht relevant sei.[181] Für die vorliegende Untersuchung können diese Ausführungen dennoch beigezogen werden. Denn anders als unter der DSGVO stützt sich das DSG auf einen verfassungsrechtlichen Datenschutz, der, wie sogleich gezeigt wird, das (deutsche) Recht auf informationelle Selbstbestimmung rezipiert hat, und sich am «herrschaftsrechtlichen» Verständnis zu orientieren scheint. Gleichwohl ist punktuell auf die genannte Kritik aus der deutschen Literatur einzugehen.

177 Cornils, 32 f. m.H.a. BVerfGE 113, 29, 46.

178 Cornils, 33; ähnlich auch für die Schweiz aber mit Blick auf die Rechtslage in der EU Thouvenin, digma 2019, 209; dazu weitergehend Rz. 76.

179 Britz, 582.

180 Fix, 40, insb. Fn. 68; darauf hinweisend, dass es beim Grundrechtsschutz nach Art. 8 GRCh nicht darum gehe, dem Individuum volle Kontrolle zu geben, sondern darum, sicherzustellen, dass die Daten in einer angemessenen Weise verarbeitet werden («in a fair manner») GDPR-Comm-Hijmans, Art. 1, 52; AuernhammerKomm-von Lewinski, Art. 1 DSGVO N 5; von Lewinski, Matrix, 44; a.A. jedoch NomosKomm-Klement, Art. 8 DSGVO N 6 m.w.N., der von Art. 8 GRCh auch die Möglichkeit geschützt sieht, seine eigenen Daten selbstbestimmt zur Verarbeitung freizugeben und darin eine Aufwertung zu einem Grundrecht auf informationelle Selbstbestimmung sieht.

181 Fix, 40, insb. Fn. 68.

D. Entwicklung in der Schweiz

1. Erstes Datenschutzgesetz (DSG)

In der Schweiz reichte Nationalrat BUSSEY 1971 die Motion «Gesetzgebung über Computer» ein. Die Speicher der Computer ermöglichten, so BUSSEY, die Schaffung von eigentlichen Datenbanken, die viele bisher verstreut vorhandene Auskünfte über Personen oder Unternehmen zusammenfassten.[182] Der Bundesrat wurde ersucht, eine Gesetzgebung zu prüfen, die den Bürger und seine Privatsphäre gegen die missbräuchliche Verwendung von Computern schützen und eine «normale» Entwicklung der Verwendung von Computern ermöglichen könnte.[183] BUSSEY spezifizierte dabei, dass die dahinterliegenden Fragen nicht ausschliesslich den Computer beträfen, sondern weitgreifender seien.[184] Seine Motion wurde schliesslich als Postulat überwiesen, blieb jedoch zunächst folgenlos.[185] 65

Zwei durch Nationalrat GERWIG eingereichte parlamentarische Initiativen forderten 1977 eine Verankerung des Persönlichkeits- und des Datenschutzes in der Verfassung resp. in einem Gesetz.[186] Der zuständige Bundesrat FURGLER betraute 1977 und 1979 zwei Arbeitsgruppen, die für die Bundesverwaltung und für den Privatbereich Datenschutzvorschriften ausarbeiten sollten.[187] 66

Schliesslich wurden den eidgenössischen Räten am 23. März 1988 eine Botschaft und ein Entwurf zum Bundesgesetz über den Datenschutz unterbreitet.[188] Der Bundesrat begründete die Notwendigkeit des neuen Gesetzes in der Schweiz mit dem Einsatz von modernen Informations- und Kommunikationstechnologien und der enormen Intensivierung der Datenverarbeitung und -verbreitung in der Gesellschaft, in der Wirtschaft und im Staat.[189] Diese hätten die Risiken von Persönlichkeitsverletzungen stark anwachsen lassen.[190] Da das bestehende Recht keinen wirksamen Schutz für die betroffenen Personen geboten hatte, sollte die Lücke mit dem aDSG geschlossen werden.[191] Die Räte 67

182 Motion Bussey 10 898.
183 Motion Bussey 10 898.
184 Motion Bussey 10 898.
185 Motion Bussey 10 898.
186 Pa.Iv. Gerwig 77.223; Pa.Iv. Gerwig 77.224.
187 Botschaft DSG 1988, 426 f.
188 Botschaft DSG 1988, 413 ff.
189 Botschaft DSG 1988, 414.
190 Botschaft DSG 1988, 414.
191 Botschaft DSG 1988, 414.

verabschiedeten das Gesetz am 19. Juni 1992; es trat am 1. Juli 1993 in Kraft. Bis zur Totalrevision wurde es anschliessend mehrfach teilrevidiert. Zudem wurde 1997 das bereits 1981 verabschiedete Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten des Europarats (sog. Konvention 108) durch die Schweiz unterzeichnet und ratifiziert. Es trat in der Schweiz 1998 in Kraft.[192]

2. Verfassungsrechtlicher Datenschutz

a. Grundlagen

68 Der verfassungsrechtliche Datenschutz stützte sich unter dem aDSG zunächst auf das ungeschriebene Grundrecht der persönlichen Freiheit und auf Art. 8 EMRK.[193] Von Bedeutung war darüber hinaus der allgemeine Gleichheitssatz nach Art. 4 aBV, der den Betroffenen eine Beteiligung an einer Datenbearbeitung garantierte.[194] Das BGer übernahm in seiner Rechtsprechung den grundrechtlichen Datenschutz und später die Terminologie des «Rechts auf informationelle Selbstbestimmung» für die Schweizer Rechtsordnung und verwies dabei auf das BVerfG.[195]

69 Mit der Totalrevision der BV wurde ein grundrechtlicher «Anspruch auf Datenschutz»[196] in Art. 13 Abs. 2 BV verankert. Die Bestimmung stellt einen Teilgehalt des «Schutzes der Privatsphäre» nach Art. 13 BV dar.[197] Das BGer stützt sich nunmehr in seiner Rechtsprechung auf die Art. 13 BV und Art. 8 EMRK.[198] Aus der Rechtsprechung des EGMR lässt sich ein Recht auf informationelle Selbstbestimmung jedoch bislang nicht explizit ableiten.[199]

---

192 Seither wurde das Übereinkommen als sog. Konvention 108+ modernisiert und von der Schweiz ratifiziert, siehe EDÖB, Medienmitteilung vom 8. September 2023. Das Inkrafttreten der Konvention 108+ steht allerdings noch aus.

193 Botschaft DSG 1988, 419.

194 Müller/Schefer, 164; Botschaft DSG 1988, 419.

195 Siehe zur Herleitung Thouvenin, ZSR Beiheft 2023, 7 ff. m.H.a. BGE 113 Ia 1 E. 4.b)bb), jedoch erst sinngemäss bezugnehmend auf die informationelle Selbstbestimmung; BGE 120 II 118 E. 3.; BGE 122 I 153 E. 6.b)aa).

196 Botschaft BV, 153; siehe dazu OFK BV-Biaggini, Art. 13 N 11.

197 Belser, Rechtliche Tragweite, 32.

198 Statt vieler BGE 147 I 103 E. 15.1; zum völkerrechtlichen Schutz SGK BV-Schweizer/Striegel, Art. 13 N 77; darauf hinweisend, dass die Verfassung die Rechtsprechung des BGer übernommen habe und nicht umgekehrt Müller/Schefer, 164.

199 AuernhammerKomm-von Lewinski, Art. 1 DSGVO N 5; Gächter/Egli, Jusletter 2010, Rz. 59; George, Prinzipien, 60 m.w.N.

Daneben kann durch Datenbearbeitungen ein Eingriff in die persönliche Freiheit nach Art. 10 Abs. 2 BV vorliegen.[200] Da Art. 10 BV jedoch als Auffanggrundrecht[201] konzipiert ist, kommt ihm seit der eigenständigen Erwähnung des Datenschutzes in der BV weniger Bedeutung zu.[202] 70

Nach ständiger Rechtsprechung des BGer, die erst unter der neuen BV etabliert wurde, bedeutet das Recht auf informationelle Selbstbestimmung, dass «grundsätzlich ohne Rücksicht darauf, wie sensibel die fraglichen Informationen tatsächlich sind, jede Person gegenüber fremder, staatlicher oder privater Bearbeitung von sie betreffenden Informationen bestimmen können muss, ob und zu welchem Zweck diese Informationen über sie bearbeitet werden».[203] In einem anderen Entscheid hielt das BGer fest, «dass grundsätzlich ohne Rücksicht darauf, wie sensibel die fraglichen Informationen tatsächlich sind, dem Einzelnen die Herrschaft über seine personenbezogenen Daten zusteht».[204] Damit schützt das Recht entgegen des (engen) Wortlauts von Art. 13 Abs. 2 BV vor jeglicher Art der Datenbearbeitung und nicht bloss vor Missbrauch der Daten.[205] Gemäss BGer schützt Art. 13 BV «in besonderer Weise die verschiedene Aspekte umfassende Privatsphäre mit ihren spezifischen Bedrohungsformen», wozu der Schutz vor Beeinträchtigungen, die durch die staatliche Bearbeitung von persönlichen Daten entstehen, gehört.[206] 71

Dem Staat obliegt zudem die Pflicht, bei privaten Datenbearbeitungen für einen Schutz des Rechts auf informationelle Selbstbestimmung zu sorgen und Regelungen zu erlassen, welche dieses Recht auch zwischen Privaten durchsetzen.[207] Gerade diese Pflicht hat angesichts der technologischen Entwicklungen an Bedeutung gewonnen.[208] Auch der Bundesrat bekräftigt konsistent, dass ein solches Grundrecht auf informationelle Selbstbestimmung exis- 72

200 Belser, Rechtliche Tragweite, 30; siehe auch das BGer in BGE 140 I 2 E. 9.1.

201 BSK BV-Tschentscher, Art. 10 N 4.

202 Belser, Rechtliche Tragweite, 30; BSK BV-Diggelmann, Art. 13 N 10 m.H.a. BGE 133 I 77 E. 3.2, nach welchem eine Beschwerde bei einem spezifischen Bezug zum Schutz vor Missbrauch persönlicher Daten (*in casu* die Aufbewahrungsdauer von Videoaufnahmen) in erster Linie unter dem Gesichtswinkel von Art. 13 Abs. 2 BV zu prüfen ist.

203 Statt vieler BGE 147 I 103 E. 15.1; ebenso SGK BV-Schweizer/Striegel, Art. 13 N 79.

204 BGE 138 II 346 E. 8.2; dieses weitgehende Verständnis der informationellen Selbstbestimmung scheint das BGer allerdings wieder aufgegeben zu haben, siehe Thouvenin, ZSR Beiheft 2023, 11.

205 Belser, Datenschutzrecht, § 6 Rz. 86; SGK BV-Schweizer/Striegel, Art. 13 N 79 und 85.

206 BGE 138 I 331 E. 5.1.

207 SGK BV-Schweizer/Striegel, Art. 13 N 115.

208 SGK BV-Schweizer/Striegel, Art. 13 N 80.

tiert.[209] Mit dem Recht auf Datenportabilität wird der betroffenen Person eine Verfügungsbefugnis zuteil, die auf den ersten Blick eng mit der Idee der informationellen Selbstbestimmung verknüpft ist. Daher ist nachfolgend kurz auf den (unklaren) Gehalt der informationellen Selbstbestimmung einzugehen.

b. Unklarer Gehalt der informationellen Selbstbestimmung

73 Der genaue Gehalt des Grundrechts bzw. dessen Schutzzweck ist umstritten.[210] Vertreten wird, dass hinter dem Recht auf informationelle Selbstbestimmung der Gedanke stecke, dass eine Einzelne sich in der Gesellschaft nur dann selbstbestimmt bewegen kann, wenn sie abzuschätzen vermag, welche persönlichen Informationen ihren Mitmenschen über sie bekannt sind.[211] Mithin solle eine Entscheidungsfreiheit bezüglich der eigenen Daten und Informationen als essentielle Voraussetzung für die Entwicklung selbstbestimmter Individuen gewährleistet werden.[212]

74 Postuliert wird mit Blick auf die bundesgerichtliche Rechtsprechung, dass die informationelle Selbstbestimmung den Datenschutz in Richtung Autonomie des Menschen erweitere und sich damit – entgegen der Marginalie von Art. 13 BV – von der deutlich eingeschränkter wirkenden Sphärentheorie entferne.[213] Andere Autoren verstehen den Schutzzweck des Grundrechts hingegen ausdrücklich informationsorientiert und nicht verhaltensbezogen.[214] Die informationelle Selbstbestimmung solle vor allumfassender, unbegrenzter und intransparenter Daten- und Informationsbearbeitung schützen.[215] Schutzobjekt seien damit die Personendaten als solche und nicht die Privatsphäre.[216] Daraus

209 Botschaft DSG 2017, 7010; implizit aber bereits auf das Urteil des BVerfG hinweisend Botschaft DSG 1988, 418.

210 Dies beginnt bereits mit der uneinheitlichen Terminologie, deren Verwendung kaum je präziser erläutert wird. Etwa von «Schutzzweck», aber auch von «Gehalt» und «Schutzziel» sprechend Glass, 157; von «Schutzzweck» sprechend Gächter/Egli, Jusletter 2010, Rz. 25 ff.; Gächter/Werder, 90; Waldmeier, 32 f.; Müller/Schefer, 164; von «Gehalt», dann aber verweisend auch von «Schutzzielen» sprechend SGK BV-Schweizer/Striegel, Art. 13 N 99; von «Schutzgehalt» sprechend BSK DSG-Vasella, Einleitung N 3.

211 Müller/Schefer, 165; Waldmeier, 32.

212 Waldmeier, 33; insoweit davon sprechend, dass nicht die Verfügungsmacht über Daten um ihrer selbst willen, sondern zur Sicherung der Verwirklichung von Freiheit bezweckt wird Glass, 156.

213 Rudin, 421. Die Sphärentheorie unterteilt den durch das Persönlichkeitsrecht zu schützenden Bereich in drei Sphären: Die Geheim- oder Intim-, die Privat- und die Gemeinsphäre, siehe dazu grundlegend Aebi-Müller, 247 ff.

214 Gächter/Egli, Jusletter 2010, Rz. 25.

215 Gächter/Egli, Jusletter 2010, Rz. 25 m.w.N.

216 Gächter/Egli, Jusletter 2010, Rz. 32.

folgern sie, dass Art. 13 Abs. 2 BV nicht nur die Privat- oder Geheimsphäre schütze, sondern auch die persönliche Freiheit, die Autonomie und Würde des Menschen, die durch eine unbegrenzte Datenbearbeitung in grundlegender Weise bedroht seien und daher als strukturelle Garantie durch den Gesetzgeber zu schützen seien.[217]

Nach einer weiteren Ansicht soll das Grundrecht nicht Daten, sondern die durch sie transportierten Informationen schützen.[218] Entsprechend sei der Schutzzweck der mit dem Recht der Betroffenen eingeräumten Verfügungsmacht darin zu sehen, grundsätzlich über die Wirkungsreichweite von persönlichen Informationen zu bestimmen.[219] Zusätzlich zur Sicherstellung der Autonomie des Einzelnen (in Form einer Entfaltung der Persönlichkeit und der Ausübung von Rechten) habe sie auch eine freiheitssichernde Funktion: Nur die informationelle Selbstbestimmung berechtige ein Individuum grundsätzlich im Rahmen der Rechtsordnung über die Verbreitung der Daten mit eigenem Personenbezug bzw. über die Wirkungsreichweite der darin codierten, personenbezogenen Informationen zu verfügen.[220] 75

c. Andere Ansätze

Für zunehmende Uneinigkeit sorgt in der Literatur aber auch ein anderer Gesichtspunkt. Aufgrund der technologischen Entwicklungen und immer umfangreicherer Datenbearbeitungen (Big Data) wird das Konzept einer informationellen Selbstbestimmung als Basis für das Datenschutzrecht und dessen Tragfähigkeit als Grundrecht teilweise grundlegend angezweifelt.[221] Bereits 1999 wurde vorgebracht, dass es sich um ein «letztlich schillerndes Wortgebilde mit unklarem Inhalt» handle.[222] Auch in jüngerer Zeit wird vertreten, dass das informationelle Selbstbestimmungsrecht in seiner modernen Bedeutung durch den Verfassungsgeber bislang weder sinnvoll ausformuliert noch positiviert worden sei, obwohl sich dessen Konzeption jüngst stark verändert habe.[223] Der Schutz- 76

217 Gächter/Egli, Jusletter 2010, Rz. 37 ff.

218 Glass, 157.

219 Glass, 157.

220 Glass, 178.

221 Belser, Rechtliche Tragweite, 26 f.; Belser, Datenschutzrecht, § 6 Rz. 117 ff.; Braun Binder et al., Jusletter 2021, Rz. 17 m.w.N.; Thouvenin, ZSR Beiheft 2023, *passim*; Thouvenin, JIPITEC 2021, *passim*.

222 Weber, ZSR 1999, 74.

223 SGK BV-Schweizer/Striegel, Art. 13 N 96; angesichts der rasanten Entwicklung der Lebensformen und der Risiken für eine teleologische Auslegung und gegen eine Anpassung der Verfassungsbestimmungen plädierend hingegen Gonin, Rz. 2092.

gehalt des Grundrechts sei wenig übersichtlich und noch immer konturlos.[224] Zudem kenne die Schweiz, anders als Deutschland, keine allgemeine Handlungsfreiheit, die sich aus dem Recht auf persönliche Freiheit ableite, weshalb es verfehlt sei, ein solches umfassendes Selbstbestimmungsrecht in das Schweizer Recht einzuführen.[225] Angezweifelt wird ferner, ob dem Grundrecht überhaupt ein eigener Gehalt zuzumessen sei, oder ob dieses nicht dem Schutz vieler anderer Rechte und Interessen diene.[226] Dies könnte die informationelle Selbstbestimmung zu einem «Grundrecht mit Vorfeldcharakter» machen, dem lediglich eine dienende Funktion beim Schutz anderer Grundrechte zukommt.[227]

77 Angesichts dieser Unsicherheiten werden in der Literatur verschiedene Lösungsansätze diskutiert. So wurde vorgeschlagen, das Konzept der Selbstbestimmung durch eine Informationszuordnung abzulösen: Eine Information gehöre ihrer Inhaberin, wenn und soweit sie sich auf ihre Person beziehe.[228] Aus diesem Grund sei es sachgerecht, das Datenschutzrecht vom Persönlichkeitsrecht zu lösen und neue Schutzmodelle zu entwickeln, welche insb. an den Aspekten der Partizipation und der Regulierungsnotwendigkeit anknüpften.[229] Weiter wurde darauf hingewiesen, dass künftig vor allem die erleichterte Kombination an sich belangloser Daten durch effiziente Suchprogramme ein Problembereich darstellen dürfte.[230] Einige Zeit später wurde Kritik laut, dass angesichts der technologischen Entwicklung und der damit einhergehenden Veränderungen der Datenverarbeitung schlechthin die traditionellen datenschutzrechtlichen bzw. allgemeinen legislativen Massnahmen eine informationelle Selbstbestimmung nicht mehr gewährleisten könnten.[231] Daraus ergebe sich die Notwendigkeit eines «Selbstdatenschutzes», der sowohl die Anbieterinnen als auch die Nutzerinnen betreffe. Dieser ziele «ganz im Sinne des informationellen Selbstbestimmungsrechts» darauf ab, dass die Nutzerin beein-

224 Aebi-Müller, 288; OFK BV-Biaggini, Art. 13 N 13; Belser, Rechtliche Tragweite, 28; ausführlich dazu, i.E. jedoch wohl a.A. Waldmeier, 45 ff.; ähnlich auch für das deutsche Recht von einer begrifflichen Unschärfe von «Datenschutz» sprechend von Lewinski, Matrix, 17 ff., der entsprechend Mühe mit der Verortung des eigentlichen Zwecks des Datenschutzes hat.

225 Gächter/Egli, Jusletter 2010, Rz. 24 m.w.N.; Waldmeier, 44. In der Schweiz sind nach bundesgerichtlicher Rechtsprechung nur all jene Freiheiten erfasst, die elementare Erscheinungen der Persönlichkeitsentfaltung darstellen und ein Mindestmass an persönlicher Entfaltungsmöglichkeit erlauben, siehe dazu BGE 127 I 6 E. 5.a).

226 Diese Frage aufwerfend Thouvenin, digma 2019, 209 m.H.a. Marsch, 87.

227 So Thouvenin, digma 2019, 209.

228 Weber, ZSR 1999, 74.

229 Weber, ZSR 1999, 75 m.w.N.

230 Weber, ZSR 1999, 76.

231 Garstka, 169.

flussen kann, welche Daten über sie bearbeitet werden und auf welche Art und Weise.[232] Dies bedeute, dass die informationelle Selbstbestimmung dann am weitestgehenden verwirklicht sei, wenn die Entscheidung zur Offenbarung von Daten und der Bestimmung, wie sie verarbeitet werden sollen, von der Betroffenen selbst stamme.[233] Darauf bezugnehmend wurde auch postuliert, dass das Recht auf informationelle Selbstbestimmung als Schutz der Entscheidungsfreiheit der einzelnen Person in Bezug auf die Verwendung ihrer Daten zu verstehen sei.[234]

Andere Autoren möchten hingegen Art. 13 Abs. 2 BV nicht als subjektiv-rechtlich geprägtes Recht auf informationelle Selbstbestimmung verstehen, sondern als strukturelle Garantie, die sich primär an den Gesetzgeber richtet und dafür zu sorgen hat, dass der Umgang mit Personendaten nicht ungebunden, unbegrenzt, undurchschaubar und an den Betroffenen vorbei laufe.[235] Dabei besitze der Staat viel Umsetzungsfreiheit, da sich eine «richtige» Ordnung staatlicher Datenflüsse nicht aus Art. 13 Abs. 2 BV ableiten lasse.[236] Darüber hinaus lasse sich aus einem strukturellen Verständnis von Art. 13 Abs. 2 BV ein gesetzlicher Handlungsauftrag an den Staat ableiten, wodurch dieser verpflichtet werde, für einen effektiven Datenschutz, auch und insb. zwischen Privaten, zu sorgen.[237] 78

Eine jüngere Lehrmeinung hebt die «rasanten Fortschritte im Bereich der Informations- und Kommunikationstechnologien» hervor und sieht im verfassungsrechtlichen Datenschutz ein «Schlüsselgrundrecht der digitalen Revolution».[238] Ihrer Ansicht nach impliziert das Recht auf informationelle Selbstbestimmung nicht nur Abwehrrechte gegen den behördlichen und privaten Umgang mit Personendaten, sondern auch Gewährleistungs- und teilweise Leistungsansprüche.[239] Durch den grenzüberschreitenden Informationsfluss und die Dezentralisierung der Datenbearbeitung gewinne die Pflicht des Staates, einen wirksamen 79

232 Garstka, 169.
233 Garstka, 170.
234 Waldmeier, 35.
235 Gächter/Werder, 93; siehe das insoweit vertiefende Gutachten, nach welchem die staatliche Daten- und Informationsbearbeitung unter den Bedingungen moderner Informations- und Kommunikationstechnologien als solche einen eigenständigen Schutzbedarf begründet, Gächter/Egli, Jusletter 2010, Rz. 78. Eine Einschränkung nur auf staatliche Bearbeitungen erscheint nicht sachgemäss, was aber dem untersuchten Themengebiet geschuldet sein dürfte.
236 Gächter/Werder, 93.
237 Gächter/Werder, 106.
238 SGK BV-Schweizer/Striegel, Art. 13 N 80.
239 SGK BV-Schweizer/Striegel, Art. 13 N 80.

Schutz personenbezogener Daten gegenüber Drittpersonen zu gewährleisten, enorm an Bedeutung.[240]

80 Schliesslich wird das Recht auf informationelle Selbstbestimmung in der Lehre fundamental kritisiert und eine grundlegende Neuausrichtung vorgeschlagen. Dabei wird daran angeknüpft, dass das BVerfG mit dem Entscheid *Recht auf Vergessen I*[241] die Bedeutung eines Rechts auf informationelle Selbstbestimmung stark relativiert habe, und es wird festgestellt, dass der Begriff den Gehalt nicht mehr spiegle.[242] Das BGer habe diese Einschränkung aber bislang nicht übernommen und auch sonst nicht begründet, was unter einer (weitgehenden) informationellen Selbstbestimmung im Sinne der höchstrichterlich verwendeten Textbausteine zu verstehen sei.[243] Tatsächlich existiere für die Bearbeitung von Personendaten durch Bundesorgane kein Recht auf informationelle Selbstbestimmung, da keine Konstellationen existierten, in welchen Bundesorgane Daten bearbeiten dürften und die Betroffenen zugleich über die Bearbeitung der sie betreffenden Daten bestimmen könnten.[244] Für Datenbearbeitungen durch Private könne zwar der Rechtfertigungsgrund der Einwilligung als Ausgestaltung der informationellen Selbstbestimmung herangezogen werden.[245] Die Bedeutung der Einwilligung sei indes gering, ganz im Gegensatz zum Vorliegen eines überwiegenden Interesses, welches eine Datenbearbeitung ebenfalls – auch entgegen dem Willen der Betroffenen – rechtfertigen kann.[246] Da der Einwilligung und einem möglichen Widerspruchsrecht (siehe Art. 30 Abs. 2 lit. b DSG) aber im Gegensatz zum Vorliegen eines überwiegenden Interesses nur eine untergeordnete Rolle zukomme, lasse sich das private Datenschutzrecht nur punktuell, aber nicht insgesamt auf das Konzept einer informationellen Selbstbestimmung stützen.[247] Für ein «herrschaftsrechtliches» Verständnis des Rechts auf informationelle Selbstbestimmung ist damit nach dieser Ansicht kein Platz.[248]

81 Lediglich in den Betroffenenrechten sieht der Autor demnach erweiterte Mitbestimmungsrechte der betroffenen Personen. Diese würden zwar noch kein

240 SGK BV-Schweizer/Striegel, Art. 13 N 80.
241 BVerfGE 152, 152, 1 ff.; dazu auch Rz. 61.
242 Thouvenin, ZSR Beiheft 2023, 12 f.
243 Thouvenin, ZSR Beiheft 2023, 14.
244 Thouvenin, ZSR Beiheft 2023, 18. Dies liegt an der für eine Datenbearbeitung durch Bundesorgane notwendigen gesetzlichen Grundlage, die Bundesorgane ermächtigt, aber auch verpflichtet, Daten zu bearbeiten (Art. 34 DSG).
245 Thouvenin, ZSR Beiheft 2023, 19.
246 Thouvenin, ZSR Beiheft 2023, 19.
247 Thouvenin, ZSR Beiheft 2023, 22.
248 Thouvenin, ZSR Beiheft 2023, 33 f.

Recht auf informationelle Selbstbestimmung darstellen, doch immerhin würden die Betroffenen durch diese zu Akteurinnen und Kontrolleurinnen der Bearbeitung der sie betreffenden Personendaten.[249] Zudem hätten Personendaten einen wirtschaftlichen Wert und die Betroffenen sollten am Wert der sie betreffenden Daten partizipieren können.[250] Entsprechend solle die Rechtsordnung Ansprüche vorsehen, die es ihnen ermöglichten, eine Kopie der Daten zu erhalten und sie selbst zu nutzen oder weiterzugeben.[251] Genannt wird hierbei ausdrücklich das Portabilitätsrecht.[252] Daraus wird gefolgert, dass anstatt eines herrschaftsrechtlich verstandenen Rechts auf informationelle Selbstbestimmung das Augenmerk auf den Schutz der Privatsphäre zu richten sei, wofür jedoch weitere Forschung erforderlich sei.[253]

Eine weitere Autorin plädiert – mit Fokus auf das Gesundheitswesen – für ein verändertes Grundrechtsverständnis. Angesichts der technologischen Entwicklungen genüge eine abwehrrechtliche Funktion der Grundrechte nicht mehr, um sämtliche Grundrechtsbeeinträchtigungen abzudecken.[254] Vielmehr seien horizontale Rechtsbeziehungen zwischen Privaten und daraus folgend eine staatliche Schutzpflicht gegenüber privaten Datenschutzgefährdungen zunehmend wichtig.[255] Grundrechte seien als «Sicherungsgarantien der technischen Funktionsbedingungen digitaler Netzwerke» zu betrachten.[256] Daraus wird u.a. gefolgert, dass ein Recht auf eine elektronische Kopie notwendig sei, um die Daten «persönlich zu kontrollieren und auf Wunsch einer Sekundärnutzung zuzuführen».[257] Damit fordert die Autorin im Wesentlichen ein Recht auf Datenportabilität. 82

Zusammenfassend zeigt sich, dass unterschiedliche Auffassungen existieren, was mit einem informationellen Selbstbestimmungsrecht gemeint ist. Einige 83

249 Thouvenin, ZSR Beiheft 2023, 27; siehe auch BSK DSG-Vasella, Einleitung N 10, der in den Betroffenenrechte die Verwirklichung der informationellen Selbstbestimmung «im eigentlichen Sinne» sieht, d.h. die eigenverantwortliche Mitwirkung der Betroffenen bei der Gestaltung und Durchsetzung des Datenschutzes. Ihr werde ein «Instrument zur fakultativen weiteren Durchsetzung des Datenschutzes in die Hand» gegeben und gleichzeitig eine Selbstverantwortung auferlegt.

250 Thouvenin, ZSR Beiheft 2023, 45.

251 Thouvenin, ZSR Beiheft 2023, 45.

252 Thouvenin, ZSR Beiheft 2023, 45.

253 Thouvenin, ZSR Beiheft 2023, 43 ff.

254 Sprecher, ZBJV 2018, Teil 2, 541.

255 Sprecher, ZBJV 2018, Teil 2, 541.

256 Sprecher, ZBJV 2018, Teil 2, 542 m.H.a. Weber, Synchronisierung, 58; Weber, Grundrechtskonzeptionen, 28.

257 Sprecher, ZBJV 2018, Teil 2, 542 f.; ähnlich Brauchbar, Bioethica Forum 2015, 55.

Stimmen votieren für eine grundlegende Neukonzeption, andere möchten das Grundrecht ganz aufgeben. Die unklare Rechtslage wirkt sich auf diese Untersuchung aus, die die Zielsetzung des Portabilitätsrechts ergründet. Darauf ist zurückzukommen.[258]

3. Revision des DSG

84 Anfang der 2010er-Jahre zeigte sich Revisionsbedarf beim DSG. Es galt als anerkannt, dass dieses in die Jahre gekommen war und aufgrund der technologischen und gesellschaftlichen Entwicklung zahlreiche Schwächen aufwies.[259] Nachdem eine Evaluation durchgeführt wurde und zahlreiche Arbeits- und Begleitgruppen sich damit befasst hatten, wurde am 21. Dezember 2016 der Vorentwurf zur Totalrevision des aDSG in die Vernehmlassung geschickt.[260] Nach deren Auswertung verabschiedete der Bundesrat am 15. September 2017 den Entwurf zu einer Totalrevision des DSG. Mit der Revision sollte das schweizerische Recht an die rasante technologische Entwicklung angepasst werden.[261] Zudem sollten die Eigenverantwortung der Verantwortlichen gefördert, ein früheres Greifen des Datenschutzes ermöglicht, und die Datenkontrolle und -herrschaft der Betroffenen verbessert werden.[262] Ferner sollte die Wettbewerbsfähigkeit der Schweiz erhalten und gestärkt werden, indem ein günstiges Umfeld geschaffen wird, mit dem der grenzüberschreitende Datenverkehr erleichtert und die Attraktivität der Schweiz für neue Aktivitäten im Zusammenhang mit der digitalen Gesellschaft gesteigert werden können.[263] Die Revision strebte auch einen Angemessenheitsbeschluss der EU-Kommission an, wodurch Datentransfers aus der EU und dem EWR ohne Nachweis weiterer Garantien zulässig sind (siehe Art. 45 DSGVO).[264] Die Räte verabschiedeten das DSG in der Schlussabstimmung am 25. September 2020;[265] es trat gemeinsam mit der zwischenzeitlich ausgearbeiteten DSV am 1. September 2023 in Kraft.

258 Dazu Rz. 270.

259 Botschaft DSG 2017, 6954; BJ, Erläuternder Bericht VE-DSG, 8; siehe bereits Bolliger et al., 225 sowie 220, wo ein Recht auf Datenportabilität anklingt.

260 BJ, Erläuternder Bericht VE-DSG, *passim*.

261 Botschaft DSG 2017, 6969.

262 Bundesrat, Bericht Evaluation DSG, 350; Botschaft DSG 2017, 6969.

263 Botschaft DSG 2017, 6969.

264 Botschaft DSG 2017, 6965 und 6998.

265 Siehe AB 2020 N 1954; AB 2020 S 1069.

4. Zweck des DSG

Laut Bundesrat soll das revidierte DSG das Recht auf informationelle Selbstbestimmung auf Gesetzesebene konkretisieren.[266] Das Gesetz nimmt diese Begrifflichkeit jedoch nicht ausdrücklich auf. Nach seinem Zweckartikel dient es dem Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Personendaten bearbeitet werden (Art. 1 DSG; im Wesentlichen deckungsgleich bereits Art. 1 aDSG). Damit wird die duale Geltung des DSG für Private und Bundesbehörden angetönt: Mit dem Hinweis auf die Persönlichkeit wird an den zivilrechtlichen Schutz nach Art. 28 ZGB angeknüpft und mit dem Hinweis auf den Grundrechtsschutz im Grundsatz auf den öffentlichrechtlichen Bereich hingewiesen.[267] Dieser Schutz der Grundrechte meint u.a. – aber nicht nur – Art. 13 BV.[268] Die Pluralform stellt jedoch klar, dass das DSG auch den Schutz vor anderen Grundrechtsverletzungen durch Datenbearbeitungen bezweckt, etwa den Schutz der persönlichen Freiheit (Art. 10 BV), der Achtung des Privat- und Familienlebens, der Wohnung sowie des Brief-, Post- und Fernmeldeverkehrs bzw. der Korrespondenz (Art. 13 Abs. 1 BV und Art. 8 EMRK).[269] Im Ergebnis verweist allerdings der Hinweis auf die Persönlichkeit ebenfalls auf die Grundrechte, stellt doch der privatrechtliche Persönlichkeitsschutz letztlich eine Konkretisierung ebendieser dar.[270] 85

266 Botschaft DSG 2017, 7010; Müller/Schefer, 174; OK DSG-Husi-Stämpfli, Art. 1 N 1, zudem den grundrechtlichen Persönlichkeitsschutz nach Art. 10 BV hervorhebend.

267 OFK DSG-Epiney/Zlatescu, Art. 1 N 14.

268 OK DSG-Husi-Stämpfli, Art. 1 N 9; OFK DSG-Epiney/Zlatescu, Art. 1 N 14.

269 BSK DSG-Schönbächler/Maurer-Lambrou/Kunz, Art. 1 N 6.

270 OFK DSG-Epiney/Zlatescu, Art. 1 N 15.

§ 2 Grundlagen

I. Chronologie des Rechts auf Datenportabilität

A. Ursprünge in der US-amerikanischen IT-Szene

86 Üblicherweise wird das Recht auf Datenportabilität der EU-Kommission zugeschrieben. In der Literatur wird jedoch darauf hingewiesen, dass deren Interesse am Portabilitätsrecht auf eine Debatte in der US-amerikanischen IT-Szene zurückzuführen sein könnte, die einige Jahre zuvor eingesetzt hatte.[271] So wurde bereits 2007 eine *Bill of Rights for the Social Web* vorgestellt, die den Usern mehr Rechte einräumen sollte, u.a. ein Recht auf Datenportabilität.[272] Dem liegt die Idee zugrunde, dass das Internet[273] ein offener, jeder Person zugänglicher Ort sein sollte, der gerade durch die freie Verknüpfbarkeit und die Möglichkeit, sich darin frei zu entfalten, so innovativ sei.[274]

87 Als Vordenker dieses Ansatzes gilt Tim Berners-Lee, der Erfinder des *World Wide Web*. Ihm zufolge könne das Web nur weiter an Nutzen und Wert gewinnen, wenn dessen Designprinzipien, die Universalität und Dezentralität, nicht in Frage gestellt würden.[275] Damit meint er, dass jede Person unabhängig von der genutzten Hardware, Software oder (menschlichen) Sprache eine Seite oder einen Hyperlink ins Web stellen können sollte, ohne dabei von einer zentralisierten Stelle eine Genehmigung zu benötigen.[276] Schlüssel für die Universalität sind demnach URLs, welche es ermöglichen jedem Hyperlink zu folgen, unabhängig davon, zu welchem Inhalt dieser führt oder wer den Inhalt veröf-

---

271 Kratz, InTeR 2019, 27; Lynskey, European Law Review 2017, 797 f.; Troiano, 162; Van Der Auwermeulen, CLSR 2017, 58.

272 Sie forderte, ohne die Datenportabilität direkt zu nennen: «[Sites shall allow] their users to syndicate their own profile data, their friends list, and the data that's shared with them via the service, using a persistent URL or API token and open data formats; Allow their users to syndicate their own stream of activity outside the site [...]», Farber Dan, «A Bill of Rights for the social Web», ZDNet vom 4. September 2007, abrufbar unter: https://perma.cc/YJL4-JYWK.

273 Und dabei besonders das *World Wide Web* als HTTP- und HTML-basierter und mittels Webbrowsers zugänglicher Teil des Internets.

274 Berners-Lee, Scientific American 2010, 82 f.; Kratz, InTeR 2019, 28.

275 Berners-Lee, Scientific American 2010, 82.

276 Berners-Lee, Scientific American 2010, 82.

fentlicht hat.[277] Erst diese Verlinkbarkeit führe dazu, dass Informationen im Web miteinander verbunden werden und daraus etwas Grösseres entstehen könne, nämlich ein *interconnected information space*.[278]

Diesen sah Berners-Lee aus mehreren Gründen bedroht, u.a. aufgrund von Monopolen, die die Innovation hemmten, und aufgrund sich bildender Datensilos bzw. *walled gardens*, mit welchen sich gerade die grossen Internetplattformen zu dieser Zeit voneinander abkapselten.[279] Ziel war es, dass die User möglichst lange auf der eigenen Website verweilten. Namentlich bemängelte er: «[Y]our site's pages are on the Web, but your data are not. You can access a Web page about a list of people you have created in one site, but you cannot send that list, or items from it, to another site.»[280] Ähnlich äusserte sich mit Larry Page ein Mitgründer von Google: «The Internet was made in universities and it was designed to interoperate. And as we've commercialized it, we've added more of an island-like approach to it, which I think is a somewhat a [sic] shame for users.»[281] 88

Dieser Überlegung folgend, lässt sich das Recht auf Datenportabilität historisch als Gegeninitiative zur damaligen Tendenz der Abschottung sehen.[282] Durch die Möglichkeit, die Daten herauszuverlangen, können Nutzerinnen die volle Kontrolle über ihre Daten erlangen, im Gegensatz zu einem API-Zugang oder den Fällen von Plattformisierung, bei welchen Anbieterinnen einen erheblichen Einfluss darüber behalten, wer auf welche Daten zugreifen kann und wie oft.[283] 89

Daraus lässt sich argumentieren, dass die Idee der Datenportabilität historisch nicht primär auf die Übertragung zwischen gleichartigen oder substitutiven Diensten abzielte, sondern darauf, dass vorhandene Daten einer Akteurin von einem andersartigen oder komplementären Dienst ausgewertet werden kön- 90

277 Berners-Lee, Scientific American 2010, 82, der darauf hinweist, dass er den auf ihn zurückgehenden *Uniform Resource Identifier*, ein Überbegriff, der auch URLs erfasst, ursprünglich *Universal Resource Identifier* genannt habe.

278 Berners-Lee, Scientific American 2010, 82.

279 Berners-Lee, Scientific American 2010, 82; Kratz, InTeR 2019, 28; ähnlich auch Expertengruppe Zukunft, 45.

280 Berners-Lee, Scientific American 2010, 82; zu den sog. *walled gardens* Rz. 298 f.

281 Helft Miguel, «Fortune Exclusive: Larry Page on Google», Fortune vom 11. Dezember 2012, abrufbar unter: https://perma.cc/QYA5-AC5L. Spätestens ab 2009 beschäftigte Google denn auch mit der «Data Liberation Front» ein Entwicklungsteam, das sich mit Angeboten zur Portierung von Daten beschäftigte, siehe https://perma.cc/5EMR-8JWF und zu den Nachfolgeprodukten Rz. 417 f.

282 Kratz, InTeR 2019, 28.

283 Siehe Nicholas/Weinberg, 5 f.

nen.[284] Das Internet als *interconnected information space* oder das *Open Web* sollte damit geschützt werden. Oder anders ausgedrückt: «Closed platforms are like ice cubes in a glass of water. They will float for a while. They will change the temperature of the liquid beneath. Ultimately, however, the ice cube must eventually melt into the wider web.»[285]

B. In der EU

91 Soweit ersichtlich wird die Datenportabilität als Rechtsinstitut erstmals ab 2009 in öffentlichen Konsultationen etwa zu einem «Rechtsrahmen für das Grundrecht auf Schutz personenbezogener Daten» sowie zu «Europe 2020» erwähnt. Die EU-Kommission hatte davor im Zuge grösser werdender Zweifel, ob die in die Jahre gekommene DSRL den modernen technischen Anforderungen noch genügt, zunächst eine öffentliche und anschliessend gezieltere Konsultationen durchgeführt.[286] Die Konsumentenschutzorganisation BEUC forderte darin ein Recht auf Datenportabilität und begründete dies damit, dass Konsumentinnen zunehmend an bestimmte Websites und soziale Netzwerke gebunden seien, und es wegen der vielen gespeicherten Daten nicht einfach sei, von einer Anbieterin zu einer anderen zu wechseln.[287] Angesichts der immer wichtiger werdenden Informations- und Kommunikationstechnologien regten Konsultationsteilnehmende ferner an, offene Standards für Interoperabilität und Datenportabilität anzuordnen.[288]

92 Am 19. Mai 2010 stellte die EU-Kommission die «Digitale Agenda für Europa» vor, deren Ziel es war, aus dem (europäischen) digitalen Binnenmarkt, der auf einem schnellen Internet und interoperablen Anwendungen beruht, einen nachhaltigen wirtschaftlichen und sozialen Nutzen zu ziehen.[289] Im Rahmen dieser Bestrebungen prüfte sie einen Rechtsrahmen für einen einheitlichen Datenschutz.[290] Im November 2010 wurde sodann ein Gesamtkonzept für den Datenschutz in der EU vorgestellt. Darin wurde angestossen, den Betroffenen eine bessere Kontrolle über ihre Daten zu geben.[291] Die Wahrnehmung der

284 Kratz, InTeR 2019, 28.
285 Saad Chris, «The data portability Landscape – An update», Blogbeitrag vom 18. Dezember 2008, abrufbar unter: https://perma.cc/29J8-GBCK.
286 Europäische Kommission, Gesamtkonzept, 3.
287 BEUC, 20.
288 Europäische Kommission, Europe 2020, 19.
289 Europäische Kommission, Digitale Agenda, 3.
290 Europäische Kommission, Digitale Agenda, 15.
291 Europäische Kommission, Gesamtkonzept, 8.

Rechte, etwa auf Berichtigung oder Löschung, sei nicht einheitlich geregelt und werde in der Online-Umgebung immer schwieriger, da die Daten dort ohne Wissen und/oder ohne Zustimmung der Betroffenen gespeichert würden.[292] Diese Probleme träten vor allem im Zusammenhang mit sozialen Netzwerken auf: So hätten sich Personen an die EU-Kommission gewandt und sich beklagt, dass es ihnen nicht immer gelungen sei, «ihre» Daten von Online-Diensteanbietern zurückzuerhalten, und sie ihr Recht auf Zugang zu den Daten, auf Berichtigung und auf Löschung nicht hätten wahrnehmen können.[293]

Die EU-Kommission veranlasste daher eine Prüfung, um die Rechte der von einer Verarbeitung Betroffenen zu erweitern, indem die «Datenübertragbarkeit» sichergestellt werden sollte, «also das Recht des Einzelnen, seine Daten (z.B. Fotos oder Freundeverzeichnisse) auf einer Anwendung oder einem Dienst zurückzuholen und die zurückgeholten Daten auf eine andere Anwendung oder einen anderen Dienst zu übertragen, sofern dies technisch möglich ist, ohne von dem für die Verarbeitung Verantwortlichen daran gehindert zu werden».[294] In seiner Entschliessung vom 6. Juli 2011 zum Gesamtkonzept für den Datenschutz betonte auch das Europäische Parlament dass eine Datenübertragbarkeit notwendig sei, da sie das reibungslose Funktionieren des Binnenmarkts sowie des Internets und seiner charakteristischen Offenheit und Interkonnektivität erleichtern werde.[295] Damit knüpfte es inhaltlich an Berners-Lee an.[296] 93

Im E-DSGVO vom 25. Januar 2012 regte die EU-Kommission ein «Recht auf Datenübertragbarkeit» an (Art. 18 E-DSGVO). Es sollte das Recht umfassen, die eigenen Daten aus einem automatisierten Datenverarbeitungssystem auf ein anderes System zu übertragen, ohne dass der für die Verarbeitung Verantwortliche die Betroffene daran hindern kann.[297] Erw.G 55 E-DSGVO führte diesbezüglich soziale Netzwerke als Beispiel für eine Übertragung auf, auch wenn der Kommissionsvorschlag keine Einschränkung auf derartige Anwendungen vorsah.[298] Dennoch waren diese Anwendungsbeispiele während des ganzen Gesetzgebungsverfahrens präsent. Meist wurde an einen Umzug eines Userprofils von einer Diensteanbieterin im Internet zu einer anderen ge- 94

292 Europäische Kommission, Gesamtkonzept, 8.
293 Europäische Kommission, Gesamtkonzept, 8.
294 Europäische Kommission, Gesamtkonzept, 8.
295 Europäisches Parlament, Gesamtkonzept Datenschutz, 7, insb. Fn. 2.
296 Dazu Rz. 86 ff.
297 E-DSGVO, 10.
298 NomosKomm-Dix, Art. 20 DSGVO N 2.

dacht.[299] Zwei Delegationen im Rat wollten denn auch den Anwendungsbereich ausdrücklich auf soziale Netzwerke beschränken, fanden aber keine Mehrheit.[300]

95 Im zuständigen Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments plädierte Berichterstatter ALBRECHT dafür, das eigenständige Recht auf Datenportabilität zu streichen.[301] Stattdessen sollte das Recht auf Auskunft zusätzlich um ein Recht auf Herausgabe der Daten erweitert werden.[302] In der Stellungnahme des Rechtsausschusses wurde dies damit begründet, dass das neue Recht den Bürgerinnen keinen Mehrwert gegenüber dem ebenfalls im Vorschlag vorgesehenen Auskunftsrecht biete.[303] Gleichzeitig wurde eingeräumt, dass die Datenportabilität das bestehende Ungleichgewicht in einem Markt, in welchem eine Dienstleistung monopolistisch oder oligopolistisch ist, nicht aufheben könne.[304] Die betroffenen Personen hätten in diesen Fällen keine wirkliche Möglichkeit, einen die Privatsphäre achtenden Dienstleister zu wählen.[305] Entsprechend könne die Datenportabilität in diesen Fällen auch den Netzwerkeffekten in grösseren sozialen Netzwerken nicht entgegentreten.[306]

96 Gleichwohl wurde das Recht auf Datenportabilität in den weiteren Vorschlägen beibehalten und im Laufe der Debatte noch punktuell angepasst. So war das Recht auf Datenübertragbarkeit in den Kompromisstexten des Rates vom 21. Juni 2013[307] und vom 11. Juni 2015[308] enthalten und findet sich in der endgültigen Version in Art. 20 DSGVO. Der Bezug zu sozialen Netzwerken wurde in der finalen Fassung aus den Erw.G entfernt und findet sich weder im Text noch in Erw.G 68 DSGVO.[309] Damit soll das Portabilitätsrecht ohne Einschränkung auf bestimmte Sektoren zur Anwendung gelangen.[310] Der Unionsgesetz-

299 FIX, 78.
300 Rat der Europäischen Union, Ratsdokument 8835/15 vom 12. Mai 2015, 45; hierzu KUKO DSGVO-KAMANN/BRAUN, Art. 20 N 5.
301 Europäisches Parlament, Bericht Albrecht, 107.
302 Europäisches Parlament, Bericht Albrecht, 102.
303 Europäisches Parlament, Bericht Albrecht, 603.
304 Europäisches Parlament, Bericht Albrecht, 610.
305 Europäisches Parlament, Bericht Albrecht, 610.
306 Europäisches Parlament, Bericht Albrecht, 610.
307 Rat der Europäischen Union, Ratsdokument 11013/13 vom 21. Juni 2013, 100.
308 Rat der Europäischen Union, Ratsdokument 9565/15 vom 11. Juni 2015, 103 f.
309 NomosKomm-DIX, Art. 20 DSGVO N 2.
310 HERMONIES, Rz. 74; JÜLICHER/RÖTTGEN/V. SCHÖNFELD, ZD 2016, 361; KUKO DSGVO-KAMANN/BRAUN, Art. 20 N 5; GK-PILTZ, Art. 20 DSGVO N 7 f.; SCHRADER, 285 f.

geber wählte also bewusst einen breiten Anwendungsbereich und wollte das Institut nicht auf soziale Netzwerke oder Plattformen beschränken.[311]

C. In der Schweiz

Die Einführung des Rechts auf Datenportabilität war in der Schweiz von Beginn an umstritten und folgte keiner klaren Linie. Bereits 2013 führte der Bundesrat in einem Bericht die Möglichkeit auf, eine «Datenmitnahme» einzuführen, allerdings beschränkt auf die sozialen Netzwerke.[312] Er verwies dabei auf Empfehlungen des Europarats und den (damaligen) Vorschlag der EU, ein Recht auf Datenübertragbarkeit einzuführen.[313] Ein 2015 eingereichtes Postulat verlangte sodann, dass der Bundesrat prüfe, inwiefern Einzelne und die Volkswirtschaft von der Weiterverwendung von Personendaten profitieren könnten und ob ein weitergehendes «Recht auf Kopie» des Einzelnen einzuführen sei.[314] In der dazugehörigen Stellungnahme vom 11. November 2015 gab der Bundesrat an, die verlangte Prüfung im Rahmen der DSG-Revision vorzunehmen.[315] 97

Im Dezember 2016 verzichtete der Bundesrat darauf, ein Recht auf Datenportabilität im Vorentwurf zum DSG zu verankern.[316] Seiner Ansicht nach war das Recht auf Datenportabilität nicht auf den Schutz der Persönlichkeit ausgerichtet, sondern solle vielmehr den betroffenen Personen die Wiederverwendung ihrer Daten ermöglichen, um den Wettbewerb spielen zu lassen.[317] Zudem merkte er an, dass die Umsetzung des Rechts schwierig sein könnte, da die gegenseitige Abstimmung unter den Verantwortlichen und eine (zumindest implizite) Einigung über die verwendeten Datenträger und Informatikstandards vorausgesetzt würde.[318] Der Bundesrat stützte sich ferner auf die durchgeführte Regulierungsfolgenabschätzung, welche hohe Implementierungskosten 98

311 Jülicher/Röttgen/v. Schönfeld, ZD 2016, 361, wonach «eindeutig» ein gegenüber jedem für die Datenverarbeitung Verantwortlichen bestehendes Recht auf Datenübertragbarkeit existiert, wobei die Banken- und Versicherungsbranche, der Online-Handel und Wearable-Anbieter als Beispiele genannt werden; in diese Richtung auch Fix, 139 f. und insb. Fn. 138.

312 Bundesrat, Bericht Social Media, 75.

313 Bundesrat, Bericht Social Media, 35.

314 Postulat Derder 15.4045.

315 Postulat Derder 15.4045.

316 BJ, Erläuternder Bericht VE-DSG, 22.

317 BJ, Erläuternder Bericht VE-DSG, 22; ebenso Botschaft DSG 2017, 6984; zu den Argumenten des Bundesrates auch Thouvenin/Weber/Früh, 143 f.

318 BJ, Erläuternder Bericht VE-DSG, 22; ebenso Botschaft DSG 2017, 6984.

in Aussicht stellte.[319] Er sah somit keine Notwendigkeit für ein Recht auf Datenportabilität und verzichtete anschliessend mit derselben Begründung auch im E-DSG darauf, ein Portabilitätsrecht in die Gesetzesvorlage aufzunehmen.[320]

99 Allerdings hatte der Bundesrat in der Zwischenzeit übergeordnete Ziele für eine kohärente und zukunftsorientierte Datenpolitik definiert. Im März 2017 erging daraus ein Auftrag an das EJPD. Dieses sollte bis Ende 2017 die «Rechtslage für eine Weiterverwendung von Personendaten, Sachdaten und anonymisierten Daten» analysieren.[321] In der Folge gaben das (zum EJPD gehörende) BJ und das BAKOM ein Gutachten in Auftrag, welches in seiner finalen Fassung Mitte Dezember 2017 publiziert wurde.[322] Beim SIR wurde zudem eine rechtsvergleichende Studie in Auftrag gegeben. Sie wurde Mitte Februar 2018 veröffentlicht.[323]

100 Im Vernehmlassungsverfahren zum DSG war der Tenor gegenüber dem Recht auf Datenportabilität – soweit sich die Teilnehmenden dazu äusserten – eher positiv gewesen; einzelne Branchenverbände sprachen sich zwar ebenfalls dagegen aus, mit der Begründung, dass ein solches Recht nicht auf den Schutz der Persönlichkeit ausgerichtet sei und erhebliche Mehrkosten zur Folge hätte.[324] Die befürwortenden Stimmen erhofften sich dagegen eine bessere Kontrolle der Daten und deren Wiederverwendung sowie die Förderung der Entwicklung neuer Dienste.[325] Auch der EDÖB befürwortete eine Aufnahme in das DSG,[326] ebenso wie eine durch das EFD in Umsetzung einer Motion eingesetzte Expertengruppe[327].

101 Der Bundesrat blieb indes bei seiner ablehnenden Haltung, wollte allerdings prüfen, ob für ein nur sektor- bzw. branchenspezifisches Portabilitätsrecht ein Bedarf bestehe.[328] Er wurde dabei allerdings von den Räten überholt: Die SPK-N fügte 2019 im Rahmen der Beratungen ein generelles «Recht auf Datenher-

319 BJ, Erläuternder Bericht VE-DSG, 22 m.H.a. PricewaterhouseCoopers AG, 37; ebenso Botschaft DSG 2017, 6984 f.
320 Botschaft DSG 2017, 6985.
321 Bundesrat, Medienmitteilung vom 22. März 2017.
322 Weber/Thouvenin, 5.
323 SIR, *passim*.
324 BJ, Zusammenfassung Vernehmlassungsverfahren, 62.
325 BJ, Zusammenfassung Vernehmlassungsverfahren, 62.
326 Botschaft DSG 2017, 6985.
327 Expertengruppe Zukunft, 9. Die Empfehlung umfasste auch die Prüfung einer Regelung der Portabilität von Sachdaten.
328 Siehe dazu BAKOM, Medienmitteilung vom 9. Mai 2018.

ausgabe oder -übertragung» in das DSG ein.[329] Sie verankerte damit ein Portabilitätsrecht, das unabhängig von bestimmten Faktoren des Datenbearbeiters, wie etwa Unternehmensgrösse oder Wirtschaftssektor, zur Anwendung gelangt und entschied sich damit für eine sektorübergreifende Regelung.[330] Mit dem Recht könnten sich, so Nationalrat GLÄTTLI, auf den die Regelung entscheidend zurückgeht, neue Wirtschaftsräume eröffnen und die Machtbalance zwischen kleinen und grossen Plattformen etwas verändern.[331] Er erklärte ferner, dass die Räte beim Recht auf Datenportabilität als einziges nicht nur darüber sprächen, «was wir verhindern müssen, um die individuelle Freiheit zu schützen, sondern darüber, wie wir durch die Schaffung eines neuen Marktes auch das Gleichgewicht der Macht verschieben können – nicht durch Verbote, sondern durch einen neuen Markt, liberal: weg von den riesigen Plattformen, weg von den riesigen Firmen und hin zu neuen, innovativen Unternehmen. Das können Genossenschaften sein, kleine Private, auch hier in der Schweiz, die die Möglichkeit haben, eine neue Datenwirtschaft zum Wohle aller zu schaffen.»[332]

Der Antrag einer Minderheit um GLÄTTLI sah zunächst vor, dass das Recht auf 102
Datenportabilität bei einem Verantwortlichen die Herausgabe *aller* Personendaten einer betroffenen Person umfasst. GLÄTTLI argumentierte, dass es sich beim Recht auf Datenportabilität im DSG um einen «Kernartikel» handle: «Es geht […] um das Auskunftsrecht 2.0, um die Portabilität oder um das Recht auf Kopie – drei verschiedene Namen für das Gleiche.»[333] Heute seien grosse Internetplattformen wie Staubsauger, die Daten von immer mehr Leuten aufsaugten. Dies geschehe meistens unter harmlosen Vorwänden oder mittels Angebots irgendeiner Gratisdienstleistung, sei das ein E-Mail-Dienst, eine Suchmaschine, ein soziales Netzwerk. Diese Plattformen seien aber auch in unzähligen anderen Branchen aktiv, unterstützten Start-ups und kauften Firmen auf. Die Idee dahinter sei, dass es nicht reiche, nur einen möglichst grossen, immer stärker in Richtung Monopol gehenden Marktanteil zu haben, der den Plattformen wegen des Netzwerkeffekts zukomme. Vielmehr sei ein möglichst grosser Kundenanteil notwendig. Entsprechend gingen diese Plattformen verschiedenen und teilweise unrentablen wirtschaftlichen Tätigkeiten

329 Siehe Fahne DSG, Entwurf 3 Herbstsession 2019, 29 f.

330 So auch ROSENTHAL, Jusletter 2020, Rz. 130, der ausdrücklich hervorhebt, dass das Portabilitätsrecht nicht nur für Facebook gelte. Damit wurde die geplante Überprüfung durch das BJ resp. das EJPD obsolet, siehe Bundesrat, Bericht Regulierungskosten, 5.

331 Votum NR Glättli, AB 2019 N 1779.

332 Votum NR Glättli, AB 2019 N 1813.

333 Votum NR Glättli, AB 2019 N 1814.

nach, um über jeden Einzelnen, den sie kennen, möglichst viel zu wissen, und zwar in möglichst vielen Lebensbereichen. Mit dem Recht auf Datenportabilität hätten die Räte die Möglichkeit, «ein neues Gleichgewicht einzuführen und den einzelnen Personen Gewicht zurückzugeben».[334] Es sei demnach ein umfassendes Recht auf Datenportabilität einzuführen, damit eine betroffene Person alle Daten, «die irgendwo auf einer dieser Riesenplattformen über sie gespeichert sind, zurückkriegen kann – also nicht nur diejenigen, die sie selbst geliefert hat, sondern auch diejenigen, die über sie errechnet wurden».[335] Nur dann sei, gemäss GLÄTTLI, noch die Möglichkeit gegeben, dass eine betroffene Person am Schluss in einer Position der Stärke sei. Sie könne dann autonom entscheiden, für welche Zwecke sie bereit sei, diese Daten zur Verwendung zu überlassen, etwa im Rahmen von Datengenossenschaften für die medizinische Forschung, im Rahmen von Projekten des Staates oder halbstaatlicher Verkehrsbetriebe zur Optimierung des öffentlichen Verkehrs, oder im Sinne der Gesundheitsvorsorge.[336] Das geistige Eigentum der Unternehmen und die dahintersteckenden Algorithmen und Regeln, mithilfe derer die persönlichen Profile errechnet werden, seien dagegen nicht umfasst, sondern nur die Resultate dieser Algorithmen, insofern, als sie der betroffenen Person zugeordnet seien.[337]

103 Nationalrat FLACH und mit ihm die Mehrheit der Kommission sprachen sich gegen eine solche weite Auslegung des Instituts aus. Er begründete dies damit, dass es «einfach zu weit [geht], wenn man damit quasi auch die Grundlagen bekommt, den Algorithmus, der hinter der Datenbearbeitung liegt.»[338] FLACH brachte dabei auch den Schutz von Geschäftsgeheimnissen vor.[339]

104 Bundesrätin KELLER-SUTTER empfahl im Nationalrat, die Kommissionsmehrheit zu unterstützen, und hielt fest, dass es sich beim Recht auf Datenportabilität um eine der zentralsten Neuerungen handle, die in der EU mit der DSGVO in Kraft getreten seien.[340] Dieser neue Anspruch berechtige im Grundsatz eine betroffene Person, vom verantwortlichen Datenbearbeiter die Herausgabe ihrer Personendaten in einem gängigen elektronischen Format oder sogar deren Übertragung auf einen anderen Verantwortlichen zu verlangen. Vom Anspruch umfasst seien aber nur jene Personendaten, welche die betroffene Person dem

334 Votum NR Glättli, AB 2019 N 1814.
335 Votum NR Glättli, AB 2019 N 1814 f.
336 Votum NR Glättli, AB 2019 N 1815.
337 Votum NR Glättli, AB 2019 N 1815.
338 Votum NR Flach, AB 2019 N 1814.
339 Votum NR Flach, AB 2019 N 1814.
340 Votum BR Keller-Sutter, AB 2019 N 1816.

Verantwortlichen bewusst und aktiv zur Verfügung gestellt habe, sowie sog. «observed data».[341] Nicht umfasst würden hingegen Personendaten, welche aus grösseren Datenanalysen oder aus Auswertungen dieser Informationen entstünden.[342] Die von der Kommissionsmehrheit gewählte Ausgestaltung des Portabilitätsrechts entsprach aus Sicht der Bundesrätin «grundsätzlich der DSGVO».[343] Demgegenüber gehe aus Sicht des Bundesrates der Vorschlag der Minderheit Glättli zu weit. Der Verantwortliche hätte ein überwiegendes Interesse daran, Informationen, die auf einer Eigenleistung beruhen, nicht herausgeben zu müssen.[344] Zudem würde diese Lösung über den EU-Datenschutzstandard hinausgehen.[345]

Schliesslich meldete sich Kommissionssprecher JAUSLIN zu Wort, der das Recht auf Datenportabilität mit parlamentarischem Pathos als «ein eigentliches Highlight» der Datenschutzgesetzgebung bezeichnete.[346] Es sei für die Bürgerin ein Mehrwert, wenn sie Zugriff auf ihre Daten habe und diese auch in einem gängigen elektronischen Format beziehen und für weitere Anwendungen benützen könne.[347] Der Antrag Glättli sei der Kommission jedoch zu weit gegangen, weshalb sie ihn mit 14 zu 6 Stimmen abgelehnt habe. Es sei entsprechend der Mehrheit zu folgen, «immer mit dem Hintergedanken, was die Angemessenheit beeinträchtigen wird und was nicht».[348] Der Nationalrat nahm den Antrag der Mehrheit schliesslich mit 143 zu 53 Stimmen bei einer Enthaltung an und votierte damit für ein Recht auf Datenportabilität.[349] Im Ständerat wurde das Recht auf Datenportabilität nur in der Kommission gesondert beraten; er stimmte dem Beschluss des Nationalrats am 18. Dezember 2019 zu.[350] 105

341 Votum BR Keller-Sutter, AB 2019 N 1816.
342 Votum BR Keller-Sutter, AB 2019 N 1816.
343 Votum BR Keller-Sutter, AB 2019 N 1816.
344 Votum BR Keller-Sutter, AB 2019 N 1816.
345 Votum BR Keller-Sutter, AB 2019 N 1816.
346 Votum Sprecher Jauslin, AB 2019 N 1817.
347 Votum Sprecher Jauslin, AB 2019 N 1817.
348 Votum Sprecher Jauslin, AB 2019 N 1817. Damit spielte er auf den Angemessenheitsbeschluss durch die EU an, siehe dazu Rz. 84.
349 AB 2019 N 1819.
350 AB 2019 S 1245.

II. Technisch-organisatorische Aspekte

A. Allgemein

106 Das Verständnis des Portabilitätsrechts hängt nicht zuletzt von technisch-organisatorischen Aspekten ab. Sie beeinflussen massgeblich, ob das Institut in der Praxis funktioniert und ob allfällige Anpassungsvorschläge umsetzbar sind. Dessen Umsetzung war denn auch bereits Gegenstand verschiedener (technischer) Erörterungen.[351] Nachfolgend sind daher nur die Grundzüge zu streifen.

107 Unabhängig von der rechtlichen Normierung in der EU und der Schweiz hat sich die ISO[352] in einem Leitfaden zu Cloud Computing der Interoperabilität und Portabilität technisch angenähert. Demnach handelt es sich bei Datenportabilität um die «Fähigkeit, Daten leicht von einem System auf ein anderes zu übertragen, ohne dass eine erneute Eingabe der Daten erforderlich ist».[353] Wesentliches Kriterium soll dabei die «Leichtigkeit» der Übertragung sein. Dieses Kriterium sei etwa dann erfüllt, wenn ein Quellsystem die Daten in genau dem Format liefert, das von einem Zielsystem akzeptiert wird, aber auch dann, wenn die Formate nicht übereinstimmen, aber die Umwandlung der Daten einfach und problemlos mit gängigen Werkzeugen erfolgen kann.[354] Technisch gesehen ist eine Portierung aber kaum je binär entweder «möglich» oder «unmöglich»: Vielmehr sei es eine Frage des Aufwands, weshalb die Beteiligten eine Kosten-Nutzen-Analyse durchführen müssten.[355]

---

351 Ausführlich etwa FIX, 275 ff., der den Auslesevorgang und Exportvorbereitung, Übermittlungsvorbereitung und Import, Datenformate und Industriestandards beleuchtet; mit Blick auf die technische Realisierbarkeit der DSGVO-Umsetzung und unterschiedlichen Lösungsansätzen HEMPEL/SCHMID, *passim*; mit Fokus auf Cloud Computing ISO/IEC 19941, *passim*; KRANZ et al., BISE 2023, *passim*, die unterschiedliche Architekturen als Grundlage für die Umsetzung aufzeigen; WILLARD et al., *passim*, die unabhängig von der gesetzlichen Regelung und am Beispiel von Google die technische Umsetzung der *Data Transfer Initiative* beschreiben.

352 Dieser Standardisierungsorganisation gehören 174 einzelstaatliche Normungsbehörden an, darunter auch alle vorliegend einbezogenen Staaten, siehe https://perma.cc/9XNZ-E3MN.

353 Eigene Übersetzung des Wortlauts «ability to easily transfer data from one system to another without being required to re-enter data» bei ISO/IEC 19941, 2.

354 ISO/IEC 19941, 2.

355 ISO/IEC 19941, 6.

Die ISO betrachtet die Datenportabilität aus unterschiedlichen Perspektiven, welche im Rahmen des Cloud Computing berücksichtigt werden müssten – einer syntaktischen, semantischen und regulatorischen Perspektive.[356] Dabei vertieft sie jeweils unterschiedliche Aspekte des Cloud Computing einzeln, namentlich Infrastruktur (*Infrastructure as a Service*), Plattformen (*Platform as a Service*) und Anwendungen (*Software as a Service*).[357] Auf die Unterscheidung wird vorliegend jedoch nicht weiter eingegangen. 108

B. Perspektiven der Portabilität gemäss ISO

1. Syntaktische Perspektive

Daten sind nur portabel, wenn die Portabilität auf der Ebene der Syntax sichergestellt wird. Dabei werden Daten von einem Quellsystem zu einem Zielsystem transferiert (Portabilitätskomponente), wobei eine bestimmte Syntax verwendet wird, um die Daten zu kodieren (Syntaxkomponente).[358] Denkbar ist die Verwendung von Formaten wie CSV, XML, JSON oder Paketformaten wie OVF oder Zip.[359] CSV stellt dabei eine Art Minimallösung dar, da die Daten einzig durch Kommas separiert werden.[360] XML oder JSON sind hingegen in der Lage, komplexere Datenstrukturen darzustellen, da sie sowohl Inhaltsdaten als auch beschreibende Metadaten enthalten.[361] 109

Notwendig ist, dass das Format vom Zielsystem dekodiert werden kann, weshalb die Daten u.U. zunächst konvertiert werden müssen, wenn das Zielsystem eine andere Datensyntax (d.h. ein anderes Datenformat) verwendet.[362] Es soll ein «strukturiertes, gängiges und maschinenlesbares» Austauschformat[363] verwendet werden, wodurch wahrscheinlicher wird, dass eine Portierung möglich ist.[364] Ist das Zielsystem in der Lage, die empfangenen Daten zu dekodieren, bedeutet 110

356 ISO/IEC 19941, 42 ff.
357 ISO/IEC 19941, 42.
358 ISO/IEC 19941, 14.
359 ISO/IEC 19941, 14 ff.
360 Karasoy/Turgut/Degeling, 330.
361 Karasoy/Turgut/Degeling, 330.
362 ISO/IEC 19941, 42.
363 Der Wortlaut von Art. 20 DSGVO ist insoweit identisch, dazu Rz. 143 ff.
364 ISO/IEC 19941, 16 und 43.

dies aber noch nicht, dass deren Inhalt verstanden wird.[365] Dafür ist auch die semantische Perspektive zu berücksichtigen.[366]

2. Semantische Perspektive

111 Die semantische Ebene der Portabilität umfasst den Transfer von Daten zu einem Zielsystem (Portabilitätskomponente) in einer Weise, dass die Bedeutung des Datenmodells in seinem sachlichen Kontext vom Zielsystem verstanden wird (Semantikkomponente).[367] Das Quellsystem sichert dem Zielsystem also eine bestimmte Bedeutung der Daten zu.[368] Dies funktioniert über ein (logisches) Datenmodell – auch Meta-Modell genannt –, welches die Datenelemente, sowie die Attribute, logischen Strukturen und Beziehungen zwischen Datenelementen ausdrückt.[369] Wie ein solches Datenmodell aussieht, hängt von der Art des Cloud-Angebots ab. Notwendig sind jedenfalls gegenseitig verstandene Ontologien und Metadaten wie bspw. OWL oder Dublin Core.[370]

3. Regulatorische Perspektive

112 Schliesslich wird darauf hingewiesen, dass bei der technischen Umsetzung die regulatorische Perspektive gebührend berücksichtigt werden muss. Darunter wird die Fähigkeit verstanden, Daten zwischen einem Quell- und einem Zielsystem zu übertragen und dabei die für beide Systeme geltenden rechtlichen, organisatorischen und politischen Rahmenbedingungen einzuhalten.[371] Dazu gehören Vorschriften über die Datenlokalisierung, Zugriffsrechte, die gemeinsame Nutzung von Daten sowie die gegenseitigen Verantwortlichkeiten im Hinblick auf Sicherheit und Datenschutz.[372]

365 ISO/IEC 19941, 43.
366 Dazu bereits Rz. 31 f.
367 ISO/IEC 19941, 14.
368 ISO/IEC 19941, 15.
369 ISO/IEC 19941, 14.
370 ISO/IEC 19941, 15; siehe https://perma.cc/22NT-KUUY sowie https://perma.cc/4A5H-Z9QL.
371 ISO/IEC 19941, 14.
372 ISO/IEC 19941, 14.

C. Interoperabilität als Wesenszug der Portabilität?

Interoperabilität bedeutet, dass mehrere Systeme oder Anwendungen fähig sind, Informationen auszutauschen und die ausgetauschten Informationen gegenseitig zu nutzen.[373] Interoperable Systeme können also miteinander nahtlos und weitgehend ohne Verluste zusammenarbeiten.[374] Damit besteht eine Ähnlichkeit zur Portabilität. Allerdings ist Interoperabilität nicht mit Portabilität gleichzusetzen.[375] Der Austausch zwischen interoperablen Systemen ist stets bidirektional, während er bei einer Portabilität unidirektional ist oder zumindest sein kann.[376] Interoperabilität geht also weiter als Portabilität, die nur die Datenübertragung zwischen zwei Organisationen, nicht aber deren Interaktion ermöglicht.[377] Ein interoperables Angebot unterstützt jedoch nicht zwingend die Portierung von Daten; umgekehrt ist ein Angebot, das portabel ist nicht zwingend interoperabel.[378] Zugleich wird Interoperabilität als Zielzustand bei Diskussionen zum Portabilitätsrecht stets genannt, teilweise sogar als Voraussetzung angenommen.[379] Die Begriffe setzen jedoch an einem unterschiedlichen Ort an: Die Datenportabilität versucht durch Formatvorgaben[380] einen Zustand der Interoperabilität zwischen zwei Systemen herbeizuführen; «interoperable Daten» liegen deswegen nicht vor.[381] Wenn eine Portierung von Daten in Echtzeit angestrebt wird, so können die Grenzen allerdings fliessend sein.[382] 113

Wird die Interoperabilität aus unterschiedlichen Perspektiven betrachtet, so werden die Gemeinsamkeiten aber auch die Unterschiede zur Portabilität besser sichtbar. Die ISO unterscheidet zwischen syntaktischer Interoperabilität, semantischer Dateninteroperabilität, Verhaltensinteroperabilität, Transportinteroperabilität und regulatorischer Interoperabilität.[383] Während die syntaktische, semantische und regulatorische Interoperabilität ähnliche Anforderungen an ein standardisiertes Datenformat, an ein Datenmodell und an das 114

373 ISO/IEC 19941, 1; ähnlich auch das BFS, siehe https://perma.cc/D8TA-7FBL.

374 Schallbruch et al., 39.

375 So ausdrücklich auch ISO/IEC 19941, 9; Siglmüller, MMR 2024, 114, wonach die beiden Konzepte «gänzlich unterschiedliche Sachverhalte betreffen».

376 Kühling/Hildebrandt/Bulowski, K&R 2022, 672.

377 Engels, Internet Policy Review 2016, 4.

378 ISO/IEC 19941, 9.

379 Für die EU Rz. 154 f. und 141 und für die Schweiz Rz. 208.

380 Dazu Rz. 205 ff.

381 Fix, 206.

382 Steffen/Wieworra/Kroon, 77; ähnlich Crémer/De Montjoye/Schweitzer, 59 und 83 f., die dabei aber von «data interoperability» sprechen.

383 ISO/IEC 19941, 10 f.

Regulationsumfeld stellen, verlangt Transportinteroperabilität eine gemeinsame Kommunikationsinfrastruktur, die einen Datenaustausch zwischen Quell- und Zielsystem ermöglicht.[384] Diese Infrastruktur kann bspw. durch ein REST HTTP/S-Protokoll zur Verfügung gestellt werden.[385] Dies dürfte bei einer Portierung ebenfalls oft der Fall sein, ist dort aber keine Bedingung.[386] Daneben muss mit der Verhaltensinteroperabilität eine weitere Bedingung erfüllt sein, die die Portabilität nicht kennt: Das Ergebnis der Nutzung der ausgetauschten Informationen muss dem vom Quellsystem erwarteten Ergebnis entsprechen.[387] Dafür ist eine sog. Dienstbeschreibung der Schnittstelle notwendig, die die durchführbaren Operationen, einschliesslich möglicher Eingaben und Ausgaben für jede Operation, vorstellt.[388] Dabei handelt es sich oft um eine API. So kann man einerseits sicherstellen, dass beide Systeme verstehen, was sie jeweils meinen und dabei gleiche Formate benützen; andererseits werden weitere technische Komponenten wie Abhängigkeiten innerhalb des Systems oder Invarianten und relevante Vor- oder Nachbedingungen berücksichtigt.[389] Nur wenn dies ebenfalls gewährleistet ist, können sich Systeme nahtlos und damit interoperabel austauschen.

D. Personal Information Management Systems (PIMS)

115 Im Zusammenhang mit der technischen Umsetzung der Datenportabilität werden oft sog. *Personal Information Management Systems* (PIMS) diskutiert. Dabei handelt es sich um ein junges Phänomen, für das sich allerdings bislang weder einheitliche Geschäftsmodelle noch feste Begrifflichkeiten etabliert haben.[390] Kennzeichnend für PIMS ist, dass ein Datentreuhänder die Personendaten für Betroffene verwalten soll. Er bietet seinen Nutzern die technische Infrastruktur in Form einer Plattform, die es ihnen ermöglicht, ihre eigenen Daten zentral zu sammeln, zu verwalten und bei Bedarf weiterzugeben.[391] Als Kernfunktionen eines PIMS werden etwa das Identitäts-, und Berechtigungsmanagement und die technische Umsetzung der Datenübertragung ge-

384 ISO/IEC 19941, 38 f.
385 ISO/IEC 19941, 13.
386 ISO/IEC 19941, 14.
387 ISO/IEC 19941, 11.
388 ISO/IEC 19941, 11.
389 Siehe diese und weitere Anwendungsbeispiele bei ISO/IEC 19941, 40.
390 Weber/Thouvenin, 15.
391 Weber/Thouvenin, 15.

nannt.[392] Dabei bleibt die Entscheidung, ob und wie die Daten weitergegeben und von Dritten verwendet werden beim Nutzer; er kann frei und abgestuft (oder «granular») in bestimmte Datenbearbeitungen einwilligen oder eine bereits erteilte Einwilligung widerrufen.[393]

Ein Nutzer erhält so die Kontrolle über die Verwendung der ihn betreffenden Personendaten und über die Datensammlung als Ganzes. Dabei erleichtert ihm ein PIMS vor allem den Umgang mit den Daten. Für ihn hat dies den Vorteil, dass er nur mit dem PIMS-Anbieter als vertrauenswürdigem Akteur interagieren muss. Umgekehrt müssen Dritte nicht individuell mit jedem Nutzer verhandeln, sondern können an den PIMS-Anbieter gelangen, welcher die Daten – mit Einverständnis der Betroffenen – bereitstellt. Grosse, viele Personen betreffende Datensätze können so durch den PIMS-Anbieter an Dritte vermittelt werden. Durch den vermittelnden PIMS-Anbieter wird eine gewisse Standardisierung der bereitgestellten Daten wahrscheinlich. Sie reicht mitunter bis zu einer umfassenden Interoperabilität. In rechtlicher Hinsicht ist das Datenportabilitätsrecht die Grundlage dafür, die Daten überhaupt erst herausverlangen bzw. an einen PIMS-Anbieter übertragen lassen zu können.[394] 116

PIMS erfordern eine auf dem Stand der Technik beruhende Datenmanagement-Architektur.[395] Die konkrete Ausgestaltung kann dabei variieren: Daten können lokal beim Nutzer verbleiben oder in einer Cloud gespeichert werden, etwa zentral beim PIMS-Anbieter oder dezentral bei unterschiedlichen Anbietern von Dienstleistungen als jeweilige Datenquellen (soziale Netzwerke, Gesundheitsinstitutionen usw.).[396] Gerade bei zentralen Lösungen sind aber hohe Ansprüche an die Datensicherheit zu stellen, da diese aufgrund der Akkumulierung von Daten besonders riskant sind.[397] Ferner sind gemeinsame Standards und APIs notwendig, damit ein PIMS in der Lage ist, auf die Daten zuzugreifen, diese zu verarbeiten und weiterzuleiten.[398] Auf das Phänomen PIMS wird bei der sektoriellen Betrachtung des Portabilitätsrechts zurückzukommen sein. 117

392 Krämer, JCLE 2021, 283.
393 Weber/Thouvenin, 15.
394 So auch Weber/Thouvenin, 7 und 37 f., sowie 31 f., wo unter dem damals noch anwendbaren aDSG diese Rolle durch das Auskunftsrecht nach Art. 8 aDSG übernommen werden musste.
395 EDSB, Rz. 18.
396 EDSB, Rz. 9.
397 Ähnlich EDSB, Rz. 38.
398 Krämer, JCLE 2021, 283.

E. Datensicherheit

118 Mit dem Datenportabilitätsrecht gehen Sicherheitsrisiken einher, einerseits während der Übertragung der Daten und andererseits aus dem sich dadurch vergrössernden Personenkreis, der über die Daten verfügen kann.[399] Der Verantwortliche ist verpflichtet, geeignete technische und organisatorische Massnahmen umzusetzen, um eine dem Risiko angemessene Datensicherheit zu gewährleisten (Art. 8 DSG).

119 Die Datensicherheit während der Herausgabe oder der Übertragung (*in transit*) hängt zunächst vom Transportweg ab: Wird das Portabilitätsrecht gewährt, indem ein USB-Stick per Post versendet wird, bestehen andere und wohl insgesamt weniger Risiken, als wenn die Portierung über einen API-Zugang erfolgt.[400] Im verbreiteteren Fall einer informationstechnologischen Übertragung, etwa indem eine E-Mail versendet oder ein Downloadlink bereitgestellt wird, sollte der Datensatz während des Transports mittels Ende-zu-Ende-Verschlüsselung (E2EE) gesichert werden.[401] Zudem ist es empfehlenswert, die Daten revisionssicher oder signiert zu übermitteln, um nachträglich nachweisen zu können, dass die richtigen und unverfälschten Daten herausgegeben wurden.[402] Diese Vorgaben lassen sich aus Art. 3 Abs. 2 lit. c DSV ableiten.

120 Sind die Daten herausgegeben oder übertragen worden (*at rest*), hat sich der Personenkreis mit Zugriff auf die Daten erhöht. Entsprechend besteht – gerade bei einer Herausgabe an die Betroffene – ein nicht unerhebliches Risiko, dass die Daten nach der Herausgabe in einem weniger gut gesicherten System abgespeichert werden.[403] Für Betroffene besteht zudem die besondere Gefahr eines Identitätsmissbrauchs, wenn Hacker Zugang zu ihrem Account erhalten und das Recht auf Datenportabilität missbräuchlich ausüben. Hacker können dann Zugang zu einem Datensatz über eine Person in weiterverwendbarer Form[404] erlangen oder diesen auf einen neuen Anbieter übertragen lassen.[405] Bei der Gewährung des Portabilitätsrechts sollten Verantwortliche daher ein

399 PC LPD-Béguin, Art. 28 N 44; Graef/Husovec/Van den Boom, EuCML 2020, 13.

400 Darauf hinweisend, dass Verantwortliche ihre internen Datenbanken mit Personendaten oft hinter Firewalls vor Zugriffen aus dem Internet schützen Lynskey, European Law Review 2017, 809 m.w.N.

401 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 23; siehe auch die Ausführungen zur Netzsicherheit beim EDÖB, Leitfaden TOM, 48 f.

402 Hempel/Schmid, 239.

403 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 23.

404 Dazu Rz. 205 ff.

405 Engels, Internet Policy Review 2016, 4; Lynskey, European Law Review 2017, 809; Swire/Lagos, Maryland Law Review 2013, 366 und 373 f.

besonderes Augenmerk auf Datensicherheitsaspekte und besonders auf die Identifizierung der Betroffenen legen, da ansonsten ein Einfallstor als *Single Point of Vulnerability* für einen aggregierten Datensatz offensteht.[406]

Verantwortliche sind in der Pflicht, den konkreten Risiken entsprechend geeignete Massnahmen vorzusehen (siehe auch Art. 1 ff. DSV). So sollten Betroffene nur auf die Daten zugreifen können, wenn deren sichere Identifizierung und Authentifizierung gewährleistet ist.[407] Dafür in Frage kommen etwa Login-Verfahren und eine mehrfache Authentifizierung der Betroffenen, bspw. durch ein hinterlegtes Geheimnis, ein einmaliges Passwort oder *Security-Tokens*.[408] Zusätzlich sollte eine Benachrichtigung über die Portierung über einen anderen Kanal erfolgen, sodass eine Betroffene auch dann davon Kenntnis nehmen kann, wenn ihr Account kompromittiert wurde.[409] Ferner ist denkbar, die Daten nicht unverzüglich, sondern erst nach einer gewissen Latenzzeit bereitzustellen und den Download nur für eine begrenzte Zeit zuzulassen.[410] Nach Ablauf dieser Zeit sollte ein neues Portierungsgesuch gestellt werden müssen.[411] 121

406 Ähnlich Lynskey, European Law Review 2017, 809.

407 Hempel/Schmid, 239; siehe weiterführend auch EDÖB, Leitfaden TOM, 37, der sich dabei zwar auf die Lage für Mitarbeitende eines Verantwortlichen bezieht. In technischer Hinsicht ist die Situation jedoch vergleichbar.

408 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 23; Hempel/Schmid, 239; International Working Group on Data Protection in Technology, 14.

409 OECD, Mapping Initiatives, 30.

410 OECD, Mapping Initiatives, 30.

411 OECD, Mapping Initiatives, 30. Ein solches Vorgehen kann indes auch konträr zu den Interessen der Betroffenen sein. Daran zeigt sich, dass die Umsetzung des Portabilitätsrechts stets anhand eines Einzelfalls zu beurteilen ist.

III. Rechtlicher Rahmen

122 Bereits gezeigt wurde, dass das Portabilitätsrecht in der Schweiz historisch auf die europäische Regelung zurückgeht. Wie dieses Kapitel zeigen wird, stimmt Art. 28 DSG in vielen Belangen mit Art. 20 DSGVO überein, wobei punktuell Unterschiede existieren. Daher wird zunächst die (ältere) europäische Regelung untersucht. Anschliessend sind die einzelnen Merkmale der (jüngeren) Schweizer Regelung darzulegen und, wo nötig, mit Art. 20 DSGVO zu vergleichen.

A. Art. 20 DSGVO

123 Die DSGVO regelt das Recht auf Datenportabilität unter dem Titel «Recht auf Datenübertragbarkeit» in Art. 20. Das Recht auf Datenübertragbarkeit umfasst den Anspruch der betroffenen Person, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die Daten bereitgestellt wurden, zu übermitteln, sofern bestimmte Voraussetzungen vorliegen. Diese einzelnen Elemente sind nachfolgend zu untersuchen.

1. Personenbezogene Daten der betroffenen Person

124 Das Recht der betroffenen Person umfasst die sie betreffenden Personendaten. Damit werden Sachdaten, anonyme Daten und Daten, die sich ausschliesslich auf andere Personen beziehen, ausgeschlossen.[412] Zweifellos nicht

412 Elfering, 26; Krause, PinG 2018, 240; BeckOK DSR-von Lewinski, Art. 20 DSGVO N 17 und 30 ff. Daraus erhellt auch, dass juristische Personen das Recht auf Datenportabilität nicht wahrnehmen können. Erw.G 27 DSGVO stellt zudem klar, dass die Daten Verstorbener ebenfalls nicht umfasst sind, siehe dazu Strubel, ZD 2017, 357. Hinzuweisen ist allerdings auf Art. 16 Abs. 4 DIRL, der für Sachdaten greifen kann. Diese Bestimmung sieht für den Fall der Beendigung eines Vertrags vor, dass ein Unternehmen dem Verbraucher auf dessen Ersuchen «alle Inhalte, die nicht personenbezogene Daten sind» bereitstellt, welche von der Verbraucherin bei der Nutzung der von der Betreiberin bereitgestellten digitalen Inhalte oder digitalen Dienstleistungen bereitgestellt oder erstellt wurden. Die digitalen Inhalte erhält die Verbraucherin kostenfrei, ohne Behinderung innerhalb einer angemessenen Frist und in einem allgemein gebräuchlichen und maschinenlesbaren Format.

erfasst sind also reine Drittdaten.[413] Lassen sich sachbezogene Daten – etwa eine Playlist oder ein Fahrtenschreiber – auf die betroffene Person zurückführen, fallen sie ebenfalls unter die Bestimmung.[414] Zudem unterliegen pseudonymisierte Daten dem Recht auf Datenportabilität, wenn sie eindeutig mit der Betroffenen in Verbindung gebracht werden können, etwa weil diese die Informationen, die die Identifizierung ermöglichen, bereitstellt.[415]

Daten Dritter werden im Einklang mit der datenschutzrechtlichen Konzeption durch die Bestimmung nicht erfasst.[416] Grundsätzlich können betroffene Personen nur über sie betreffende Daten verfügen. Art. 20 Abs. 1 DSGVO beschränkt sich jedoch nicht auf Daten, die *ausschliesslich* die Betroffene und keine weiteren Personen betreffen. Verlangt wird lediglich, dass das Recht auf Empfang der Daten die Grundrechte und Grundfreiheiten anderer betroffener Personen unberührt lässt (Erw.G 68 DSGVO).[417] Nur so kann dem ausdrücklichen Hinweis in Art. 20 Abs. 4 DSGVO eine Wirkung zukommen, wonach die direkte Übertragung von einem Verantwortlichen an eine andere Verantwortliche «die Rechte und Freiheiten anderer Personen nicht beeinträchtigen» darf. Daraus folgt, dass ein Kontaktverzeichnis oder ein Profilbild, das neben der betroffenen Person noch weitere Personen zeigt, vom Portabilitätsrecht erfasst ist.[418] Wäre dies nicht der Fall, würde das Recht auf Datenportabilität in seinem Anwendungsbereich derart eingeschränkt, dass das Rechtsinstitut ins Leere laufen würde.[419] Praktisch dürfte 125

413 BeckKompaktKomm-Paal, Art. 20 DSGVO N 17a.

414 Etwa weil Metadaten den Rückschluss zulassen, siehe NomosKomm-Dix, Art. 20 DSGVO N 5; a.A. jedoch BeckOK DSR-von Lewinski, Art. 20 DSGVO N 17 m.H.a. Werkmeister/Brandt, CR 2016, 237, die im Kontext von Big Data die Datenportabilität dann eingeschränkt sehen wollen, wenn die Daten ohne zusätzliche Datenverknüpfung noch gar nicht personenbezogen sind. Dies widerspricht indes der Definition von Art. 4 Abs. 1 DSGVO, wonach Daten personenbezogen sind, wenn sie sich auf eine bloss identifizierbare (nicht bereits identifizierte) Person beziehen. Diese Problematik kann zudem unter dem Blickwinkel des «Bereitstellens» betrachtet werden. Dazu sogleich Rz. 126 ff.

415 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 10; NomosKomm-Dix, Art. 20 DSGVO N 6; Elfering, 26; BeckOK IT-Recht-Steinrötter, Art. 20 DSGVO N 15; BeckOK DSR-von Lewinski, Art. 20 DSGVO N 17 und 31.

416 NomosKomm-Dix, Art. 20 DSGVO N 5; Elfering, 26; KUKO DSGVO-Kamann/Braun, Art. 20 N 15.

417 BeckKomm-Herbst, Art. 20 DSGVO N 3 und 10.

418 BKartA, Sektoruntersuchung, 32 f.; a.A. Golland, 318.

419 Krause, PinG 2018, 240. Im Fall von Messengerdiensten könnten etwa einzig die bei der Anmeldung angegebenen Daten, also das Benutzerprofil, portiert werden. (Nur) dies kann nicht gemeint sein. Dies gilt umso mehr, wenn die Zielsetzung der Normierung beachtet wird, siehe dazu Rz. 245 ff. Zu beachten ist zudem, dass die DSGVO in Erw.G 18 festhält, dass persönliche oder familiäre Tätigkeiten (i.S.v. Art. 2 Abs. 2 lit. c DSGVO) auch die Nutzung sozialer Netze und Online-Tätigkeit im Rahmen solcher Tätigkeiten umfassen kön-

es jedoch schwierig sein zu bestimmen, welche Daten im Einzelfall übertragen werden dürfen und welche nicht.[420]

2. Betroffene Person hat die Daten dem Verantwortlichen bereitgestellt

126 Die Daten müssen von der betroffenen Person dem Verantwortlichen bereitgestellt («fournies», «forniti», «provided») worden sein. Wann genau Daten als bereitgestellt gelten, ist bislang nicht restlos geklärt und führt in der europäischen Literatur bis heute zu Diskussionen.[421] Die Voraussetzung wird denn auch unterschiedlich ausgelegt. Bereits begrifflich zeigen sich Schwierigkeiten und anders als im Schweizer Recht lässt sich die Voraussetzung nicht im Ausführungsrecht präzisieren.[422]

127 Bisweilen wird die Ansicht vertreten, dass lediglich «willentlich»[423] oder «wissentlich und willentlich»[424] durch die Betroffene dem Verantwortlichen zur Verfügung gestellte Daten vom Portabilitätsrecht erfasst seien – etwa durch das Ausfüllen eines Formulars.[425] Dass es sich bei solchen Daten um bereitgestellte Daten nach Art. 20 DSGVO handelt, ist in der Lehre seit jeher unbestritten.[426] Nach der mittlerweile wohl herrschenden Auffassung sind aber zusätzlich zu diesen aktiv bereitgestellten auch jene Daten umfasst, die aus der Beobachtung einer Tätigkeit einer Nutzerin (durch den Verantwortlichen) resultieren und dem Verantwortlichen damit auf passivem Weg zur Verfügung gestellt wurden.[427] Darunter können Daten fallen wie bspw. Suchverläufe, Ver-

nen. Für Betroffene kommt die DSGVO also meist gar nicht zur Anwendung; ähnlich DULLER, 134; a.A. jedoch hinsichtlich eines E-Mail-Accounts HERMONIES, Rz. 76; kritisch auch BeckKomm-HERBST, Art. 20 DSGVO N 11 m.w.N.

420 So das anschauliche Beispiel der Übertragung von Fahrzeugdaten eines Fahrers an den (dritten) Halter SCHÄTZLE, PinG 2016, 74 f.

421 Den Meinungsstand aufzeigend PAAL/GÖTZ, ZD 2023, 68 f.; BeckOK DSR-VON LEWINSKI, Art. 20 DSGVO N 38 ff.

422 Dazu Rz. 176 ff.

423 NomosKomm-DIX, Art. 20 DSGVO N 8.

424 KUKO DSGVO-KAMANN/BRAUN, Art. 20 N 14.

425 GRAEF/HUSOVEC/PURTOVA, GLJ 2018, 1372; BeckOK DSR-VON LEWINSKI, Art. 20 DSGVO N 41.

426 Dabei handelt es sich regelmässig um sog. Stammdaten, die bspw. über ein Patientenformular beim Spitalbesuch oder im Rahmen einer Anmeldung für ein neues Kundekonto in einem Onlineshop erhoben werden, BeckOK DSR-VON LEWINSKI, Art. 20 DSGVO N 41.

427 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 12; diese Haltung vertritt auch der neue EDSA, der die Artikel 29-Datenschutzgruppe 2018 ablöste, siehe EDSA, 38 f.; ferner DE HERT et al., CSLR 2018, 200; DULLER, 132 f.; ELFERING, 27 f.; BeckKomm-HERBST, Art. 20 DSGVO N 11, der beobachtete Daten dazuzählt, soweit die betroffene Person von

kehrs- oder Standortdaten sowie gewisse gesundheitsbezogene Daten, wie Puls und Herzfrequenz.[428]

Nicht unter den Begriff des «Bereitstellens» fallen gemäss dieser Auslegung bloss abgeleitete Daten.[429] Diese beinhalten personenbezogene Daten, welche ein Verantwortlicher erzeugt hat, bspw. algorithmische Ergebnisse.[430] Abgeleitete Daten werden aus bereits bereitgestellten Daten erzeugt und damit aus anderen (ihrerseits oft personenbezogenen) Daten abgeleitet.[431] Sie können, anders als beobachtete Daten, nur mit zusätzlichem Aufwand – etwa einer analytischen Auswertung – produziert werden.[432] Die Lehre ist sich einig darin, dass solche abgeleitete Daten nicht vom Recht auf Datenportabilität erfasst sind.[433] 128

der Datenerfassung Kenntnis hat und die Offenlegung bewusst zulässt; Jülicher/Röttgen/v. Schönfeld, ZD 2016, 359; ReMKomm-Spindler/Dalby, Art. 20 DSGVO N 7, die zwar einräumen, dass der Begriff der Bereitstellung tatsächlich ein aktives Tun nahelege, die Bestimmung jedoch im Zeitalter des Internet of Things der technischen Wirklich entsprechend ausgelegt werden müsse, weswegen die Vorstellung eines «aktiven» Betätigens eines Knopfs zur Übermittlung antiquiert sei; BeckOK IT-Recht-Steinrötter, Art. 20 DSGVO N 20; Tombal, 514 f., mit der Begründung, dass es sich bei beobachteten Daten um solche handelt für die es keinen eigenen Leistungsschritt des Verantwortlichen bedürfe und dass es dem Nutzer oft genau auf die Erhebung dieser Daten ankomme; wohl auch Nebel, ZD-Aktuell 2019, 04380.

428 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 11.

429 Die englischsprachige Literatur nimmt bei abgeleiteten Daten teilweise ausserdem noch eine weitere Unterscheidung vor, wohl zurückgehend auf OECD Committee, Expert Roundtable, 5. Diese erstellten eine Taxonomie basierend auf der Herkunft von Daten und unterscheiden dabei zwischen «provided», «observed», «derived» und «inferred» data. «Derived data» wird dabei auf eine «mechanische», mathematischen Prinzipien folgende Weise aus bestehenden Daten abgeleitet, z.B. die Profitabilität eines Kunden basierend auf dem Verhältnis seiner Besuche und tatsächlicher Einkäufe. «Inferred data» soll demgegenüber das Resultat probabilistischer analytischer Prozesse sein, die auf bestehenden Daten basieren, z.B. individuelle Lebenserwartung oder Bonitätsscore. Siehe ebenfalls OECD, Data Portability, 11; Graef/Husovec/Purtova, GLJ 2018, 1373.

430 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 12; kritisch Strubel, ZD 2017, 355 ff.

431 Strubel, ZD 2017, 357.

432 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 12; Graef/Husovec/Purtova, GLJ 2018, 1372.

433 BeckKomm-Herbst, Art. 20 DSGVO N 11; Janal, 327; BeckKompaktKomm-Paal, Art. 20 DSGVO N 17; GK-Piltz, Art. 20 DSGVO N 18; ReMKomm-Spindler/Dalby, Art. 20 DSGVO N 8; siehe auch die (seltene) Rechtsprechung, etwa VG Weimar, Beschluss vom 2. März 2021 – 3 E 209/21 We, E. 1a.

3. Berechtigter Grund der Verarbeitung

129 Art. 20 Abs. 1 lit. a DSGVO stellt klar, dass das Recht auf Datenportabilität nur anwendbar ist, wenn die betroffene Person die Daten mit ihrer Einwilligung zur Verfügung gestellt hat oder die Verarbeitung zur Erfüllung eines Vertrags erforderlich ist. Entsprechend kann das Recht gemäss Erw.G 68 DSGVO «naturgemäss» nicht gegen Verantwortliche ausgeübt werden, die Personendaten in Erfüllung ihrer öffentlichen Aufgaben verarbeiten. Es gilt damit nicht, wenn die Verarbeitung der Personendaten zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, welcher der Verantwortliche unterliegt, oder die für die Wahrnehmung einer ihm übertragenen Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung einer ihm übertragenen öffentlichen Gewalt erfolgt (Erw.G 68 DSGVO). Das Recht auf Datenportabilität kann nur ausgeübt werden, wenn sich die Datenbearbeitung auf eine der beiden in lit. a genannten Rechtmässigkeitsbedingungen stützt.[434]

a. Verarbeitung beruht auf einer Einwilligung

130 Die Verarbeitung kann auf einer Einwilligung beruhen. Je nach Art der verarbeiteten Daten muss somit die Rechtmässigkeitsbedingung gemäss Art. 6 Abs. 1 lit. a (für gewöhnliche Personendaten) oder Art. 9 Abs. 2 lit. a DSGVO (für besondere Kategorien von Personendaten) erfüllt sein. Nicht aufgrund einer Einwilligung (und auch nicht aufgrund eines Vertrags) werden etwa Personendaten durch ein Finanzinstitut verarbeitet, wenn es damit seiner Pflicht zur Verhinderung von Geldwäsche nachkommt.[435] Betroffene können eine Einwilligung auch gegenüber Behörden abgeben, obwohl die Norm primär auf privatrechtliche Verhältnisse zugeschnitten ist.[436]

131 Nicht geklärt ist die Frage, ob bei einer unwirksamen Einwilligung der Anspruch entfallen soll.[437] Dagegen spricht, dass die Verarbeitung an sich in dieser Konstellation, vorbehältlich anderer Rechtmässigkeitsbedingungen, nicht rechtmässig war und es dem Verantwortlichen grundsätzlich obliegt, der Betroffenen die Ausübung ihres Rechts nach Art. 20 DSGVO zu erleichtern (Art. 12 Abs. 2 DSGVO).[438] Wird eine Einwilligung widerrufen, ist ein Portie-

434 Kritisch dazu Hustinx, Rz. 151.

435 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 9 f.

436 BeckOK DSR-von Lewinski, Art. 20 DSGVO N 34; dazu Rz. 166 f.

437 Westphal/Wichtermann, ZD 2019, 194; insgesamt ebenfalls kritisch GK-Piltz, Art. 20 DSGVO N 20.

438 Ähnlich BeckOK DSR-von Lewinski, Art. 20 DSGVO N 36; i.E. gleich BeckOK IT-Recht-Steinrötter, Art. 20 DSGVO N 24; ReMKomm-Spindler/Dalby, Art. 20 DSGVO N 4.

rungsanspruch jedenfalls für die bis zum Zeitpunkt des Widerrufs bereitgestellten Daten anzunehmen.[439]

b. Verarbeitung beruht auf einem Vertrag

Alternativ steht das Recht auf Datenportabilität offen, wenn die Datenverarbeitung auf einem Vertrag gemäss Art. 6 Abs. 1 lit. b DSGVO beruht. Beispiele dafür sind Buchtitel, die eine Betroffene in einer Online-Buchhandlung gekauft hat, oder Lieder, die sie über einen Musik-Streaming-Dienst gehört hat.[440] Anders als der Verordnungstext hält Erw.G 68 DSGVO fest, dass die Verarbeitung «zur Erfüllung eines Vertrags erforderlich» sein soll, was die Frage aufwirft, ob auch bereits vorvertragliche Datenverarbeitungen vom Anwendungsbereich der Bestimmung gedeckt sind.[441] 132

Unklar ist zudem, ob die Betroffene ihr Portabilitätsrecht noch ausüben kann, nachdem das Vertragsverhältnis beendet ist. Da sich die Rechtmässigkeit nach Beendigung nicht mehr auf den Vertrag (oder eine Einwilligung) stützen lässt, sondern etwa zur Erfüllung rechtlicher Verpflichtungen erforderlich ist (Art. 6 Abs. 1 lit. c DSGVO), könnte der Anspruch der Betroffenen auf Übertragung der Daten dahinfallen. Dies scheint mit Blick auf die Entstehungsgeschichte und Zielsetzung des Instituts allerdings unbefriedigend: Genau in solchen Fällen sollte das Recht auf Datenportabilität zur Anwendung gelangen, weil etwa eine Betroffene im Hinblick auf einen Anbieterwechsel den Vertrag kündigt.[442] Somit erschiene es formalistisch zu verlangen, dass sie ihr Recht *vor* Beendigung des Vertragsverhältnisses ausübt. 133

Auch wenn die Norm primär auf privatrechtliche Verhältnisse zugeschnitten ist, kann die Verarbeitung auf öffentlich-rechtlichen Verträgen beruhen.[443] In diesem Fall kann auch eine Behörde verpflichtet sein.[444] 134

439 Fix, 116.

440 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 9.

441 Befürwortend BeckOK IT-Recht-Steinrötter, Art. 20 DSGVO N 24; ReMKomm-Spindler/Dalby, Art. 20 DSGVO N 4, jedoch mit anderer Begründung; ablehnend mit Blick auf ebendiesen Erw.G 68 DSGVO etwa Fix, 114 f.; KUKO DSGVO-Kamann/Braun, Art. 20 N 19; Menz, Rz. 35.

442 Fix, 116 ff.; KRKomm-Munz, Art. 20 DSGVO N 32; i.E. ähnlich auch NomosKomm-Dix, Art. 20 DSGVO N 9.

443 BeckOK DSR-von Lewinski, Art. 20 DSGVO N 34.

444 BeckOK IT-Recht-Steinrötter, Art. 20 DSGVO N 24.

4. Verarbeitung erfolgt mithilfe automatisierter Verfahren

135 Die Verarbeitung der personenbezogenen Daten muss mithilfe automatisierter Verfahren erfolgen (Art. 20 Abs. 1 lit. b DSGVO). Dies schränkt den sachlichen Anwendungsbereich ein. Die DSGVO gilt grundsätzlich auch für nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Art. 2 Abs. 1 DSGVO). Darunter fallen die meisten Dokumente in Papierform, etwa ein manuelles Karteikartensystem.[445] Solche Verarbeitungen erfasst das Recht auf Datenportabilität jedoch nicht. Nur wenn eine Datenverarbeitungsanlage eingesetzt wird, liegt ein automatisiertes Verfahren vor. Solche sind heute stets in der Lage, automatisierte Auswertungen durchzuführen.[446] Verlangt wird somit ein computergestütztes Verfahren, auch wenn der EU-Gesetzgeber einen technologieneutralen Begriff verwendet hat.[447] Diese Voraussetzung dürfte heute nur selten nicht erfüllt sein. Denkbar sind etwa handschriftliche Akten im Medizinbereich.

5. Rechtsfolge: Übertragung

136 Sind die Voraussetzungen erfüllt, kann die Betroffene die personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format erhalten. Dies soll sie befähigen, die Daten problemlos weiterzuverarbeiten und sie der neuen Verantwortlichen so zur Verfügung zu stellen, dass eine sofortige Weiterverarbeitung möglich ist.[448] Die Betroffene kann dabei wählen, ob sie die sie betreffenden personenbezogenen Daten selbst erhalten möchte (Art. 20 Abs. 1 DSGVO) oder ob die Daten direkt vom alten zur neuen Verantwortlichen übermittelt werden sollen, soweit dies technisch machbar ist (Abs. 2).

a. Indirekte Übertragung

137 Art. 20 Abs. 1 DSGVO sieht vor, dass die Betroffene das Recht hat, die sie betreffenden Daten zu erhalten und diese einer anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten

445 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 10; BeckOK IT-Recht-Steinrötter, Art. 20 DSGVO N 25.

446 Jülicher/Röttgen/v. Schönfeld, ZD 2016, 359; BeckOK IT-Recht-Steinrötter, Art. 20 DSGVO N 25.

447 Thouvenin/Weber/Früh, 148.

448 NomosKomm-Dix, Art. 20 DSGVO N 11.

bereitgestellt wurden, zu übermitteln. Bei der indirekten Übertragung finden also die personenbezogenen Daten ihren Weg zunächst zur betroffenen Person und anschliessend zur neuen Verantwortlichen. Abs. 1 enthält dabei zwei Elemente: Einerseits den unmittelbar geltenden Anspruch gegen den alten Verantwortlichen auf Übermittlung der Daten oder auf eine sonstige Form der Bereitstellung.[449] Andererseits hat die Betroffene das Recht, die Daten einer anderen Verantwortlichen zu übermitteln, ohne dabei durch den alten Verantwortlichen behindert zu werden.

Als Behinderung fällt jede rechtliche, technische oder finanzielle Hürde in Betracht, mit welcher der Datenzugriff, die Datenübertragung oder die Datenwiederverwendung verlangsamt oder verhindert wird.[450] Eine solche Hürde können vertragliche Abreden darstellen, wonach die Daten gegen Vergünstigungen nicht an Wettbewerberinnen weitergegeben werden dürfen.[451] Jedenfalls nach Vertragsbeendigung dürften solche Abreden eine Behinderung darstellen.[452] Gleichwohl darf nicht jede «Verhinderung» als unzulässige Behinderung gelten: Zulässig sind notwendige technische Hürden (etwa eine gewisse Zeitdauer, um die bereitzustellenden Daten zusammenzustellen) aber auch Anreize, damit die betroffene Person nicht abwandert (bspw. ein günstigeres Vertragsangebot).[453] 138

Nach der Übertragung der Daten ist die Empfängerin und nicht mehr der alte Verantwortliche für die übermittelten Daten verantwortlich.[454] Die neue Verantwortliche hat sicherzustellen, dass für die Datenbearbeitung ein Ermächtigungstatbestand vorliegt und dass die Vorgaben zur Gewährleistung der Datensicherheit befolgt werden.[455] 139

b. Direkte Übertragung

Die Betroffene kann nach Art. 20 Abs. 2 DSGVO erwirken, dass der alte Verantwortliche die Daten direkt an die neue Verantwortliche übermittelt, «soweit 140

449 KUKO DSGVO-Kamann/Braun, Art. 20 N 21.

450 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 18; ausführlich Fix, 210 ff.; davon ausgehend, dass vorwiegend technische Behinderungen untersagt und etwa rechtliche Behinderungen nicht ausgeschlossen seien Durmus/Kaplan, DSB 2023, 204.

451 Schätzle, PinG 2016, 73.

452 Schätzle, PinG 2016, 73; wohl ebenso Krause, PinG 2019, 15.

453 BeckKomm-Herbst, Art. 20 DSGVO N 22; siehe auch Krause, PinG 2019, 16, der es für zulässig erachtet, die Datenübertragbarkeit mit einem Feedback-Bogen zu koppeln.

454 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 6. Dies gilt selbstredend nur für die portierten Daten. Soweit der alte Verantwortliche diese Daten auch weiterhin bei sich bearbeitet, indem er sie etwa aufbewahrt, bleibt er für diese verantwortlich.

455 Nebel, ZD-Aktuell 2019, 04380.

dies technisch machbar ist». Die direkte Übertragung soll den Wechsel der Anbieterin im Vergleich zu Art. 20 Abs. 1 DSGVO noch einmal erleichtern und ein höheres Sicherheitsniveau ermöglichen, da der Datentransfer um eine Übermittlungsaktion verkürzt wird.[456] Denkbar ist, dass eine automatisierte Übermittlung angestossen wird, wenn die betroffene Person dies verlangt, etwa durch Anklicken eines entsprechenden Felds bei der Nutzung des Diensts des alten Verantwortlichen.[457] Entgegen dem Wortlaut der Bestimmung («von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden») muss der alte Verantwortliche nicht selbst tätig werden, sondern kann bspw. für häufig genutzte Portierungen eine API anbieten, die eine automatisierte Datenübertragung zu anderen Systemen erlaubt.[458] Die Betroffene sollte dabei einzelne Daten ausschliessen können, die nicht an die neue Verantwortliche übermittelt werden sollen.[459] Damit wird die Betroffene gegenüber der indirekten Übertragung, wo sie entsprechende Anpassungen und Einschränkungen eigenständig ebenfalls vornehmen kann, nicht schlechter gestellt.

141 Fraglich ist, was der Einschub «soweit dies technisch machbar ist» bedeutet. Es lässt sich einwenden, dass jede Übertragung, die von einem alten Verantwortlichen an die Betroffene möglich ist – und genau dieses Recht umfasst Abs. 1 – auch nach Abs. 2 für den alten Verantwortlichen «technisch machbar» sein sollte.[460] Zielführend ist es daher anzunehmen, dass die technische Machbarkeit sich auf alte *und* neue Verantwortliche beziehen muss. Sie besteht damit aus der Machbarkeit der Übermittlung durch den alten Verantwortlichen und der Kompatibilität der Datenverarbeitungssysteme des alten und der neuen Verantwortlichen.[461] Darin wird teils ein Bezug zur Interoperabilität gesehen, welche auch durch die Erwähnung der Interoperabilität in Erw.G 68 DSGVO bestätigt wird.[462] Gleichwohl ist darin keine Interoperabilitätsverpflichtung zu sehen. Wie Erw.G 68 DSGVO ebenfalls festhält, begründet das Recht der betroffenen Person nicht die Pflicht, technisch kompatible Datenverarbeitungssysteme zu übernehmen oder beizubehalten. Entsprechend ist die neue Verantwortliche nicht verpflichtet, ein kompatibles System bereitzustellen. Tut sie dies jedoch, so ist es technisch machbar, die Daten i.S.v. Art. 20

456 BeckKomm-Herbst, Art. 20 DSGVO N 24; Krause, PinG 2019, 19; dazu Rz. 118 ff.
457 BeckKomm-Herbst, Art. 20 DSGVO N 25.
458 BeckKomm-Herbst, Art. 20 DSGVO N 25; Krause, PinG 2019, 19.
459 Krause, PinG 2019, 19.
460 In diese Richtung Janal, 339.
461 Krause, PinG 2019, 19.
462 Janal, 339. So weit wie Erw.G 68 DSGVO, der festhält, die betroffene Person habe ein Recht, die sie betreffenden Daten «in einem [...] interoperablen Format zu erhalten [...]», dürfte die Vorgabe jedoch nicht gehen. Zur Interoperabilität Rz. 113 f. und Rz. 154 f.

Abs. 2 DSGVO zu portieren.[463] Die Voraussetzung bezieht sich damit auch auf Eigenschaften der neuen Verantwortlichen, ohne diese in die Pflicht zu nehmen. Denn das Recht auf Übermittlung begründet keine Pflicht der (potenziell) neuen Verantwortlichen, die Daten tatsächlich entgegenzunehmen. Ob diese die Daten entgegennehmen möchte, bleibt allein ihr überlassen.[464]

Der zeitliche und wirtschaftliche Aufwand, den ein Verantwortlicher auf sich nehmen muss, um die direkte Übertragung zu ermöglichen, ist im Einzelfall unter Würdigung der Umstände zu bewerten.[465] Allerdings wurden subjektive Umstände des (alten) Verantwortlichen nicht in die endgültige Fassung aufgenommen, weshalb sie i.d.R. nicht zu berücksichtigen sind.[466] Entsprechend ist das Kriterium eng auszulegen. Nach hier vertretener Ansicht ist eine Übermittlung nach Art. 20 Abs. 2 DSGVO nur in Ausnahmefällen aufgrund subjektiver Umstände des alten Verantwortlichen als nicht technisch machbar zu betrachten.[467] In aller Regel muss auf die Voraussetzungen nach Abs. 1 abgestellt werden. Da die Regelung in Abs. 2 Bezug auf den ersten Absatz nimmt, sind die dort aufgeführten Voraussetzungen, namentlich das Behinderungsverbot, ebenfalls stets zu erfüllen.[468] 142

463 Klink-Straub/Straub, ZD 2018, 462, die die technische Machbarkeit als erfüllt ansehen, wenn beide Verantwortlichen ein «gemeinsames Datenformat» unterstützen.

464 Brüggemann, 11; BeckKomm-Herbst, Art. 20 DSGVO N 22; Krause, PinG 2019; KUKO DSGVO-Kamann/Braun, Art. 20 N 28 und 32 m.w.N.; KRKomm-Munz, Art. 20 DSGVO N 44; BeckKompaktKomm-Paal, Art. 20 DSGVO N 22; BeckOK DSR-von Lewinski, Art. 20 DSGVO N 57; wohl a.A. Hermonies, Rz. 83; wohl ebenso a.A. GK-Piltz, Art. 20 DSGVO N 31; mit Hinweis auf den wettbewerbsbeeinflussenden Charakter der Norm eher eine Pflicht befürwortend zudem Jülicher/Röttgen/v. Schönfeld, ZD 2016, 362; differenzierend NomosKomm-Dix, Art. 20 DSGVO N 15, wonach bei einem Vertragsverhältnis mit der neuen Verantwortlichen diese eine grundsätzliche Kooperationspflicht habe und gängige, maschinenlesbare Daten nicht ablehnen dürfe.

465 KUKO DSGVO-Kamann/Braun, Art. 20 N 31; Reichlin, 411.

466 Siehe den Wortlaut von Abs. 2 im Entwurf gemäss Rat der Europäischen Union, Ratsdokument 14481/15 vom 27. November 2015, 95, der lautete «where technically feasible and available, or unless this would involve disproportionate efforts for the controllers». Dieser Einschub wurde in der endgültigen Fassung entfernt und lediglich «technically feasible» beibehalten. Etwas anders die Schweizer Regelung, siehe dazu Rz. 202.

467 Nicht allzu hohe Anforderungen an die technische Machbarkeit stellen Klink-Straub/Straub, ZD 2018, 462; Reichlin, 411. Schlechthin «irrelevant» ist das Kriterium der wirtschaftlichen Zumutbarkeit, siehe ReMKomm-Spindler/Dalby, Art. 20 DSGVO N 11; gleicher Ansicht mit dem Hinweis, dass wirtschaftliche Verhältnismässigkeitsabwägungen während des Gesetzgebungsprozesses verworfen wurden GK-Piltz, Art. 20 DSGVO N 31.

468 Krause, PinG 2019, 19; KRKomm-Munz, Art. 20 DSGVO N 45.

c. Form

aa. Strukturiertheit

143 Die Personendaten müssen strukturiert sein. Gemeint ist damit die Anordnung der Daten bzw. der darin enthaltenen Informationen.[469] Die genaue Tragweite dieser Voraussetzung ist jedoch unklar. Einerseits wird vertreten, dass jeder Datensatz notwendigerweise über eine Struktur verfügt, weshalb dieses Tatbestandsmerkmal wenig relevant sei.[470] Andererseits wird argumentiert, dass, gerade weil elektronische Datensätze immer strukturiert seien, eine darüber hinausgehende Struktur verlangt werde.[471] Mit Blick auf die Betroffene wird auch gefordert, dass die Strukturiertheit des Datensatzes dafür sorgen müsse, dass der Inhalt des Datensatzes primär für die Betroffene nachvollziehbar sei, sodass diese entscheiden könne, wie mit ihren Daten zu verfahren sei.[472] Dies kann allerdings von vornherein nur gelten, wenn die Betroffene keine direkte Übertragung wünscht.

144 Ob ein Datensatz die notwendige Strukturiertheit aufweist, ist im Einzelfall und mit Blick auf den jeweiligen Sektor zu beantworten.[473] Die zumeist wohl nur graduellen Unterschiede lassen sich dabei am besten anhand von Beispielen erklären. So ist anzunehmen, dass etwa PDF-Fassungen eines E-Mail-Posteingangs die notwendige Strukturiertheit nicht erreichen würden.[474] Sie wären als Ansammlung von .pdf-Dateien in einer einfachen Ordnerstruktur zu wenig strukturiert, um den Anforderungen von Art. 20 Abs. 1 DSGVO zu genügen. Ausreichend strukturiert wäre ein solcher Datensatz allerdings, wenn Metadaten es erlaubten, die E-Mails chronologisch (oder anderweitig) zu ordnen.[475] So enthalten .eml-Dateien oder .msg-Dateien etwa weitgehende Metadaten, namentlich bezüglich Versanddatum, Absenderin und Empfängerin. Diese können das Erfordernis der Strukturiertheit erfüllen (siehe Anhang 1). Notwendig ist dafür jedoch, dass neben der einzelnen E-Mail (etwa im .eml-Format) auch die Summe an E-Mails (d.h. der ganze Posteingang) strukturiert ge-

469 Fix, 193 f.; GK-Piltz, Art. 20 DSGVO N 26; BeckOK DSR-von Lewinski, Art. 20 DSGVO N 70 m.w.H.

470 Hennemann, PinG 2017, 7.

471 Schätzle, PinG 2016, 74.

472 Fix, 196; siehe auch BeckOK DSR-von Lewinski, Art. 20 DSGVO N 71.

473 BeckOK DSR-von Lewinski, Art. 20 DSGVO N 73.

474 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 21; ebenso Beck-Komm-Herbst, Art. 20 DSGVO N 20; NomosKomm-Dix, Art. 20 DSGVO N 11.

475 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 21; ähnlich auch Brorsen/Falk, MMR 2025, 9.

liefert wird. Dafür dürfte eine übliche Ordnerstruktur, wie sie von den gängigen Betriebssystemen bekannt ist, ausreichen.[476]

bb. Gängigkeit

Das Format muss gängig («couramment utilisé», «di uso comune», «commonly used») sein. Es wird mithin darauf abgestellt, welches Format im relevanten Sektor allgemein gebräuchlich und verbreitet ist. Es muss sich um ein auf dem Markt bekanntes und oft genutztes Format handeln, wobei mehrere Formate gängig sein können.[477] Dabei ist den sektorspezifischen Besonderheiten Rechnung zu tragen: Eine .dcm-Datei mag für eine Patientin ungewöhnlich sein, ist aber in der medizinischen Datenbearbeitung und besonders in der Radiologie durchaus gängig.[478] Die Gängigkeit ist aus Sicht des alten Verantwortlichen zu beurteilen. Die Betroffene muss es sich gefallen lassen, wenn sie in einer bestimmten Branche nicht spezialisiert ist. Dies zeigt sich auch daran, dass Art. 20 DSGVO primär auf eine Weiterverwendung der portierten Daten durch Dritte abzielt und nicht ausdrücklich eine unmittelbare Nutzung durch die Betroffene vorsieht. Der Markt sollte zudem nicht geographisch, sondern sektorspezifisch abgegrenzt werden.[479] 145

Nicht gleichzusetzen ist die Gängigkeit mit dem Stand der Technik. Es geht nicht darum, was am «besten» erscheint, sondern was am verbreitetsten ist und sich damit praktisch bewährt hat.[480] Proprietäre Formate, die möglicherweise nur zu hohen Kosten lizenzierbar sind, sind nicht gängig, ebenso wenig wie lediglich intern verwendete Formate.[481] Umgekehrt sind offene Formate nicht per se gängig, sondern müssen auf dem Markt allgemein gebräuchlich und verbreitet sein.[482] 146

Gibt es in einem Sektor noch keine gängigen Formate, etwa, weil dieser erst im Entstehen ist, sollte auf gemeinhin verwendete offene Formate, die sich be- 147

476 Ebenso SCHNEIDER, Rz. 120.

477 GK-PILTZ, Art. 20 DSGVO N 26; BeckOK DSR-VON LEWINSKI, Art. 20 DSGVO N 76.

478 FIX, 316 f.; DREPPER/SCHLÜNDER/BUCKOW, 189; zum Dateiformat weitergehend https://perma.cc/T94Q-BY7U.

479 KRAUSE, PinG 2019, 15; SCHNEIDER, Rz. 122 f.; siehe auch FIX, 184.

480 KRAUSE, PinG 2019, 15; den Stand der Technik aber berücksichtigend FIX, 181 m.w.N.

481 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 21; KRAUSE, PinG 2019, 14; BeckOK DSR-VON LEWINSKI, Art. 20 DSGVO N 77; a.A. hingegen FIX, 187 m.w.N., nach welchem auch proprietäre, verbreitete Formate grundsätzlich das Merkmal der Gängigkeit erfüllen können.

482 BeckOK DSR-VON LEWINSKI, Art. 20 DSGVO N 77.

reits sektorübergreifend etabliert haben, zurückgegriffen werden.[483] Solche Datenformate, die darauf ausgelegt sind, beliebige Daten zwischen verschiedenen IT-Systemen auszutauschen, können i.d.R. als gängig anerkannt werden.[484] Zudem ist zu bedenken, dass Verantwortliche kaum auf unternehmerisch sinnvolle Formate verzichten werden, bloss um Ansprüchen auf Datenübertragbarkeit entgehen zu können.[485]

148 Bereits erwähnt wurde, dass das Portabilitätsrecht entstehungsgeschichtlich nicht nur auf Datenübermittlungen zwischen gleichartigen, sondern auch zwischen andersartigen Verantwortlichen abzielte.[486] Dem steht die Voraussetzung der Gängigkeit nach dem eben dargelegten Verständnis allerdings entgegen. Eine sektorspezifische Prüfung des Kriteriums seitens des alten Verantwortlichen wird kaum ein gängiges Format in einem völlig anderen Sektor hervorbringen.[487] Eine Orientierung an der neuen Verantwortlichen wiederum lässt sich kaum fordern.[488] Damit kann das Erfordernis der Gängigkeit bei einer Portierung zu einer andersartigen Anbieterin ein tatsächliches Hindernis darstellen.[489]

149 Art. 18 Abs. 3 E-DSGVO sah noch vor, dass die EU-Kommission das elektronische Format festlegen kann. Eine solche Standardisierung findet sich in der endgültigen Version nicht mehr. Wenngleich diese Flexibilität angesichts rascher technologischer Entwicklungen zu begrüssen ist, kann sie zu praktischen Problemen führen, wenn Uneinigkeit über die Gängigkeit eines Formats besteht. Zudem kann sich die Situation ergeben, dass der alte Verantwortliche ein gängiges Format benutzt und die neue Verantwortliche ein anderes, jedoch ebenfalls gängiges Format. Beide Formate sind dann gängig, die Daten aber u.U. nur erschwert übertragbar.[490]

cc. Maschinenlesbarkeit

150 Die DSGVO definiert den Begriff «maschinenlesbar» («lisible par machine», «leggibile da dispositivo automatico», «machine-readable») nicht. Nach dem

483 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 21. Genannt werden etwa XML, JSON oder CSV.
484 Schneider, Rz. 123.
485 HK DSGVO-Sydow/Wilhelm-Robertson, Art. 20 N 14.
486 Dazu Rz. 90.
487 Ähnlich Fix, 188.
488 Fix, 188.
489 Fix, 188 f.
490 Krause, PinG 2019, 15; Schätzle, PinG 2016, 74; dazu auch Rz. 106 f.

Unionsrecht ist ein maschinenlesbares Format hingegen «[…] so strukturiert […], dass Softwareanwendungen konkrete Daten, einschließlich einzelner Sachverhaltsdarstellungen und deren interner Struktur, leicht identifizieren, erkennen und extrahieren können» (Art. 2 Ziff. 13 der RL 2019/1024).[491] Dokumente sollten demnach als maschinenlesbar gelten, wenn sie in einem Dateiformat vorliegen, das so strukturiert ist, dass Softwareanwendungen die konkreten Daten einfach identifizieren, erkennen und extrahieren können (Erw.G 35 der RL 2019/1024). Die Maschinenlesbarkeit stellt somit ein eigentliches «Formerfordernis» für die digitale Gesellschaft dar, welche erst eine maschinelle Verarbeitung von Informationen durch Computer ermöglicht.[492] Die Voraussetzung zeigt, dass das Portabilitätsrecht nur elektronische Datenverarbeitungen erfassen soll und grenzt das Institut von rein analogen Auskünften ab.

Unklar ist, ob analoge Formate wie Papierausdrücke oder PDF-Dateien ebenfalls maschinenlesbar sind. Mit heutiger Technik können solche Aufzeichnungen ohne Weiteres mittels Texterkennungssoftware (sog. OCR) durch eine Maschine gelesen und anschliessend weiterverarbeitet werden. Entsprechend wird in der Literatur auch die Haltung vertreten, dass diese Formate den Anforderungen an die Maschinenlesbarkeit genügten.[493] Wird berücksichtigt, dass beim Auskunftsrecht nach Art. 15 DSGVO die Informationen in einem «gängigen elektronischen Format» (Abs. 3) zur Verfügung zu stellen sind, erscheint der Anwendungsbereich tatsächlich weiter.[494] 151

Die blosse Möglichkeit, die Extraktion der Daten auch maschinell auszuführen, sollte m.E. jedoch nicht ausreichen, um ein Format als maschinenlesbar zu betrachten.[495] Dem Kriterium käme aufgrund der neuen technischen Möglichkeiten nahezu keine Bedeutung mehr zu.[496] Zwar lassen sich die begrifflichen Unterschiede zum Auskunftsrecht nicht von der Hand weisen. Die Ausgangslage ist bei beiden Instrumenten jedoch unterschiedlich: Während das Auskunftsrecht der Informationsbefriedigung der betroffenen Person dient und 152

491 Sowohl die Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 20, als auch weitere Autoren verweisen auf diese Richtlinie resp. auf deren Vorgängerrichtlinien 2013/37/EU und 2003/98/EG, die jedoch von der zitierten Richtlinie abgelöst wurden (siehe Anhang II, Teil A der RL 2019/1024). Materiell ergeben sich daraus keine Änderungen. Auch der EuGH orientiert sich daran, siehe EuGH C-319/22 vom 9. November 2023, Rz. 15; dazu ferner Durchholz, PinG 2024, 210.

492 Brorsen/Falk, MMR 2025, 8.

493 Hennemann, PinG 2017, 7; KRKomm-Munz, Art. 20 DSGVO N 36.

494 KRKomm-Munz, Art. 20 DSGVO N 36.

495 Ebenso BeckOK DSR-von Lewinski, Art. 20 DSGVO N 75 f.; Schätzle, PinG 2016, 74.

496 KRKomm-Munz, Art. 20 DSGVO N 36 m.w.H.

damit prinzipiell technologieneutral ist,[497] ist das Recht auf Datenportabilität auf computergestützte Verfahren ausgerichtet.[498] Es wäre nicht schlüssig, solche Umgehungen zuzulassen, zumal die Datenportabilität wesentlich auf die Weiterverarbeitung der Personendaten abzielt und dem normalen Sprachgebrauch entsprechend ein Ausdruck auch nicht als «Format» qualifiziert werden kann. Das Portabilitätsrecht soll eine reibungslose Datenübertragung ermöglichen, was nicht der Fall ist, wenn zunächst eine OCR-Umwandlung erfolgen muss.[499]

153 Anzufügen ist, dass sich dogmatisch das Kriterium der Gängigkeit als Korrektiv nutzen liesse, wenn die Maschinenlesbarkeit von Computerausdrucken bejaht werden sollte: Ein Ausdruck, gefolgt von einer anschliessenden OCR, dürfte zwar gelegentlich vorkommen. Allerdings ist diese Vorgehensweise eher unüblich und jedenfalls nicht gängig, auch wenn nicht der Stand der Technik als Massstab gelten darf.[500] In jedem Fall sollten Ausdrucke also nach hier vertretener Ansicht nicht als maschinenlesbar gelten.

dd. Interoperabilität

154 Erw.G 68 DSGVO zählt neben der Strukturiertheit, Gängigkeit und Maschinenlesbarkeit zusätzlich die Interoperabilität auf. Die Betroffene soll demnach berechtigt sein, die Daten in einem «interoperablen Format zu erhalten und sie einem anderen Verantwortlichen zu übermitteln». Im nächsten Satz fordert Erw.G 68 DSGVO die Verantwortlichen sodann unmittelbar auf, interoperable Formate zu entwickeln. Die Interoperabilität ist jedoch keine Voraussetzung des Datenportabilitätsrechts und im Verordnungstext in Art. 20 DSGVO auch nicht aufgeführt.[501]

---

497 Der Verantwortliche muss die Auskunft nach Art. 15 Abs. 3 DSGVO nur in einem gängigen elektronischen Format erteilen, wenn bereits der Antrag elektronisch gestellt wurde.

498 Dies ergibt sich aus dem eingeschränkten Anwendungsbereich der Datenportabilität, die nur offensteht, wenn die Verarbeitung der zu portierenden Daten mithilfe automatisierter Verfahren erfolgt, siehe GK-Piltz, Art. 20 DSGVO N 23; dazu auch Rz. 135.

499 Brorsen/Falk, MMR 2025, 9; siehe auch BeckOK DSR-von Lewinski, Art. 20 DSGVO N 75 f., wonach ein Dokument nicht nur theoretisch für eine Weiterverwendung geeignet, sondern zu diesem Zweck auch konzeptioniert und bestimmt sein sollte.

500 Dazu Rz. 146.

501 Vgl. noch Art. 18 Ziff. 1 E-DSGVO, wonach die Betroffene Daten «in einem von ihr weiter verwendbaren strukturierten gängigen elektronischen Format» verlangen kann. Die finale Fassung hielt an diesem Wortlaut jedoch nicht fest. Siehe Hennemann, PinG 2017, 6; i.E. eine Interoperabilitätsvorgabe sieht hingegen Janal, 339; zur Interoperabilität Rz. 113 f.

Hierzu ist festzuhalten, dass ein «interoperables Format» noch keine (umfassende) Interoperabilität zwischen Systemen herbeizuführen vermag.[502] Eine technische Kompatibilität, die eine solche umfassende Interoperabilität herbeiführen würde, kann gestützt auf das Portabilitätsrecht nicht erzwungen werden – einzig die eben abgehandelten Voraussetzungen sind durch den alten Verantwortlichen zwingend einzuhalten.[503] Aus der Aufforderung, interoperable Formate zu entwickeln, lässt sich demnach einzig der Wunsch des Gesetzgebers ablesen, eine Interoperabilität zwischen Systemen herbeizuführen, während die Übertragbarkeit in einem strukturierten, gängigen und maschinenlesbaren Format ein Mittel für eine solche Zielerreichung darstellen soll.[504] Eine Interoperabilität stellt damit einen Zielzustand und nicht eine Voraussetzung dar. 155

d. Modalitäten

Der alte Verantwortliche muss der Betroffenen die Daten «unverzüglich» («dans les meilleurs délais», «senza ingiustificato ritardo», «without undue delay»), in jedem Fall aber innert eines Monats nach Eingang des Antrags zur Verfügung stellen (Art. 12 Abs. 3 DSGVO). Wenn es unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist, kann der Verantwortliche die Frist um weitere zwei Monate verlängern. Eine Pflicht zur Echtzeitübertragung von Daten besteht damit nicht.[505] Die Daten sind der Betroffenen unentgeltlich zu übertragen (Art. 12 Abs. 5 DSGVO).[506] 156

Die Form der Übermittlung gibt die DSGVO nicht vor. Denkbar ist alles, was die Betroffene in die Lage versetzt, ihre Daten zu erhalten – etwa das Zurverfügungstellen mittels Downloads (über ein Web-Portal oder einen SFTP-Server), oder das physische Übermitteln mittels Versands eines USB-Sticks.[507] 157

502 Überzeugend darauf hinweisend, dass nicht «ein Format» interoperabel ist, sondern dass sich unterschiedliche Systeme zueinander interoperabel verhalten können Fix, 198; siehe auch Elfering, 22; Krause, PinG 2019, 15.

503 BKartA, Sektoruntersuchung, 32.

504 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 20; ähnlich auch Durmus/Kaplan, DSB 2023, 204; Fix, 197 m.w.N.

505 Graef/Husovec/Van den Boom, EuCML 2020, 10; Janal, 339; Kerber/Gill, 96; Schallbruch et al., 40; Schweitzer, GRUR 2019, 576; Wendehorst/Schwamberger, DAR 2022, 543.

506 Weitergehend dazu Thouvenin/Weber/Früh, 148 f.

507 Siehe weitergehend Fix, 281 ff.; Krause, PinG 2019, 14.

6. Unberührtheit des Rechts auf Löschung nach Art. 17 DSGVO

158 Gemäss Art. 20 Abs. 3 Satz 1 DSGVO lässt die Ausübung des Rechts nach Art. 20 Abs. 1 DSGVO das Recht auf Löschung gemäss Art. 17 DSGVO unberührt. Da die direkte Übertragung nach Abs. 2 notwendigerweise auch die Voraussetzungen nach Abs. 1 umschliesst, findet die Bestimmung allerdings auch auf die direkte Übertragung Anwendung.[508]

159 Übt die betroffene Person das Recht auf Datenportabilität aus, entsteht dadurch beim alten Verantwortlichen keine Pflicht zur Löschung der Daten.[509] Eine Löschung kann etwa im Fall einer parallelen Nutzung des alten und des neuen Diensts oder auch beim sog. *Multi-Homing*[510] von der Betroffenen gar nicht gewünscht sein.[511] Das Portabilitätsrecht bedeutet «insbesondere nicht […], dass die Daten, die sich auf die betroffene Person beziehen und von ihr zur Erfüllung eines Vertrags zur Verfügung gestellt worden sind, gelöscht werden, soweit und solange diese personenbezogenen Daten für die Erfüllung des Vertrags notwendig sind» (Erw.G 68 DSGVO). Von der Ausübung des Rechts ist das (Vertrags-)Verhältnis zwischen betroffener Person und altem Verantwortlichen mithin nicht tangiert. Es ist insb. nicht als (konkludente) Kündigung zu verstehen.[512]

7. Nichtbeeinträchtigung der Rechte und Freiheiten anderer Personen

160 Nach Art. 20 Abs. 4 DSGVO darf das Recht gemäss Abs. 1 die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.[513] Erw.G 68 DSGVO konkreti-

508 KUKO DSGVO-Kamann/Braun, Art. 20 N 33.

509 Hennemann, PinG 2017, 7.

510 Der Begriff *Multi-Homing* wird in der Literatur uneinheitlich verwendet. Nach dem vorliegenden Verständnis geht es dabei um eine gleichzeitige Nutzung mehrere Dienste in bidirektionaler Weise und damit um eine Form von Interoperabilität. Nach einem anderen Verständnis geht es darum, dass zwei Dienste lediglich parallel, aber unabhängig voneinander genutzt werden. Die Nutzung des alten Diensts wird also nicht durch die Nutzung des neuen Diensts ersetzt. Siehe dazu Landolt, 156, insb. Fn. 672 sowie 193 m.w.N.

511 BeckOK IT-Recht-Steinrötter, Art. 20 DSGVO N 50.

512 Hennemann, PinG 2017, 7; Jülicher/Röttgen/v. Schönfeld, ZD 2016, 360; BeckOK IT-Recht-Steinrötter, Art. 20 DSGVO N 51.

513 Die deutsche Fassung der DSGVO verwies ursprünglich auf Abs. 2. Dieser Redaktionsfehler wurde in ABl. L 127 vom 23. Mai 2018 berichtigt. Die anderen Sprachfassungen verwiesen bereits initial auf Abs. 1, siehe KUKO DSGVO-Kamann/Braun, Art. 20 N 34.

siert, dass «das Recht auf Empfang der Daten die Grundrechte und Grundfreiheiten anderer betroffener Personen nach dieser Verordnung unberührt lassen» sollte, wenn Daten von mehr als einer Person tangiert sind.

Unklar ist aufgrund des Wortlauts, ob sich der (alte) Verantwortliche ebenfalls auf die Rechte und Freiheiten nach Abs. 4 berufen kann. Dafür spricht, dass Abs. 4 im Entwurf darauf zielte, «die Rechte an geistigem Eigentum unberührt» zu lassen.[514] Damit waren insb. die Rechte an geistigem Eigentum des Verantwortlichen gemeint.[515] Da das Recht auf Datenportabilität Risiken für das geistige Eigentum und die Geschäftsgeheimnisse des Verantwortlichen birgt, wird vertreten, dass die Rechte des Verantwortlichen ebenfalls berücksichtigt werden müssen.[516] Diesem Gedanken entsprechend könnte auch die finale Fassung die Rechte und Freiheiten (*in toto*) des Verantwortlichen umfassen. 161

Dagegen spricht aber Erw.G 68 DSGVO, der darauf hindeutet, dass mit «anderen Personen» Drittpersonen gemeint sind.[517] Zudem erwähnt die DSGVO den Verantwortlichen ansonsten ausdrücklich als solchen.[518] Da es dem Gesetzgeber offen gestanden wäre, nur auf betroffene Personen i.S.v. Art. 4 lit. 1 DSGVO und damit auch auf andere betroffene natürliche Personen zu verweisen, er dies aber nicht getan hat, ist davon auszugehen, dass Verantwortliche ebenfalls umfasst sind.[519] 162

Entsprechend können Betriebs- und Geschäftsgeheimnisse oder geistiges Eigentum (wie Urheberrechte) des alten Verantwortlichen die Übermittlung beschränken.[520] Der Verantwortliche kann sich aber nicht pauschal auf seine Rechte und Freiheiten berufen und damit das Recht auf Datenportabilität faktisch verhindern.[521] Vielmehr hat er dafür zu sorgen, dass das Recht gewährt werden kann und muss hierfür eine Abwägung vornehmen.[522] Dies deckt sich 163

514 Rat der Europäischen Union, Ratsdokument 11013/13 vom 21. Juni 2013, 100; KUKO DSGVO-Kamann/Braun, Art. 20 N 36.

515 KUKO DSGVO-Kamann/Braun, Art. 20 N 36.

516 KUKO DSGVO-Kamann/Braun, Art. 20 N 36.

517 BeckOK DSR-von Lewinski, Art. 20 DSGVO N 102.

518 BeckOK DSR-von Lewinski, Art. 20 DSGVO N 102.

519 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 14 f.; Brüggemann, 8; Klink-Straub/Straub, ZD 2018, 462; KRKomm-Munz, Art. 20 DSGVO N 53; GK-Piltz, Art. 20 DSGVO N 38; sich für einen Schutz sämtlicher geschützter Individualinteressen aussprechend BeckOK DSR-von Lewinski, Art. 20 DSGVO N 93; a.A. Elfering, 29.

520 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 14; NomosKomm-Dix, Art. 20 DSGVO N 18; KRKomm-Munz, Art. 20 DSGVO N 55 m.w.N.; HK DSGVO-Sydow/Wilhelm-Robertson, Art. 20 N 19.

521 NomosKomm-Dix, Art. 20 DSGVO N 18.

522 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 14; KUKO DSGVO-Kamann/Braun, Art. 20 N 36.

auch mit der allgemeinen Pflicht des Verantwortlichen nach Art. 12 Abs. 2 DSGVO, der Betroffenen die Ausübung ihrer Rechte zu erleichtern.

164 Eine weitere Problematik bei Abs. 4 liegt in der Rechtmässigkeit der Verarbeitung von Daten Dritter: Während für Daten der betroffenen Person die Rechtmässigkeit der Verarbeitung bei der neuen Verantwortlichen in der Einwilligung oder im Vertrag zu finden ist, liegt eine solche für Daten Dritter (i.d.R.) nicht vor. In solchen Konstellationen ist die Rechtmässigkeit allerdings gestützt auf das berechtigte Interesse gemäss Art. 6 Abs. 1 lit. f DSGVO denkbar, etwa wenn der Zweck der Verantwortlichen darin besteht, der Betroffenen einen Dienst bereitzustellen, der es ihr ermöglicht, personenbezogene Daten ausschliesslich zu persönlichen oder familiären Tätigkeiten zu verarbeiten.[523] Eine Verarbeitung von Daten soll in dem Umfang zulässig sein, in dem die Daten unter der alleinigen Kontrolle des anfragenden Nutzers bleiben und ausschliesslich für persönliche oder familiäre Zwecke verwaltet werden.[524] Die Nutzung der Drittdaten zu eigenen Zwecken, etwa um den Drittpersonen Marketingprodukte oder Dienste anzubieten, ist entsprechend unzulässig.[525]

165 Wenn der Zweck der Verarbeitung beim alten und bei der neuen Verantwortlichen identisch ist, dürfen die Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden.[526] Eine Beeinträchtigung der Rechte und Freiheiten Dritter sollte allerdings nicht vorschnell angenommen werden. Mit Blick auf die zu diskutierende wettbewerbsrechtliche Zielsetzung der Bestimmung muss Raum bleiben für eine sinnvolle Ausübung des Rechts auf Datenportabilität. Eine einseitig datenschutzrechtliche Auslegung liesse den wettbewerblichen Ansatz ins Leere laufen.[527]

---

523 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 13. Für die betroffene Person kommt dann gemäss Erw.G 18 DSGVO die DSGVO gar nicht zur Anwendung, da die sog. Haushaltsausnahme greift. Für den Verantwortlichen ist sie jedoch anwendbar.

524 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 13; NomosKomm-Dix, Art. 20 DSGVO N 18.

525 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 13 f.

526 BeckOK DSR-von Lewinski, Art. 20 DSGVO N 97. Dies ist etwa dann der Fall, wenn bei einer Portierung der Daten eines Bankkontos auch Transaktionen mit Bezug auf Drittpersonen weitergegeben werden. Sofern die Angaben über Drittpersonen weiterhin einzig als Kontaktadresse von der betroffenen Person verwendet wird, dürfte dies im Lichte von Abs. 4 unproblematisch sein, siehe Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 13.

527 BeckOK DSR-von Lewinski, Art. 20 DSGVO N 98; siehe auch Schantz, NJW 2016, 1845, der mit Verweis auf die wettbewerbspolitische Zielsetzung Daten, die Dritte betreffen, ausdrücklich zulassen möchte.

8. Weitere Einschränkungen

Das Portabilitätsrecht gilt nicht für Verarbeitungen, die auf einer anderen Rechtsgrundlage als einer Einwilligung oder einem Vertrag basieren. Dies ergibt sich bereits aus Art. 20 Abs. 1 lit. a DSGVO *e contrario*.[528] Dennoch erwähnt die DSGVO, dass das Recht nicht anwendbar ist für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (Art. 20 Abs. 3 Satz 2 DSGVO).[529] Damit bezieht sie sich auf die gleichlautende Rechtmässigkeitsbedingung in Art. 6 Abs. 1 lit. e DSGVO. Vom Recht auf Datenportabilität ausgeschlossen werden damit die Datenverarbeitungen der öffentlich-rechtlich tätigen Verwaltung und von nichtöffentlichen Stellen, die mit der Wahrnehmung öffentlicher Aufgaben betraut sind.[530] 166

Grund für diese Präzisierung ist, dass mehrere Rechtmässigkeitsbedingungen gleichzeitig vorliegen können und in diesem Fall eine Portierungsverpflichtung verhindert werden soll. In der Literatur wird dazu vorgebracht, dass bei Verantwortlichen, die öffentliche Aufgaben erfüllen, gerade keine Wettbewerbssituation auf Seiten der Verantwortlichen gefördert werden müsse.[531] Erw.G 68 DSGVO, der zusätzlich zur erwähnten Ausnahme für die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, eine Ausnahme vorsieht und sich dabei auf die Rechtmässigkeitsbedingung nach Art. 6 Abs. 1 lit. c DSGVO bezieht, wird als Redaktionsfehler betrachtet.[532] 167

Eine weitere Einschränkung des Rechts auf Datenportabilität kann durch Unionsrecht oder durch das Recht der einzelnen Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, auf dem Weg von Gesetzgebungsmassnahmen vorgenommen werden (Art. 23 Abs. 1 DSGVO). Eine solche muss den Wesensgehalt der Grundrechte und Grundfreiheiten achten, in einer demokratischen Gesellschaft eine notwendige und verhältnismässige 168

528 NomosKomm-Dix, Art. 20 DSGVO N 17. Dazu bereits Rz. 129 ff.

529 ReMKomm-Spindler/Dalby, Art. 20 DSGVO N 13; siehe auch Fix, 250, für den die Bedeutung des Ausschlusses gemäss Abs. 3 weniger in der praktischen Wirkung als in der Bedeutung für die rechtsgebietsbezogene Einordnung des Instituts liegt.

530 BeckKomm-Herbst, Art. 20 DSGVO N 14.

531 Sackmann, 157.

532 BeckKomm-Herbst, Art. 20 DSGVO N 15; a.A. Sackmann, 157, der im Handeln zur Erfüllung einer rechtlichen Verpflichtung ebenfalls keine Wettbewerbssituation sieht, eine solche aber verlangt, damit die Datenportabilität sinnvoll ist. Nicht geklärt ist damit aber, warum Abs. 1 lit. c dann nicht in der Bestimmung erwähnt wurde.

Massnahme darstellen und ein in Art. 23 Abs. 1 lit. a–j DSGVO aufgelistetes Ziel verfolgen.[533]

169 Nach Art. 85 Abs. 2 DSGVO sehen die Mitgliedstaaten für die Verarbeitung zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken Abweichungen von Kapitel III vor, wenn dies erforderlich ist, um das Recht auf Schutz der Daten mit der Freiheit der Meinungsäusserung und der Informationsfreiheit in Einklang zu bringen.[534] Entsprechend sind weitere Einschränkungen des Portabilitätsrechts möglich.

170 Art. 89 Abs. 3 DSGVO sieht schliesslich vor, dass bei Daten, die für im öffentlichen Interesse liegende Archivzwecke verarbeitet werden, im Unionsrecht oder im Recht der Mitgliedstaaten Ausnahmen vom Recht auf Datenportabilität vorgesehen werden können.[535]

9. Folgen der Nichteinhaltung

171 Ein Verstoss gegen die Pflichten gemäss Art. 20 DSGVO kann nach Art. 83 Abs. 5 lit. b DSGVO eine Geldbusse nach sich ziehen. Diese kann bis zu EUR 20 Mio. oder im Fall eines Unternehmens bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs betragen.

172 Art. 83 DSGVO benennt keinen Adressatenkreis, weshalb die Sanktionsdrohung der Pflicht in Art. 20 DSGVO folgt.[536] Damit wird der alte Verantwortliche in die Pflicht genommen. Keine Sanktion droht hingegen der potenziell neuen Verantwortlichen, die die Annahme eines Datensatzes verweigert. Wie bereits aufgeführt, ist sie dazu nicht verpflichtet.[537]

B. Art. 28 DSG

173 Das Portabilitätsrecht ist in der Schweiz in Art. 28 DSG geregelt, Art. 29 DSG führt mögliche Einschränkungsgründe auf. Zudem wird vereinzelt auf andere Bestimmungen im DSG verwiesen und die gesetzliche Regelung im Verordnungsrecht (DSV) konkretisiert. Zur Ausübung des Portabilitätsrechts aktivlegitimiert ist die antragstellende natürliche Person, über die ein Verantwortli-

533 Siehe hierzu weitergehend BeckKomm-Bäcker, Art. 23 DSGVO 1 ff.
534 Hennemann, PinG 2017, 8; ausführlich BeckKompaktKomm-Paal, Art. 83 DSGVO 5 ff.
535 Hennemann, PinG 2017, 8; BeckKompaktKomm-Paal, Art. 83 DSGVO N 16.
536 BeckKomm-Bergt, Art. 83 DSGVO N 22.
537 Brüggemann, 10 f.; dazu bereits Rz. 141.

cher Daten bearbeitet.[538] Passivlegitimiert ist der Verantwortliche, der die vom Portabilitätsrecht erfassten Daten der anfragenden Person bearbeitet oder durch einen Auftragsbearbeiter bearbeiten lässt.[539] Dafür in Frage kommen private Personen oder Bundesorgane, nicht aber kantonale oder kommunale öffentliche Organe (Art. 2 Abs. 1 DSG).[540] Nachfolgend werden die einzelnen Elemente des Portabilitätsrechts besprochen.

1. Personendaten der betroffenen Person

a. Nicht Sachdaten

Vom Recht auf Datenportabilität umfasst sind nur Personen- und keine Sachdaten oder anonymisierte Daten. Auch Daten von juristischen Personen sind nicht erfasst. Dies ergibt sich bereits aus dem Geltungsbereich des Gesetzes (Art. 2 Abs. 1 DSG). Relevant kann die Unterscheidung sein, wenn eine Person einem Verantwortlichen Daten übermittelt, die keinen Bezug zu ihrer Person aufweisen (und der Verantwortliche sie auch nicht mit ihr verknüpfen kann) oder wenn der Verantwortliche die Daten nachträglich anonymisiert. Pseudonymisierte Daten, die der Verantwortliche mit der betroffenen Person in Verbindung bringen kann, stellen hingegen Personendaten dar.[541] 174

b. Datenumfang

Die betroffene Person kann die Herausgabe *ihrer* Personendaten verlangen. Damit gemeint sind diejenigen Daten, die einen Personenbezug zur Betroffenen aufweisen. Insofern präziser sind die französische und italienische Fassung, welche von «les données personnelles la concernant» bzw. «i dati personali che lo concernono» sprechen und sich damit am Wortlaut der DSGVO orientieren. Reine Drittdaten unterliegen somit nicht der Portierung. Wie unter der DSGVO können allerdings Daten, die *auch* Dritte betreffen, unter die Bestimmung fallen.[542] 175

538 Götzinger/Vasella, SZW 2021, 42; Landolt, 157; Rosenthal, Jusletter 2020, Rz. 132, wonach faktisch nur der Kunde eines Verantwortlichen Daten herausverlangen könne.

539 Götzinger/Vasella, SZW 2021, 42; Landolt, 157.

540 Diese unterliegen aufgrund der föderalistischen Kompetenzregelung und der Organisationsautonomie der Kantone dem kantonalen Recht, siehe SHK DSG-Rudin, Art. 2 N 5.

541 PC LPD-Béguin, Art. 28 N 17; BJ, Erläuternder Bericht DSV, 45; Götzinger/Vasella, SZW 2021, 42; siehe auch Landolt, 158, insb. Fn. 680.

542 Dazu sogleich Rz. 185 ff.

2. Von betroffener Person bekanntgegeben

176 Erfasst sind diejenigen Daten, die die Betroffene dem Verantwortlichen bekanntgegeben hat. Da die Bekanntgabe in Art. 5 lit. e DSG definiert wird, liegt der Schluss nahe, diese als ein «Übermitteln oder Zugänglichmachen von Personendaten» zu verstehen.[543] Während die italienische Fassung ein solches Verständnis ebenfalls zulassen würde («comunicazione» bzw. «che ha comunicato»), ist die französische Fassung diesbezüglich weniger klar. Sie spricht in Art. 5 lit. e DSG zwar ebenfalls von «communication» und definiert diese als «le fait de transmettre des données personnelles ou de les rendre accessibles», nimmt beim Portabilitätsrecht allerdings nicht auf diesen Begriff Bezug («qu'il lui remette»).

177 Wie bereits dargelegt, existieren diese begrifflichen Unklarheiten unter der DSGVO ausgeprägter und sorgen anhaltend für Diskussionen rund um das Merkmal der «Bereitstellung».[544] Dies war dem Bundesrat allerdings während des Gesetzgebungsverfahrens bewusst, weshalb die zuständige Bundesrätin zuhanden der Materialien klarstellte, welche Daten als bekanntgegeben gelten sollen.[545] Eine Auslegung gestützt auf die Begriffsdefinition ist angesichts dieser Klarstellung und namentlich der Konkretisierung in der DSV folglich gar nicht nötig.

178 Nach Art. 20 Abs. 1 DSV sind einerseits Daten erfasst, die die Betroffene dem Verantwortlichen «wissentlich und willentlich zur Verfügung stellt» (lit. a) und andererseits diejenigen Daten, die der Verantwortliche über die betroffene Person und ihr Verhalten im Rahmen der Nutzung eines Dienstes oder Geräts erhoben hat (lit. b). Das Portabilitätsrecht erfasst somit alle direkt und bewusst bekanntgegebenen Daten, etwa im Rahmen einer Onlinebestellung eingegebene Adressdaten (sog. Stammdaten).[546] Nicht umfasst sind hingegen Passwörter oder *private keys*, soweit diese verschlüsselt sind und daher auch vom Verantwortlichen nicht mit der Betroffenen in Verbindung gebracht werden können.[547] Gemäss lit. b fallen auch beobachtete Daten unter das Portabilitätsrecht, d.h. Daten, die (wissentlich oder unwissentlich) von der Betroffenen in-

543 Siehe dazu auch Götzinger/Vasella, SZW 2021, 43; kritisch Landolt, 161.
544 Dazu Rz. 126 ff.
545 Votum BR Keller-Sutter, AB 2019 N 1816; zum Gesetzgebungsprozess Rz. 97 ff.
546 PC LPD-Béguin, Art. 28 N 20; BJ, Erläuternder Bericht DSV, 45; auf die diesbezüglich unter der DSGVO bestehende Einigkeit hinweisend Fix, 147 und 168.
547 So auch PC LPD-Béguin, Art. 28 N 20.

direkt bei der Nutzung eines Dienstes oder Gerätes erzeugt werden.[548] Darunter fallen bspw. Werte einer Fitnessapp auf einer Smartwatch, die aufgrund der sportlichen Leistung erzeugt wurden.[549]

Nicht umfasst sind wie unter der DSGVO abgeleitete Daten, d.h. Daten, die aus grösseren Datenanalysen oder aus Auswertungen der bekanntgegebenen Daten resultieren.[550] Sie gelten gemäss Art. 20 Abs. 2 DSV ausdrücklich nicht als dem Verantwortlichen bekanntgegeben. Dies wird damit begründet, dass es sich dabei um eigenständige Leistungen des Verantwortlichen handle, die geschützt werden sollen.[551] Der Schutz der Eigenleistung und der eigenen Investitionen sei bei diesen durch den Verantwortlichen erzeugten Personendaten höher zu gewichten als das Recht der Betroffenen, eine Weiterverwendung ihrer Personendaten zu ermöglichen.[552] Eine derart weite Ausgestaltung des Portabilitätsrechts wurde, wie bereits erläutert, durch das Parlament ausdrücklich verworfen.[553] Darunter fallen würde etwa die Bewertung des Gesundheitszustands eines Nutzers oder Kreditrisikoanalysen.[554] 179

Ebenfalls nicht von der Betroffenen bekanntgegeben sind Daten, die aus Drittquellen stammen.[555] Damit sind bspw. Rezensionen durch Dritte oder Erwähnungen in einem Chat zwischen Dritten nicht vom Recht auf Datenportabilität erfasst, selbst wenn diese die portabilitätsanfragende Person betreffen.[556] 180

Trotz der eben geschilderten Fallgruppen ist im Einzelfall unter Würdigung der konkreten Umstände zu prüfen, ob Daten vom Recht auf Datenportabilität 181

548 BJ, Erläuternder Bericht DSV, 45; siehe auch Landolt, 164, der auch ohne Auslegung der DSV beobachtete Daten erfasst haben möchte. Er begründet die Anwendbarkeit des Portabilitätsrechts auf solche «Nutzungsdaten» mit dem wettbewerbsfördernden Zweck und der technologieneutralen Zielsetzung des Portabilitätsrechts. Daten würden namentlich auf IoT-Märkten mehrheitlich durch Messungen und Aufzeichnungen von Aktivitäten der Nutzerinnen generiert, wobei die Produkte durch Mikrofone und Sensoren bewusst so ausgestaltet seien, dass eine Datenerhebung im Vergleich zu herkömmlichen Märkten der Datenwirtschaft viel subtiler und ohne aktive Mitwirkung der Nutzerinnen erfolgten. Wären diese Nutzerdaten nicht erfasst, hätte das Portabilitätsrecht im Kontext der nunmehr entstehenden IoT-Wirtschaft keinen praktischen Nutzen.

549 Beispiel nach SHK DSG-Baeriswyl, Art. 28 N 27.

550 PC LPD-Béguin, Art. 28 N 20; BJ, Erläuternder Bericht DSV, 46; Votum BR Keller-Sutter, AB 2019 N 1816; Steiner, 121.

551 SHK DSG-Baeriswyl, Art. 28 N 29; BJ, Erläuternder Bericht DSV, 46; Landolt, 165 f., der anreizökonomische Gründe aufführt.

552 BJ, Erläuternder Bericht DSV, 46.

553 Dazu Rz. 102 ff.

554 PC LPD-Béguin, Art. 28 N 20; BJ, Erläuternder Bericht DSV, 46.

555 Rosenthal, Jusletter 2020, Rz. 134; dazu auch Rz. 185 ff.

556 PC LPD-Béguin, Art. 28 N 18; für die DSGVO Fix, 173 f.

umfasst sind.[557] Dies liegt u.a. daran, dass die Ausgangslage und die bearbeiteten Daten in verschiedenen Branchen unterschiedlich sein können. Deshalb lassen sich nur im Ansatz und jeweils nur unter Berücksichtigung sektorieller Eigenheiten allgemein verbindliche Aussagen über erfasste Daten treffen.[558]

182 In der Lehre wird überwiegend erwartet, dass die Betroffene spezifiziert, welche Daten oder welcher Art von Daten sie portieren möchte.[559] Dies wird damit begründet, dass das Portabilitätsrecht eine weite Fülle an Daten umfasse, so etwa auch beobachtete Daten, welche für die Betroffene nutzlos seien und gar nicht gewünscht sein könnten.[560] Spezifiziere die Betroffene den Umfang der zu portierenden Daten nicht, so könne der Verantwortliche ohne Rechtsverletzung vorerst auch nur die direkt bekanntgegebenen Daten übertragen.[561]

183 Zwar darf die Betroffene (*a maiore ad minus*) die Portierung sämtlicher oder nur gewisser bekanntgegebener Daten verlangen.[562] Die Betroffene soll die für sie relevanten Daten erhalten und nicht einen unübersichtlichen *data dump*, der sie mit Daten überschwemmt und überfordert und damit das Recht auf Datenportabilität unterläuft. Gleichwohl hat der Verantwortliche die besondere Natur des Rechts auf Datenportabilität zu berücksichtigen. Anders als das Auskunftsrecht sind die zu portierenden Daten nicht zwingend darauf angelegt, *tel quel* von der Betroffenen betrachtet oder genutzt zu werden.[563] Die Portierung soll nicht primär das Informationsbedürfnis der Betroffenen befriedigen. Deshalb ist es nicht notwendig, dass die Betroffene sämtliche Daten versteht oder überblickt. Vielmehr zielt das Portabilitätsrecht darauf ab, die Daten weiterzuverwenden, weshalb es auf eine Computerlesbarkeit auszurichten ist.[564]

184 Die Beurteilung muss allerdings im Einzelfall und gestützt auf die konkreten Umstände der Portierung erfolgen. Dabei sind die Eigenheiten des Sektors, in welchem die Portierung stattfindet, zu berücksichtigen. So können gerade im IoT-Kontext und bei *Multi-Homing* beobachtete Daten (etwa aus unterschiedlichen Sensoren) zu einem besseren Kundenerlebnis führen und sollten daher

557 PC LPD-Béguin, Art. 28 N 21; Reichlin, 406.
558 Dazu § 4.
559 PC LPD-Béguin, Art. 28 N 39; Götzinger/Vasella, SZW 2021, 48; BSK DSG-Laux/Steiner, Art. 28 N 63.
560 Götzinger/Vasella, SZW 2021, 48.
561 BSK DSG-Laux/Steiner, Art. 28 N 63.
562 PC LPD-Béguin, Art. 28 N 28; hervorhebend, dass alle und nicht nur «nützliche» Daten portiert werden müssen Charlet, 576; Götzinger/Vasella, SZW 2021, 48.
563 Zum Auskunftsrecht Rz. 346 ff.
564 So auch BJ, Erläuternder Bericht DSV, 47.

standardmässig umfasst sein. Dies kann bspw. im Gesundheitssektor anders sein, wenn die Betroffene um eine Datenherausgabe ersucht und davon ausgegangen werden darf, dass sie die Daten zu persönlichen Zwecken benötigt.[565] Schliesslich ist darauf hinzuweisen, dass das Ausführungsrecht beobachtete Daten ausdrücklich umfasst, weshalb diese grundsätzlich in jedem Fall herauszugeben sind (siehe Art. 20 Abs. 1 lit. b DSV).

3. Personendaten Dritter

a. Allgemein

Gibt die Betroffene einem Verantwortlichen Daten bekannt, können darunter solche sein, die *auch* einen Personenbezug zu Dritten aufweisen. Ob diese ebenfalls herauszugeben sind, ist umstritten. Art. 29 Abs. 1 i.V.m. Art. 26 Abs. 1 lit. b DSG sieht jedenfalls vor, dass eine Herausgabe verweigert werden kann, wenn dies aufgrund überwiegender Interessen Dritter erforderlich ist. Dies deutet darauf hin, dass grundsätzlich auch Personendaten Dritter der Portierung unterliegen können und im Einzelfall abzuwägen ist.[566] 185

Ein Ansatz ist es, die Betroffene wie eine Verantwortliche zu behandeln. Entsprechend dürfte der alte Verantwortliche davon ausgehen, dass die betroffene Person zur Bekanntgabe der Daten an ihn berechtigt war, und daher auch davon ausgehen, dass die Herausgabe oder die Übertragung an eine neue Verantwortliche zulässig ist.[567] Das DSG spricht davon, dass jede Person die Herausgabe «ihrer Personendaten» verlangen kann. In der DSGVO ist demgegenüber von den «sie betreffenden Personendaten» die Rede. Argumentiert wird, dass Angaben über Dritte Teil der Persönlichkeitssphäre der betroffenen Person werden könnten.[568] Entsprechend soll das Recht auf Datenportabilität auch für Daten gelten, die Angaben über Dritte enthalten, sofern sie berechtigterweise «in die Sphäre der anspruchsberechtigten Person gelangt sind».[569] Verlangt wird ein «Doppelbezug», also eine gewisse Nähe der Personendaten zur betroffenen Person, selbst wenn sich die Daten nicht auf diese beziehen.[570] Nur wenn überwiegende Interessen Dritter vorlägen oder es sich um reine 186

565 Dazu Rz. 556.

566 So auch PC LPD-Béguin, Art. 28 N 18; CR LPD-Benhamou, Art. 28 N 20; Götzinger/Vasella, SZW 2021, 42 f.; Landolt, 159.

567 Laux, digma 2019, 168; wohl ebenso Götzinger/Vasella, SZW 2021, 46 f.

568 BSK DSG-Laux/Steiner, Art. 28 N 12; Laux, digma 2019, 168.

569 Laux, digma 2019, 168; ähnlich BSK DSG-Laux/Steiner, Art. 28 N 12.

570 OFK DSG-Bieri/Heymann/Odermatt, Art. 28 N 12.

Drittdaten handle, soll eine Herausgabe nicht erfolgen.[571] Dem ist mit Blick auf die vorgesehenen Anwendungsfälle des Portabilitätsrechts zuzustimmen, auch wenn die Herleitung mit Blick auf die lateinischen Sprachfassungen nicht überzeugt.[572] Allerdings soll in der Schweiz die Regelung ebenfalls nicht aufgrund eines zu engen Anwendungsbereichs ins Leere laufen.[573]

187 Damit ist in einem ersten Schritt zu prüfen, ob im Allgemeinen die Voraussetzungen nach Art. 28 DSG erfüllt sind, insb. ob die in Frage stehenden Personendaten von der betroffenen Person bekanntgegeben wurden.[574] Betreffen die in Frage stehenden Daten *auch* Dritte (nicht aber *nur* Dritte) und weisen sie damit einen Doppelbezug auf, so ist in einem zweiten Schritt im Sinne eines «einschränkenden Korrektivs» abzuwägen, ob überwiegende Interessen Dritter eine Einschränkung erforderlich machen.[575] Liegen keine überwiegenden Interessen Dritter vor, können die Daten portiert werden.

188 Ein solches überwiegendes Interesse ist m.E. bei Daten mit Doppelbezug nur zurückhaltend anzunehmen.[576] Denn es handelt sich in jedem Fall um von der Betroffenen bekanntgegebene Daten, und nicht um solche, die von einem Dritten stammen. Aus diesem Grund dürfte einer Herausgabe an die Betroffene regelmässig nichts im Weg stehen.[577] Daran ändert nichts, dass die Daten u.U. direkt an die neue Verantwortliche übertragen werden, weil dies ebenfalls einzig auf Initiative der Betroffenen geschieht.[578] Die zu übertragenden Daten muss daher primär die Betroffene prüfen, zumal das Institut gerade ihr die Kontrolle über die Daten einräumen soll.[579] Somit können auch Daten mit Personenbezug zu Dritten vom Recht auf Datenportabilität erfasst sein. Konkret ist etwa ein Gruppenfoto, auf welchem neben der portabilitätsberechtigten

571 PC LPD-Béguin, Art. 28 N 18; OFK DSG-Bieri/Heymann/Odermatt, Art. 28 N 12.

572 Dazu Rz. 175.

573 Ähnlich Landolt, 159, wonach die Datenportabilität bei einem Ausschluss von Daten mit Drittbezug auf viele Geschäftsmodelle der Datenwirtschaft faktisch nicht anwendbar wäre.

574 Für die DSGVO ähnlich KUKO DSGVO-Kamann/Braun, Art. 20 N 18.

575 Für die DSGVO ähnlich KUKO DSGVO-Kamann/Braun, Art. 20 N 18.

576 Ebenso CR LPD-Benhamou, Art. 29 N 8; Landolt, 180; Rosenthal, Jusletter 2020, Rz. 132.

577 So auch Rosenthal, Jusletter 2020, Rz. 132.

578 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 6; Götzinger/Vasella, SZW 2021, 47 f.

579 Götzinger/Vasella, SZW 2021, 47 m.H.a. europäische Literatur; a.A. Landolt, 180, der darauf hinweist, dass die Betroffene ihrer Prüfpflicht von Drittdaten mangels Fachkenntnisse faktisch wohl kaum nachkommen dürfte und sie sich auf die Haushaltsausnahme (Art. 2 Abs. 2 lit. c DSG) berufen könnte, was zu einer Schutzlücke führe.

Person noch weitere Personen abgebildet sind, und das die Betroffene auf einen Bilderdienst geladen hat, vom Recht auf Datenportabilität erfasst.[580]

b. Pflichten in Bezug auf Dritte

Umstritten ist, ob der Verantwortliche Pflichten gegenüber der Drittperson hat und, wenn ja, welche. Einzelne Lehrmeinungen sehen ihn in der Pflicht zu überprüfen, ob der Dritte eine Einwilligung für die Datenherausgabe erteilt hat.[581] Dies ist m.E. jedoch nicht notwendig. Denn die Datenbearbeitung dürfte in vielen Fällen keine Persönlichkeitsverletzung darstellen, da die Daten nicht entgegen den Grundsätzen nach Art. 6 und 8 DSG bearbeitet werden (Art. 30 Abs. 2 lit. a DSG). Namentlich ist ein Verstoss gegen das Zweckbindungsprinzip nicht per se auszumachen, da der Zweck der Bearbeitung durch die Betroffene und die neue Verantwortliche i.d.R. mit dem Zweck bei der Beschaffung vereinbar sein dürfte (Art. 6 Abs. 3 DSG).[582] Allerdings können sich in Fällen, in welchen Drittdaten an einen andersartigen Dienst[583] übertragen werden, Probleme bezüglich der Zweckbindung ergeben. 189

Liegt eine Persönlichkeitsverletzung vor, sollte nach hier vertretener Ansicht die gesetzgeberische Entscheidung zugunsten der Datenbekanntgabe ebenfalls gewürdigt werden. Sie dürfte regelmässig durch ein überwiegendes Interesse gerechtfertigt und damit nicht widerrechtlich sein.[584] Hierbei ist erneut zu betonen, dass es sich dabei notwendigerweise um Personendaten mit einem Doppelbezug und nicht um reine Drittdaten handelt, und überdies nur um solche, die die Betroffene bekanntgegeben hatte. Entsprechend muss einzig die Betroffene prüfen, ob Daten mit Doppelbezug übertragen werden.[585] Einzuräumen ist jedoch, dass der Verantwortliche angesichts einer möglichen sanktionierbaren Verletzung von Drittrechten eine Verletzung des Datenpor- 190

580 A.A. jedoch für die DSGVO Golland, 318.

581 CR LPD-Benhamou, Art. 28 N 20; noch zur Regelung unter der DSGVO Reichlin, 406.

582 Ähnlich Götzinger/Vasella, SZW 2021, 47 m.w.N. Dies gilt demnach sofern der alte Verantwortliche die Daten löscht oder anonymisiert oder nicht mehr produktiv nutzt. Sie ziehen ferner eine Parallele zu einem Verkauf der Kundenbasis, welche i.d.R. als unproblematisch angesehen werde.

583 Dazu Rz. 180.

584 Auch Landolt, 180, der zumindest nur im Ausnahmefall ein überwiegendes Interesse Dritter an einer Einschränkung des Portabilitätsrechts sieht, weil die Interessen an einer datenbezogenen Marktöffnung überwiegten. Die Weitergabe von nichtsensitiven Drittdaten sollte demnach in den meisten Fällen gerechtfertigt sein.

585 Götzinger/Vasella, SZW 2021, 47. Es sei denn, die eben erwähnte Haushaltsausnahme greift, siehe Fn. 579.

tabilitätsrechts – welche unter dem DSG keiner Sanktionierung unterliegt – eher in Kauf nehmen dürfte.[586]

c. Spezialfragen beim Doppelbezug

191 Wer bestimmte Daten bekanntgegeben hat und ob ein Doppelbezug vorliegt, hängt oft davon ab, aus welcher Perspektive die Datenbearbeitung betrachtet wird. Nicht erfasst wird, wie erläutert, die Bekanntgabe von Personendaten durch Dritte, etwa Buchrezensionen auf Websites, die Daten über die Autorenschaft enthalten.[587] Bei anders gelagerten Fällen muss eine Datenportierung jedoch möglich sein, auch wenn bestimmte Daten bei genauer Betrachtung durch Dritte bekanntgegeben wurden. Dies ist namentlich dann der Fall, wenn eine Interdependenz zwischen Daten der Betroffenen und Drittdaten besteht und sich diese Daten nicht praktikabel auftrennen lassen. Dabei ist zu berücksichtigen, wie der Verantwortliche die Daten selbst aufbewahrt: Sind die Drittdaten klar der Sphäre der betroffenen Person zugehörig, weil sie eng verwoben und technisch kaum von den Daten der betroffenen Person trennbar sind und entsprechend aufbewahrt werden, so ist ein Doppelbezug eher anzunehmen und die Herausgabe sollte erfolgen dürfen. Beispielhaft ist etwa ein Chatverlauf zwischen mehreren Personen. Ein Teil der Daten (in Form von Chatnachrichten) wird dabei nicht von der portabilitätsberechtigten Person bekanntgegeben, sondern von anderen Chatteilnehmern.[588] In der Literatur wird zurecht, aber kaum differenzierend, davon ausgegangen, dass auch in diesen Fällen die Daten mit Drittbezug herauszugeben sind.[589]

192 Tatsächlich dürfte es in vielen Fällen schwierig sein, eine präzise Aufschlüsselung der einzelnen Datenelemente vorzunehmen. Zwar könnten diese auf der syntaktischen Ebene fast beliebig weit – jedenfalls bis zu den Zahlen Null und Eins – differenziert und entsprechend nach der jeweils bekanntgebenden Person entflechtet werden. Dies erscheint aber als unverhältnismässig, da der Verantwortliche einen immensen organisatorischen und technischen Aufwand auf sich nehmen müsste, um die Daten aufzutrennen und herauszugeben.[590] Sie wären ohne Kontext weitgehend wertlos; das Portabilitätsrecht wirkungs-

586 Landolt, 179 f.

587 Dazu Rz. 180.

588 So auch BKartA, Sektoruntersuchung, 33; Duller, 133.

589 CR LPD-Benhamou, Art. 28 N 20; OFK DSG-Bieri/Heymann/Odermatt, Art. 28 N 12; wohl auch Cattaneo, 63 f.; BSK DSG-Laux/Steiner, Art. 28 N 14; Laux, digma 2019, 168; a.A. jedoch etwa BeckKomm-Herbst, Art. 20 DSGVO N 11.

590 BKartA, Sektoruntersuchung, 33; Krause, PinG 2018, 240.

los.[591] Im Ergebnis wären nur Stammdaten von der Regelung erfasst.[592] Wenn solche Drittdaten daher einen engen Konnex zur portabilitätsanfragenden Person aufweisen und interdependent zu den (herauszugebenden) Personendaten der betroffenen Person sind, so sind sie nach der hier vertretenen Ansicht ebenfalls Daten mit Doppelbezug und unterliegen damit dem Portabilitätsrecht.

Grenzfälle sind indes auch hier denkbar, etwa wenn eine Person ein Auto über längere Zeit vom Fahrzeughalter ausleiht und dieses während der Nutzung Personendaten über den Ausleiher (statt über den Fahrzeughalter) erhebt. In solchen Fällen, in denen die Interessen der Drittperson überwiegen und keine Interdependenz zu Daten der betroffenen Person auszumachen ist, kann es angezeigt sein, die Herausgabe einzuschränken. 193

4. Mit Einwilligung oder in unmittelbarem Zusammenhang mit Vertragsabschluss erhoben

a. Allgemein

Die Bearbeitung muss mit der Einwilligung der betroffenen Person oder in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der Betroffenen erfolgen (Art. 28 Abs. 1 lit. b DSG). Damit wurde eine weitere Voraussetzung unverändert aus der DSGVO übernommen. Dort ist der Hintergrund jedoch ein anderer: Unter der DSGVO muss der Verantwortliche die betroffene Person über die Rechtsgrundlage der Verarbeitung informieren (Art. 13 Abs. 1 lit. c resp. Art. 14 Abs. 1 lit. c DSGVO) und aufzeigen können, dass für eine konkrete Datenverarbeitung mindestens eine der Rechtsgrundlagen einschlägig ist.[593] Ein solches Verbot mit Erlaubnisvorbehalt gibt es unter dem DSG nicht: Datenbearbeitungen, die die Persönlichkeit der Betroffenen nicht verletzen, sind für Private ohne Weiteres zulässig (siehe Art. 30 DSG; sog. Erlaubnis mit Verbotsvorbehalt).[594] Sie benötigen keine Rechtfertigung oder – in der Terminologie der DSGVO – eine Rechtsgrundlage. Nur wenn die Persönlichkeit verletzt wird, namentlich in den Fällen von Art. 30 Abs. 2 DSG, ist ein Rechtfertigungsgrund nach Art. 31 DSG erforderlich. 194

591 Ähnlich Götzinger/Vasella, SZW 2021, 47; siehe auch Weber/Thouvenin, 72 f.
592 Dazu für die DSGVO bereits Rz. 125.
593 Steiner, 123 f.
594 Götzinger/Vasella, SZW 2021, 44; Rosenthal, Jusletter 2020, Rz. 7.

195 Wird Art. 28 Abs. 1 lit. b DSG eng ausgelegt, würde dies bedeuten, dass nur gerechtfertigte Datenbearbeitungen, und dabei nur solche basierend auf dem Rechtfertigungsgrund der Einwilligung (Art. 31 Abs. 1 DSG) oder dem überwiegenden Vertragsinteresse (Art. 31 Abs. 2 lit. a DSG) vom Recht auf Datenportabilität umfasst sind. Dies dürfte der Gesetzgeber jedoch nicht beabsichtigt haben.[595] Vielmehr übernahm er das Institut wohl zu wörtlich aus der DSGVO. Es wird daher in der Literatur zurecht dafür plädiert, dass Daten, die die Betroffene freiwillig (im Sinne der Einwilligung) oder im Rahmen einer Vertragserfüllung (im Sinne des überwiegenden Vertragsinteresses) bekanntgegeben hat, portabilitätsberechtigt sein sollen.[596] Ob ein Rechtfertigungsgrund vorliegt oder überhaupt notwendig ist, kann keine Rolle spielen. Insgesamt muss daher m.E. die Initiative für die konkrete Datenbearbeitung zumindest (auch) von der Betroffenen ausgegangen sein. Die Datenbearbeitung darf nicht völlig vom Willen der Betroffenen entkoppelt erfolgen. Dies ist immer dann der Fall, wenn eine Einwilligung vorliegt oder die Daten im Zusammenhang mit einem Vertrag bearbeitet werden. Möglich ist es aber auch in weiteren Fällen.

b. Datenbearbeitungen durch Bundesorgane

196 Nach dem Gesagten wird deutlich, weshalb die Schweizer Regelung den ausdrücklichen Ausschluss von Verarbeitungen in Wahrnehmung öffentlicher Aufgaben nicht übernommen hat: Die DSGVO bezieht sich damit, wie oben aufgezeigt, auf die Rechtmässigkeitsbedingung nach Art. 6 Abs. 1 lit. e DSGVO.[597] Aus Schweizer Sicht muss dies nicht klargestellt werden, da die Schweiz kein System der Rechtmässigkeitsbedingungen für Bundesorgane kennt. Während unter der DSGVO mehrere Rechtmässigkeitsbedingungen vorliegen können, ist für Bundesorgane in der Schweiz grundsätzlich einzig die

595 So auch STEINER, 124; nicht ausdrücklich darauf eingehend, aber doch einen Rechtfertigungsgrund fordernd hingegen SHK DSG-BAERISWYL, Art. 28 N 21; LANDOLT, 167, wonach die Übernahme der Voraussetzungen aus der DSGVO unter dem DSG «zu gewissen dogmatischen Unschärfen» führe; sich zumindest fragend ob die Räte das tatsächlich beabsichtigt hatten MÉTILLE, Obligations, 21; nunmehr deutlicher und eine Auslegung nach dem Zweck und nicht dem Wortlaut fordernd MÉTILLE, Nouveautés, 40.

596 GÖTZINGER/VASELLA, SZW 2021, 44; STEINER, 124, welcher bezugnehmend auf die Bekanntgabe verlangt, dass es sich um Daten handeln müsse, welche die betroffene Person bei der Inanspruchnahme einer Dienstleistung freiwillig und selbstbestimmt generiert oder vom jeweiligen Verantwortlichen im Rahmen dieser selbstgewählten Vertragssituation hat beobachten lassen; siehe auch LANDOLT, 167 f., wonach die beiden Sachverhalte von ihrer Funktion als Rechtfertigungstatbestand entkoppelt und stattdessen als eigenständige Voraussetzung beim Portabilitätsrecht verstanden werden sollen.

597 Siehe Art. 20 Abs. 3 DSGVO und dazu Rz. 166 f.

gesetzliche Grundlage die Basis für eine Datenbearbeitung (Art. 34 Abs. 1 DSG). Diese fällt jedoch klarerweise nicht unter Art. 28 Abs. 1 lit. b DSG. Damit stellt bereits diese Einschränkung klar, dass öffentlich-rechtliche Datenbearbeitungen, die sich auf eine gesetzliche Grundlage zu stützen haben, grundsätzlich ausgeschlossen sind.[598] Dies wirkt sich auf die Zielsetzung des Instituts aus.[599]

Punktuell sind aber Unterschiede zur europäischen Regelung ersichtlich, da sich Bundesorgane im Einzelfall ebenfalls auf eine Einwilligung stützen (Art. 34 Abs. 4 lit. b DSG) oder Daten «im Wettbewerb mit Privaten» bearbeiten können.[600] Dabei ist zu berücksichtigen, dass die Einschränkung nach Art. 28 Abs. 1 lit. b DSG im Wesentlichen auf die Freiwilligkeit der Datenbekanntgabe abstellt.[601] Trifft dies auf eine Datenbearbeitung durch Bundesorgane zu, kann das Portabilitätsrecht im Einzelfall geltend gemacht werden.[602] Damit erscheint der Anwendungsbereich in der Schweiz einerseits etwas weiter.[603] Andererseits unterstehen aber kantonale und kommunale öffentliche Organe nicht dem DSG und damit auch nicht Art. 28 DSG, weshalb der Anwendungsbereich auch enger ist.[604] 197

5. Automatisierte Bearbeitung durch den Verantwortlichen

Das Erfordernis der automatisierten Bearbeitung in Art. 28 Abs. 1 lit. a DSG schliesst diejenigen Personendaten aus, welche ein Verantwortlicher in Papierform aufbewahrt.[605] Das Recht auf Datenportabilität umfasst damit nur elektronisch bearbeitete Daten. Der Verantwortliche ist dabei nicht verpflichtet, physisch vorhandene Daten zu digitalisieren und für das Datenportabili- 198

598 So auch OFK DSG-Bieri/Heymann/Odermatt, Art. 28 N 17; BJ, Erläuternder Bericht DSV, 45.

599 Für die DSGVO Fix, 94 f.; dazu ausführlich Rz. 245 ff.; für die Schweizer Regelung Rz. 268 f. und Rz. 318.

600 So BJ, Erläuternder Bericht DSV, 45.

601 Dazu Rz. 195.

602 OFK DSG-Bieri/Heymann/Odermatt, Art. 28 N 17; BJ, Erläuternder Bericht DSV, 45.

603 Siehe Fix, 249 f., wonach eine Anwendung auf öffentliche Stellen unter der DSGVO «eher theoretisch, als praktisch» denkbar sei, da jedenfalls klassische Staatsaufgaben ausgeschlossen seien; BeckKomm-Herbst, Art. 20 DSGVO N 14 will daher etwa die Forschung an einem Universitätsklinikum von Art. 20 DSGVO nicht erfasst sehen. Dies verhält sich m.E. in der Schweiz anders, soweit es sich bei den Forschenden um Bundesorgane handelt, dazu Rz. 492 f. und 530 f.

604 Dazu Rz. 173 und ausführlich am Beispiel des Gesundheitswesens Rz. 494 und 506 ff.

605 BJ, Erläuternder Bericht DSV, 45; Cattaneo, 63; Charlet, 575.

tätsrecht aufzubereiten.[606] Denn auch in der Schweiz zielt das Institut auf den digitalen Verkehr ab und soll in besonderem Mass auf den Datenverkehr im Internet Anwendung finden.[607] In seinem tatsächlichen Wirkungsbereich ist aber keine Einschränkung nur auf den Datenverkehr im Internet oder auf Internetplattformen auszumachen, da heute ein Grossteil der Datenbearbeitungen automatisiert erfolgen dürfte. Insofern ist die Rechtslage übereinstimmend mit derjenigen unter der DSGVO und die Voraussetzung faktisch kaum eine Einschränkung.

6. Rechtsfolge: Portierung

199 Liegen die genannten Voraussetzungen in Art. 28 DSG vor, hat der Verantwortliche die Daten an die Betroffene (Abs. 1) oder die neue Verantwortliche (Abs. 2) in einem gängigen elektronischen Format herauszugeben resp. zu übertragen.

a. An die betroffene Person (Datenherausgabe)

200 Die Herausgabe hat – als Normalfall – an die betroffene Person zu erfolgen (Art. 28 Abs. 1 DSG). Nicht erwähnt wird in Abs. 1 die Übermittlung an eine andere Verantwortliche. Insofern unterscheidet sich die Datenherausgabe von der indirekten Übertragung unter der DSGVO, welche die Herausgabe an die Betroffene zwar als eigenes Recht verankert,[608] dieses aber wohl nur als Zwischenschritt sieht, bevor die Daten ihren Weg zur neuen Verantwortlichen finden.[609] Konsequenterweise spricht Art. 20 DSGVO denn auch als Ganzes von einem Recht auf Datenübertragbarkeit – eine Unterteilung zwischen Datenherausgabe und -übertragung gibt es nicht. In materieller Hinsicht ergeben sich daraus keine Unterschiede. Allerdings stellt die Schweizer Regelung die Betroffene deutlicher ins Zentrum, da nicht ausdrücklich vorgesehen ist, dass die portierten Daten von der Betroffenen an einen Dritten weitergegeben

606 SHK DSG-Baeriswyl, Art. 28 N 22; Steiner, 123.

607 Zu den entsprechenden Voten in den parlamentarischen Beratungen Rz. 101 ff.; zu den Gründen dafür Kratz, InTeR 2019, *passim*; ferner Elfering, 19, für welche primär Onlineplattformen, insb. soziale Netzwerke im Fokus standen.

608 BeckOK IT-Recht-Steinrötter, Art. 20 DSGVO N 34, der einräumt, dass das Übertragungsrecht auch als nachwirkende Nebenpflicht des Herausgaberechts konstruiert werden könnte.

609 Von einem «zweistufigen Recht» sprechend KUKO DSGVO-Kamann/Braun, Art. 20 N 21; ebenso GK-Piltz, Art. 20 DSGVO N 9; siehe aber auch De Hert et al., CSLR 2018, 197, die von drei verschiedenen Rechten sprechen; ähnlich BeckKompaktKomm-Paal, Art. 20 DSGVO N 16, der von zwei voneinander zu trennenden Ansprüchen spricht.

werden.[610] Die Betroffene kann also die Daten für den rein persönlichen Gebrauch verwenden (etwa eine Fotosammlung nunmehr lokal speichern) *oder* sie an eine neue Verantwortliche übertragen.[611] Letzteres ist indes kein Vorgang, der sich auf Art. 28 DSG stützt.

b. An die neue Verantwortliche (Datenübertragung)

Alternativ kann die Übertragung nach Art. 28 Abs. 2 DSG direkt an eine andere Verantwortliche erfolgen, wenn die Voraussetzungen nach Abs. 1 erfüllt sind und die Übertragung keinen unverhältnismässigen Aufwand erfordert. Ob die Übertragung an die neue Verantwortliche erfolgen soll, bestimmt die betroffene Person. Ebenfalls möglich ist, dass die neue Verantwortliche eigenständig auf die Daten zugreift, etwa weil der alte Verantwortliche ihr via eine API den Zugang gewährt hat.[612] 201

Die DSV hält fest, wann ein unverhältnismässiger Aufwand vorliegt: Immer dann, wenn die Übertragung technisch nicht möglich ist (Art. 21 Abs. 3 DSV).[613] Damit ist in der Schweiz das Kriterium der Verhältnismässigkeit verankert, welches im europäischen Gesetzgebungsprozess weggefallen war.[614] Die Verordnung konkretisiert dieses allerdings wieder kongruent mit der Regelung in der DSGVO, weshalb sich materiell keine Unterschiede ergeben. 202

Kein unverhältnismässiger Aufwand lässt sich aus den Kosten ableiten, welche für den Verantwortlichen anfallen.[615] Beim Recht auf Datenportabilität handelt es sich um ein Betroffenenrecht, welches ungeachtet allfälliger Implementierungskosten gewährt werden muss. Die für die Übertragung an eine neue Ver- 203

---

610 Zwar ist dies schlüssig, da die potenziell neue Verantwortliche die portierten Daten nicht annehmen muss und sie unter dem Portabilitätsrecht keinerlei Verpflichtungen hat. Dies verhält sich auch unter der DSGVO nicht anders. Allerdings nimmt diese mit dem Behinderungsverbot den alten Verantwortlichen dennoch besonders in die Pflicht und geht damit von einer Übermittlung an ihn aus. Dies ist in der Schweiz nicht der Fall. Dennoch nehmen verschiedene Autoren ein Behinderungsverbot auch für die Schweiz an, siehe CR LPD-Benhamou, Art. 28 N 17; BJ, Erläuternder Bericht DSV, 48, sich dabei aber auf die Datenübertragung nach Art. 28 Abs. 2 DSG beziehend; BSK DSG-Laux/Steiner, Art. 28 N 46.

611 BJ, Erläuternder Bericht DSV, 44; siehe auch PC LPD-Béguin, Art. 28 N 13, der in Abs. 1 nur die Grundlage für eine Herausgabe «zu rein persönlichen Zwecken» sieht und klarstellt, dass sich die Bestimmung nicht auf die Übertragung von einem Verantwortlichen auf eine andere Verantwortliche bezieht.

612 PC LPD-Béguin, Art. 28 N 54.

613 Siehe hierzu BJ, Erläuternder Bericht DSV, 48, das jedoch etwas unglücklich – wohl irrtümlicherweise – davon spricht, dass Art. 21 Abs. 3 DSV den Art. 28 Abs. 3 DSG konkretisiere.

614 Dazu Rz. 142, insb. Fn. 466.

615 A.A. jedoch PC LPD-Béguin, Art. 28 N 30.

antwortliche anfallenden Kosten lassen sich daher nicht vorbringen, besonders, da kaum ersichtlich ist, inwiefern eine Übertragung an einen Dritten mit höheren Kosten verbunden sein sollte als die Herausgabe an die betroffene Person.[616] Mit denselben Gründen wird in der Literatur teils vertreten, dass ein unverhältnismässiger Aufwand, d.h. eine technische Unmöglichkeit, kaum je vorliegen dürfte, da in technischer Hinsicht die Datenherausgabe an die Betroffene weder einfacher noch komplexer sei als die Datenübertragung an die neue Verantwortliche, sofern die neue Verantwortliche die Daten entgegennehmen möchte.[617] Diese ist allerdings – wie unter der DSGVO – nicht verpflichtet, die Daten entgegenzunehmen oder auch nur für die technische Durchführbarkeit der Übertragung zu sorgen.[618]

204 Nach den Erläuterungen des BJ darf der alte Verantwortliche die Übermittlung der Daten zudem nicht ungerechtfertigt behindern, indem er technische Hürden schafft, die den Datenzugriff, die -übertragung oder -wiederverwendung verlangsamen oder verhindern.[619] Dabei geht das BJ etwa von einer Behinderung aus, wenn übermässige Verzögerungen auftreten oder Daten absichtlich verschleiert werden, aber auch bereits wenn keine Dateninteroperabilität oder keine API angeboten wird.[620] Das BJ orientiert sich in diesem weitgehenden Verständnis an der DSGVO, allerdings ohne dass dafür eine Verankerung im DSG oder der DSV vorliegen würde.

c. In einem gängigen elektronischen Format

205 Im Gegensatz zur DSGVO muss eine Portierung unter dem DSG in einem *gängigen elektronischen* Format («un format électronique couramment utilisé», «un formato elettronico usuale») erfolgen, und nicht in einem *strukturierten, gängigen* und *maschinenlesbaren* Format. Die DSV konkretisiert kaum, was darunter zu verstehen ist. Gängige elektronische Formate sollen solche sein, die es ermöglichen, dass die Personendaten mit verhältnismässigem Aufwand übertragen und von der betroffenen Person oder einer anderen Verantwortlichen weiterverwendet werden können (Art. 21 Abs. 1 DSV).

206 Möglich ist es, sich bei der Auslegung des gängigen elektronischen Formats an der Auslegung zu Art. 20 DSGVO zu orientieren, wenngleich der Schweizer

616 Thouvenin/Weber/Früh, 173.
617 Zur Diskussion unter der DSGVO Rz. 141.
618 PC LPD-Béguin, Art. 28 N 36; Rosenthal, Jusletter 2020, Rz. 131.
619 BJ, Erläuternder Bericht DSV, 48.
620 BJ, Erläuternder Bericht DSV, 48; a.A. wohl Jotterand, 28.

Wortlaut näher an demjenigen in Art. 15 DSGVO ist.[621] Entsprechend wird darauf hingewiesen, dass die Daten unter dem DSG wohl ebenfalls in einer strukturierten und maschinenlesbaren Form erhältlich sein müssten.[622] Dem ist zu folgen. Das Erfordernis eines elektronischen Formats meint in der Sache dasselbe wie dasjenige der Maschinenlesbarkeit unter der DSGVO: Die Daten sollen elektronisch verarbeitbar und so zu den Zwecken des Portabilitätsrechts weiterverwendbar sein. Wie unter der DSGVO grenzt sich das Institut damit von anderen Betroffenenrechten ab, welche auch rein analoge Auskünfte betreffen können.[623] Der unter dem DSG gewählte Wortlaut führt aber zu weniger Abgrenzungsschwierigkeiten – Ausdrucke, die mittels OCR als maschinenlesbar gelten können, sind klarerweise nicht erfasst.

In Bezug auf die Gängigkeit wird ausgeführt, dass die in der jeweiligen Branche für die betreffende Art der Daten und im relevanten geografischen Gebiet verbreiteten Formate in der Schweiz gängig sein dürften.[624] Dem ist grundsätzlich zuzustimmen. Gleichwohl ist m.E. nicht zu stark auf geografische Gebiete abzustellen, da sonst die Schwelle, bei welcher eine Gängigkeit angenommen werden kann, möglicherweise unnötig hoch angesetzt würde. Primär ist auf Branchenstandards und -üblichkeit abzustellen. Damit kann, auch vor dem Hintergrund, dass die Schweiz keine Technikinsel ist, grundsätzlich auf die für die DSGVO gemachten Ausführungen verwiesen werden.[625] 207

Die Erläuterungen des BJ führen zusätzlich auf, dass die übermittelten Informationen in interoperablen Formaten mit geeigneten und verständlichen Metadaten genau beschrieben werden sollen, damit sie sinnvoll in ein neues System übernommen werden können.[626] Die Metadaten sollen dabei umfangreich genug sein, um die Nutzung und Wiederverwendung der Daten zu ermögli- 208

621 Siehe Art. 15 Abs. 3 DSGVO. Damit – so ein Argument – grenzen sich die drei Kriterien von Art. 20 DSGVO bis zu einem gewissen Punkt innerhalb der DSGVO denn auch vom Auskunftsrecht ab, da bei gleicher Bedeutung auch der gleiche Wortlaut hätte gewählt werden können, siehe dazu Rz. 151 f.

622 SHK DSG-Baeriswyl, Art. 28 N 18.

623 Dazu Rz. 150.

624 Götzinger/Vasella, SZW 2021, 48; Métille, Nouveautés, 40; Swiss Data Alliance, Leitlinien Datenportabilität, 9; siehe auch OFK DSG-Bieri/Heymann/Odermatt, Art. 28 N 26, die die Frage aufwerfen, ob zu unterscheiden ist, ob es sich um eine Datenherausgabe oder um eine -übertragung handelt, mithin in gewissen Fällen der technische Wissensstand der Betroffenen berücksichtigt werden muss.

625 Dazu Rz. 145 ff.

626 BJ, Erläuternder Bericht DSV, 47; den Bericht ebenfalls aufgreifend SHK DSG-Baeriswyl, Art. 28 N 19; Cattaneo, 64; zur umstrittenen Frage, was ein interoperables Format umfasst Rz. 155.

chen, ohne Geschäftsgeheimnisse offenzulegen.[627] Soweit damit eine Pflicht zur Aufbereitung (neuer) Metadaten suggeriert wird, ist dem nicht zu folgen. Das Recht auf Datenportabilität begründet einen Anspruch auf die Daten «*as is*»; dies umfasst allfällige Metadaten, die es etwa ermöglichen, einen grösseren Datensatz zu strukturieren. Eine Pflicht zur Ergänzung der Metadaten (etwa um solche Daten, die der alte Verantwortliche möglicherweise in seinem System gar nicht benötigt) lässt sich daraus jedoch nicht ableiten.[628] Dies vor allem, da die Schweizer Regelung, anders als diejenige der DSGVO, eine Strukturiertheit nicht als Erfordernis nennt. Wie ausgeführt, ergeben sich materiell wohl keine Unterschiede, doch wäre die Pflicht zur Einbringung von Metadaten am ehesten noch aufgrund des Erfordernisses der Strukturiertheit denkbar. Ferner kann sich je nach (gängigem) Format unterscheiden, welche Metadaten technisch überhaupt enthalten sein können.[629] Es müssen daher nur diejenigen Metadaten herausgegeben werden, die in einem gängigen elektronischen Format i.S.v. Art. 28 DSG enthalten sind.

209 Art. 21 Abs. 2 DSV hält fest, dass mit dem Portabilitätsrecht keine Pflicht für den alten Verantwortlichen besteht, technisch kompatible Datenbearbeitungssysteme zu übernehmen oder beizubehalten. Diese Pflicht gibt es selbstredend auch nicht für die neue Verantwortliche, die die portierten Daten gar nicht erst übernehmen muss. Auch eine Pflicht zur Schaffung einer Interoperabilität zwischen Systemen ergibt sich aus den Vorgaben des DSG und der DSV nicht.[630]

627 BJ, Erläuternder Bericht DSV, 47.

628 Ebenfalls kritisch hierzu OFK DSG-Bieri/Heymann/Odermatt, Art. 28 N 26; ähnlich auch für die DSGVO-Regelung Fix, 277, der aber darauf hinweist, dass eine praktische Umsetzung und die zur Anspruchserfüllung notwendige Kategorisierung ohne Metadaten kaum umsetzbar sei. Siehe auch a.a.O., 206 f., wonach faktisch eine Interoperabilität durch den alten Verantwortlichen vielfach zumindest vorbereitet werden müsse. Dies könne auch durch Versehung der Datensätze mit Metadaten geschehen.

629 Bspw. enthalten unkomprimierte digitale Audiodateien wie PCM neben ihrem Dateinamen keine Metadaten, während sich etwa die (freilich gängigeren) MP3-Dateien mittels sog. «ID3-Tags» mit einer Vielzahl an Metadaten (etwa Titel, Interpret, Album, Genre usw.) ausstatten lassen, siehe https://perma.cc/QG38-UDSB und https://perma.cc/2CM4-HKEF.

630 OFK DSG-Bieri/Heymann/Odermatt, Art. 28 N 26; Götzinger/Vasella, SZW 2021, 48 f.; BSK DSG-Laux/Steiner, Art. 28 N 49 und 57; Landolt, 170 f.; Laux, digma 2019, 167; a.A. wohl PC LPD-Béguin, Art. 28 N 53, der davon ausgeht, dass Formate interoperabel sein müssen, wenn sie in einem «gängigen elektronischen Format» herausgegeben werden müssen; siehe auch Roth, SZW 2020, 678, welcher zwar keine Pflicht zur Schaffung einer Interoperabilität zwischen Systemen sieht, etwa durch standardisierte APIs, jedoch davon auszugehen scheint, dass eine Pflicht besteht, die Daten in einem «innerhalb des jeweiligen Sektors interoperablen Format» bereitzustellen.

d. Modalitäten, Frist und Zuständigkeit

Art. 22 DSV verweist für die Modalitäten, Frist und Zuständigkeit sinngemäss auf die Bestimmungen zum Auskunftsrecht. Die Betroffene muss somit zur Geltendmachung ihres Rechts zunächst ein schriftliches Gesuch einreichen, in welchem sie sich identifiziert (Art. 22 i.V.m. Art. 16 Abs. 1 und 5 DSV).[631] Mit dem Einverständnis des Verantwortlichen kann das Gesuch auch mündlich gestellt werden (Art. 22 i.V.m. Art. 16 Abs. 1 DSV), wobei in diesem Fall die Identifizierung der Betroffenen schwieriger (und weniger beweissicher) sein dürfte.[632] Nach Art. 22 i.V.m. Art. 16 Abs. 5 DSV obliegt es der Betroffenen, an der Identifizierung mitzuwirken. Wird ein Gesuch direkt vom (eingeloggten) Account einer Betroffenen aus gestellt, so dürfte dies für eine Identifizierung ausreichen, wobei mit Blick auf die Vorgaben zur Datensicherheit besondere Vorkehrungen getroffen werden sollten (bspw. Mechanismen zur Erkennung ungewöhnlicher Anmeldeversuche von fremden IP-Adressen).[633] 210

Der Anspruch richtet sich gegen den Verantwortlichen, auch wenn die Daten bei einem Auftragsbearbeiter gespeichert sind.[634] Dieser muss allerdings den Verantwortlichen bei der Beantwortung der Anfrage unterstützen oder kann diese, im Auftrag des Verantwortlichen, beantworten (Art. 22 i.V.m. Art. 17 Abs. 2 DSV). Den Auftragsbearbeiter trifft mithin die Pflicht, portabilitätsrelevante Daten dem Verantwortlichen zu liefern, wenn dieser nicht selbst darüber verfügt.[635] Existieren mehrere Verantwortliche, kann die betroffene Person ihr Recht bei jedem Verantwortlichen geltend machen (Art. 22 i.V.m. Art. 17 Abs. 1 DSV). Die Verantwortlichen sind dabei jeweils verpflichtet, das Gesuch zu behandeln und nicht bloss weiterzuleiten.[636] 211

Die Daten sind grundsätzlich innert 30 Tagen seit Eingang des Gesuchs zu portieren (Art. 22 i.V.m. Art. 18 Abs. 1 DSV). Ist dies nicht möglich, muss die betroffene Person darüber informiert und ihr mitgeteilt werden, innert welcher Frist die Portierung erfolgen kann. Verweigert der Verantwortliche die Portierung, schränkt er sie ein oder schiebt er sie auf (Art. 29 DSG),[637] so muss er dies 212

631 Praktisch findet diese Identifikation i.d.R. mittels einer Ausweiskopie statt, die dem Gesuch beigelegt oder angehängt wird.

632 Ähnlich OFK DSG-Bieri/Heymann/Odermatt, Art. 28 N 22.

633 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 16 f.; zu den Aspekten der Datensicherheit Swire/Lagos, Maryland Law Review 2013, 374 f.

634 BSK DSG-Laux/Steiner, Art. 28 N 7.

635 BJ, Erläuternder Bericht DSV, 42.

636 BJ, Erläuternder Bericht DSV, 42.

637 Dazu Rz. 221 ff.

innert derselben Frist mitteilen. Damit ist das Portabilitätsrechts als statischer Übertragungsmechanismus konzipiert, als «Momentaufnahme»,[638] aus der sich weder ein Anspruch auf Bereitstellung einer technischen Infrastruktur für einen kontinuierlichen Datenfluss noch ein Anspruch auf einen Datenzugang ableiten lässt.[639]

213 Die Portierung kann wie unter der DSGVO auf jedem Weg erfolgen, d.h. etwa als postalischer Versand eines USB-Sticks oder per E-Mail.[640] Denkbar ist ferner, gerade bei grösseren Datensätzen, eine Anbindung an eine API[641] oder ein Download direkt von den Servern des alten Verantwortlichen (bspw. von einem SFTP-Server, einer sicheren Web-Schnittstelle oder einem Web-Portal).[642]

214 Nach Art. 28 Abs. 3 DSG ist die Ausübung des Portabilitätsrechts grundsätzlich kostenlos. Ausnahmsweise ist eine Beteiligung von bis zu CHF 300 zulässig, wenn die Portierung mit einem unverhältnismässigen Aufwand verbunden ist (Art. 22 i.V.m. Art. 19 Abs. 1 und 2 DSV).[643] Dies kann etwa dann der Fall sein, wenn eine aufwändige Triage zwischen Drittdaten und denjenigen der Betroffenen nötig ist.[644] Die Höhe der Beteiligung ist der Betroffenen vorab mitzuteilen (Art. 22 i.V.m. Art. 19 Abs. 3 DSV).

e. Keine Löschung beim alten Verantwortlichen

215 Das Portabilitätsrecht ändert nichts an der Zulässigkeit der Datenbearbeitung beim alten Verantwortlichen. Weder gilt durch die Ausübung des Portabilitätsrechts eine einmal erteilte Einwilligung durch die Betroffene als widerrufen noch ändert sich etwas an einem Vertragsverhältnis zwischen den beiden Parteien.[645] Allfällige Rechtfertigungsgründe kann der Verantwortliche weiterhin geltend machen. Dies bedeutet, dass der alte Verantwortliche die herausgegebenen Daten nicht löschen muss.[646] Ihren Rechtsanspruch auf Löschung oder

638 Landolt, 173.

639 BJ, Erläuternder Bericht DSV, 44, wonach die neue Verantwortliche die Pflicht hat, «die herausverlangten Personendaten binnen vernünftiger Zeit aggregiert zur Verfügung zu stellen»; Graef/Husovec/Van den Boom, EuCML 2020, 10.

640 CR LPD-Benhamou, Art. 28 N 35.

641 PC LPD-Béguin, Art. 28 N 47; BJ, Erläuternder Bericht DSV, 48.

642 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 19 und 22; weitergehend Fix, 281 ff.

643 SHK DSG-Baeriswyl, Art. 28 N 33.

644 EDÖB, Das neue DSG, 7; dies ebenfalls aufgreifend PC LPD-Béguin, Art. 28 N 51.

645 OFK DSG-Bieri/Heymann/Odermatt, Art. 28 N 24; Laux, digma 2019, 169.

646 PC LPD-Béguin, Art. 28 N 55; OFK DSG-Bieri/Heymann/Odermatt, Art. 28 N 24; Laux, digma 2019, 69.

Vernichtung der Daten muss die Betroffene eigenständig geltend machen (Art. 32 Abs. 2 lit. c DSG). Allerdings sind in der Praxis Mischformen möglich, etwa wenn bei der Ausübung des Portabilitätsrechts der Wille deutlich zum Ausdruck kommt, dass die Betroffene die Daten löschen lassen möchte. Dogmatisch lässt sich ein solcher Anspruch aber nicht aus dem Recht auf Datenportabilität ableiten. Daran ändert auch nichts, dass Art. 28 DSG dies – anders als Art. 20 DSGVO – nicht ausdrücklich festhält.

f. Folgen der Nichteinhaltung

Kommt der Verantwortliche dem Portierungsgesuch nicht oder nicht rechtzeitig nach, so sieht das DSG keine Sanktionen vor. Eine Verletzung des Rechts auf Datenportabilität ist namentlich nicht strafbewehrt.[647] Möchte die Betroffene ihr Recht auf Datenportabilität durchsetzen, muss dies auf dem Zivilweg geschehen oder vom EDÖB verfügt werden (Art. 51 DSG).[648] 216

7. Rechtsnatur

a. Allgemein

Die Rechtsnatur des Datenportabilitätsrechts ist bislang nicht restlos geklärt. Vertiefte Untersuchungen dazu gibt es nicht. Einzelne Autoren äussern jedoch die Ansicht, dass es sich um ein höchstpersönliches Recht handle, auf welches die Betroffene nicht im Voraus verzichten kann.[649] 217

Damit ziehen sie Parallelen zum zweiten Betroffenenrecht des DSG, dem Auskunftsrecht: Dieses ist nach der herrschenden Lehre relativ-höchstpersönlich, unverjährbar und nicht vererblich.[650] Ist eine Betroffene nicht urteilsfähig, kann die gesetzliche Vertretung das Auskunftsrecht ausüben.[651] Art. 25 Abs. 5 DSG hält zudem ausdrücklich fest, dass niemand im Voraus auf das Auskunfts- 218

647 Rosenthal, Jusletter 2020, Rz. 136. Anders die vorsätzliche Verletzung von Art. 25 DSG, indem etwa eine falsche oder unvollständige Auskunft erteilt wird.

648 Rosenthal, Jusletter 2020, Rz. 136.

649 PC LPD-Béguin, Art. 28 N 33; CR LPD-Benhamou, Art. 28 N 76.

650 Botschaft DSG 2017, 7066; BJ, Erläuternder Bericht VE-DSG, 66; SHK DSG-Pärli/Flück, Art. 25 N 18; Rosenthal, Jusletter 2020, Rz. 115; OK DSG-Steiger, Art. 25 N 9; Weber/Thouvenin, 54 f.

651 BSK ZGB I-Fankhauser, Art. 19c N 4; Rosenthal, Jusletter 2020, Rz. 115.

recht verzichten kann. Eine entsprechende Regelung fehlt in Art. 28 DSG.[652] Daraus lässt sich m.E. aber nicht ableiten, dass es sich beim Recht auf Datenportabilität anders verhält. Die beiden Institute müssen zwar auf konzeptioneller Ebene getrennt werden, da sie, wie noch zu zeigen sein wird, andere Zielsetzungen verfolgen.[653] Es würde allerdings den Zielen von Art. 28 DSG zuwiderlaufen, wenn eine Betroffene vorab auf das Portabilitätsrecht verzichten könnte.[654] Zudem steht sowohl beim Auskunftsrecht als auch beim Portabilitätsrecht die betroffene Person im Zentrum: Die beiden Betroffenenrechte weisen also auch Gemeinsamkeiten auf. Daher ist es generell angebracht, von einer identischen Rechtsnatur auszugehen. Das Recht auf Datenportabilität ist nach hier vertretener Ansicht ebenfalls ein höchstpersönliches Recht, welches grundsätzlich der Stellvertretung offensteht.[655]

b. Keine Portierung nach dem Tod

219 Das DSG erfasst nur lebende Menschen; einen postmortalen Persönlichkeitsschutz kennt das schweizerische Recht grundsätzlich nicht.[656] Somit ist das DSG für Daten über verstorbene Personen nicht anwendbar. Unter der aVDSG war für das Auskunftsrecht noch ausdrücklich die Möglichkeit vorgesehen, unter bestimmten Umständen Auskunft über die Daten verstorbener Personen zu erhalten (siehe Art. 1 Abs. 7 aVDSG). Diese Bestimmung wurde allerdings stark kritisiert, da sie auf keiner ausreichenden gesetzlichen Grundlage basierte. Anlässlich der Revision verzichteten die Räte darauf, eine solche im DSG zu schaffen.[657] Mit Blick auf die Rechtsprechung des BGer, wonach Tote nicht rechtsfähig und damit nicht parteifähig sind und auch niemand als deren Vertretung einen Prozess führen kann,[658] kommt ein Portabilitätsrecht nach dem Tod einer Person daher nicht in Frage.

220 Diese Problematik wird, anders als für das Auskunftsrecht, in der Literatur kaum thematisiert. Vertreten wird einzig und wohl mit Blick auf den vom BGer anerkannten Andenkensschutz,[659] dass Angehörige «ein» Recht auf Datenpor-

652 Der Gesetzgeber verweist an unterschiedlichen Stellen auf das Auskunftsrecht (dazu Rz. 221 und zu den Verweisen innerhalb der DSV Rz. 210), verzichtete jedoch auf einen Verweis auf Art. 25 Abs. 5 DSG.

653 Grundlegend dazu Rz. 62 f.; zur Abgrenzung zum Auskunftsrecht Rz. 346 ff.

654 PC LPD-Béguin, Art. 28 N 33; zu den Zielen Rz. 245 ff., insb. 250 ff. und 294 ff.

655 CR LPD-Benhamou, Art. 28 N 76; Charlet, 575, verweisend auf 526.

656 BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt, Art. 5 N 43.

657 AB 2019 N 1805; ausführlich hierzu BSK DSG-Gramigna, Art. 25 N 7 f.

658 BGE 129 I 302 E. 1.2.4.

659 BGE 129 I 302 E. 1.2.2.

tabilität gestützt auf ihr eigenes Persönlichkeitsrecht nach Art. 28 ZGB geltend machen könnten, das nach einer Interessenabwägung gewährt werde.[660] Dabei handelt es sich aber kaum mehr um das datenschutzrechtliche Datenportabilitätsrecht, sondern um eine davon unabhängige Geltendmachung zivilrechtlicher Ansprüche gestützt auf Art. 28 ZGB, auf welche lediglich im Ergebnis (teilweise) die Herausgabe der gleichen Daten erfolgen kann, wie dies unter dem Portabilitätsanspruch nach Art. 28 DSG geschehen wäre.

8. Einschränkungen nach Art. 29 DSG

Nach Art. 29 DSG kann der Verantwortliche die Herausgabe oder Übertragung einschränken. Für die Begründung wird auf das Auskunftsrecht nach Art. 26 Abs. 1 und 2 DSG verwiesen. Dies ist einerseits schlüssig, da so vermieden wird, dass mit dem Portabilitätsrecht die Einschränkungen des Auskunftsrechts – angesichts der nicht deckungsgleich erfassten Daten zumindest bis zu einem gewissen Grad – umgangen werden können.[661] Andererseits gilt dieser Verweis aber als missglückt, weil er in der Sache kaum auf das Portabilitätsrecht passt.[662] 221

Art. 29 Abs. 1 i.V.m. Art. 26 Abs. 1 DSG sieht vor, dass die Herausgabe oder Übertragung verweigert, eingeschränkt oder aufgeschoben werden kann, wenn ein formelles Gesetz dies vorsieht (namentlich, um ein Berufsgeheimnis zu schützen, lit. a), wenn dies aufgrund überwiegender Interessen Dritter erforderlich ist (lit. b) oder wenn das Gesuch offensichtlich unbegründet ist (lit. c). Gesetzlich vorgesehene Einschränkungen sind im Einzelfall zu untersuchen. Das Berufsgeheimnis hingegen dürfte beim Portabilitätsrecht kaum relevant sein, da es primär die Betroffene schützt, welche mit dem Portabilitätsrecht die sie betreffenden Daten herausverlangt.[663] Bei den möglichen überwiegenden Interessen Dritter steht der Doppel- oder Drittbezug von Daten erneut im Vordergrund, aber auch Geschäftsgeheimnisse oder Immaterialgüterrechte Dritter sind denkbar.[664] 222

Offensichtlich unbegründet soll ein Gesuch sein, wenn es «einen datenschutzwidrigen Zweck verfolgt, oder offensichtlich querulatorisch ist» (Art. 29 Abs. 1 223

660 CR LPD-Benhamou, Art. 28 N 12.

661 CR LPD-Benhamou, Art. 29 N 10; OFK DSG-Bieri/Heymann/Odermatt, Art. 29 N 1; Götzinger/Vasella, SZW 2021, 46; Landolt, 176; zur Abgrenzung Rz. 346 ff.

662 SHK DSG-Baeriswyl, Art. 29 N 1; BSK DSG-Laux/Steiner, Art. 29 N 6.

663 SHK DSG-Baeriswyl, Art. 29 N 3; ähnlich Rosenthal, Jusletter 2020, Rz. 132.

664 OFK DSG-Bieri/Heymann/Odermatt, Art. 29 N 6 f.; siehe auch Landolt, 178 ff., der faktisch eine Prüfpflicht für den Verantwortlichen sieht; dazu auch Rz. 191 ff.

i.V.m. Art. 26 Abs. 1 lit. c DSG). Gerade die Möglichkeit bei einem datenschutzwidrigen Zweck das Gesuch verweigern zu können, ist angesichts der noch zu diskutierenden datenschutz- *und* wettbewerbsrechtlichen Zielsetzung nur schwer mit dem Portabilitätsrecht vereinbar. Vorwegzunehmen ist, dass das Portabilitätsrecht u.a. auf einen freien Datenfluss abzielt[665] und deswegen ein Gesuch nicht leichthin als offensichtlich unbegründet gelten sollte.[666] Es ist somit unklar, in welchen Fällen der Verantwortliche ein Gesuch verweigern darf. Mit dem Portabilitätsrecht sollen Daten gerade möglichst standardisiert und befreit von Einzelfallgerechtigkeit zwischen unterschiedlichen Akteuren verschoben werden können.[667] Unbegründetheit liegt aber immerhin dann vor, wenn das Portabilitätsrecht rechtsmissbräuchlich ausgeübt wird. Genannt wird ferner der Fall einer Beweisbeschaffung gegen den Verantwortlichen in einem Zivilprozess.[668]

224 Auch die Einschränkungsgründe nach Art. 26 Abs. 2 lit. a DSG, wonach der Verantwortliche überwiegende Interessen geltend machen kann, wenn er die in Frage stehenden Personendaten nicht Dritten bekanntgibt, passen kaum auf das Recht auf Datenportabilität.[669] Adressiert sein sollen Geschäftsgeheimnisse und Immaterialgüterrechte des Verantwortlichen.[670] Schliesslich dürfte den Einschränkungsgründen für Bundesorgane kaum eine Bedeutung zukommen, da diese nur in Ausnahmefällen zu einer Portierung verpflichtet sind. In jedem Fall muss der Verantwortliche die Verweigerung, Einschränkung oder Aufschiebung begründen (Art. 29 Abs. 2 DSG).

225 Damit erscheinen sämtliche Einschränkungsgründe nach Art. 26 DSG in Bezug auf das Datenportabilitätsrecht als unbefriedigend und kaum auf die Verhältnisse des Portabilitätsrechts zugeschnitten. Somit spricht vieles dafür, den Einschränkungsgründen nicht zu viel Gewicht beizumessen und sie im Kontext des Portabilitätsrechts generell eng auszulegen.

665 Dazu Rz. 328 ff.

666 SHK DSG-Baeriswyl, Art. 29 N 6.

667 BSK DSG-Laux/Steiner, Art. 29 N 6.

668 OFK DSG-Bieri/Heymann/Odermatt, Art. 29 N 8.

669 Siehe dazu CR LPD-Benhamou, Art. 29 N 7 und 12; Landolt, 177, der von einem gesetzgeberischen Versehen ausgeht und dass dieser Einschränkungsgrund unbeachtlich sei.

670 OFK DSG-Bieri/Heymann/Odermatt, Art. 29 N 7.

IV. Erkenntnisse

Das Recht auf Datenportabilität übernahm die Schweiz aus der DSGVO. Aus Sicht der Räte spielte dabei die Notwendigkeit eines Angemessenheitsbeschlusses durch die EU eine Rolle und diente als Argument für die Verankerung im DSG. Diese Argumentation verfing in den Räten möglicherweise gegenüber derjenigen des Bundesrates, welcher zunächst einzelne sektorielle Portabilitätsrechte prüfen wollte und sich bewusst war, dass mit dem Institut zahlreiche neue Fragen aufgeworfen würden. Angestrebt wurde durch die Verankerung im DSG insoweit ein Gleichlauf mit der DSGVO. Dies macht deutlich, dass sich die europäische Regelung bei der Interpretation der schweizerischen Regelung unmittelbar heranziehen lässt. 226

Bereits die in diesem Kapitel untersuchten Grundlagen lassen erkennen, dass es sich beim Datenportabilitätsrecht nicht nur um ein neues, sondern auch um ein neuartiges Rechtsinstitut handelt. Die Möglichkeit einer weitgehenden Übertragung von Daten ist auf grundlegende Designprinzipien des Webs zurückzuführen und auf die Idee, dass erst eine weitgehende Verlinkbarkeit, Offenheit und Interkonnektivität innovative Angebote, wie wir sie heute kennen, schaffen konnten. Solche innovativen Angebote stellen etwa die sozialen Netzwerke und andere Internetplattformen dar, welche sich jedoch seit einigen Jahren zunehmend abschotten und *walled gardens* bilden, die von aussen nicht mehr zugänglich sind. Gerade die in jüngerer Zeit entstandenen grossen Internetplattformen (sog. *Big Tech*) und dabei besonders die sozialen Netzwerke standen beim Erlass des Instituts im Vordergrund und bildeten aus gesetzgeberischer Sicht den primären Regulierungsgegenstand. 227

Die parlamentarischen Beratungen zeigen, dass beim Recht auf Datenportabilität – nach Vorbild der EU – nicht nur datenschutzrechtliche Aspekte berücksichtigt wurden. Eine mögliche wettbewerbsrechtliche Komponente dominierte die Diskussionen von Beginn weg und war auch der Grund, weshalb der Bundesrat zunächst zuwarten wollte. In den Voten des Nationalrats kam der Wille, Monopolen vorzubeugen und Netzwerkeffekte zu verringern, deutlich zur Geltung. Besonders erwähnt wurden dabei jeweils sowohl in der EU als auch in der Schweiz die Internetplattformen und sozialen Netzwerke. In der EU wurden ausdrückliche Hinweise auf soziale Netzwerke jedoch während des Gesetzgebungsprozesses aus dem Verordnungstext entfernt und der zuständige Berichterstatter wies darauf hin, dass das Instrument in diesen Fällen ohnehin teilweise leerlaufen dürfte, weil es Netzwerkeffekten nicht entgegenzu- 228

treten vermöge. Dies lässt darauf schliessen, dass ein breiterer (persönlicher) Anwendungsbereich vom europäischen Gesetzgeber gewollt und umgekehrt eine Einschränkung nur auf soziale Netzwerke oder Plattformen nicht gewünscht war. Dies widerspiegelt nunmehr der weite Anwendungsbereich von Art. 20 DSGVO, der grundsätzlich sämtliche Verantwortliche als Normadressatinnen erfassen kann.

229 Eine Einschränkung der Normadressatinnen stand in der Schweiz nicht zur Debatte, obwohl die Räte das Recht stets mit Verweis auf die Internetplattformen diskutierten. Zwar verwiesen sie in ihren Beratungen auf Datengenossenschaften, den öffentlichen Verkehr, die medizinische Forschung oder die Gesundheitsvorsorge. Sie wollten also gerade auch die Übertragung von Daten zu andersartigen Anbietern, wie von Vertreterinnen der US-amerikanischen IT-Szene vorgedacht, ermöglichen und waren sich des übergreifenden Potenzials des Instituts bewusst. Die Ratsmitglieder bezogen sich bei diesen Anwendungsbeispielen aber ausschliesslich auf Anbieterinnen in der Rolle als *neue* Verantwortliche, also auf die Frage, wem die Daten zur Verwendung überlassen werden könnten. Nicht diskutiert wurde in diesem Kontext, wen das Recht auf Datenportabilität als alten Verantwortlichen und damit Normadressaten in die Pflicht nehmen soll.

230 Aus der Entstehungsgeschichte lässt sich damit nicht eindeutig rekonstruieren, ob die Räte – wie von Nationalrat Glättli festgehalten – vor allem den Abfluss der Daten «weg von den riesigen Plattformen, weg von den riesigen Firmen und hin zu neuen, innovativen Unternehmen» meinten,[671] oder ob sie – wie im Wortlaut in Art. 28 DSG verankert – das Portabilitätsrecht weitergehend verstanden haben wollten. Geschaffen wurde jedenfalls ein weitreichendes, sektorübergreifend anwendbares Portabilitätsrecht, das auf alle Verantwortlichen anwendbar ist. Es handelt sich beim nunmehr in Art. 28 DSG verankerten Portabilitätsrecht also um ein auf den Datenverkehr im Internet abzielendes Institut, das in seinem tatsächlichen Anwendungsbereich potenziell weiter geht. Damit führt die historische Betrachtung zur widersprüchlichen Erkenntnis, dass das Ergebnis in Art. 28 DSG die Debatte in den Räten nur beschränkt widerspiegelt und der Gesetzgeber nicht umfassend verschriftlichte, was er diskutierte.

231 Hinsichtlich der rechtlichen Umsetzung des Portabilitätsrechts sind für die Schweizer Regelung nur punktuell Unterschiede zur DSGVO feststellbar. So erscheint die DSG-Regelung bei einer sprachlich-grammatikalischen Ausle-

671 Votum NR Glättli, AB 2019 N 1813.

gung etwas nutzerzentrierter. Der Betroffenen steht nach Art. 28 Abs. 1 DSG das Recht zu, die Herausgabe an sie zu verlangen. Damit ist, anders als unter der DSGVO, nicht ausdrücklich vorgesehen, dass die Daten an Dritte übermittelt werden. Die Herausgabe stellt nach diesem Wortlaut den Endzustand und nicht bloss einen Zwischenschritt dar. Dies ist bei näherem Hinsehen konsequent, da Dritten ohnehin keine datenschutzrechtliche Rolle und insb. keine Pflicht zukommt, die Daten anzunehmen. Allerdings wird das in der DSGVO verankerte Behinderungsverbot teils auch in der Schweiz als Pflicht des alten Verantwortlichen angenommen. Gleichwohl treten aufgrund des Wortlauts bei der Datenherausgabe persönlichkeitsrechtliche Aspekte in den Vorder- und wettbewerbsrechtliche Aspekte in den Hintergrund. Dies ist bei der teleologischen Auslegung zu berücksichtigen.

232 Ein weiterer Unterschied ist, dass in der Schweiz eine Rechtfertigung für private Verantwortliche nicht immer notwendig ist. Nach dem Prinzip der Erlaubnis mit Verbotsvorbehalt können in der Schweiz Datenbearbeitungen zulässig sein, ohne dass eine Rechtfertigung vorliegt. Aus diesem Grund ist bei der Auslegung von Art. 28 Abs. 1 lit. b DSG auf die Freiwilligkeit der Datenbearbeitung abzustellen. Wesentlich ist, ob die Initiative für eine konkrete Datenbearbeitung von der Betroffenen ausgegangen ist.

233 Dies gilt auch für staatliche Datenbearbeitungen in der Schweiz. Anders als unter der DSGVO sind Datenbearbeitungen in Wahrnehmung öffentlicher Aufgaben nicht ausdrücklich vom Anwendungsbereich des Portabilitätsrechts ausgeschlossen. Zwar wurde dargelegt, dass kantonale und kommunale öffentliche Organe von vornherein nicht dem DSG und folglich nicht dem Recht auf Datenportabilität unterliegen. Gleichzeitig können aber in der Schweiz Bundesorgane in bestimmten Fällen vom Institut erfasst sein. Es zeigte sich jedoch, dass unter dem Rechtfertigungsregime des DSG ein Ausschluss wie ihn die DSGVO vorsieht, nicht notwendig ist.

234 In einer Hinsicht ist die Schweizer Regelung zudem klarer als ihr europäisches Vorbild: Die Ausführungsbestimmungen in der DSV legen fest, dass das Recht auf Datenportabilität nicht für abgeleitete Daten, wohl aber für beobachtete Daten zur Anwendung gelangt. Diese Haltung vertraten Parlament und Bundesrat bereits in den Beratungen dezidiert; sie ist in der Schweiz unbestritten. Damit bleibt weniger Interpretationsspielraum als unter der DSGVO, wo sich diesbezüglich in der Lehre noch immer keine einheitliche Meinung gebildet hat.

235 Weniger eindeutig ist der Umgang mit Daten mit Doppelbezug. Vom Wortlaut von Art. 28 DSG erfasst sind lediglich die Personendaten der Betroffenen. Wei-

sen sie einen Doppelbezug auf und beziehen sich damit auch auf Dritte, so ist umstritten, ob die Daten zu portieren sind. Vorliegend wurde postuliert, dass eine Portierung weitgehend möglich sein muss, damit das Portabilitätsrecht nicht ins Leere läuft. Zudem fallen von Dritten bekanntgegebene Daten ebenfalls unter das Portabilitätsrecht, wenn sie interdependent sind zu den bekanntgegebenen Daten der Betroffenen. Würde dies verneint, so wäre gerade bei den gesetzgeberisch anvisierten sozialen Netzwerken die Folge, dass relevante Drittdaten nicht vom Portabilitätsrecht erfasst wären.

236 Für die Modalitäten verweist die DSV pauschal auf das Auskunftsrecht. Eine Portierung ist somit etwa per Post oder E-Mail zulässig und muss innert 30 Tagen erfolgen. Diese Modalitäten entsprechen kaum einem auf den Internetverkehr abzielenden Institut. Zwar ist das Portabilitätsrecht, wie gezeigt, von seinem Wortlaut her weitergehend anwendbar, sofern Daten nur schon automatisiert bearbeitet werden. Dennoch scheinen diese Modalitäten kaum zeitgemäss und dürften jedenfalls nicht dem gesetzgeberischen Verständnis entsprechen, wonach Daten gerade von Internetplattformen wegbewegt werden sollen. Der Verweis auf die Modalitäten des Auskunftsrechts ist damit unbefriedigend.

§ 3 Rechtsdogmatische Einordnung

I. Einleitung

237 Nach den historischen Aspekten, den technischen Grundlagen und der positivrechtlichen Normierung des Rechts auf Datenportabilität ist das schweizerische Rechtsinstitut mit vergleichendem Blick auf die DSGVO im gesamten (datenschutz-)rechtlichen Gefüge zu analysieren. Dabei ist evident, dass ein besonderes Augenmerk auf datenschutzrechtliche Ziele und dabei insb. die informationelle Selbstbestimmung gelegt werden muss. Mittlerweile scheint denn auch die Lehre mehrheitlich davon auszugehen, dass das Recht auf Datenportabilität (auch) solche Ziele verfolgt.[672] Auf was solche «datenschutzrechtlichen Ziele» genau abzielen, ist aber, wie bereits aufgeführt wurde, ebenso unklar wie der genaue Gehalt eines Rechts auf informationelle Selbstbestimmung. Eine konzeptionelle Klärung wird in der Literatur kaum je vorgenommen.[673] Zumeist wird lediglich pauschal auf die Existenz solcher Zielsetzungen verwiesen.

238 Bereits die historischen Grundlagen zeigten, dass wettbewerbsrechtliche Ziele ebenfalls eine Rolle im Gesetzgebungsprozess spielten. Durch den Einbezug der neuen Verantwortlichen bei der Datenübertragung ergibt sich eine Nähe zum Wettbewerbsrecht auch aus den rechtlichen Grundlagen. Entsprechend finden solche Ziele in der Literatur ebenfalls oft Erwähnung, wenn das Recht auf Datenportabilität untersucht wird.[674]

239 Diese Stossrichtungen sind auch in der EU zu beobachten: Ein datenschutzrechtliches *Empowerment* der Betroffenen[675] wird wettbewerbsrechtlichen

672 Von einer Stärkung der «autonomie informationelle» sprechend CR LPD-Benhamou, Art. 28 N 4; die «Kontrolle der betroffenen Person über ihre Personendaten» ansprechend Charlet, 573; ebenso Epiney/Nüesch/Rovelli, 178; die Einschätzung noch auf dem E-DSG basierend Frei, Jusletter 2018, Rz. 57; einen «doppelten Zweck» erkennend: Götzinger/Vasella, SZW 2021, 41; differenzierend Laux, digma 2019, 166 und 170, der auf einen Paradigmenwechsel hinweist, diesen aber im Datenschutz verankert sieht; von Autonomie als Aspekt des Persönlichkeitsschutzes spricht etwa Métille, Nouveautés, 39; Roth, SZW 2020, 677; SGK BV-Schweizer/Striegel, Art. 13 N 109; Steiner, 125; differenzierend und auch auf Wechselwirkungen zwischen datenschutzrechtlicher und kartellrechtlicher Zielsetzung hinweisend Weber/Thouvenin, 69.

673 In diese Richtung auch Thouvenin, digma 2019, 208 f.

674 CR LPD-Benhamou, Art. 28 N 4; Botschaft DSG 2017, 6984; Bundesrat, Bericht Handlungsfelder, 25 f.; Götzinger/Vasella, SZW 2021, 41; Métille, Obligations, 19 f.; Roth, SZW 2020, 677; Weber/Thouvenin, 68 f.; i.E. solche Ziele ablehnend, dies jedoch ebenfalls aufgreifend Laux, digma 2019, 170.

675 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 4; beide Aspekte aufbringend Artikel 29-Datenschutzgruppe, Stellungnahme Berechtigtes Interesse, 60 f., wobei

Zielen[676] gegenübergestellt. Bisweilen werden die Ziele auch verbunden: So soll das *Empowerment* einem grösseren Zweck dienen, namentlich den Wettbewerb fördern und Lock-In-Effekte verhindern.[677] Dabei fällt es zunehmend schwer, das Institut dem «klassischen» Datenschutzrecht oder dem «klassischen» Wettbewerbsrecht zuzuordnen, gerade weil es teilweise in andere, grössere Zusammenhänge gestellt und etwa festgehalten wird, dass es um «datenpolitische Fragen»[678] oder um ein «Signal in die Zukunft»[679] gehe und es sich um ein Institut handle, welches «mit der tradierten Zweckausrichtung des Datenschutzrechts» breche[680]. Damit lässt sich bereits vorwegnehmen, dass die Zielsetzungen eng verflochten und nicht immer trennscharf unterscheidbar sind.

Um die genauen Ziele des Datenportabilitätsrechts zu erkennen, wird das Institut in diesem Kapitel systematisch eingeordnet und anschliessend teleologisch ausgelegt. Abschliessend wird es von anderen Instituten abgegrenzt und gestützt darauf der erste Teil der Forschungsfrage beantwortet. 240

die englische Sprachfassung ausdrücklich von *Empowerment* spricht; Graef, CPI Antitrust Chronicle 2020, 35; International Working Group on Data Protection in Technology, 6; Janal, 320; Tombal, 514; beide Argumente aufbringend Kratz, InTeR 2019, 27; OECD, Mapping Initiatives, 8; ebenfalls in diese Richtung Thouvenin/Weber/Früh, 172; Weber/Thouvenin, 68 ff. und insb. 70.

676 Beide Aspekte aufbringend Artikel 29-Datenschutzgruppe, Stellungnahme Berechtigtes Interesse, 60 f.; ebenso Graef, CPI Antitrust Chronicle 2020, 35; Hennemann, PinG 2017, 6; beide Aspekte aufbringend Kratz, InTeR 2019, 27; Nebel/Richter, ZD 2012, 413; Reichlin, 414; Schätzle, PinG 2016, 74.

677 Janal, JIPITEC 2017, 60; ähnlich Thouvenin/Weber/Früh, 171.

678 Votum SR Bruderer, AB 2018 S 617.

679 BSK DSG-Laux/Steiner, Art. 28 N 72.

680 Landolt, 153.

II. Systematische Einordnung

241 In systematischer Hinsicht ist zunächst schlicht festzuhalten, dass Art. 28 im *Datenschutz*gesetz verankert ist, nur auf Personendaten Anwendung findet (Art. 2 Abs. 1 DSG) und somit systematisch im Lichte des DSG auszulegen ist.[681] Art. 1 DSG hält allgemein fest, dass das DSG den Schutz der Persönlichkeit und der Grundrechte derjenigen Personen, über die Personendaten bearbeitet werden, bezweckt.

242 Diese Tatsache kann dazu verleiten, anzunehmen, dass es sich um eine Norm mit datenschutzrechtlicher Zielsetzung handelt, sie also den Schutz der Persönlichkeit und der Grundrechte der Betroffenen bezweckt.[682] Dieser Schluss ist jedoch umstritten, gerade wenn für das Datenschutzrecht ein blosser Vorfeldcharakter zum Schutz anderer Grundrechte angenommen wird.[683] So lässt die Formulierung von Art. 1 DSG (*Grundrechte*; im Plural) die Auffassung zu, dass ein Datenschutzgrundrecht vor allem anderen Interessen und Rechten diene.[684] Namentlich kann daraus auch auf wettbewerbsrechtliche Ziele geschlossen werden. In der europäischen Literatur wird entsprechend teilweise dezidiert vertreten, dass aus der Regelung in der DSGVO keine datenschutzrechtlichen Ziele abgeleitet werden könnten.[685] Dabei wird vorgebracht, dass aus der datenschutzrechtlichen Ausgestaltung des Portabilitätsrechts nicht auf dessen datenschutzrechtliche Konzeption geschlossen werden könne.[686]

243 Tatsächlich wurde auch in der Schweiz vor der Revision des DSG diskutiert, ob das Recht auf Datenportabilität überhaupt datenschutzrechtliche Ziele verfolge, und ein solches Recht daher im DSG verankert werden sollte.[687] Die auf-

681 Vereinzelt wurde in der europäischen Literatur sogar verlangt, dass nicht-datenschutzrechtliche Zwecke bei der Auslegung eine untergeordnete Rolle spielen sollten und «maximal hilfsweise» hinzugezogen werden sollten, siehe KRAUSE, PinG 2018, 240.

682 Siehe dazu die theoretischen Ausführungen unter Bezugnahme auf den Zweckartikel in Art. 1 aDSG bei KRAMER/ARNET, 174 f.; BSK DSG-LAUX/STEINER, Art. 28 N 68.

683 Dazu Rz. 63 und 76.

684 MARSCH, 87; THOUVENIN, digma 2019, 209.

685 FIX, 65 und 103 f., der für die DSGVO-Regelung einen Schluss vom Ergebnis der Aufnahme in die DSGVO auf die Frage der Berechtigung ebendieser Aufnahme sieht, welche «allerhöchstens als ein Indiz» für einen datenschutzrechtlichen Zweck angesehen werden könne.

686 MARSCH, 102 f.; siehe auch FIX, 50.

687 Botschaft DSG 2017, 6984; BJ, Erläuternder Bericht VE-DSG, 22; zu den Argumenten des Bundesrates ferner THOUVENIN/WEBER/FRÜH, 143 f.; die gleichen Diskussionen auch im europäischen Gesetzgebungsprozess feststellend FIX, 36 f. m.w.N.

geführte Kritik ist daher nicht unberechtigt und es ist heikel, wenn aus der Tatsache, dass eine Regelung im DSG erfolgte, *eo ipso* eine datenschutzrechtliche Regelung angenommen wird. In erster Linie war die Verankerung im DSG jedoch eine gesetzgeberische Entscheidung, die auch anders hätte erfolgen können.[688] Nachdem sich das Institut aber nunmehr im DSG findet, ist es im Gefüge des DSG zu betrachten, weshalb die Regelung – bei rein systematischer Betrachtung – auch datenschutzrechtlich verstanden werden muss. Denn die Normierung führt im Ergebnis zu einer nur beschränkten Anwendbarkeit auf Personendaten. Dies legt einen Konnex zur Persönlichkeit der Betroffenen und ihrer informationellen Selbstbestimmung auf konzeptioneller Ebene zumindest nahe.

Gleiches gilt, wenn die Systematik innerhalb des DSG betrachtet wird: Das Institut wird im vierten Kapitel neben dem Auskunftsrecht als einziges Betroffenenrecht aufgeführt. Unter der DSGVO ist die Bestimmung ebenfalls als Betroffenenrecht verankert. Daraus lässt sich ablesen, dass die Betroffene ins Zentrum gestellt und ihr ein Instrument gegeben werden soll, um über Daten zu verfügen, die sie betreffen. Damit liegt der Schluss nahe, dass das Portabilitätsrecht zumindest auch datenschutzrechtlich zu verstehen ist. Dies schliesst freilich nicht aus, dass es daneben weitere Ziele geben kann, die keine Nähe zur Persönlichkeit der betroffenen Person aufweisen. 244

688 Siehe für die DSGVO auch Kratz, InTeR 2019, 30, nach welchem die Einordnung ins Datenschutzrecht weder als richtig noch als falsch zu qualifizieren sei, sondern «schlicht eine gesetzgeberische Entscheidung zugunsten des Betroffenen» darstelle.

III. Teleologische Einordnung

A. Datenschutzrechtliche Ziele

1. Europäische Konzeption: Teilhabesicherung an privater, sozialer und öffentlicher Kommunikation

a. Kritik an der herrschaftsrechtlichen Auslegung

245 In der europäischen Literatur werden die datenschutzrechtlichen Ziele des Rechts auf Datenportabilität, sofern sie überhaupt bejaht werden, nur selten vertieft untersucht. Meist wird eher pauschal festgehalten, dass den Betroffenen die Kontrolle über ihre Daten zurückgegeben werden soll.[689] Damit wird an eine herrschaftsrechtliche Vorstellung des Datenschutzes angeknüpft, welche, wie bereits erläutert, auf europäischer Ebene und wohl auch auf deutscher Ebene so nicht (mehr) existiert.[690] Sie gründet auf einem Recht auf informationelle Selbstbestimmung und ist eng an die deutsche Konzeption geknüpft, die auf die Rechtsprechung des BVerfG zurückgeht und in der (oft deutschen) Literatur vertreten wird.[691] Diese wurde jedoch, wie ebenfalls bereits aufgezeigt, unter der hier massgeblichen europäischen Rechtslage gar nicht übernommen.[692]

246 Fix vertieft dies, soweit ersichtlich als einziger, und spricht hierbei von einem kontrollorientierten «individuell-herrschaftsrechtlichen» Datenschutzverständnis.[693] So deute die historische Auslegung des Rechts auf Datenportabilität zwar darauf hin, dass der Unionsgesetzgeber den Datenschutz tatsächlich herrschaftsrechtlich verstanden habe.[694] Doch zuletzt sei selbst bei eigentlichen Befürworterinnen eines herrschaftsrechtlichen Verständnisses eine Ab-

---

689 Brüggemann, 5; ReMKomm-Spindler/>Dalby, Art. 20 DSGVO N 1; KUKO DSGVO-Kamann/Braun, Art. 20 N 4; Paal/Götz, ZD 2023, 67; BeckKompaktKomm-Paal, Art. 20 DSGVO N 4; GK-Piltz, Art. 20 DSGVO N 3; Troiano, 164; Zanfir, IDPL 2012, 155; a.M. hingegen BeckKomm-Herbst, Art. 20 DSGVO N 4 m.w.N.

690 Dazu Rz. 61 ff.

691 Brüggemann, 1; Kratz, InTeR 2019, 29; Lynskey, European Law Review 2017, 810; Zanfir, IDPL 2012, 152.

692 Dazu Rz. 64.

693 Fix, 36 ff.

694 Fix, 49, der insoweit von einem «Kontrollnarrativ» spricht; ähnlich auch Marsch, 105.

kehr von dieser Haltung zu beobachten, so namentlich in der jüngeren Rechtsprechung des BVerfG.[695] Nach dem herrschaftsrechtlichen Verständnis müsste das Selbstbestimmungsrecht zudem eine unmittelbare Drittwirkung auch auf den Verantwortlichen haben, was jedoch nicht der Fall sei.[696] Ein allgemeines oder gar umfassendes Selbstbestimmungsrecht über die Nutzung der eigenen Daten komme bereits nach dem deutschen Verständnis der informationellen Selbstbestimmung nicht in Frage und müsse daher umso mehr für die DSGVO abgelehnt werden.[697] Fix räumt zwar ein, dass eine herrschaftsrechtliche Zielsetzung des Portabilitätsrechts möglich sei. Dies würde aber bedingen, dass das europäische Datenschutzrecht im Sinne des deutschen Rechts auf informationelle Selbstbestimmung verstanden würde, und dass dieses Verständnis auch auf private Datenverarbeitungen im Sinne einer unmittelbaren Drittwirkung der Grundrechte zuträfe.[698] Dies ist kaum der Fall.

b. Votum für ein erweitertes Datenschutzverständnis

Im Zusammenhang mit der Ausübung des Rechts auf Datenportabilität führen europäische Autorinnen vielfach das Ziel eines neuartigen *Empowerments* der Betroffenen ins Feld.[699] Denn das Recht auf Datenportabilität vermittelt der Betroffenen einen positiven Rechtsanspruch und nicht bloss einen datenschutzrechtlichen Abwehranspruch.[700] Das Recht scheint also weiterzugehen und betritt tatsächlich datenschutzrechtliches Neuland. 247

Einige Autorinnen postulieren, das Recht auf Datenportabilität führe zu einer «dogmatischen Neuausrichtung» des traditionellen Verständnisses des Rechts auf informationelle Selbstbestimmung.[701] Darin spiegle sich der verhaltene 248

695 Fix, 50; zum Entscheid *Recht auf Vergessen I* bereits Rz. 61 und für die Schweiz Rz. 80.

696 Fix, 46.

697 Fix, 41 f., insb. Fn. 72; Marsch, 104; ebenfalls auf Fix verweisend BeckOK DSR-von Lewinski, Art. 20 DSGVO N 14.

698 Fix, 47.

699 So etwa Anciaux et al., GPLR 2021, 16 ff.; Artikel 29-Datenschutzgruppe, Guidelines Data Portability, 3; siehe auch die deutsche Version Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 3, wonach die betroffene Person «mit einer entsprechenden Befugnis auszustatten» sei; Crémer/De Montjoye/Schweitzer, 81; Janal, JIPITEC 2017, 60; GDPR-Comm-Lynskey, Art. 20, 502; Polański, EuCML 2018, 141.

700 Bitter/Straker, 750; Jülicher/Röttgen/v. Schönfeld, ZD 2016, 361; Weber/Thouvenin, 68.

701 Jülicher/Röttgen/v. Schönfeld, ZD 2016, 360, die nicht vertieft darauf eingehen, dass das Konzept der informationellen Selbstbestimmung in der EU nicht übernommen wurde aber immerhin darauf hinweisen, dass eine «kategorische Verengung» der Interpretation des Rechts der informationellen Selbstbestimmung am deutschen Massstab verkenne,

Versuch wider, die zunehmende Kommerzialisierung von Daten rechtlich abzubilden und das Institut sei als erste Weichenstellung für einen Datenhandel zu verstehen.[702] Vertieft äussert sich in diesem Zusammenhang abermals FIX, für den das Datenportabilitätsrecht Ausdruck eines «erweiterten regulatorischen Datenschutzverständnisses» ist, das nicht bloss ein «Mehr an Rechten» für die Betroffene darstelle, sondern als wettbewerbsregulatorisches Instrument zur Teilhabesicherung an privater, sozialer und öffentlicher Kommunikation funktioniere.[703] Dies gründe auf der Tatsache, dass das Konzept des Rechts auf informationelle Selbstbestimmung in seinem traditionellen Verständnis das gewandelte Gefährdungspotenzial moderner Datenbearbeitungen hinsichtlich der Persönlichkeitsrechte, aus denen dieses Recht abgeleitet wurde, kaum mehr ausreichend erfassen könne.[704]

249 Entgegen den Ausführungen zur herrschaftsrechtlichen Auslegung sei das Recht auf Datenportabilität damit eher als ein Teilhaberecht an Kommunikationsprozessen in der Gesellschaft zu verstehen.[705] Gerade auf europäischer Ebene werde die Datenverarbeitung und der Verkehr der Daten auch als wirtschaftliche Aktivität aufgefasst, weshalb der Datenschutz automatisch der Marktregulierung diene, indem er Regeln für den Umgang mit Daten aufstelle.[706] Entsprechend trete das Dogma einer klassisch herrschaftsrechtlichen Konzeption des Verbots mit Erlaubnisvorbehalt hinter ein regulatorisches Verständnis des Datenschutzgrundrechts als ein «Recht auf adäquate gesetzgeberische Ausgestaltung».[707] Damit erfahre das Recht auf informationelle Selbstbestimmung nach verfassungsrechtlicher Prägung resp. das Datenschutzgrundrecht mit der Einführung des Portabilitätsrechts einen «bedeutungsschweren Wandel».[708] Diese Ausführungen sind *mutatis mutandis* unter der Schweizer Rechtslage zu berücksichtigen, wobei insb. auf die Vorarbeiten von FIX abgestellt wird.

---

dass das Recht auf Datenportabilität vom europäischen Gesetzgeber entwickelt worden sei, der sich auf Art. 8 Abs. 1 GRCh beziehe.

702 JÜLICHER/RÖTTGEN/V. SCHÖNFELD, ZD 2016, 361; ähnlich auch SATTLER, Personenbezug, 83; SPERLICH, DuD 2017, 377.

703 FIX, 48; in diese Richtung auch AuernhammerKomm-SCHÜRMANN, Art. 20 DSGVO N 3.

704 FIX, 51 f.; WIELSCH, JZ 2020, 109 f.

705 FIX, 52.

706 FIX, 53; ähnlich auch BKartA, Sektoruntersuchung, 31.

707 FIX, 54. Kritisch anzumerken ist, dass die geforderte «gesetzgeberische Ausgestaltung» in letzter Konsequenz eine Drittwirkung unter Privaten darstellen kann und wird, wenn der Gesetzgeber entsprechend legiferiert. Damit nähert sie sich durchaus wieder dem herrschaftsrechtlichen Verständnis des Rechts auf informationelle Selbstbestimmung an.

708 JÜLICHER/RÖTTGEN/V. SCHÖNFELD, ZD 2016, 361; von einer «Modernisierung und Fortentwicklung des Datenschutzrechts» sprechend AuernhammerKomm-SCHÜRMANN, Art. 20 DSGVO N 3; ähnlich BKartA, Sektoruntersuchung, 31.

2. Verwirklichung der informationellen Selbstbestimmung als Ausgangspunkt der Schweizer Konzeption

a. Allgemein

In der Schweiz ist die Ausgangslage bezüglich der informationellen Selbstbestimmung allerdings in zweifacher Hinsicht anders. Einerseits hat das BGer – anders als das BVerfG – das Recht auf informationelle Selbstbestimmung bislang nicht präzisiert.[709] Andererseits stellt dieses – anders als unter der DSGVO – das Fundament für das DSG dar.[710] Auch in der parlamentarischen Beratung anlässlich der DSG-Revision gingen die Räte nicht davon aus, dass die informationelle Selbstbestimmung enger interpretiert werden könnte – im Gegenteil.[711] Ausgangspunkt ist damit in der Schweiz weiterhin das Recht auf informationelle Selbstbestimmung gemäss der aufgeführten Rechtsprechung und dazugehörigen Lehre als Fundament der datenschutzrechtlichen Zielsetzung des Portabilitätsrechts. 250

b. Selbstbestimmte Datendisposition als Ausfluss der informationellen Selbstbestimmung

Durch die Herausgabe und Übertragung der Daten bewirkt die Betroffene, dass Verantwortliche gewisse Daten an sie oder an Dritte transferieren. Sie kann somit die Zuordnung der Daten in beschränktem Umfang eigenständig kontrollieren.[712] Dadurch wird die Herrschaft über die Daten an die Betroffene (rück-)übertragen. Diese Herrschaft ist zwar bloss teilweise und nicht exklusiv. Dennoch stellt das Portabilitätsrecht für die Betroffene ein wirksames Instrument dar, das sie datenschutzrechtlich besserstellt. Denn über diese Daten 251

709 Siehe Thouvenin, ZSR Beiheft 2023, 14; ausführlich zum aktuellen Stand Rz. 73 ff.

710 Dazu für die Schweiz Rz. 68 ff.; zur Situation in der EU Rz. 61 ff.

711 Votum NR Glättli, AB 2018 N 963; grundlegend auch Votum NR Glättli, AB 2019 N 1778; Votum BR Sommaruga, AB 2018 S 618, wonach das Recht auf informationelle Selbstbestimmung letztlich nichts anderes bedeute, als das Recht, «selber über die eigenen Daten und deren Bearbeitung zu bestimmen». Dieses Recht gewinne «laufend an Bedeutung». In diesem Sinn bereits Botschaft DSG 2017, 7071; siehe auch Marsch, 105, nach welchem das von der EU-Kommission betonte und in den Erw.G vielfach betonte Ziel, den Bürgerinnen die Kontrolle über ihre Daten zu geben eher als politische PR denn als rechtliches Postulat anzusehen sei.

712 Ähnlich Fix, 41, der dann aber, wie erläutert, ein solches «herrschaftsrechtliches Verständnis» ablehnt.

konnte sie vorher nicht verfügen,[713] oder kannte sie noch gar nicht, wie etwa bei beobachteten Daten. Indem sie das Recht ausübt, kann sie nunmehr über «ihre» Daten selbstbestimmt disponieren. Das Recht auf Datenübertragung ermöglicht ihr sogar, den Zugangskreis zu den Daten zu erweitern, wenn sie dies möchte.[714] Dabei nimmt das DSG den alten Verantwortlichen unmittelbar in die Pflicht. Darin sieht die Literatur zurecht einen substanziellen Beitrag zur Stärkung des Rechts auf informationelle Selbstbestimmung.[715] Diese nähere sich sogar ein Stück weit einem Dateneigentum an.[716]

c. Grundrechtsverwirklichung unter Privaten

252 Der Staat ist verpflichtet, dafür zu sorgen, dass Grundrechte auch unter Privaten wirksam werden (sog. indirekte Drittwirkung; siehe Art. 35 Abs. 3 BV). Dies gilt auch für die informationelle Selbstbestimmung. Folglich muss der Staat Einzelne vor ungewollter Datenbearbeitung durch Dritte bewahren, indem er Regelungen erlässt, welche die informationelle Selbstbestimmung auch zwischen Privaten durchsetzen.[717] Da es am Gesetzgeber liegt, die Regeln zu definieren, nach welchen ein alltagstauglicher Umgang mit Daten zwischen Privaten möglich ist,[718] kann das Portabilitätsrecht als gesetzgeberische Ausgestaltung ebendieses Grundrechts verstanden werden. Damit berücksichtigt das primär drittwirkende Institut, dass die informationelle Selbstbestimmung heute ausgeprägter auf die Gefahr durch private Datenbearbeitungen zu reagieren hat.

253 Auch inhaltlich wägt Art. 28 DSG die unterschiedlichen Interessen ab, denn nur in bestimmten Konstellationen wird der Verantwortliche zur Portierung verpflichtet. Solche Interessenabwägungen finden sich zudem an anderen Stellen im DSG, etwa in den Art. 30 ff. DSG und insb. bei der Möglichkeit eine Persönlichkeitsverletzung unter Privaten zu rechtfertigen (Art. 31 DSG). Der Gesetzgeber adressierte also im Portabilitätsrecht nur diejenigen Fälle, für

713 Siehe auch die Ausführungen zu Art. 1 DSG in der Botschaft DSG 2017, 7071, wonach die informationelle Selbstbestimmung das «individuelle Verfügungsrecht über personenbezogene Daten» schütze. Freilich war zu diesem Zeitpunkt kein Portabilitätsrecht im DSG vorgesehen. Von einem grundrechtlich geschützten Verfügungsrecht über die eigenen Daten sprechend, im Ganzen jedoch kritisch Belser, Rechtliche Tragweite, 24.

714 Fix, 45.

715 SGK BV-Schweizer/Striegel, Art. 13 N 109; ähnlich auch Weber/Thouvenin, 70; Ziegler/Vasella, digma 2019, 162.

716 Götzinger/Vasella, SZW 2021, 41; Thouvenin, SJZ 2017, 27; ähnlich auch KRKomm-Munz, Art. 20 DSGVO N 8; siehe zum «Dateneigentum» Rz. 285.

717 SGK BV-Schweizer/Striegel, Art. 13 N 115 m.w.N.; so auch das BGer in BGE 140 I 2 E. 9.1; BGE 138 II 346 E. 8.2.

718 So Waldmeier, 38.

welche das Interesse der Betroffenen gegenüber den anderen privaten Interessen überwiegt. Insofern kann das Portabilitätsrecht als Ausfluss von Art. 35 Abs. 3 BV gelten, indem es die informationelle Selbstbestimmung auf Gesetzesebene konkretisiert.

d. Diskussion

Das eben geschilderte Verständnis des Datenportabilitätsrechts lässt sich auf das Grundrecht einer informationellen Selbstbestimmung stützen. Dabei bleiben aber einige Punkte unklar. So ist zunächst festzuhalten, dass eine selbstbestimmte Datendisposition nicht voraussetzt, dass das Portabilitätsrecht ein Löschen oder Vernichten der Daten beim alten Verantwortlichen bewirkt. Das Recht auf Datenportabilität ist kein Ausschliesslichkeitsrecht und zielt daher nicht auf eine Veränderung beim alten Verantwortlichen ab.[719] 254

Zudem sind die Bestimmungen des DSG als Ganzes stets Konkretisierungen der Grundrechte.[720] Eine Bestimmung deckt somit immer nur einen Teilbereich ab. Erst im Gesamtbild sollen die Bestimmungen die Grundrechte – oder eine informationelle Selbstbestimmung – verwirklichen. Das Recht auf Datenportabilität zielt nur auf eine beschränkte Datenkontrolle der Betroffenen und die Wiedererlangung einer eingeschränkten Datenautonomie über die bearbeiteten Daten ab, während andere Rechtsinstitute andere Facetten der informationellen Selbstbestimmung abdecken.[721] Die Zielsetzung wird daher nicht dadurch gemindert, dass der alte Verantwortliche durch das Institut nicht eingeschränkt wird: Eine absolute Herrschaft im Sinne eines uneingeschränkten Verfügungsrechts vermittelt das Institut nicht. 255

Hingegen sind bei diesem Verständnis der informationellen Selbstbestimmung die Beweggründe für die verschiedenen Einschränkungen des Portabilitätsrechts kritisch zu hinterfragen. Namentlich bleibt unklar, weshalb das Institut auf automatisierte Bearbeitungen beschränkt sein sollte. Auch die Begrenzung auf freiwillig bearbeitete Daten, die faktisch staatliche Datenbearbeitungen von der Portierung ausnimmt, steht im Widerspruch zur Annahme einer informationellen *Selbstbestimmung*. Sie kann zwar, wie ausgeführt, mit der indirekten Drittwirkung des Instituts begründet werden und damit, dass das Institut 256

719 Darauf zielen andere Institute ab, etwa das Recht auf Löschung oder Vernichtung in Art. 32 Abs. 2 lit. c DSG. Am Verhältnis zwischen der Betroffenen und dem alten Verantwortlichen ändert sich durch die Geltendmachung des Portabilitätsrechts nichts, dazu bereits Rz. 158 f. und Rz. 215.

720 Botschaft DSG 2017, 7010; Müller/Schefer, 174.

721 Etwa das Auskunftsrecht oder das eben genannte Recht auf Löschung oder Vernichtung.

besonders den von privaten Datenbearbeitungen ausgehenden Gefahren Rechnung tragen soll. Wird jedoch von einem Recht auf informationelle Selbstbestimmung im Sinne der bundesgerichtlichen Rechtsprechung ausgegangen,[722] so wäre anzunehmen, dass ein entsprechendes Recht primär oder zumindest auch im Verhältnis zum Staat zum Tragen kommt.[723] Zudem wären unter Privaten einschränkende Voraussetzungen kaum angezeigt, da die Betroffene «ihre» Daten im Regelfall kontrollieren können sollte. Dies dürfte unabhängig davon gelten, ob die Daten automatisiert bearbeitet werden oder nicht.

257 Damit erscheint fraglich, ob das Portabilitätsrecht tatsächlich eine so verstandene informationelle Selbstbestimmung verwirklichen soll.[724] Vor diesem Hintergrund ist die Kritik in Erinnerung zu rufen, wonach das Recht auf informationelle Selbstbestimmung weder ausformuliert noch positiviert noch dessen Konzeption den aktuellen Begebenheiten angepasst worden sei.[725] Gerade beim Recht auf Datenportabilität, das konzeptionell das neuartigste Instrument der DSG-Revision darstellt, führt dies zu besonderen Auslegungsschwierigkeiten. Es sollten daher m.E. die jüngsten technologischen Entwicklungen und die damit einhergehenden grundlegenden Veränderungen für Betroffene berücksichtigt werden, damit das Portabilitätsrecht auf einem tragfähigen Fundament stehen kann. Dafür kann es nicht ausreichen, das Institut einzig über eine wettbewerbsrechtlich begründete Zielsetzung herzuleiten und die genannten Entwicklungen aus jener Warte zu beleuchten.[726] Denn die mit dem Institut beabsichtigten Zielsetzungen sind – bereits in datenschutzrechtlicher Hinsicht – auf dem Nährboden der sogleich zu schildernden Entwicklungen gewachsen und lassen sich nur in diesem Kontext erläutern. Dies bedingt aber möglicherweise, dass sich das grundrechtliche Verständnis des Datenschutzes wandeln muss.

722 D.h. davon, dass jede Person die Möglichkeit haben muss, «gegenüber einer fremden, staatlichen oder privaten Bearbeitung von sie betreffenden Informationen bestimmen zu können, ob und zu welchem Zweck diese Informationen bearbeitet und gespeichert werden ohne Rücksicht darauf, wie sensibel die fraglichen Informationen tatsächlich sind», siehe statt vieler BGE 147 I 103 E. 15.1. Dazu Rz. 71.

723 Siehe hierzu THOUVENIN, ZSR Beiheft 2023, 17 ff.

724 Kritisch auch LANDOLT, 373, der dabei indes nicht explizit das Portabilitätsrecht, sondern die unternehmensübergreifende Nutzbarmachung von Personendaten als nur schlecht mit den stark verfassungsrechtlich geprägten Abwehrrechten des Datenschutzes in Einklang gebracht sieht.

725 SGK BV-SCHWEIZER/STRIEGEL, Art. 13 N 96.

726 Dazu Rz. 295 ff.

3. Das Recht auf Datenportabilität als Folge grundlegend veränderter Rahmenbedingungen

a. Etablierung einer Datenwirtschaft als Ursprung

Zwar hängt das Datenschutzrecht als Rechtsgebiet seit seiner Entstehung eng mit technologischen Entwicklungen zusammen.[727] Doch jüngste Entwicklungen haben zu Umwälzungen geführt, deren Tragweite sich erst ansatzweise begreifen lässt.[728] Die Menge an Daten ist exponentiell angestiegen und deren Vernetzung und Auswertung durch neue Analyseinstrumente stetig erweitert worden.[729] Die Übertragung dieser Daten wird immer schneller möglich, kennt keine Landesgrenzen und die Kosten für Speicherung und Verarbeitung nehmen laufend ab.[730] Zugleich werden die Datensätze immer intransparenter beschafft.[731] Heute gibt es kaum noch Bereiche, die nicht von dieser Entwicklung betroffen sind.[732] Personendaten sind in die Gesellschaft des 21. Jahrhunderts eingebunden und stellen ein Abbild der sozialen Realität dar.[733] 258

In der Folge hat sich eine Datenwirtschaft etabliert, die darauf basiert, Daten zu erheben und weiterzuverwenden. Die Daten stellen dabei nicht mehr nur Ware, sondern auch Währung dar.[734] Betroffene können mit ihren Daten «bezahlen» und erhalten im Gegenzug eine Leistung dafür.[735] Aus datenschutzrechtlicher Perspektive wird bei dieser Transaktion allerdings das Ungleichgewicht zwischen den beteiligten Akteurinnen zunehmend kritisch angesehen, insb. wird von grossen Wissens- und Informationsungleichgewichten aufsei- 259

727 Schon Botschaft DSG 1988, 416 f.; so auch Fix, 52, der im Datenschutz eine Reaktion auf geänderte gesamtgesellschaftliche Kommunikationsumstände sieht. Die Daseinsberechtigung liege indessen darin, die für einen gesellschaftlichen Diskurs notwendigen Grundlagen zu legen bzw. zu erhalten und vor der Gefährdung von Grundrechten zu schützen, die auf eine Weise ausgeübt würden, bei der Daten verarbeitet werden. Dazu bereits Rz. 65 ff.

728 Zu den Folgen und die damit einhergehende wettbewerbsrechtliche Zielsetzung des Rechts auf Datenportabilität Rz. 294 ff.

729 Expertengruppe Zukunft, 24 und 34 ff.

730 Rubinstein, IDPL 2013, 77; ähnlich Dewenter/Bernhardt, Rz. 49.

731 Botschaft DSG 2017, 6969.

732 Expertengruppe Zukunft, 24.

733 Freilich im Kontext, dass ein «totaler Schutz» nicht gewährleistet werden könne das BGer in BGE 138 II 346 E. 10.6.6; Weber, ZSR 1999, 75.

734 BeckOK DSR-Gusy/Eichenhofer, § 1 BDSG N 14.

735 Janal, 326; von Lewinski, Matrix, 51; Yildiz, Rz. 204 f.; siehe auf europäischer Ebene auch Art. 3 Abs. 1 DIRL.

ten der Betroffenen ausgegangen.[736] Diese erschweren deren Entscheidfindung, auch in Bezug auf den Schutz ihrer Privatsphäre.[737]

260 Die Ungleichgewichte haben in der Datenwirtschaft eine neue Qualität erhalten, da sie sich nicht mehr auf Produkteigenschaften, die Qualität einer Dienstleistung oder auf externe Risiken beziehen, sondern auf die Betroffene als Person: Ein Verantwortlicher weiss bisweilen mehr über seine Kundinnen als diese über sich selbst.[738] Wer also Zugang zu den entsprechenden Daten hat, kann daraus neue Zusammenhänge erkennen, Präferenzen sichtbar machen und Vernetzungslösungen ermöglichen, die davor nicht einmal bekannt waren – und so die Innovation monopolisieren.[739] Daher werden Betroffene heute vielfach bloss als Summe ihrer Daten betrachtet und objektifiziert. Gerade in diesem Kontext ist regelmässig von «Überwachungskapitalismus» die Rede, womit eine Logik gemeint ist, welche Menschen als «Rohstoff» für sie betreffende Verhaltensdaten (aus-)nutzt.[740]

261 Die genannten Umstände in der Datenwirtschaft schränken die Betroffene oft (und besonders in den gesetzgeberisch angedachten Fällen der Internetplattformen) in ihrer Autonomie ein. Dies ist nicht bloss wettbewerbsrechtlich relevant, denn die Betroffene wird auch in datenschutzrechtlicher Hinsicht eingeschränkt, da sie daran gehindert wird, Daten zu erhalten oder sie frei weiterzugeben.[741] Werden grosse Datenmengen bei einer Akteurin kumuliert, kann dies zu einer «gläsernen Bürgerin» führen, deren Privatsphäre zumindest in hohem Mass gefährdet ist und deshalb geschützt werden sollte.[742] Durch die

---

736 Aebi-Müller, 266; Denoth/Kaufmann, sic! 2016, 501; Gasser, ZSR 2015, 366 f.; Landolt, 155, der von systematischen Machtasymmetrien spricht, welchen das Portabilitätsrecht entgegenwirke; Steffen/Wieworra/Kroon, 73; Zuboff, JIT 2015, 83; in diese Richtung UVEK/EDA, 10; ähnlich Botschaft DSG 2017, 6969; Bundesrat, Strategie «Digitale Schweiz» 2018, 5982; siehe auch Bijok, 196, der aber gerade anzweifelt, ob solche Asymmetrien durch das Portabilitätsrecht eingefangen werden können. Die Reaktion auf informationsbedingte Machtasymmetrien ist eine Kernaufgabe des Datenschutzrechts, siehe dazu Spiecker genannt Döhmann, 176.

737 Gasser, ZSR 2015, 405; ähnlich Thouvenin, ZSR Beiheft 2023, 45.

738 Metzger/Schweitzer/Wagner, ZfPW 2023, 255.

739 Podszun, 111.

740 Zuboff, JIT 2015, *passim*. Sie geht sogar soweit, auf diese Weise angeeignete Daten als «stolen goods» zu bezeichnen. Dies ausdrücklich auch aufgreifend Votum NR Glättli, AB 2018 N 963.

741 Thouvenin/Weber/Früh, 171; Weber/Thouvenin, 69; CR LPD-Benhamou, Art. 28 N 4; für die europäische Regelung davon sprechend, dass diese mittelbar die Betroffene in datenschutzrechtlicher Hinsicht stärke Bijok, 161; Drexl, Challenges, 38.

742 Thouvenin, ZSR Beiheft 2023, 44, der dabei aber ausdrücklich die Privatsphäre und nicht ein informationelles Selbstbestimmungsrecht diskutiert; siehe auch Palfrey/Gasser,

Machtasymmetrien willigen die Betroffenen ferner oft in Datenbearbeitungen ein, ohne deren Tragweite abschätzen zu können. Dazu kommt, dass eine Betroffene aufgrund von Lock-In-Effekten[743] eher geneigt ist, ungünstige datenschutzrechtliche Bedingungen zu akzeptieren.[744] Alle diese Entwicklungen können sie daran hindern, selbstbestimmt am gesellschaftlichen Diskurs teilzuhaben,[745] obwohl die Nutzung digitaler Geräte und Dienste heute als Voraussetzung für eine umfassende Teilhabe am modernen Leben angesehen wird.[746]

b. Selbstbestimmte Datendisposition als Reaktion

Der Siegeszug der Datenwirtschaft[747] und die mit dem Datenhandel entstandenen Ungleichgewichte zwischen Betroffenen und Verantwortlichen haben zu neuen datenschutzrechtlichen Schutzbedürfnissen geführt. So hat sich die Haltung durchgesetzt, dass Betroffene vom Nutzen der von ihnen bekanntgegebenen Personendaten profitieren sollen.[748] Dieser Nutzen kann darin bestehen, dass die Betroffene über ihre Daten autonom verfügen kann und sie so der ausschliesslichen Verwertung durch den Verantwortlichen entzieht. Des Weiteren kann der Nutzen auch darin liegen, dass Betroffene wirtschaftlich von ihren Daten profitieren und eigenständig an den Märkten partizipieren können.[749] Die faktische Ausschliessungsmöglichkeit, die dem Verantwortli- 262

34 ff., die mit Fokus auf eine Interoperabilität zwischen Systemen die Konsequenzen einer ungehinderten Interkonnektivität für die *personal privacy* beleuchten.

743 Inwieweit diese ausschlaggebend sind, ist jedoch umstritten, gerade angesichts möglicher Netzwerkeffekte, dazu aus wettbewerbsrechtlicher Perspektive Rz. 300 ff.

744 Collovà et al., 8; ähnlich Duller, 145.

745 Fix, 52.

746 Gasser, ZSR 2015, 364; ähnlich Zuboff, JIT 2015, 83.

747 Von einem «Siegeszug der unstrukturierten Daten» sprechend Expertengruppe Zukunft, 35.

748 Thouvenin, ZSR Beiheft 2023, 45; Weber, Jusletter IT 2013, Rz. 31.

749 Ähnlich von einem «Signal in die Zukunft» sprechend BSK DSG-Laux/Steiner, Art. 28 N 72; Landolt, 154, der von einer «Kontrolle über die kommerzielle Nutzung der eigenen Daten» spricht und der Betroffenen eine «datenbezogene Bewegungsfreiheit auf digitalen Märkten» zuspricht; Mahon, 59, der dabei offen lässt ob es sich dabei um ein Ziel des Portabilitätsrechts handelt oder lediglich um dessen Wirkung; Thouvenin, ZSR Beiheft 2023, 45, der für die Aufgabe des Rechts auf informationelle Selbstbestimmung plädiert, aber in der Rechtsordnung Ansprüche verankert sehen will, die vorsehen, dass die Betroffenen am Wert der sie betreffenden Daten partizipieren können, indem sie eine Kopie der Daten erhalten und diese selbst nutzen oder an Dritte weitergeben können. Er scheint diese Ansprüche jedoch nicht unter dem Titel der Persönlichkeit bzw. der Privatsphäre verankern zu wollen. Ein Schutzbedürfnis scheint er aber gleichwohl zu sehen. Siehe auch Weber,

chen ohne ein Portabilitätsrecht zukommen würde, soll durchbrochen werden[750] und die bisher zum Datenobjekt degradierte Person zum Datensubjekt aufsteigen, indem sie über die Verwendung der Daten mitbestimmen und diese ggf. autonom monetarisieren kann.[751] Damit adressiert das Portabilitätsrecht die entstandenen Ungleichgewichte.[752] Die Betroffene erhält also erstmals rechtliche Mittel, um eigenständig in die entstandene Datenwirtschaft einzugreifen und am Potenzial der Daten teilhaben zu können.[753] Die nunmehr geschaffene Datendispositionsmöglichkeit bringt den gesetzgeberischen Willen zum Ausdruck, neu Rechte an bestimmten Daten vorzusehen.[754] Der Gesetzgeber beschränkte sich dabei aber auf diejenigen Daten, die im Zuge der technologischen Entwicklung zur Grundlage der Wirtschaft geworden sind. Dies erklärt bereits aus datenschutzrechtlicher Perspektive die Einschränkungen nach Art. 28 Abs. 1 lit. a und b DSG.[755]

263 Ohnehin ist allerdings zwischen dem Recht auf Datenherausgabe und dem Recht auf Datenübertragung zu unterscheiden: Ersteres berechtigt die Betroffene, ihre Daten zu erhalten und geht dabei, anders als die DSGVO, nicht ausdrücklich davon aus, dass die Daten an eine neue Verantwortliche weitergegeben werden.[756] Im Zentrum steht damit der Gedanke, dass die Betroffene nicht an einen Verantwortlichen gebunden sein soll, nur weil sie ihm in der Vergangenheit Daten bekanntgegeben hat. Das Portabilitätsrecht ist damit auch ein Gegengewicht zur freiwillig erfolgenden Bekanntgabe. Denn die Freiwilligkeit

Jusletter IT 2013, Rz. 31 f.; davon sprechend, dass Daten «verkehrsfähig» und gleichsam «verdinglicht» würden ZIEGLER/VASELLA, digma 2019, 162.

750 SCHWEITZER, GRUR 2019, 574.

751 BIERI/POWELL, Jusletter 2020, Rz. 23; Expertengruppe Zukunft, 105 f.; THOUVENIN, ZSR Beiheft 2023, 27, nach welchem die Betroffenen «nicht blosse Objekte der Datenbearbeitung sein sollen» und sie so «immerhin zu Akteuren und Kontrolleuren der Bearbeitung der sie betreffenden Personendaten» werden.

752 MAHON, 59, wobei unklar ist, ob er diese wettbewerbsrechtlich versteht; ausdrücklich davon sprechend «den einzelnen Personen [mit dem Portabilitätsrecht] Gewicht zurückzugeben» Votum NR Glättli, AB 2019 N 1814; zur Debatte in den Räten Rz. 97 ff.

753 LANDOLT, 155, der das Portabilitätsrecht als «konsequente Aufdatierung ‹prädigitaler› Konzepte wie dem Auskunftsrecht oder der Einwilligung auf die heutigen Bedürfnisse in der Datenwirtschaft» versteht; LAUX, digma 2019, 170.

754 Siehe auch GÖTZINGER/VASELLA, SZW 2021, 41, wonach das Recht auf Datenportabilität die Autonomie der betroffenen Person stärken soll. Indem der betroffenen Person autonom über die Verwendung von Personendaten entscheiden kann, finde auch eine Annäherung an das «Dateneigentum» statt. Sie beziehen sich damit auf eine lebhafte Diskussion, ob an Daten sachenrechtlich Eigentum begründet werden können solle. Die Notwendigkeit eines solchen Dateneigentums wird heute überwiegend verneint. Dazu Rz. 285.

755 Dazu ferner Rz. 267 ff.

756 Dazu Rz. 200.

ist in der Praxis angesichts der grossen Machtasymmetrien oftmals zweifelhaft.[757] Die Betroffene soll daher zumindest «ihre» Daten zurückerhalten und sie selbstbestimmt verwalten können. Ihr wird damit eine Datenautonomie über die sie betreffenden Daten in der Datenwirtschaft zugestanden.

Beim Recht auf Datenübertragung entscheidet sich die Betroffene dafür, eine neue Verantwortliche miteinzubeziehen. Damit werden, wie noch zu sehen sein wird, vor allem wettbewerbsrechtliche Folgen impliziert. Diese lassen sich, soweit sie die Betroffene anbelangen, nicht immer trennscharf von den datenschutzrechtlichen Zielen abgrenzen. Es waren jedoch technologische Umwälzungen, die die gesetzgeberische Reaktion in Form von Art. 28 DSG ausgelöst haben. Dass damit wettbewerbliche Ziele verfolgt und entsprechende Auswirkungen beabsichtigt werden, ändert nichts daran, dass das Portabilitätsrecht auch datenschutzrechtliche Ziele verfolgt. Auch wettbewerbliche Elemente können einen Bezug zum Datenschutz haben, wenn sie – wie vorliegend – eine (nicht exklusive) Herrschaft über die eigenen Daten ermöglichen.[758] Da es sich durchwegs um Daten handelt, die einen Personenbezug aufweisen, und es allein die Entscheidung der Betroffenen ist, die Übertragung zu verlangen, liegt in den Fällen nach Abs. 2 ebenfalls eine Nähe zur Persönlichkeitsentfaltung der Betroffenen vor.[759] Dieses Mitspracherecht über den Datenfluss ist eine weitere Form der Autonomie, die letztlich den Schutz der Persönlichkeit der Betroffenen bezweckt und so das Ungleichgewicht in der Datenwirtschaft beheben soll. 264

757 Baeriswyl, digma 2020, 66, nach welchem sich die Einwilligung im privatrechtlichen Bereich zum Schutz der persönlichen Freiheit nicht bewährt habe; Fasnacht, Rz. 385 m.w.N., der zumindest im Massengeschäft der Einwilligung eine «Scheinfreiwilligkeit» sieht.

758 So auch Frei, Jusletter 2018, Rz. 57; ferner Baeriswyl, Konsumentenschutz, 406, nach welchem wettbewerbsrechtliche Bestimmungen das Recht auf informationelle Selbstbestimmung stärken können; Weber/Thouvenin, 71; wohl a.A. Götzinger/Vasella, SZW 2021, 41.

759 Götzinger/Vasella, SZW 2021, 41, die jedoch anmerken, dass jedes Betroffenenrecht die Autonomie der Betroffenen stärkt, alleine weil es ein Recht ist und zudem zu Bedenken geben, dass sich diese Auslegung dem «berüchtigten» Dateneigentum annähere; kritisch hierzu aus europäischer Perspektive Marsch, 102 f. Ein anderes Verständnis könnte im Übrigen dazu führen, dass in Fällen von Abs. 2 bei einer strengen Auslegung stets von «datenschutzwidrigen Zwecken» i.S.v. Art. 29 i.V.m Art. 26 Abs. 1 lit. c DSG auszugehen wäre, was kaum denkbar ist. Freilich gilt der Verweis, wie bereits diskutiert, ohnehin als verunglückt, weshalb daraus nicht allzu viel abgeleitet werden sollte.

c. Einschränkungen als Resultat der auf Internetplattformen zugeschnittenen Zielsetzung

265 Das Portabilitätsrecht wirkt nicht umfassend, sondern ist in unterschiedlicher Hinsicht eingeschränkt. Die Einschränkungen sind schlüssiger erklärbar, wenn nicht von einem umfassenden Herrschaftsrecht, sondern von einem auf die Datenwirtschaft ausgerichteten und auf diese abzielenden Institut ausgegangen wird. Aus diesem Blickwinkel erscheint etwa die Eingrenzung auf automatisierte Datenbearbeitungen nachvollziehbar. Erfasst sein sollten lediglich Daten, für welche die geschilderten Ungleichgewichte zulasten der Betroffenen existieren und welche einfach weiterverwendbar sind. Dabei ist datenschutzrechtlich nicht von Belang, ob Betroffene (Art. 28 Abs. 1 DSG) oder Dritte (Abs. 2) die Daten anschliessend weiterverwenden.

266 Auch die Einschränkung nach Art. 28 Abs. 1 lit. b DSG lässt darauf schliessen, dass auf die oben erwähnten Ungleichgewichte reagiert werden sollte. Gemäss den Materialien hatte der Gesetzgeber beim Erlass vorwiegend die grossen Internetplattformen vor Augen, die sozialen Netzwerke, Suchmaschinenbetreiberinnen und Onlinemarktplätze.[760] Bei diesen besteht ein besonderes Ungleichgewicht durch deren Kumulation von Daten. Demzufolge wäre der Kreis der Normadressatinnen enger zu fassen. Tatsächlich sind aber vom Portabilitätsrecht deutlich mehr Verantwortliche erfasst, da heute Verantwortliche in allen Sektoren Daten automatisiert bearbeiten und dies im privatrechtlichen Kontext oft gestützt auf eine Einwilligung oder im Zusammenhang mit einem Vertrag. Da die Betroffene – auch nach dem Willen des Gesetzgebers – im Zentrum des Datenportabilitätsrechts steht, kann aus der Ausgestaltung des Instituts keine Einschränkung auf Internetplattformen abgeleitet werden, dies trotz der gesetzgeberischen Absichten. Das Institut sollte zwar auf Internetplattformen zugeschnitten sein, ist es in seinem tatsächlichen Anwendungsbereich aber nicht.

d. Einschränkungen als Resultat der Abwägung konfligierender Ziele

267 Die Einschränkungen des Portabilitätsrechts sind dennoch die Folge einer Interessenabwägung. So berücksichtigt das Institut, dass nicht einzig die Betroffene den Wert eines (Personen-)Datensatzes schafft, sondern ebenso die Verantwortlichen, welche die Daten sammeln, speichern, aufbereiten und

760 Dazu Rz. 97 ff., insb. 102.

auswerten.[761] Die gegensätzlichen Interessen der Beteiligten hatte der Gesetzgeber abzuwägen, weshalb er das Institut in gewissen Bereichen beschränkte, etwa durch den Ausschluss abgeleiteter Daten.[762]

In diesem Sinn lassen sich auch die weiteren Einschränkungen in Art. 28 DSG verstehen.[763] Nur bei automatisiert bearbeiteten und freiwillig bekanntgegebenen Daten kann eine Autonomie und ein Mitspracherecht in der Datenwirtschaft überhaupt beabsichtigt sein und ein Portabilitätsrecht erforderlich erscheinen. Von diesem Ziel sind nicht nur die grossen Internetplattformen umfasst, sondern alle anderen Verantwortlichen, welche Daten so bearbeiten. 268

Werden demgegenüber Daten nicht bekanntgegeben oder freiwillig bearbeitet, sondern aufgrund einer gesetzlichen Grundlage bearbeitet oder bei Dritten erhoben, sind die partizipativen Möglichkeiten zurecht anders gelagert. Ein Recht auf Datenportabilität, das darauf angelegt ist, das von der Datenwirtschaft ausgehende Ungleichgewicht abzumildern, erscheint nicht angebracht. Damit wird bereits die wettbewerbsrechtliche Dimension des Portabilitätsrechts offenkundig. 269

4. Neues Verständnis der informationellen Selbstbestimmung

a. Bisherige Konzeption kaum tragfähig

Es bleibt die Frage, worauf sich das eben geschilderte Verständnis abstützen kann, namentlich ob es sich mit dem Recht auf informationelle Selbstbestimmung vereinbaren lässt. Bereits bei der europäischen Konzeption wurde auf die insoweit in der EU gleich ablaufenden Entwicklungen hingewiesen: Das Recht auf informationelle Selbstbestimmung kann, selbst wenn von dessen Existenz ausgegangen wird, in seinem traditionellen Verständnis das gewandelte Gefährdungspotenzial moderner Datenbearbeitungen hinsichtlich der Persönlichkeitsrechte kaum mehr ausreichend erfassen.[764] Diese Zweifel treffen, wie dargelegt, für die Schweiz ebenfalls zu, zumal sich das Gefährdungspotenzial in der Schweiz und der EU angesichts der ähnlichen gesellschaftlichen Rahmenbedingungen kaum unterscheidet. Bereits einleitend wurde 270

761 Thouvenin, ZSR Beiheft 2023, 45; für die DSGVO von einem Kompromiss sprechend Gatti, EJPLT 2024, 161.

762 Dazu Rz. 179.

763 Steiner, 124; für die DSGVO ebenso Gatti, EJPLT 2024, 161 f.

764 Fix, 51 f.; Wielsch, JZ 2020, 109 f.

zudem festgehalten, dass die Tragfähigkeit der informationellen Selbstbestimmung in der Schweiz ebenfalls zunehmend angezweifelt wird.[765] Im Unterschied zum BVerfG hat das BGer allerdings seine Rechtsprechung und damit sein Verständnis einer informationellen Selbstbestimmung bislang nicht angepasst. Dieses bundesgerichtliche Verständnis vermag die aufgeführten (neuen) Verwendungskontexte und Schutzbedürfnisse aber nicht genügend zu erfassen. Es drängt sich folglich ein zeitgemässeres Verständnis des Rechts auf informationelle Selbstbestimmung auf, welches diese Entwicklungen berücksichtigt.[766]

271 Das Recht auf informationelle Selbstbestimmung umfasst Abwehrrechte der Betroffenen gegen ungewünschte Datenbearbeitungen.[767] Entsprechend ist das diesen Datenbearbeitungen zugrundeliegende Schutzbedürfnis primär auf eine negative Wirkung resp. auf eine negative Seite der Persönlichkeit ausgerichtet. So kann sich die Betroffene seit jeher als Ausfluss ihres informationellen Selbstbestimmungsrechts gegen ein Verhalten des Staats oder von Privaten wehren, indem sie mit einem Auskunftsgesuch Transparenz einfordert. Von Privaten kann sie zudem prinzipiell verlangen, dass diese ihre Daten löschen.[768] Dieses Verständnis basiert auf dem Grundsatz der Datenminimierung und der Annahme, dass möglichst wenige Datenbearbeitungen die Persönlichkeit der Betroffenen am besten schützen,[769] und ist letztlich Ausfluss des Ver-

765 Dazu Rz. 76 ff.

766 Die Notwendigkeit eines zeitgemässen Datenschutzrechts im Sinne des kodifizierten DSG war dem Gesetzgeber jedenfalls anlässlich der Revision des DSG bewusst, siehe Votum SR Bruderer, AB 2018 S 617. Ebenfalls hervorgehoben hatte dies im Kontext des Rechts auf informationelle Selbstbestimmung die zuständige Bundesrätin, siehe Votum BR Sommaruga, AB 2018 S 618.

767 Aebi-Müller, 294, die sich jedoch primär auf das Persönlichkeitsrecht bezieht und gegenüber einer informationellen Selbstbestimmung kritisch eingestellt ist, gerade da der Begriff unterstelle, dass es sich beim Persönlichkeitsschutz um (umfassende) Verfügungsrechte handle. Nach ihrer Ansicht ist die informationelle Selbstbestimmung denn auch «kein eigentliches Persönlichkeitsrecht»; a.A. jedoch wohl Belser, Datenschutzrecht, § 2 Rz. 25, nach welcher sich bereits mit der ursprünglichen Anerkennung eines Rechts auf informationelle Selbstbestimmung durch das BVerfG die Ausrichtung des Datenschutzes geändert habe und es nicht länger (nur) darum gehe, den Einzelnen vor Missbräuchen zu schützen, sondern «sein Recht zu sichern, selbst über die eigenen Daten zu verfügen», m.H.a. von Lewinski, Geschichte, 199.

768 Eine ähnliche Parallele ziehend mit der negativen Seite von Eigentumsrechten Thouvenin, SJZ 2017, 26 f. Dabei wird auch das Portabilitätsrecht der negativen Seite zugeordnet.

769 Botschaft DSG 1988, 417 f., wonach das DSG gewisse Leitplanken für die Datenbearbeitung setze, um zu garantieren, dass die Persönlichkeit nicht «durch unnötige und unerwünschte Informationstätigkeiten beeinträchtigt werde». Ferner: «Die Privatsphäre einer Person soll von Informationsbedürfnissen anderer Personen, oder staatlicher Stellen ab-

hältnismässigkeitsprinzips, das im Datenschutzrecht auch für den privaten Bereich gilt (Art. 6 Abs. 2 DSG).[770] Diese Annahme und der Grundsatz der Datenminimierung liegen dem Schweizer Datenschutzrecht seit jeher zugrunde, wurden aber im Vergleich zur europäischen Regelung stets weniger konsequent umgesetzt.[771] Wie bereits aufgeführt, kennt das DSG namentlich kein Verbot mit Erlaubnisvorbehalt, sondern erlaubt Datenbearbeitungen für Private grundsätzlich (Erlaubnis mit Verbotsvorbehalt).[772]

b. Neuer Ansatz nötig

Durch den veränderten Verwendungskontext von Daten, die einen (wirtschaftlichen) Wert aufweisen und deren Weitergabe auch im Interesse der Betroffenen sein kann, sind allerdings Schutzbedürfnisse entstanden, die nicht mehr allein abwehrrechtlich verstanden werden können. Vielmehr sind sie als positive Ausprägung der Persönlichkeit zu verstehen. Damit vollzieht das Portabilitätsrecht einen Richtungswechsel und bricht mit der geschilderten Zweckausrichtung des Datenschutzrechts.[773] Der betroffenen Person soll als eigenständige Akteurin ein Mitspracherecht in der Datenwirtschaft als Ausdruck ihrer Persönlichkeitsentfaltung zugestanden werden. Wenn sie Daten (mit-)«produziert» hat, welche aufgrund ihres Personenbezugs als ihrer Persönlichkeit zugehörig betrachtet werden, soll sie mitentscheiden, wie diese verwertet werden.[774] Während das Datenschutzrecht die Betroffene bislang primär *vor einer Weitergabe* der Daten schützte, ist nunmehr ein positiv gelagertes Recht *auf Weitergabe* der Daten vorgesehen. Dabei handelt es sich um 272

geschirmt werden [...]». Siehe aber auch der Hinweis, dass das DSG verhindern müsse, dass «der einzelne zu einem rechtlosen Objekt von Informationstätigkeiten wird». Siehe auch GLATTHAAR, 20, wonach das Datenschutzrecht die Persönlichkeit betroffener Personen vor ungewollten und überschiessenden Datenbearbeitungen schütze. Dazu auch FIX, 64, nach welchem der Versuch, Sicherheit allein durch Minimierung der Datenmengen zu erzeugen als Abwehrrecht gegenüber dem Staat womöglich überzeugt, aber nicht auch auf die Bearbeitung durch Private übernommen werden kann, weil dies «vor dem Gedanken der Teilhabesicherung an der in privaten Kommunikationsstrukturen stattfindenden Kommunikation nicht sinnvoll» sei.

770 Botschaft DSG 2017, 7024; so bereits Botschaft DSG 1988, 450.

771 Siehe aber Art. 5 Ziff. 1 und Ziff. 2 lit. c der Konvention 108+.

772 Dazu Rz. 194.

773 LANDOLT, 153, der von einem Bruch «in vieler Hinsicht» mit der tradierten Zweckausrichtung des Datenschutzrechts spricht.

774 Siehe in diese Richtung auch EDA, 14, wonach «digitale Selbstbestimmung» bedeute, dass ein Individuum die Weiterverwendung von Daten «zu einem Grossteil» selbst steuern könne und die Teilhabe an der digitalen Welt nicht mehr mit dem «Kontrollverlust über die eigenen Daten einhergehen» solle.

einen neuartigen Aspekt der (informationellen) Selbstbestimmung, welcher das bislang geltende daten*schutz*rechtliche Paradigma um einen positiven Teilbereich ergänzt.[775]

273 Dass tatsächlich ein grundlegender Wandel stattgefunden hat, zeigt sich daran, dass das Institut vom Grundsatz der Datenminimierung Abstand nimmt.[776] Mit dem Portabilitätsrecht geht es nicht (mehr) bloss darum, eine Datenbearbeitung möglichst zu verhindern, sondern darum, diese zu lenken, mitzubestimmen und davon zu profitieren. Dieses Ziel lässt sich m.E. kaum auf ein ausschliesslich abwehrend wirkendes, negatives Verständnis eines Rechts auf informationelle Selbstbestimmung abstützen.[777] Es ist zu prüfen, ob dieser Ansatz mit der bisherigen Lehre vereinbar ist.

c. Haltung der Lehre

aa. Europäische Literatur

274 Aus deutscher Perspektive wird in der Lehre für ein «Datenverkehrs-» bzw. «Datenwirtschaftsrecht» plädiert, welches eine informationelle Selbstbestimmung erst ganz verwirklichen könne.[778] Die informationelle Selbstbestimmung bedürfe nicht nur des Freiraums, der durch das geltende Datenschutzrecht hergestellt wird, und welchen der Autor «informationelle Fremdbestimmung» nennt, sondern auch einer Normierung dieses Freiraums, um darin agieren zu können.[779] Eine Regelung bedeute in diesem Zusammenhang daher nicht nur (negativ) Beschränkung, sondern Ermöglichung.[780] Im Recht auf Datenportabilität sei nach diesem Verständnis jedoch eine informationelle Fremdbestimmung zu sehen, weil es die Rechtsmacht gebe, die Herausgabe der Gesamtheit

775 Angelehnt an die grundlegenden Ausführungen zum Begriff der «negativen» und der «positiven Freiheit», die oft verkürzt mit «Freiheit von» und «Freiheit zu» erläutert wird, siehe dazu Berlin, 197 ff., insb. 201 ff. und 211 ff.

776 Auch auf die wirtschaftlichen Anreize bei der Datenerhebung hinweisend Krämer, JCLE 2021, 273 m.w.N.; Krämer/Schnurr, JCLE 2022, 308, die «particularly strong tensions» sehen; Troiano, 169 f.; ähnlich auch Landolt, 153 f.

777 Fix, 131; siehe auch Stiftung Datenschutz, Zusammenfassung, 3, die jedoch primär die Vervielfältigung eines Datensatzes infolge der Nicht-Löschung beim alten Verantwortlichen kritisch sehen; etwas weniger ausdrücklich Stiftung Datenschutz, Praktische Umsetzung, 39; dazu ausführlich Rz. 270 f.

778 von Lewinski, Matrix, 55.

779 von Lewinski, Matrix, 55.

780 von Lewinski, Matrix, 55.

der Daten bei einem Verantwortlichen in einem bestimmten Dateiformat zu fordern.[781]

Ebenfalls vertreten wird, dass das Portabilitätsrecht als Teil einer weiterentwickelten informationellen Selbstbestimmung zu betrachten sei.[782] Daraus ergebe sich, dass das Recht auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten «in dieser positiven Form der Zugriffsverschaffung geltend gemacht werden kann, und nicht nur negativ in Form von Zugriffsverweigerung bzw. -entzug».[783] Ferner wird betont, dass das historisch gewachsene Instrumentarium der Abwehrrechte mit dem Portabilitätsrecht um ein «positives Element» ergänzt werde, neben welchem das Auskunftsrecht deutlich weniger schlagkräftig anmute.[784] Das Portabilitätsrecht sei als «eine Art positives Nutzungsrecht» zu begreifen.[785] Schliesslich wird das Portabilitätsrecht als Beispiel für einen Wandel «eines sich auf Abwehrrechte stützenden herrschaftsrechtlichen hin zu einem sich auf Einflussnahmerechte erweiternden regulatorischen Verständnis des Datenschutzes» gesehen.[786] Das regulatorische Verständnis des Datenschutzgrundrechts soll ein Recht auf «adäquate gesetzgeberische Ausgestaltung» umfassen.[787] Ohnehin seien die Selbstbestimmung im Umgang mit den eigenen Daten und eine Teilhabe an der Wertschöpfung aus diesen Daten zwei Seiten derselben Medaille.[788] 275

bb. Schweizer Literatur

Derart deutliche Voten finden sich in der Schweizer Literatur, soweit ersichtlich, nicht. Die informationelle Selbstbestimmung bzw. der verfassungsrechtliche Datenschutz generell werden in der Literatur bislang nur vereinzelt und kaum vertieft unter solchen «positiven» und «negativen» Aspekten diskutiert. So wird etwa nach einer Meinung in der informationellen Selbstbestimmung nicht nur die Grundlage für Abwehransprüche gegenüber rechtswidrigen Eingriffen gesehen, sondern auch die Basis für die Disposition der Einzelnen über die Kommerzialisierung ihrer eigenen Daten.[789] Daraus folge, dass die Betroffene nicht nur das Recht habe, den Kreis der Datenbearbeiter durch den Wi- 276

781 von Lewinski, Matrix, 48.
782 Krause, PinG 2018, 240.
783 Krause, PinG 2018, 239.
784 Jülicher/Röttgen/v. Schönfeld, ZD 2016, 361.
785 Jülicher/Röttgen/v. Schönfeld, ZD 2016, 361.
786 Fix, 54.
787 Fix, 53 m.w.N.; dazu bereits Rz. 247 ff.
788 Metzger, GRUR 2019, 129.
789 Weber/Henseler, SZW 2019, 337 m.w.N.; ähnlich auch Landolt, 154.

derruf einer Einwilligung nach Art. 30 Abs. 2 lit. b DSG zu verkleinern, sondern auch, diesen durch Ausübung des Portabilitätsrechts jederzeit zu erweitern.[790] An anderer Stelle wird von einem «datenschutzrechtlichen Ansatz» des Portabilitätsrechts gesprochen, der als positiver Rechtsanspruch Steuerungsbefugnisse vermitteln soll, die über die bestehenden datenschutzrechtlichen Abwehrbefugnisse hinausgehen sollen.[791] Soweit an einer Stelle gar die Einführung eines Dateneigentums gefordert wird, wird dies damit begründet, dass es der in technisch-ökonomischer Hinsicht neuartige Kontext erfordere, die Herrschaft über Daten in den Stand eines Grundrechts zu erheben, damit eine «echte Eigentumsordnung» für Personendaten geschaffen werden könne.[792]

277 Ein weiterer Autor versucht die Kategorie der «Privatheit» zu umschreiben, und knüpft dabei an den Begriff der Freiheit an.[793] Demnach sei jene Freiheit, die durch Datenschutzmassnahmen zu bewahren sei, «vor allem wenn auch nicht ausschliesslich die negative, nämlich diejenige, welche dem Individuum erlaubt und ermöglicht mit Dingen, welche er [sic] ablehnt, nicht konfrontiert werden zu müssen».[794] Die positive Freiheit sei hingegen diejenige, welche den Individuen erlaube, ihre natürliche und soziale Umwelt nach ihren Vorstellungen zu gestalten und zu verändern.[795] Dabei wird u.a. Bezug auf grundlegende philosophische Ausführungen von BERLIN zu negativer und positiver Freiheit genommen. Nach diesem widmet sich die Verteidigung der Freiheit dem «negativen» Ziel, Einmischung abzuwehren.[796] Die «positive» Bedeutung der Freiheit leite sich hingegen aus dem Wunsch des Individuums ab, sein eigener Herr und Werkzeug der eigenen und nicht fremder Willensakte zu sein.[797] Dieses Verständnis wurde im schweizerischen Verfassungsrecht rezipiert[798] und ist im Kontext des Auffanggrundrechts der persönlichen Freiheit verbreitet.

278 Auf die persönliche Freiheit stützt sich ein weiterer Autor ab und verweist dabei ausdrücklich auf den verfassungsrechtlichen Datenschutz. Einerseits schütze die persönliche Integrität als solche vor äusserlichen Beeinträchtigungen und sei damit ein «Integritätsschutz» oder eine «Freiheit von».[799] Ande-

790 LANDOLT, 154 f.
791 WEBER/THOUVENIN, 68.
792 FLÜCKIGER, AJP 2013, 862.
793 BONDOLFI, 130.
794 BONDOLFI, 130.
795 BONDOLFI, 130. Er hält hierzu indes fest, dass diese Freiheit nicht primär der Privacy zugeordnet werden könne.
796 BERLIN, 208.
797 BERLIN, 211.
798 Statt vieler MÜLLER, 6 ff.
799 VAN SPYK, 30 f.

rerseits werde die Selbstbestimmung über die Lebensgestaltung geschützt und damit die Verfügungsfreiheit einer Person über die Gehalte der persönlichen Integrität.[800] Es handle sich um einen «Aktivitätsschutz» oder eine «Freiheit zu».[801] Der Schutz der «informationellen Privatheit» vor einer staatlichen Bearbeitung von Personendaten nach Art. 13 Abs. 2 BV stelle einen Teilgehalt des – negativen – Integritätsschutzes dar.[802] Die Freiheit der Betroffenen, darüber zu entscheiden, welche Informationen sie preisgibt, sowie der Anspruch auf Einsicht in amtliche Daten, die sie persönlich betreffen, fallen hingegen in den Bereich der positiven informationellen Selbstbestimmung nach Art. 13 Abs. 2 BV.[803]

Es finden sich aber auch dezidiert ablehnende Stimmen gegenüber einer möglichen positiven Ausprägung der informationellen Selbstbestimmung. Nach einer Ansicht gewährt das Persönlichkeitsrecht einen Schutz, woraus sich folgern lasse, dass dessen Wirkungen einzig negativ und «repressiv bzw. defensiv» seien.[804] Dies gelte auch für Daten: Das Konzept der informationellen Selbstbestimmung unterstelle unzutreffenderweise, dass der Persönlichkeitsschutz umfassende Verfügungsrechte verleihe.[805] Es gehe gerade nicht um eine eigentümerähnliche Position der Betroffenen, «sondern ‹nur› um Schutz- bzw. Abwehrrechte, die dort eingreifen, wo die Persönlichkeit des Einzelnen auf dem Spiel» stehe.[806] Die Einzelne bedürfe keiner Verfügungsgewalt über eigene Daten, sondern es sei lediglich zu gewährleisten, dass die Betroffene gegenüber Dritten im Interaktionsprozess ein selbstbestimmtes Eigenbild abgeben könne.[807] 279

Diese ablehnende Haltung scheint indes auf einem umfassend verstandenen Verfügungsrecht zu basieren, welches die Verfügungsmacht *einzig* bei der Betroffenen sieht.[808] Dies entspricht gerade nicht dem Portabilitätsrecht und nicht dem hier vorgeschlagenen Verständnis eines informationellen Selbstbestimmungsrechts. Zudem stützt sich die Argumentation für eine positive Seite der informationellen Selbstbestimmung auf Entwicklungen, die im Jahr 2005, als die erwähnte Lehrmeinung erschien, noch nicht sichtbar waren. 280

800 VAN SPYK, 31.
801 VAN SPYK, 31.
802 VAN SPYK, 32.
803 VAN SPYK, 36.
804 AEBI-MÜLLER, 10.
805 AEBI-MÜLLER, 294.
806 AEBI-MÜLLER, 294.
807 AEBI-MÜLLER, 290.
808 So AEBI-MÜLLER, 291 f.

cc. Analogien zum sachenrechtlichen Eigentum

281 Vereinzelt werden im Kontext der Diskussionen zu einem möglichen «Dateneigentum» Analogien zur positiven und negativen Seite des (sachenrechtlichen) Eigentums gezogen. Namentlich wird die negative Seite des Eigentums im Datenschutzrecht bereits weitgehend als durch verschiedene Rechte – etwa dem Einwilligungserfordernis oder dem Auskunftsrecht – verwirklicht betrachtet.[809] Eine positive Seite, im Sinn einer Zuweisung von Personendaten oder die Möglichkeit der Übertragung fehle allerdings noch.[810] Dabei fällt auf, dass das Portabilitätsrecht ausdrücklich angesprochen, aber als Ausfluss der negativen Seite betrachtet wird. Dies dürfte jedoch damit zusammenhängen, dass der Autor das Portabilitätsrecht als Erweiterung des Auskunftsrechts versteht.[811] In der Sache handelt es sich beim Portabilitätsrecht allerdings um eine faktische Möglichkeit der Datenübertragung, wenngleich damit noch keine rechtliche Zuweisung erfolgt. Auch ein Gutachten sah im Portabilitätsrecht und der damit einhergehenden Datenübertragung eine Parallele zum sachenrechtlichen Verfügungsrecht als positive Seite des Eigentums.[812]

d. Alter Wein in neuen Schläuchen: Kommerzialisierung der Persönlichkeit

282 Wenn das DSG den wirtschaftlichen Wert von Personendaten als Aspekt der Persönlichkeit der Betroffenen aufgreift, indem es Daten durch einen Anspruch auf Herausgabe und Übertragung teilweise «verkehrsfähig» macht, so erinnert dies an eine ältere Diskussion bezüglich einer Kommerzialisierung der Persönlichkeit.[813] Denn Persönlichkeitsrechte sollen den Menschen in seiner Würde und Einzigartigkeit schützen; sie sind untrennbar mit der Trägerperson verbunden und daher nach überwiegender Auffassung unübertragbar.[814] Sie sollen der Wahrung ideeller Interessen dienen, weshalb zwischen ideellen Rechten und Vermögensrechten – zwischen Abwehr- und Verwertungsrechten – unterschieden wird.[815]

283 Eine Tendenz zur Annäherung dieser beiden unterschiedlich gearteten Rechte lässt sich indes seit längerem beobachten. So kam um die Jahrtausendwende

809 Thouvenin, SJZ 2017, 26 f.
810 Thouvenin, SJZ 2017, 25 f., noch in Bezug auf das aDSG.
811 So jedenfalls Thouvenin/Weber/Früh, 12 f., ebenso 173 und 175.
812 Expertengruppe Zukunft, 113.
813 Grundlegend Meyer, *passim*.
814 Büchler, 178 f.
815 Büchler, 179; Büchler, AcP 2006, 311.

eine Diskussion darüber auf, ob Prominente neben dem Urheberrecht an ihren Werken auch einer eigenen Verwertungsmöglichkeit über Aspekte ihrer Persönlichkeit bedürfen. Der kulturelle Zeitgeist, gepaart mit neuen Möglichkeiten der (Selbst-)Vermarktung, führte zu dieser Zeit dazu, dass sich Prominente nicht mehr einzig über ihre Werke im Sinne des Urheberrechts vermarkteten, sondern über alles, was den «Stempel ihrer Persönlichkeit» trug, also etwa Namen, Bilder, Stimmen oder Slogans.[816] Die Lehre stellte fest, dass ein Funktionswandel des Persönlichkeitsrechts stattgefunden habe, nach welchem sich das Recht auf Individualität von einem blossen Verbotsrecht in ein Quasi-Immaterialgüterrecht gewandelt habe, also in ein positives ausschliessliches Verwertungsrecht.[817] Daraus ergibt sich, dass bereits das reine Persönlichkeitsrecht durchaus eine positive Seite umfassen kann, welche (für die hier genannten Persönlichkeitsgüter) die Möglichkeit einer ausschliesslichen Nutzung vorsieht.[818] In Bezug auf das Recht am eigenen Bild hat das BGer seither die kommerzielle Verwertung von Persönlichkeitsrechten denn auch nicht per se für unzulässig erachtet.[819]

e. Folgerung

Insgesamt scheint die Lehre einer positiven Ausprägung der informationellen Selbstbestimmung gegenüber offen zu sein. Dies gilt unabhängig davon, ob sie als eine Folge der Diskussion um die Kommerzialisierung der Persönlichkeit bewertet wird oder nicht. Mit dem Recht auf Datenportabilität fand m.E. ein «Funktionswandel» statt. Dies gilt zumindest für den hier interessierenden Teilbereich der Persönlichkeit, selbst wenn sich die Diskussion zur Kommerzialisierung der Persönlichkeit nicht unverändert auf Daten übertragen lässt: Namentlich ist wohl unbestritten, dass Personendaten seit jeher (faktisch) wirtschaftlich verwertbar sind.[820] Dabei ermöglicht die Einwilligung der be- 284

816 SEEMANN, sic! 1997, 260.

817 BÜCHLER, 183; SEEMANN, sic! 1997, 261; MEYER, 348.

818 So ausdrücklich BÜCHLER, 183.

819 BGE 136 III 401. Es hielt fest, dass die Beschwerdegegnerin im konkreten Fall kein Recht zum Rücktritt vom Vertrag ohne Bezahlung der vereinbarten Rücktrittsentschädigung hatte, da sie zulässigerweise eine vertragliche Verpflichtung einging, durch welche das Recht am eigenen Bild veräussert wurde (siehe insb. E. 5.3.2 und 5.5); Parallelen auch zum Datenschutzrecht ziehend SCHMIDT, digma 2019, 180; hingegen kritisch gegenüber einer Übertragung auf das Datenschutzrecht EGGEN/TONEATTI, Jusletter 2024, Rz. 39 und 47; ebenso OFK DSG-KLAUS/THOMANN, Art. 6 N 48.

820 DREXL et al., Data Ownership, 3; SCHMIDT, 113.

troffenen Person die Verwertung der Daten.[821] Ferner stützt sich das Datenschutzrecht zwar letzten Endes ebenfalls auf das Persönlichkeitsrecht, es hat jedoch durch seine eigenständige grundrechtliche Verankerung und seine Konkretisierung im DSG eine eigene Prägung erhalten, was sich bereits darin zeigt, dass der für den Persönlichkeitsschutz massgeblichen Sphärentheorie keine Bedeutung zukommt.[822] Personendaten werden durch das DSG in jedem Fall und per se als schützenswert erachtet.

285 Allerdings hatte bislang das Datenschutzrecht von der Schaffung von Rahmenbedingungen, die eine Verwertung ermöglichen, abgesehen. So wurde namentlich ein Dateneigentum überwiegend kritisch betrachtet und gesetzgeberisch nicht weiterverfolgt.[823] Mit dem Recht auf Datenportabilität erhalten Betroffene erstmals ansatzweise solche Verwertungsrechte, indem sie über die Daten disponieren können.[824] Damit ist zu konstatieren, dass das Portabilitätsrecht keine abwehrrechtliche, sondern eine «verwertungsrechtliche» Funktion einnimmt, die sich aber dennoch auf die Persönlichkeit der Betroffenen abstützt.

286 Somit vollzieht das Datenschutzrecht – und mit ihm womöglich das Verständnis der informationellen Selbstbestimmung – eine Neuausrichtung.[825] Dieser «Paradigmenwechsel»[826] ist angesichts des neuen Verwendungskontexts von Daten sachgerecht und, wie gezeigt, in seinem persönlichkeitsrechtlichen Kern nicht neu. Relativierend ist dabei anzufügen, dass die Möglichkeit zur Verwertung stark eingeschränkt ist, da sich durch das Portabilitätsrecht beim alten Verantwortlichen nichts ändert. Dadurch ist in jedem Fall weiterhin primär die Betroffene in ihrer Persönlichkeit tangiert. Dies zeigt sich deutlich am Recht auf Datenherausgabe nach Art. 28 Abs. 1 DSG. Dadurch lässt sich das

821 SCHMIDT, 74, die dabei auch auf die damit einhergehenden Probleme, namentlich die grundsätzliche Widerrufbarkeit der Einwilligung eingeht. Dies ist vorliegend nicht zu vertiefen, da einzig die betroffene Person von ihrem Portabilitätsrecht Gebrauch machen kann. Siehe aber immerhin THOUVENIN, SJZ 2017, 31, der im bereits erwähnten BGE 136 III 401 die Grundlage dafür sieht, den Grundsatz der freien Widerrufbarkeit der Einwilligung auch im Datenschutzrecht fallen zu lassen.

822 BSK DSG-SCHÖNBÄCHLER/MAURER-LAMBROU/KUNZ, Art. 1 N 15 f.; differenzierend auch FLÜCKIGER, AJP 2013, 855.

823 FRÜH, digma 2019, 173 m.w.N.; PICHT, Jusletter IT Flash 2017, *passim*; SCHMIDT, digma 2019, *passim*; THOUVENIN, SJZ 2017, *passim*; WEBER/THOUVENIN, ZSR 2018, *passim*. Der Bundesrat beurteilte eine solche Lösung als «nicht umsetzbar», da sie zu stark von den Entwicklungen auf internationaler Ebene abweichte, siehe Botschaft DSG 2017, 6988.

824 DREXL, Data Access, 8 ff.; KRKomm-MUNZ, Art. 20 DSGVO N 8.

825 Für das europäische Recht JÜLICHER/RÖTTGEN/V. SCHÖNFELD, ZD 2016, 360.

826 LAUX, digma 2019, 170.

Portabilitätsrecht indes umso mehr auf den verfassungsrechtlichen Datenschutz stützen und ist mit seiner Zielsetzung als datenschutzrechtliches Institut zu qualifizieren.

5. Allgemeiner Persönlichkeitsschutz als eigenständige Zielsetzung

Im Zentrum einer datenschutzrechtlichen Auslegung des Rechts auf Datenportabilität steht regelmässig das soeben erläuterte Recht auf informationelle Selbstbestimmung. Gleichwohl gibt es weitere Bereiche der Persönlichkeit, auf deren Schutz das Recht auf Datenportabilität abzielen könnte, gerade angesichts der weitgehend unklaren Bedeutung des verfassungsrechtlichen Datenschutzes. 287

Auf zahlreiche Bedrohungen für die Persönlichkeit hat der Gesetzgeber denn auch bereits vor der Übernahme eines Rechts auf informationelle Selbstbestimmung durch das BGer reagiert.[827] In Art. 10 BV ist der verfassungsrechtliche Schutz und in den Art. 27 ff. ZGB der privatrechtliche Schutz der Persönlichkeit verankert.[828] Art. 28 ZGB stellt dabei den Grundsatz dar und bestimmt den Begriff der Persönlichkeit nicht abschliessend.[829] Das Grundrecht der persönlichen Freiheit umfasst das Recht auf Selbstbestimmung und auf individuelle Lebensgestaltung sowie den Schutz der elementaren Erscheinungen der Persönlichkeitsentfaltung.[830] Das BGer hat hierzu festgehalten, dass Art. 13 BV im Vergleich zu Art. 10 BV «in besonderer Weise die verschiedene Aspekte umfassende Privatsphäre mit ihren spezifischen Bedrohungsformen» schützt.[831] Dem allgemeinen Persönlichkeitsschutz kommt jedoch in Bezug auf Sachverhalte, die vom Recht auf informationelle Selbstbestimmung ebenfalls abgedeckt sind, keine weitergehende Bedeutung zu.[832] In datenschutzrechtlicher Hinsicht lassen sich daher aus dem allgemeinen Persönlichkeitsschutz keine weitergehenden Zielsetzungen ableiten. 288

In der Literatur finden sich allerdings Voten, wonach das Recht auf Datenportabilität dem Schutz der Persönlichkeit vor übermässiger Bindung an eine An- 289

827 Waldmeier, 15 f.

828 SGK BV-Schweizer/Bongiovanni, Art. 10 N 5.

829 SGK BV-Schweizer/Bongiovanni, Art. 10 N 6.

830 Erstmals BGE 97 I 45 E. 3.; jüngst etwa BGE 148 I 1 E. 6.2.1; BGE 138 IV 13 E. 7.1 SGK BV-Schweizer/Bongiovanni, Art. 10 N 11.

831 So BGE 138 I 331 E. 5.1.

832 BGE 144 I 126 E. 4.2; BGE 138 I 256 E. 4.; SGK BV-Breitenmoser, Art. 13 N 5; SGK BV-Schweizer/Striegel, Art. 13 N 97.

bieterin dienen soll (siehe Art. 27 Abs. 2 ZGB).[833] Eine solche übermässige Bindung entstehe durch Investition in den Aufbau von Profilen und die Umständlichkeit eines Wechsels der Anbieterin.[834] Eine übermässige Bindung beruht allerdings entweder auf dem Gegenstand der Bindung oder auf dem Übermass.[835] Ob ein Übermass vorliegt, ist in erster Linie anhand von Intensität und Dauer zu ermitteln.[836] Dies dürfte in den Anwendungsfällen des Datenportabilitätsrecht kaum zutreffen. Da auch der Gegenstand der Bindung im hier interessierenden Bereich nur selten unzulässig ist, lässt sich aus einer dem Portabilitätsrecht unterliegenden Datenbearbeitung eines Verantwortlichen m.E. nicht generell eine übermässige Bindung ableiten.

6. Erkenntnisse

290 Aus den vorstehenden Ausführungen zeigt sich, dass das seit längerem kritisierte Konzept und Verständnis des Rechts auf informationelle Selbstbestimmung möglicherweise an seine Grenzen gestossen ist. Dabei geht die Kritik in der Schweiz und der EU in eine ähnliche Richtung – gemeinsam ist ihr, dass ein uneingeschränkt verstandenes Recht auf informationelle Selbstbestimmung im Sinne eines umfassenden Herrschaftsrechts abgelehnt wird und Alternativen diskutiert werden. Dennoch wird in der Schweiz, im Gegensatz zur EU, ein Recht auf informationelle Selbstbestimmung derzeit (noch) anerkannt, wenngleich unklar ist, was es genau schützt. Dies verleitet dazu, das Portabilitätsrecht hinsichtlich seiner Ziele auf dieses unklare Konstrukt abzustellen, was die Suche nach den datenschutzrechtlichen Zielen des Portabilitätsrechts erschwert. Wie gezeigt wurde, kann das Recht auf Datenportabilität zwar im klassischen Sinn als Ausgestaltung einer unter Privaten zur Geltung kommenden Drittwirkung der informationellen Selbstbestimmung verstanden werden: Das Institut ermöglicht der Betroffenen tatsächlich eine selbstbestimmte Datendisposition und damit zumindest eine teilweise Herrschaft über «ihre» Daten. Bei diesem Verständnis zeigten sich jedoch Ungereimtheiten.

291 Vorliegend wird die selbstbestimmte Datendispositionsmöglichkeit der Betroffenen daher nicht als ein von seiner grundrechtlichen Veranlagung her eigentlich umfassend konzipiertes, aber als Portabilitätsrecht nur eingeschränkt umgesetztes Institut verstanden. Vielmehr wird es bereits in grundrechtlicher und besonders datenschutzrechtlicher Hinsicht mit der Entwicklung einer

833 Steiner, 125.
834 Steiner, 125.
835 BSK ZGB I-Reitze, Art. 27 N 9.
836 BSK ZGB I-Reitze, Art. 27 N 10 m.w.N.

Datenwirtschaft begründet, die es notwendig gemacht hat, der Betroffenen ein rechtliches Mittel zu geben, um in diese Datenwirtschaft eingreifen zu können. Dabei handelt es sich nicht um eine wettbewerbsrechtliche Zielsetzung, sondern um ein datenschutzrechtliches *Empowerment* in Form des Portabilitätsrechts, das nach hier vertretener Ansicht als (eine erste) Reaktion auf diese Umwälzungen (und daraus entstandenen Schutzbedürfnisse) betrachtet werden muss. Dies trifft auf das Recht auf Datenübertragung zu, aber besonders auch auf das Recht auf Datenherausgabe, das ein eigenständiges Recht darstellt und das die Betroffene aus irgendwelchen Gründen geltend machen kann. Namentlich müssen die Gründe keinerlei wettbewerbliche Relevanz haben. Bei diesem Verständnis sind die gesetzgeberisch vorgesehenen Einschränkungen nur auf Daten, die automatisiert und freiwillig bearbeitet werden, denn auch schlüssiger.

Die Reaktion des Gesetzgebers erfolgte jedoch noch bevor die Rechtsprechung 292
oder der Verfassungsgeber eine den veränderten Umständen angepasste Konturierung des verfassungsrechtlichen Datenschutzes vorgenommen hat. Eine solche Konturierung wird auch vorliegend nur mit Bezug auf das Portabilitätsrecht angestrebt. Daraus folgt, dass jedenfalls der verfassungsrechtliche Datenschutz, auf welchen sich das Portabilitätsrecht stützt, die veränderten Umstände der Datenwirtschaft ebenfalls berücksichtigen sollte. Das Portabilitätsrecht sollte sich insb. auf einen positiven, gestalterischen Aspekt der Persönlichkeit der von einer Datenbearbeitung betroffenen Person stützen können. In der Lehre finden sich Stimmen, die diesem Verständnis eines positiv gelagerten Persönlichkeitsrechts gegenüber offenstehen. Im Kontext des Datenportabilitätsrechts wurde ein solches Verständnis in der Schweiz aber bislang nicht vertieft untersucht.

Das Portabilitätsrecht mag damit als Anlass dienen, die Interpretation des ver- 293
fassungsrechtlichen Datenschutzes grundlegend zu überdenken, zumal dessen rechtlicher Status auch ohne Portabilitätsrecht umstritten ist. Hierzu wären weitere Untersuchungen notwendig, die an dieser Stelle aber mit Blick auf die Forschungsfrage unterbleiben können.

B. Wettbewerbsrechtliche Ziele

Neben den datenschutzrechtlichen Zielen werden beim Recht auf Datenpor- 294
tabilität wettbewerbsrechtliche Ziele vorgebracht. Dass unterschiedliche Ziele parallel bestehen, ist keineswegs ausgeschlossen und wird in der Literatur re-

gelmässig angenommen.[837] Dabei sind, anders als bei der datenschutzrechtlichen Konzeption, die Rahmenbedingungen in der EU nicht grundsätzlich anders, weshalb nachfolgend die europäische Literatur ebenfalls heranzuziehen ist. Zunächst sind die wettbewerbsrechtlichen Ziele jedoch kurz in das Gefüge des Wettbewerbsrechts einzubetten.

1. Ökonomische Einordnung

a. Daten als wirtschaftliche Güter

295 Einer möglichen wettbewerbsrechtlichen Zielsetzung des Rechts auf Datenportabilität liegen ökonomische Überlegungen zugrunde. Daten weisen in dieser Hinsicht einige Besonderheiten auf. Sie werden als wirtschaftliche Güter gehandelt,[838] sind dabei jedoch nicht rivalisierend, sondern beliebig replizier- und mehrfach verwendbar.[839] Die Nutzung durch eine Person beeinträchtigt die Nutzung oder den Zugang durch andere Personen also nicht.[840] Haben Daten den eigenen Einflussbereich bzw. das eigene Ökosystem verlassen, ist es schwierig, Dritte von deren Nutzung auszuschliessen.[841] Dies trifft besonders auf semantische Information zu, aber auch auf syntaktische Information in Form von Daten.[842]

296 Daten sind ihrer Natur nach nicht ausschliessbar und somit grundsätzlich öffentliche Güter.[843] Sie sind gleichzeitig für viele Personen nutzbar, ohne dass die Nutzung durch eine Person diejenige durch eine andere Person beeinträchtigt.[844] Die Daten werden dabei weder verbraucht noch verschlechtern sie sich.[845] Die Grenzkosten für Daten entsprechen daher dem Preis, der für

837 CR LPD-Benhamou, Art. 28 N 4; Epiney/Nüesch/Rovelli, 178; Götzinger/Vasella, SZW 2021, 41; für die DSGVO-Regelung Fix, 69 m.w.N.

838 Zu Daten als Güter Schmidt, 45 ff.; Zech, 216; zum ökonomischen Wert von Daten Schweitzer/Peitz, 15 ff.; für die Mobilität im Besonderen siehe Bundesministerium für Verkehr und digitale Infrastruktur, 67.

839 Martens, Data Access, 75; Schweitzer/Peitz, 18; Zech, 118.

840 IGE, 13; Yildiz, Rz. 252.

841 Collovà et al., 7; Jentzsch, 26.

842 Zech, 118. Dazu auch Rz. 31.

843 Collovà et al., 7; Martens, Economic Perspective, 5; Thouvenin/Weber/Früh, 9 f.; Thouvenin, SJZ 2017, 24; Zech, 117 m.w.N. aus den Wirtschaftswissenschaften; siehe jedoch Dewenter/Bernhardt, Rz. 46; zur Möglichkeit, Personen von der Nutzung auszuschliessen siehe Rz. 297.

844 Thouvenin/Weber/Früh, 9.

845 Dewenter/Bernhardt, Rz. 43.

deren Reproduktion anfällt – und sind damit nahezu null.[846] Dies kann zu Anreizproblemen hinsichtlich der Investition in Erzeugung, Sammlung und Speicherung von Daten führen,[847] da Daten – anders als körperliche Gegenstände und die abschliessend geregelten Immaterialgüterrechte – nicht absolut geschützt sind.[848] Weil öffentliche Güter nicht-rivalisierend sind, ist deren Nutzen für die Gesellschaft am grössten, wenn sie von allen genutzt werden können.[849] Sollen also bestimmte Rechte an Daten gewährt werden, muss dies gerechtfertigt sein, namentlich weil ein Marktversagen vorliegt oder die Betroffenen vor Schäden oder anderen rechtlich relevanten Nachteilen, die durch die Bearbeitung von Personendaten verursacht werden, geschützt werden müssen.[850] Dies ist in Bezug auf die Produktion von Personendaten nicht der Fall, wohl aber hinsichtlich der Nutzung einmal erhobener Personendaten.[851] Der Zugang zu und die Erhaltung von Daten sind in bestimmten Märkten unabdingbar, entweder weil die Daten selbst monetarisierbar sind (bspw. um gezielt Werbung zu vermitteln) oder weil sich dank der Daten Erkenntnisse über das Verhalten und die Vorlieben von Personen und dadurch Möglichkeiten zur Verbesserung des eigenen Dienstes ergeben.[852] Die aus den Daten ableitbaren Informationen können sodann zur Steigerung der Gewinne und zur Stärkung der Wettbewerbsfähigkeit genutzt werden.[853] Mehr Wissen führt mithin zu mehr Profit.[854] Für Unternehmen ist es zudem vorteilhaft, über möglichst grosse und umfassende Datensätze zu verfügen. Denn um ein Angebot zu entwickeln, müssen sie in der Datenwirtschaft typischerweise hohe Fixkosten tragen.[855] Notwendig ist eine Dateninfrastruktur, um Daten zu sammeln, zu speichern und zu analysieren.[856] Mit zunehmender Datenmenge nehmen die Durchschnittskosten für die Dateninfrastruktur jedoch stark ab.[857] Die Grenzkosten für zusätzlich gesammelte, gespeicherte oder analysierte Daten

846 Martens, Data Access, 74.

847 Dewenter/Bernhardt, Rz. 73; IGE, 13; Schweitzer/Peitz, 18; in diesem Sinne auch Bijok, 192.

848 Siehe dazu Thouvenin, Immaterialgüterrecht, Rz. 17; ebenso Landolt, 49; mit Blick auf Sachdaten auch Jotterand, sic! 2025, 443 f.

849 Thouvenin, ZSR Beiheft 2023, 38; OECD, Data-Driven Innovation, 180 m.w.N.

850 Thouvenin, ZSR Beiheft 2023, 39.

851 Thouvenin, ZSR Beiheft 2023, 39, insb. Fn. 110.

852 Beispiele nach Steffen/Wieworra/Kroon, 25; ähnlich auch Sadowski, Big Data & Society 2019, 5; Weber, ZWeR 2014, 171.

853 Fast/Schnurr/Wohlfarth, 753.

854 Sadowski, Big Data & Society 2019, 5; dazu auch Yan/He, JCLE 2022, 884 ff.

855 Dewenter/Bernhardt, Rz. 55; IGE, 14; Yildiz, Rz. 58.

856 Dewenter/Bernhardt, Rz. 55.

857 Dewenter/Bernhardt, Rz. 55.

sind dabei, wie erwähnt, vernachlässigbar (Grenzkostendegression).[858] Daher verfügen Unternehmen mit grösseren Datensätzen über strukturelle Vorteile gegenüber kleineren Unternehmen (Skaleneffekte).[859] Daneben profitieren sie von Verbundvorteilen (sog. *economies of scope*), wenn sich Daten für mehrere verschiedene Angebote nutzen lassen.[860] Unternehmen auf einem Markt befinden sich damit in einem Wettbewerb nicht nur um die Betroffenen, sondern auch um deren Daten.

b. Ökonomische Relevanz des Rechts auf Datenportabilität

297 Von der Nutzung von Daten können andere Personen gleichwohl ausgeschlossen werden, entweder durch technische bzw. faktische Massnahmen oder weil die Gesetzgebung entsprechende rechtliche Absicherungen vorsieht (sog. «Club-Güter»).[861] Ist dies der Fall, stellen Daten keine öffentlichen Güter dar. Als Beispiel für eine technische Massnahme ist etwa die Verschlüsselung von Daten oder deren Speicherung in proprietären Systemen zu nennen.[862] Eine rechtliche Massnahme stellt bspw. der rechtliche Schutz von Betriebs- und Geschäftsgeheimnissen[863] oder die (nur *inter partes* wirkende) vertragliche Absicherung[864] dar. Auch Rechtsgebiete wie das Persönlichkeits-, das Datenschutz- oder das Urheberrecht können Massnahmen enthalten, die (bestimmte) Daten von der Nutzung für andere ausschliessen.[865] Schliesslich können Daten faktisch ausschliessbar bleiben, indem sie geheim gehalten werden.[866]

298 Während in Bezug auf die Produktion von Daten kein Marktversagen vorliegt, stellen heute die von Unternehmen angebotenen Dienste, zumal in der Datenwirtschaft, vermehrt *walled gardens* dar. Kunden bewegen sich nur innerhalb dieser *walled gardens*, ihre Daten verbleiben in einem Silo.[867] Dies soll Kunden

858 IGE, 14; Yildiz, Rz. 58.
859 Yildiz, Rz. 58.
860 Dewenter/Bernhardt, Rz. 60.
861 Krämer/Senellart/De Streel, 51; Schmidt, 17 ff.; sind die Daten ausserdem nicht ausschliessbar, handelt es sich um öffentliche Güter, siehe Thouvenin, SJZ 2017, 24; zu den Club-Gütern Jentzsch, 26.
862 Thouvenin/Weber/Früh, 9.
863 Thouvenin/Weber/Früh, 9; dazu ausführlich Jotterand, sic! 2025, 444; Picht, Jusletter IT Flash 2017, Rz. 1 ff.
864 Jotterand, sic! 2025, 444 f.; Martens, Economic Perspective, 5.
865 Siehe für das deutsche Recht die Ausführungen bei Podszun, 59 ff. Eine umfassende Datenrechtsgesetzgebung gibt es in der Schweiz bislang nicht.
866 Zech, 119.
867 Collovà et al., 8.

dazu bewegen, möglichst viel Zeit bei einem Anbieter zu verbringen.[868] Ein Beispiel für einen solchen *walled garden* ist das Ökosystem von Apple, das aus zahlreichen unterschiedlichen Produkten besteht, die aufeinander abgestimmt und jeweils interoperabel, gegenüber anderen Anbietern aber kaum durchlässig sind.[869]

Mit Blick auf seine historischen Ursprünge ist das Portabilitätsrecht dabei (auch) eine Antwort auf die zunehmende Abschottung des *World Wide Web* in Silos und *walled gardens*. Das Funktionieren des Marktes mit seiner charakteristischen Offenheit und Interkonnektivität soll erleichtert, der idealistische Open-Web-Ansatz zugunsten möglicher Innovationen gestärkt werden.[870] Der Gesetzgeber hat mit dem Recht auf Datenportabilität daher (auch) aus wirtschaftspolitischen Gründen in den Markt eingegriffen, um unerwünschte Marktergebnisse zu beheben.[871] Die portierten Daten werden, nach Massgabe der Betroffenen, entweder dieser selbst oder einem Dritten zugänglich gemacht. Damit stellt das Portabilitätsrecht ein Institut dar, das die aufgeführten Mechanismen durchbrechen kann, indem es Verantwortliche rechtlich zur Portierung verpflichtet. Ob dies die Zielsetzung war und ob dies die Grundlagen für die Erreichung dieser Zielsetzung schaffen konnte, wird nachfolgend untersucht. 299

2. Wechselkosten senken und Lock-In-Effekt verhindern

a. Allgemein

Unternehmen möchten ihre Kunden an sich binden.[872] Dieser Logik folgt auch die Datenwirtschaft, in welcher Daten als wirtschaftliche Güter gehandelt werden. Während jedoch einmal erhobene Daten im Konsum nicht-rivalisie- 300

868 KRATZ, InTeR 2019, 28.

869 Anschaulich BERNERS-LEE, Scientific American 2010, 83. Konkret waren etwa Verlinkungen auf das Programm «iTunes» lange nicht mittels (öffentlichen) «http:»-Protokolls möglich, sondern nur mit dem proprietären «itunes:»-Protokoll. Auch heute noch haben Nutzer anderer Ökosysteme (etwa Windows oder Android) Schwierigkeiten, den proprietären «App Store» von Apple zu öffnen. Ebenfalls das Beispiel von BERNERS-LEE aufnehmend FIX, 90 f., insb. Fn. 237. Dies adressiert die EU nunmehr auch im DMA, dazu Rz. 419 ff.

870 Europäisches Parlament, Gesamtkonzept Datenschutz, 7, insb. Fn. 2; FIX, 71; KRATZ, InTeR 2019, *passim*; dazu bereits ausführlich Rz. 86 ff.

871 Mit Blick auf Deutschland ZSCHOCH, 264.

872 HILDEBRAND, 57 ff., insb. im Onlinekontext auch 67 f.

rend sind, kann deren eigentliche Erhebung durchaus rivalisierend sein, namentlich wenn eine hohe Marktkonzentration besteht und nur einige wenige Unternehmen dazu in der Lage sind.[873] Das Interesse eines Unternehmens ist damit zweierlei: Es stellt an sich einen Wettbewerbsvorteil bzw. Informationsvorsprung dar, wenn ein Unternehmen Daten über seine Kunden beschaffen kann (und ein anderes Unternehmen nicht).[874] Ein Unternehmen kann sich dadurch ein *first mover advantage* verschaffen und seine eigene Attraktivität steigern, was zu höheren Markteintrittsschranken führt.[875] Überdies und unabhängig davon hat ein Unternehmen ein Interesse daran, dass einmal erhobene Daten (ausschliesslich) bei ihm verbleiben.[876] Es stellt daher ein Wettbewerbsvorteil dar, wenn Wettbewerbern der Zugang zu Daten verschlossen bleibt.[877] Der konkrete ökonomische Wert der Daten kann davon abhängen, wer sonst noch Zugriff darauf hat und daraus Erkenntnisse ableiten kann.[878] Unternehmen können daher versuchen, ihre Kunden daran zu hindern, die Daten zu einem anderen Anbieter mitzunehmen.[879] Dies erklärt die Entstehung der bereits erwähnten *walled gardens*.[880] Heute haben in den meisten Sektoren einige wenige Unternehmen die Kontrolle über die relevanten Datensätze.[881]

301 Kunden, die einen Anbieter wechseln wollen, haben Wechselkosten zu tragen, also Kosten, die (zusätzlich und) nur aufgrund des Wechsels anfallen.[882] Diese Kosten sind nicht notwendigerweise finanzieller Natur, sondern können admi-

873 Krämer/Senellart/De Streel, 52 f. m.w.H.; in diese Richtung auch Denoth/Kaufmann, sic! 2016, 510, die festhalten, dass das Interesse am Errichten von Zugangsbarrieren nicht primär die Datensätze an sich, sondern vielmehr die Datenlieferanten betreffe.

874 UVEK/EDA, 9.

875 Yildiz, Rz. 532. Zu den Markteintrittsschranken Rz. 312 f.

876 Denoth/Kaufmann, sic! 2016, 507; Europäische Kommission, Aufbau Datenwirtschaft, 10. Das eigentliche Geschäftsmodell besteht nach Collovà et al., 8, daraus, dass das Unternehmen die aufbereiteten persönlichen Daten der Kunden entweder selbst nutzen oder anderen Akteuren zugänglich machen, um bspw. zielgerichtete Werbung schalten zu können. Im zweiten Fall wird das Unternehmen für die Weitergabe der Daten (oder daraus abgeleiteten Erkenntnisse) entschädigt.

877 Bijok, 185; Ensthaler/Üge, BB 2022, 2053; ähnlich auch Schweitzer/Peitz, NJW 2018, 275 m.w.N.

878 Krämer/Senellart/De Streel, 53 m.H.a. Ichihashi, RJE 2021, 523 f.

879 Europäische Kommission, Free Flow, 47; Graef/Verschakelen/Valcke, LJHSE 2013, 59.

880 Dazu oben Rz. 298 f.

881 Denoth/Kaufmann, sic! 2016, 507.

882 Graef/Verschakelen/Valcke, LJHSE 2013, 69; Weber/Thouvenin, 69; grundlegend dazu Klemperer, The Quarterly Journal of Economics 1987, *passim*.

nistrativer oder sonstiger Art sein (etwa in Form von Zeitaufwand).[883] Durch zu hohe Wechselkosten entsteht für die Kunden ein Lock-In-Effekt: Ein Wechsel wird teuer, oder der Kunde wird ganz daran gehindert zu wechseln – er bleibt «eingeschlossen».[884] Dies führt in der Tendenz dazu, dass ein Kunde für einen bestimmten Zweck nur einen Anbieter nutzt (sog. *Single-Homing*),[885] obwohl die Parallelnutzung mehrerer Dienste (sog. *Multi-Homing*) möglich wäre.[886] Hier soll das Portabilitätsrecht ansetzen.

Ein Lock-In-Effekt greift häufig, wenn ein Unternehmen ohnehin schon zu den grössten auf dem Markt gehört und es aufgrund dieser Grösse und der Netzwerkeffekte besonders attraktiv ist.[887] Dabei verhilft dem Unternehmen einerseits die Anzahl der Nutzer zu ausgeprägten Netzwerkeffekten, andererseits aber auch der vorhandene Datensatz. Es verfügt über einen *big data advantage*.[888] In der Literatur werden diese Netzwerkeffekte teilweise auch als Unterfall der Wechselkosten, als sog. Kompatibilitätskosten, diskutiert.[889] Gerade im Kontext von Datenökosystemen führen Netzwerkeffekte also durchaus zu höheren Wechselkosten, was die Nachteile, die die Betroffene bei einem Wechsel tragen muss, nochmals erhöht.[890] Dies kann dazu führen, dass der kontrollierbare Verhaltensspielraum für Unternehmen nicht mehr durch wettbewerbliche Kräfte alleine beeinflusst werden kann.[891] Unternehmen können die Qualität ihres Angebots senken, weil sie auf die «eingesperrten» Kunden zählen können.[892] Es findet mithin kein funktionierender Wettbewerb mehr statt. 302

Das Recht auf Datenportabilität soll Wechselkosten senken.[893] Es soll die Hemmschwelle für einen Anbieterwechsel nach unten nivellieren und so als Korrektiv gegen diejenigen Effekte wirken, die einen funktionierenden Wett- 303

883 Fix, 72; bspw. kann der zeitliche Aufwand, um sämtliche Playlists von einem Musikanbieter zu einem anderen zu portieren, erheblich sein und Nutzer daher davon abhalten, zu einem anderen Anbieter zu wechseln, Beispiel nach Krämer/Senellart/De Streel, 56.

884 Europäische Kommission, Impact Assessment, 28; Graef/Verschakelen/Valcke, LJHSE 2013, 5 f.; Steffen/Wieworra/Kroon, 21; Zhang, HJLT 2023, 669 m.w.N.

885 Europäische Kommission, DMA Impact Assessment Report, 23.

886 Schweitzer/Peitz, NJW 2018, 277.

887 Fix, 73; siehe dazu auch die Ausführungen zum Netzwerkeffekt in Rz. 49 ff.

888 Martinelli, 137.

889 Zhang, HJLT 2023, 669, auch unter Berücksichtigung solcher Stimmen, die Netzwerkeffekte separat zu Wechselkosten behandeln.

890 Martinelli, 137; Steffen/Wieworra/Kroon, 22.

891 Fix, 74.

892 Yildiz, Rz. 576.

893 Krämer/Senellart/De Streel, 56; Landolt, 184 f.; BSK DSG-Laux/Steiner, Art. 28 N 41; Zhang, HJLT 2023, 665 m.w.N.

bewerb aushebeln. Damit zielt das Recht darauf ab, einen Lock-In-Effekt zu verhindern und dadurch den Wettbewerb zwischen verschiedenen Unternehmen zu stärken.[894] Die Verhinderung eines *Lock-In* ist somit das Mittel, um eine Senkung der Wechselkosten für die Betroffene als Ziel zu erreichen. Folglich soll der Wettbewerb gestärkt werden, indem die Möglichkeit der ökonomischen Verwertung der Daten gefördert wird. Letzteres zeigt sich daran, dass das Recht auf Datenportabilität nicht nur die Herausgabe unmittelbar an die betroffene Person ermöglicht, sondern auch die Übertragung an eine andere Verantwortliche ausdrücklich vorsieht.[895] Damit bezieht das Gesetz die neue Verantwortliche mit ein – und implizit den wettbewerbsrechtlichen Aspekt. Aus der datenschutzrechtlich geprägten Wechselwirkung zwischen altem Verantwortlichen und Betroffener wird eine mehrseitige Beziehung, die die neue Verantwortliche ebenfalls umfasst. Diese vom Gesetzgeber geschaffene und von der Betroffenen initiierte Beziehung zwischen alten und neuen Verantwortlichen lässt sich kaum mehr allein durch datenschutzrechtliche Überlegungen rechtfertigen. Dies zeigt sich zudem daran, dass die neue Verantwortliche gar keine datenschutzrechtliche Rolle innehat, bis sie die Daten erhält (und folglich bearbeitet), Art. 28 DSG sie aber dennoch erwähnt.

b. Daten- oder userinduzierter Lock-In?

304 Das Recht auf Datenportabilität zielt auf eine Senkung der Wechselkosten ab, indem es der Betroffenen ermöglicht, die sie betreffenden Daten mitzunehmen. Offen ist jedoch, ob diese Senkung im Kern auf einen *Lock-In* der Daten (dateninduzierter *Lock-In*) oder einen *Lock-In* der User (userinduzierter oder sozialer *Lock-In*[896]) reagieren soll.

305 Einige Stimmen in der Literatur sind der Ansicht, dass besonders bei Internetdiensten die Wechselkosten auf einen dateninduzierten *Lock-In* zurückgehen könnten.[897] In spieltheoretischen Modellen liess sich nachweisen, dass etablierte Anbieter (sog. *incumbents*) ohne Portabilitätsrecht Anreize haben, mehr Daten zu erfassen als in einer Monopolstellung, um die Wechselkosten für die

894 PC LPD-Béguin, Art. 28 N 6; CR LPD-Benhamou, Art. 28 N 4; Bundesrat, Bericht Handlungsfelder, 25 f.; Elfering, 52; Engels, Internet Policy Review 2016, 7; Fix, 71; Graef/Verschakelen/Valcke, LJHSE 2013, 2; OECD, Mapping Initiatives, 7 f.; Weber/Thouvenin, 68 f.

895 So auch PC LPD-Béguin, Art. 28 N 27; Reichlin, 404.

896 So Graef, Telecommunications Policy 2015, 510.

897 Crémer/De Montjoye/Schweitzer, 82; Fast/Schnurr/Wohlfarth, 766; generell auch Schweitzer/Peitz, 50.

Betroffenen künstlich zu erhöhen.[898] In der Lehre wird denn auch teils vertreten, dass mit dem Portabilitätsrecht ein dateninduzierter *Lock-In* behoben werden soll.[899]

Von gewissen Wirkungen eines solchen dateninduzierten *Lock-In* ist durchaus auszugehen. Nicht zu unterschätzen sind allerdings die Netzwerkeffekte, die Wechselkosten erhöhen und aus Sicht einer Betroffenen einen Wechsel unattraktiv machen können. Dies gilt besonders für die im Gesetzgebungsverfahren häufig genannten Internetplattformen und sozialen Netzwerke, deren soziale Komponente regelmässig zu einem *Lock-In* aufgrund von Netzwerkeffekten führt.[900] Für soziale Netzwerke stellt die Anzahl Nutzer die wichtigste Kennzahl dar, weshalb sie besonders von Netzwerkeffekten betroffen sind.[901] Wer also ein bestimmtes soziales Netzwerk nutze, werde nicht zu einem anderen sozialen Netzwerk wechseln, wenn sämtliche Kontakte ebenfalls das alte Netzwerk nutzen, auch wenn dies technisch unter Mitnahme der Daten problemlos möglich wäre, so das Argument.[902] Dies deutet darauf hin, dass mit dem Portabilitätsrecht einem userinduzierten *Lock-In* entgegengetreten werden sollte. 306

Nach der hier vertretenen Ansicht nehmen die Betroffenen in Bezug auf den *Lock-In* eine Schlüsselrolle ein, indem sie entscheiden, ob sie vom Recht auf Datenportabilität Gebrauch machen, um ihre Daten zu verschieben.[903] Im Zentrum stehen damit auch in wettbewerblicher Hinsicht die Betroffenen, denen ein Wechsel ermöglicht werden soll. Behoben werden soll vor allem der *Lock-In* der Person und nicht der Daten. Die persönlichkeitsrechtlichen Aspekte des Portabilitätsrechts lassen sich bei der Untersuchung der wettbewerbsrechtlichen Zielsetzung nicht ignorieren, denn das Portabilitätsrecht ist in seinem 307

898 Wohlfarth, BISE 2019, 557.

899 Hennemann, PinG 2017, 6; Schweitzer/Peitz, NJW 2018, 277; Schweitzer/Peitz, 50; Schweitzer/Welker, 119.

900 Thouvenin/Weber/Früh, 173; Elfering, 52, die allerdings Netzwerkeffekte unabhängig und nicht in einem Zusammenhang mit den Lock-In-Effekten bespricht; Fix, 80; Votum NR Glättli, AB 2019 N 1814; Graef, Telecommunications Policy 2015, 511; siehe auch BKartA, Beschluss B6-22/16 vom 6. Februar 2019, Rz. 448, dort am Beispiel Facebook.

901 Siehe hierzu Steffen/Wieworra/Kroon, 22; ähnlich Yildiz, Rz. 572.

902 Dumermuth, 149; Fix, 80; ähnlich Elfering, 52; Martinelli, 139; Sperlich, 88; Yildiz, Rz. 573; Ziegler/Vasella, digma 2019, 163. Daneben wären bei einer umfassenden Betrachtung auch weitere Faktoren zu untersuchen, etwa der mögliche Einfluss eines «kognitiven *Lock-In*» dadurch, dass die Betroffene bei einem ihr bekannten Angebot bspw. auf einer Website schneller zu einer automatisierten Verarbeitung der Informationen übergehen kann (etwa, weil sie weiss, was sich wo auf der Seite befindet) und dies dadurch auf einer metabolischen Ebene weniger «kostspielig» für die Betroffene ist Sénécal et al., Journal of Internet Commerce 2015, *passim*.

903 Zhang, HJLT 2023, 667.

Wesen stets nutzer- und nicht datenzentriert: Als Betroffenenrecht ausgestaltet, erfasst es nur Personendaten und dies nur dann, wenn die Betroffene es initiiert.[904] Das Institut knüpft zwar bei den Daten an, setzt damit aber bloss Anreize, damit die Betroffene die Daten von einem Verantwortlichen erhält und damit ggf. zu einem anderen Anbieter wechseln kann. Gesenkt werden sollen damit die Wechselkosten für die Betroffene und ihr *Lock-In* soll verhindert werden. «Eingesperrt» sind in diesem Sinn also die User und nicht einzig deren Daten.

308 Damit kann ein userinduzierter und nicht bloss ein dateninduzierter *Lock-In* vorliegen. Das ist zu berücksichtigen, wenn ein solcher Lock-In-Effekt verhindert werden soll. Denn wenn Betroffene keine Datenübertragung initiieren, obwohl die Daten bei einem Anbieter gar nicht «eingesperrt» sind, bestehen die relevanten Hindernisse weiterhin und es liegt kein wirksamer Wettbewerb vor.[905] Die Betroffenen sind nach wie vor «eingesperrt». Die Gründe dafür liegen regelmässig in den starken Netzwerkeffekten. Dies wird in den einzelnen Sektoren zu vertiefen sein. Ob das Recht auf Datenportabilität auch Netzwerkeffekten entgegenzutreten vermag, lässt sich kaum für alle Sektoren und Konstellationen verallgemeinern.[906]

309 Es ist zu konstatieren, dass das Portabilitätsrecht konzeptionell auch auf die Verhinderung eines userinduzierten *Lock-In* zielte. In seiner Ausgestaltung dürfte das Portabilitätsrecht aber eher den *Lock-In* der Daten mindern, da oft Netzwerkeffekte dafür sorgen, dass Betroffene einen Wechsel nicht vollziehen (können).

c. Kein Lock-In der beobachteten Daten?

310 Damit drängt sich in Bezug auf den Anwendungsbereich des Instituts eine weitere Frage auf. Wenn in vielen Fällen bereits ein relevanter dateninduzierter Lock-In-Effekt und daraus resultierende hohe Wechselkosten durch die Daten angezweifelt werden, muss dies umso mehr für Nutzungsdaten («observed data») gelten, die ohne Wissen der betroffenen Person erhoben werden können, aber vom Recht auf Datenportabilität ebenfalls umfasst sind. Solche Da-

904 Von einem «human-centric approach» sprechend Copetti Cravo, EDPL 2022, 53; dies ebenfalls aufgreifend Troiano, 167.

905 Zhang, HJLT 2023, 667.

906 Fix, 82; für soziale Netzwerke ist das eher nicht der Fall, siehe Krämer, JCLE 2021, 274 f. Dies wurde auch bereits während des europäischen Gesetzgebungsverfahrens festgestellt, dazu Rz. 95.

ten dürften regelmässig nicht imstande sein, die Wechselkosten für die Betroffene zu erhöhen,[907] da diese gar nicht um sie weiss.

Zwar wird argumentiert, dass Nutzungsdaten für die Betroffene ebenfalls von Interesse sein können, also dass diese etwa nicht nur eine selbst erstellte Playlist, sondern auch das gesamte Archiv der angehörten Titel bei einem Musikstreaminganbieter portieren können will.[908] Dies mag zutreffen. Dabei lässt sich jedoch bezweifeln, ob eine Person Daten, die sie gar nicht kennt, als Hindernis für einen Wechsel wahrnimmt. Damit ist unklar, ob die Wechselkosten tatsächlich sinken. Mit Blick auf sämtliche Zielsetzungen des Instituts ist jedoch davon auszugehen, dass der Einbezug von Nutzungsdaten primär anderen Zielen dient. Diese Daten dürften vorwiegend zum Zweck einer allgemeinen Wettbewerbsförderung, namentlich zur Schaffung neuer Angebote, vom Recht auf Datenportabilität umfasst sein. 311

3. Markteintrittsschranke für Konkurrenten verringern

Wechselkosten können Konkurrenten vom Eintritt in einen Markt abhalten, sodass die Marktgegenseite (etwa Kunden, die eine bestimmte Leistung in Anspruch nehmen wollen) das Angebot weiterhin beim bisherigen Anbieter nachfragt.[909] Die Innovation wird so gehemmt und der Wettbewerb konzentriert sich, da etablierte Anbieter geschützt werden und bestehende Machtpositionen sich verfestigen.[910] Das Verhalten der Kunden als Nachfrager der Angebote wirkt folglich weniger disziplinierend auf den Wettbewerb ein, weshalb sich die Ressourcenallokation nicht zwingend am besten Angebot orientiert.[911] Dies kann zu einem Marktversagen führen.[912] Die Kunden beschränken ihre Nachfrage auf nur einen Anbieter, wodurch ein ganzer Markt «kippen» kann,[913] und dieser vom Zustand eines Wettbewerbs in die Dominanz eines quasi-monopolistischen Unternehmens übergeht (*market tipping*).[914] Ein Eintritt in den Markt ist dann nur noch möglich, wenn ein Anbieter zunächst die Hürde der 312

907 Weber/Thouvenin, 72, hierbei von einem kartellrechtlichen Ansatz sprechend.
908 Krämer, JCLE 2021, 272 f.; Krämer/Senellart/De Streel, 56.
909 Fix, 77; Krämer/Senellart/De Streel, 56.
910 Fix, 74; Krämer/Senellart/De Streel, 56.
911 Fix, 77.
912 Collovà et al., 8 f.
913 Martens, Economic Perspective, 12.
914 Steffen/Wieworra/Kroon, 19 m.w.N.

real existierenden Netzwerkeffekte überwinden kann – dies schadet dem Wettbewerb.[915]

313 Indem das Recht auf Datenportabilität die Wechselkosten zu senken versucht, soll es solche Eintrittsschranken für Konkurrenten abbauen.[916] Dies kann auch für *Multi-Homing* Angebote gelten, für welche das Portabilitätsrecht die Eintrittsschranken ebenfalls verringern kann.[917] Da das Portabilitätsrecht jedoch nicht an einzelne Sektoren gebunden ist, lassen sich kaum verallgemeinerbare Aussagen zu dessen Effektivität treffen.[918]

4. Allgemeine Wettbewerbsförderung

a. Fehlende Einschränkungen – Bug or Feature?

314 Das Recht auf Datenportabilität ist nicht beschränkt auf Fälle, in denen ein Lock-In-Effekt existiert oder existieren kann. Es ist auch kein Nachweis nötig, dass Markteintrittsschranken existieren oder verringert werden. Der alte Verantwortliche muss ferner weder eine besondere Marktstellung innehaben,[919]

915 Martens, Economic Perspective, 12 ; Yildiz, Rz. 575.

916 Landolt, 156; Lam/Liu, IJIO 2020, 8; i.E. wohl ebenso Métille, Nouveautés, 39; darauf hinweisend, dass dies ein erklärtes Ziel des Kartellrechts ist Weber/Thouvenin, 69 m.w.N.; weitergehend hierzu BSK KG-Reinert/Wälchli, Art. 4 Abs. 2 N 318 ff. Siehe allerdings auch Lam/Liu, IJIO 2020, 10, wonach das Recht auf Datenportabilität Markteintrittsschranken tatsächlich erhöhen und so den Wettbewerb verringern könne. In einem statischen Umfeld könnten die Konsumenten gleichwohl profitieren, da diese sich der Auswirkungen ihrer initialen Datenbekanntgabe auf die Wechselentscheidungen zum Zeitpunkt der Ausübung des Portabilitätsrechts voll bewusst seien und diese berücksichtigten, so dass sie von dem höheren Wert der Daten durch eine verbesserte Datenübertragbarkeit profitieren.

917 Engels, Internet Policy Review 2016, 5; Landolt, 156 m.w.N.; Schweitzer/Peitz, NJW 2018, 277; Steffen/Wieworra/Kroon, 72.

918 Konkret in Bezug auf die Effektivität der Netzwerkeffektebekämpfung Fix, 82.

919 Kratz, InTeR 2019, 27; Swire/Lagos, Maryland Law Review 2013, 338 f. und 351, die darin eine «deutliche Abkehr vom Wettbewerbsrecht» sehen; siehe auch Paal, ZWeR 2020, 224 f., der aufgrund der teleologischen Auslegung von Art. 20 DSGVO die Marktmacht als mögliche ungeschriebene Voraussetzung diskutiert, dann aber verwirft, da das Recht auf Datenportabilität auch datenschutzrechtliche Ziele verfolge; Buchner, WRP 2019, 1245, vertritt hingegen, dass das Datenschutzrecht eine wettbewerbliche Prägung aufweise, auch wenn dieses keine Regelung kenne, die sich ausdrücklich nur an marktbeherrschende Unternehmen richtet. Der Aspekt der Marktmacht sei im Datenschutzrecht jedoch von zentraler Bedeutung, insb. wenn es um die Frage der Freiwilligkeit einer Einwilligung gehe. Da das Recht auf Datenportabilität nach Art. 28 Abs. 2 lit. b DSG ebenfalls auf eine Einwilligung oder einen (freiwillig abgeschlossenen) Vertrag abstellt, könnte diese Argumentation übernommen werden.

noch gibt es eine Einschränkung auf gleichartige Angebote, obwohl eine solche mit Blick auf die eben besprochenen wettbewerbsrechtlichen Zielsetzungen angezeigt sein könnte.[920] Auch ein mandatierter Anspruch auf Datenportierung, etwa für Wettbewerber, ist nicht zwingend und liegt im Ermessen der Betroffenen.[921]

Es mag unter dem wettbewerbsrechtlichen Blickwinkel zunächst atypisch anmuten, dass die Ausübung des Rechts auf Datenportabilität stets möglich ist, sofern nur die Voraussetzungen von Art. 28 DSG vorliegen. Die Bestimmung bürdet zahlreichen Verantwortlichen die Pflicht zur Herausgabe von Daten auf, obwohl wettbewerbs- und besonders kartellrechtlich womöglich keine Notwendigkeit dafür bestünde.[922] Gerade kartellrechtliche Bestimmungen sind i.d.R. *ex post* anwendbar und knüpfen an bereits begangene Wettbewerbsbeschränkungen an.[923] Beim Recht auf Datenportabilität ist hingegen nicht einmal nötig, dass ein Wettbewerbsverhältnis vorliegt. 315

Dieser Umstand wurde in der europäischen Literatur verschiedentlich als «überschiessendes Wettbewerbsrecht» kritisiert.[924] So wurde moniert, dass KMU kaum je marktmächtig seien, aber relativ gesehen einen grösseren Verwaltungsaufwand tragen müssten, ohne vom Recht auf Datenportabilität wirklich zu profitieren.[925] Zudem würden kleinere Softwareunternehmen, die entsprechende Lösungen anbieten, weniger innovativ, da sich deren Tätigkeit nur noch auf *ein* gängiges Format ausrichten werde.[926] Ferner wurde beanstandet, dass bei gleichartigen Diensten die Datenportabilität im Fall eines Missbrauchs einer marktbeherrschenden Stellung zwar die beabsichtigte Wirkung entfalte, das Portabilitätsrecht aber auch marktverzerrend wirken könne, wenn kein wettbewerbswidriges Verhalten vorliege.[927] Auch ist die zu überwindende 316

920 Brüggemann, K&R 2018, 1; Fix, 86; ähnlich auch Hermonies, Rz. 81.

921 Bijok, 196.

922 In diese Richtung auch Swire/Lagos, Maryland Law Review 2013, 352; mit Blick auf kleinere Unternehmen, für die hohe Umsetzungskosten anfallen können Weber, ZWeR 2014, 179.

923 Heinemann, 226 f.; Magnin, Rz. 765 ff. Beide Autorinnen halten allerdings fest, dass das Kartellrecht nicht ausschliesslich *ex post* wirkt.

924 Hennemann, PinG 2017, 6; kritisch Kratz, InTeR 2019, 27 und 29 f.; Swire/Lagos, Maryland Law Review 2013, 352 f.; ausführlich auch etwa Fix, 86 ff. m.w.N., der jedoch überzeugend darlegt, dass das Fehlen einer Notwendigkeit von Schwellenwerten oder eines Marktversagens unumgänglich sei, um die vom Recht auf Datenportabilität beabsichtigten Wirkungen erreichen zu können.

925 Swire/Lagos, Maryland Law Review 2013, 352.

926 Swire/Lagos, Maryland Law Review 2013, 352; ähnlich auch Engels, Internet Policy Review 2016, 8.

927 Engels, Internet Policy Review 2016, 7.

Markteintrittsschranke für Anbieter gleichartiger Angebote ungleich höher als für solche mit andersartigen Angeboten. Für Letztere existiert u.U. keine Schranke, da die neue Verantwortliche mit ihrem andersartigen Angebot gar nicht mit dem alten Verantwortlichen konkurriert und nicht mit diesem im Wettbewerb steht. Gleichwohl können andersartige Anbieter von einer Datenübertragung profitieren.

317 Diese Punkte ändern nichts an den bereits diskutierten Zielen, die besonders hinsichtlich der Internetplattformen im Gesetzgebungsprozess eine Rolle gespielt haben mögen. Sie lassen sich historisch als Teil der (wettbewerbsrechtlichen) Zielsetzung des Portabilitätsrechts erklären, die besonders darauf abzielt, den Missbrauch von Marktmacht zu unterbinden.[928] Die darüberhinausgehende Anwendbarkeit vermag aber den bislang eher kartellrechtlich gelagerten Fokus in Richtung einer allgemeinen Wettbewerbsförderung zu verschieben. Damit handelt es sich beim Portabilitätsrecht um eine Form der *ex ante*-Regulierung.[929] Das Institut gelangt trotz seines Fokus auf die Internetplattformen bewusst sektorübergreifend zur Anwendung.[930] Auch die verfolgte Idee eines *Open Web* steht im Einklang mit einem solch breiten Verständnis.

318 Allerdings nahm der Gesetzgeber mit der Voraussetzung nach Art. 28 Abs. 1 lit. b DSG in gewissem Mass eine Einschränkung auf zumindest potenziell wettbewerbsrechtlich relevante Sachverhalte vor. Damit zusammenhängend spricht für eine wettbewerbsrechtliche Ausrichtung des Instituts, dass diese Voraussetzung behördliche Datenbearbeitungen in den meisten Fällen faktisch vom Recht auf Datenportabilität ausnimmt, da es auf Fälle beschränkt ist, in welchen die Betroffene Daten freiwillig bekanntgegeben hat.[931] Damit sind zumindest wettbewerbsrechtlich potenziell relevante Konstellationen betroffen, die im Umgang mit dem Staat i.d.R. gar nicht existieren. Dies deckt sich mit dem datenschutzrechtlichen Verständnis, das auf den durch die Datenwirtschaft entstandenen Ungleichgewichten gründet.

319 Vorteilhaft ist die sektorübergreifende Anwendbarkeit des Rechts auf Datenportabilität jedoch auf eine andere Weise: Grosse Anbieter, auf die das Institut

928 Kratz, InTeR 2019, 30.

929 Engels, Internet Policy Review 2016, 13; Reimsbach-Kounatze/Molnar, 8; differenzierend OECD, Mapping Initiatives, 11; Zufall/Zingg, 222.

930 Siehe ausdrücklich Jülicher/Röttgen/v. Schönfeld, ZD 2016, 361, wobei anders als unter der DSGVO in der Schweiz eine entsprechende Eingrenzung von Anfang an nicht vorgesehen war; dazu bereits Rz. 94 ff. und 101.

931 Dazu Rz. 195. Dass die Person freiwillig handelt, bedeutet aber noch nicht, dass ein Wettbewerb existiert, bspw. wenn Forschungsdaten einer betroffenen Person, für welche eine Einwilligung notwendig war, an ein anderes Forschungsteam portiert werden sollen.

abzielte,[932] könnten leichter in neue Sektoren vorstossen, wenn Portabilitätsrechte nur sektorspezifisch anwendbar wären. Ausgehend von ihrem ohnehin immensen Datensatz könnten sie einseitig das (sektorspezifische) Portabilitätsrecht ausüben und die erhaltenen Daten für den Eintritt in den neuen Sektor nutzen, was sich langfristig negativ auswirken könnte.[933] Dieser Ansatz würde zu Asymmetrien führen, die sich kaum rechtfertigen lassen.[934]

b. Fokus auf andersartige Anbieter

Gerade weil das Recht auf Datenportabilität nicht an wettbewerbsrechtliche Merkmale anknüpft, kann das Institut eine wettbewerbs- und innovationsfördernde Wirkung haben, wenn es sich bei den alten und neuen Verantwortlichen um jeweils andersartige Anbieter handelt. So ist denkbar, dass beide Anbieter von neuen Usern profitieren können, wodurch die Qualität und Vielseitigkeit des Angebots zunimmt.[935] Folglich können positive Netzwerkeffekte zwischen zwei Anbietern wirken, auch wenn diese nicht konkurrieren. 320

Bereits erwähnt wurde, dass das Recht auf Datenportabilität auf ein Internet bestehend aus *walled gardens* und damit auf stark veränderte tatsächliche Umstände reagiert.[936] Es zielt wesentlich auf Internetplattformen ab, bei welchen die ökonomischen Verhältnisse äusserst dynamisch sind und sich rascher ändern können als bei traditionellen Geschäftsmodellen.[937] Deren Datensätze stammen ausserdem regelmässig aus einer Vielzahl von Quellen in ganz unterschiedlichen Bereichen.[938] Eine Einschränkung in Form von Schwellenwerten o.ä. könnte die Wirksamkeit des Instituts schmälern, nicht zuletzt weil wettbewerbsrechtliche Verfahren langwierig sind.[939] Darin ist eine weitere Begründung zu sehen, dass keine sektorspezifische Regulierung erfolgt ist.[940] Das 321

---

932 Votum NR Glättli, AB 2019 N 1814; ausführlich dazu Rz. 97 ff.

933 Kerber, 453, insb. Fn. 25; weitergehend für den Bankensektor: Di Porto/Ghidini, IIC 2020; Reimsbach-Kounatze/Molnar, 10.

934 In diese Richtung gehend OECD, Mapping Initiatives, 13; dazu auch Landolt, 390 ff., der sich indes im Kontext der weiter verstandenen Datenzugangsrechte aus wettbewerbsrechtlicher Sicht für eine Regelung ausspricht, in welcher der Kreis der zugangsberechtigten Akteure gesetzlich begrenzt wird, wie dies etwa in der DV der Fall ist.

935 Engels, Internet Policy Review 2016, 9; Schweitzer/Peitz, NJW 2018, 274.

936 Kratz, InTeR 2019, 30; dazu Rz. 86 ff.

937 Engels, Internet Policy Review 2016, 13; Fix, 92; Schiess/Schaller, 125 ff.

938 Krämer/Schnurr/Broughton Micova, 82.

939 Fix, 92 f.; Weber/Thouvenin, 61 f., zudem auf weitere Möglichkeiten zur Streiterledigung hinweisend.

940 Mit Blick auf Märkte mit massgeblichen Netzwerkeffekten allgemein Brenner, EuR 2014, 690.

Recht auf Datenportabilität soll kein Rechtsinstitut sein, das der Logik des Kartellrechts folgt; vielmehr soll es den Wettbewerb fördern, indem es eingreift, bevor ein Marktversagen entsteht, etwa weil Markteintrittsschranken zu hoch sind oder Lock-In-Effekte zu stark wirken.[941] Das Ziel soll es m.a.W. sein, andersartigen Anbietern den Eintritt in neue Märkte und Nischenmärkte des Internets zu erleichtern, und dies nicht nur in ihrem Heimatmarkt.[942]

322 Daneben soll das Institut kleineren schweizerischen Unternehmen den Zugriff auf die Datenpools der grossen Unternehmen ermöglichen.[943] Dies gilt allerdings nur, wenn Betroffene dies ermöglichen; ein mandatierter Zugang ist für Wettbewerber nicht zwingend.[944] In diese Richtung wird auch für die EU-Regelung argumentiert, dass nicht primär ein marktmachtabhängiges Marktversagen beseitigt, sondern einem durch das Datenschutzrecht induzierten Marktversagen entgegengewirkt werden soll.[945]

323 Ohnehin stehen in mehrseitigen Märkten der Datenwirtschaft die Internetplattformen nicht nur mit Unternehmen in Wettbewerb, die das identische Geschäftsmodell verfolgen, sondern sie treffen auf einzelnen Marktseiten auf Wettbewerber mit einseitigen Geschäftsmodellen.[946] Solche Plattformen stehen regelmässig (nur) auf derjenigen Marktseite, auf der die Daten monetari-

941 Fix, 94.

942 So für Datenzugangsrechte im Allgemeinen Krämer/Schnurr/Broughton Micova, 76 ff.; in diese Richtung auch NomosKomm-Dix, Art. 20 DSGVO N 15, der zwar einräumt, dass die ursprüngliche Motivation gewesen sei, den Wechsel zwischen sozialen Netzwerken zu erleichtern. Eine solche Einschränkung auf eine «Ähnlichkeit» der Verantwortlichen lasse sich aber nicht aus dem Wortlaut ableiten, die Verantwortlichen müssten also nicht dem gleichen Wirtschaftszweig angehören; siehe auch Landolt, 185 f., der dabei von vertikalen Wettbewerbseffekten spricht und gerade im IoT-Kontext in jüngerer Zeit eine Fokusverlagerung auf den Einsatz der Datenportabilität zur Anbindung von Sekundärnutzung sehen will.

943 Für die EU Fix, 84. Damit könne auch erklärt werden, weshalb während des Gesetzgebungsverfahrens ein starker Fokus auf die sozialen Netzwerke existierte. Diese hätten während jener Zeit einen bedeutenden Anteil dieser Pools dargestellt. Dies dürfte in der Schweiz nicht anders sein. Ferner Votum NR Glättli, AB 2019 N 1813: «[Wir sprechen] darüber, wie wir durch die Schaffung eines neuen Marktes auch das Gleichgewicht der Macht verschieben können – nicht durch Verbote, sondern durch einen neuen Markt, liberal: weg von den riesigen Plattformen, weg von den riesigen Firmen und hin zu neuen, innovativen Unternehmen. Das können Genossenschaften sein, kleine Private, auch hier in der Schweiz, die die Möglichkeit haben, eine neue Datenwirtschaft zum Wohle aller zu schaffen».

944 Dazu bereits Rz. 314.

945 Schweitzer/Peitz, NJW 2018, 277; ähnlich Fix, 94.

946 Fast/Schnurr/Wohlfarth, 765.

siert werden, im Wettbewerb zu anderen Anbietern.[947] Auf der anderen Marktseite ist dies nicht notwendigerweise der Fall. Die angebotenen Dienste stellen aus Sicht der User nicht unbedingt Substitute dar (etwa Google als Suchanbieterin und Instagram als soziales Netzwerk).[948] Auch aus diesem Blickwinkel ist die gesetzgeberische Entscheidung, das Portabilitätsrecht nicht auf einzelne Anwendungsfälle zu beschränken, schlüssig.

c. Fokus auf ein Open Web

Mit seiner *ex ante*-Wirkung entfernt sich das Portabilitätsrecht vom Kartellrecht und rückt in die Nähe eines «Regulierungsrechts». Dieses soll nicht einzig den Wettbewerb fördern, sondern durch eine Grundversorgung ein bestimmtes Marktergebnis erreichen.[949] Die Grundversorgung strebt eine flächendeckende und eine bestimmte Mindestleistungen umfassende Versorgung mit Infrastrukturgütern und -dienstleistungen an.[950] Dies lässt sich auf das *World Wide Web* übertragen, in welchem die Idee eines *Open Web* ebenfalls eine bestimmte Funktionsweise anstrebt.[951] In diesem Sinn kann argumentiert werden, dass das Portabilitätsrecht nicht nur punktuell auf einzelne (andersartige) Anbieter abzielt und so allgemein wettbewerbsfördernd wirken soll. Das Institut zielt auf einer viel grundlegenderen Ebene auf die bereits genannte Offenheit und Interkonnektivität ab und soll in diesem Sinne wettbewerbsfördernd sein.[952] 324

Die einheitliche und breite Anwendbarkeit des Rechts auf Datenportabilität – ohne Schwellenwerte, Sektoren oder marktbeherrschende Stellung – zielt somit darauf ab, den Wettbewerb allgemein zu fördern.[953] Das Recht auf Datenportabilität soll *gerade* dann greifen können, wenn keine Marktmacht vorliegt oder die Daten (bloss) für einen andersartigen Dienst verwendet werden sol- 325

947 Fast/Schnurr/Wohlfarth, 765.

948 Fast/Schnurr/Wohlfarth, 765.

949 Heinemann, 225. Ob Daten als grundlegende Infrastruktur zu betrachten sind ist umstritten, kann vorliegend aber offenbleiben; ausführlich dazu am Beispiel der Internetplattformen Savary, 228 ff.; siehe auch Yan/He, JCLE 2022, 895.

950 Heinemann, 225.

951 Kratz, InTeR 2019, 28; siehe auch Fix, 84, der darin aber vor allem den Fokus im europäischen Gesetzgebungsverfahren auf die sozialen Netzwerke erklärt sieht. Dazu bereits Rz. 86 ff.

952 Europäisches Parlament, Gesamtkonzept Datenschutz, 7, insb. Fn. 2. In der Schweiz sind keine derart klaren Positionen aus dem Gesetzgebungsprozess zu finden. Die Beratung der SPK-N vom 23. Mai 2019 lässt aber immerhin ein gewisses Bewusstsein anklingen; für die EU Fix, 71; ferner Kratz, InTeR 2019, *passim*.

953 Fix, 87.

len,[954] und damit die grundlegende Funktionsweise des *World Wide Web* erhalten.

d. Datenschutz zur allgemeinen Wettbewerbsförderung

326 Ein weiterer Teilgehalt der allgemeinen Wettbewerbsförderung dürfte ein Wettbewerb um datenschutzfreundliche Technologien darstellen.[955] Für Betroffene kann bei der Auswahl eines Anbieters entscheidend sein, wie dieser mit den Daten umgeht.[956] Anbieter, die das Recht auf Datenportabilität gewähren (müssen), verfügen daher über einen Wettbewerbsvorteil gegenüber anderen Anbietern. Das Recht auf Datenportabilität zielt so auf datenschutzrechtliche Wettbewerbsvorteile einerseits und auf eine Berücksichtigung als «Standortfaktor» andererseits. Nicht nur zwischen den einzelnen Anbietern, sondern insb. auch im Wettbewerb der Schweiz mit der EU dürften hier wettbewerbliche Überlegungen eine Rolle gespielt haben.[957] Ferner dürften Souveränitätsüberlegungen massgeblich gewesen sein, also der Gedanke einer «Repatriierung» von Daten, die bei ausländischen Anbietern hinterlegt sind.[958] Anzufügen ist indes, dass die tatsächliche Wirkung solcher wettbewerblicher Elemente zumindest im Endkundenbereich angesichts des *privacy paradox* anzuzweifeln ist.[959] Gleichwohl dürften solche Wettbewerbsvorteile beabsichtigt gewesen sein.

954 Fix, 91; ebenso De Hert et al., CSLR 2018, 203; Kratz, InTeR 2019, 30; Landolt, 155 f.; ähnlich auch NomosKomm-Dix, Art. 20 DSGVO N 15.

955 Fix, 84.

956 Fix, 84 f.; Zanfir, IDPL 2012, 161, die davon ausgeht, dass Anbieter auch ausserhalb der EU anbieten werden müssen, damit das Vertrauen von Kunden gestärkt werde.

957 So etwa das Votum SR Bruderer, AB 2018 S 617, wonach «heute die EU-DSGVO mit ihren Richtlinien uns Schweizerinnen und Schweizern einen besseren Datenschutz bietet, auch gegenüber den grossen Konzernen aus den USA usw., als unser eigenes Gesetz. Dessen müssen wir uns einfach bewusst sein. Das muss uns auch zu denken geben».

958 Götzinger/Vasella, SZW 2021, 41.

959 Fix, 85. Das *privacy paradox* bezeichnet ein Phänomen, wonach die Privatsphäre bei Personen subjektiv einen hohen Stellenwert einnimmt, sie aber gleichzeitig bereit sind persönliche Daten für relative geringe Gegenwerte bekanntzugeben, siehe dazu Kokolakis, Computers & Security 2017, *passim*; siehe ebenfalls Kerber/Specht-Riemenschneider, 31, die die Probleme darin verorten, dass es den betroffenen Personen oft nicht klar sein dürfte welche Daten gesammelt und mit wem diese geteilt werden, dass Daten erhoben werden, ohne dass die betroffenen Personen informiert werden, dass Datenschutzerklärungen oft lange und unverständlich seien und dass betroffene Personen sich des Werts ihrer Personendaten oft nicht bewusst seien und diesen nicht richtig einschätzen könnten.

e. Innovationsförderung

Verschiedentlich wird die Förderung von Innovation als Zielsetzung genannt.[960] Folgt man der bereits mehrfach genannten Argumentation, wonach ein *Open Web* beabsichtigt war, so kann diese Zielsetzung durchaus begründet sein.[961] Dabei wird davon ausgegangen, dass sich die Entwicklung datengestützter Dienste fördern lässt, wenn diese von andersartigen Diensten gestützt auf das Recht auf Datenportabilität relevante Daten erhalten können, die für den Aufbau oder Betrieb ihres Dienstes hilfreich sind. Die neuen Verantwortlichen müssen selbst weniger in die Erfassung und Bearbeitung von Daten investieren, wenn sie Daten von anderen Anbietern als alte Verantwortliche erhalten können.[962] Auch hier findet sich der Gedanke des *Open Web* wieder.[963] Insofern ist von einer innovationsfördernden Zielsetzung auszugehen. 327

5. Datenpolitische Strategie und freier Datenfluss

Eine mögliche datenpolitische Zielsetzung mit Blick auf einen freien Datenfluss findet in der Schweiz wenig Beachtung. Namentlich existieren hierzulande, anders als in der EU,[964] keine Vorgaben für einen freien Datenverkehr,[965] und eine solche Zielsetzung wurde beim Erlass des DSG auch nicht ausdrücklich thematisiert.[966] Dies ist insofern nicht erstaunlich, als es für die Schweiz in Bezug auf den digitalen Binnenmarkt weniger Handelshemmnisse abzu- 328

960 OFK DSG-Bieri/Heymann/Odermatt, Art. 28 N 3; Cattaneo, 63; Epiney/Nüesch/Rovelli, 178. Auch die Beratung der SPK-N vom 23. Mai 2019 lässt darauf schliessen, dass die Räte eine solche Zielsetzung vor Augen hatten. Differenzierend und auch bezugnehmend auf Interoperabilität Swire/Lagos, Maryland Law Review 2013, 357 f.; ebenso Palfrey/Gasser, 111 ff.

961 Kratz, InTeR 2019, 30.

962 Engels, Internet Policy Review 2016, 8.

963 Siehe auch Fix, 89.

964 Siehe für die EU die VO 2018/1807, die den freien Verkehr von Sachdaten innerhalb der EU gewährleisten soll (Art. 1 VO 2018/1807). Sie ermöglicht es, dass Sachdaten innerhalb Europas frei übertragen werden dürfen. Mit der VO 2018/1807 sollen auf dem Wege der regulierten Selbstregulierung, Verhaltensregeln gefördert werden, die zu einer wettbewerbsfähigen Datenwirtschaft auf der Grundlage der Grundsätze der Transparenz und der Interoperabilität und unter angemessener Berücksichtigung offener Standards beitragen. Siehe dazu weitergehend Thouvenin/Weber/Früh, 146.

965 Das EJPD lehnte eine Prüfung des Regelungsbedarfs für das Schweizer Recht 2019 ab mit der Begründung, dass dies angesichts der gewählten Selbstregulierungslösung der EU nicht sinnvoll erschiene, siehe UVEK, 22.

966 Siehe indes George, Prinzipien, 74, wonach das DSG einen Beitritt zur Konvention 108+ ermöglichen soll, die ihren Vertragsstaaten Beschränkungen des Datenverkehrs untersagt.

bauen gilt als für die EU.[967] Der freie Datenfluss wird in der EU jedoch nicht nur grenzüberschreitend, sondern auch systemübergreifend verstanden.[968] Die EU misst ihm ein hohes Gewicht bei. Bereits Erw.G 2 DSGVO hält fest, dass die Verordnung zur Vollendung einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen beitragen soll. Erw.G 3 DSGVO hebt sodann die Dichotomie der Zwecke der DSGVO[969] hervor: Den Schutz der Grundrechte und Grundfreiheiten einerseits sowie die Gewährleistung des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten andererseits. Dies hält auch Art. 1 Abs. 1 DSGVO ausdrücklich fest. Das Recht auf Datenportabilität wird in der EU also als ein Teilstück des Aufbaus einer paneuropäischen Datenstrategie betrachtet, zu welcher der freie Datenverkehr resp. Datenfluss gehört.[970]

329 In der Schweizer Literatur und in den Materialien finden sich zu diesem Thema nur wenige Ausführungen.[971] Der Zweckartikel des DSG enthält jeden-

967 So gibt es in der Schweiz – soweit ersichtlich – keine subnationalen Vorgaben etwa in Bezug auf den Standort von Daten. In der EU wurden zudem eine uneinheitliche Umsetzung von Urheberrechtsvorschriften und eine mangelnde Klarheit der Datennutzungsrechte bemängelt, siehe Europäische Kommission, Strategie digitaler Binnenmarkt, 16.

968 Siehe die Hinweise auf das Gesetzgebungsverfahren zur Datenportabilität bei Fix, 71; ferner Li, 47; ähnlich wohl auch Europäische Kommission, Aufbau Datenwirtschaft, 4, 9 ff., und insb. 13; mit dem Hinweis, dass in einer «florierenden datengesteuerten Wirtschaft» der Datenfluss über Sektoren, Sprachen und Grenzen hinweg durch keine unangemessenen Beschränkungen behindert wird Europäische Kommission, Datengesteuerte Wirtschaft, 6. Dieses nicht Verständnis spiegelt auch die VO 2018/1807 wider, welche die Übertragung zwischen Diensteanbietern generell regelt resp. zumindest zur Selbstregulierung mahnt.

969 Im Wortlaut wird auf die Richtlinie 95/46/EG verwiesen. Art. 94 Abs. 2 DSGVO stellt jedoch klar, dass solche Verweise als Verweise auf die DSGVO gelten.

970 Siehe Europäische Kommission, Aufbau Datenwirtschaft, 17 und 19; Li, 42; a.A. Louven, K&R 2018, 232, nach welchem aus Art. 20 DSGVO keine Zielsetzung der Förderung eines einheitlichen Datenmarktes abzuleiten ist.

971 Bezugnehmend auf das Recht auf Datenportabilität Expertengruppe Zukunft, 106, nach welchen ein geregelter Markt für Personendaten entstehen könnte; Landolt, 357 f., der Ansätze einer auf die Förderung des freien Verkehrs abzielenden Sichtweise auf das Datenschutzrecht auch im DSG sieht. Er fordert den Gesetzgeber auf, eine solche «dualistische Sichtweise» künftig besser abzubilden. Immerhin in Bezug auf ein Zugangsrecht, das *de lege ferenda* eingeführt werden könnte Schmid/Schmidt/Zech, sic! 2018, 633, nach welchen ein solches Recht dem freien Datenfluss dienen würde; ferner Swiss Data Alliance, Whitepaper Datenraum, 24, welche im Kontext von Datenräumen einen freien Datenfluss fordern.

falls keine entsprechende Zielsetzung.[972] Auch die Botschaft zum DSG äussert sich dazu nur am Rand, etwa wenn sie die Open-Government-Data-Strategie des Bundes erwähnt, welche die freie (Wieder-)Verwendbarkeit von Behördendaten ermöglichen soll.[973]

Zunehmend kommen in der Schweiz jedoch Diskussionen auf, ob, von wem und für welche Zwecke vorhandene Daten genutzt werden dürfen. Beispielhaft dafür ist ein Rahmengesetz für die Sekundärnutzung von Daten, welches der Bund aktuell ausarbeitet. Es dürfte in «strategisch relevanten Bereichen» Regelungen zum Datenfluss vorsehen.[974] Der Bundesrat hat die Vorlage in seinen Zielen für das Jahr 2026 als Schwerpunkt aufgeführt und die Vernehmlassungsvorlage für Ende 2026 angekündigt.[975] Mangels anderweitiger Regelungen ist das Datenschutzrecht aber bislang nach wie vor das «faktische Kernregularium» der Datenwirtschaft, das im Bereich der Personendaten dem Datenfluss Grenzen zieht.[976] 330

Entsprechend ist das Portabilitätsrecht bezeichnend für eine Entwicklung weg von einem reinen Daten*schutz*recht, hin zu einem ganzheitlichen Datenrecht. Diese Entwicklung geht mit datenpolitischen Diskussionen einher, die sich nicht mehr ausschliesslich auf persönlichkeitsrechtliche Aspekte von Daten beschränken lassen. Sie lassen sich auch nicht einzig mit der Kommerzialisierung der Persönlichkeit erklären.[977] Die Diskussionen sind vielmehr auf einer grundlegenderen datenpolitischen Ebene anzusiedeln und gehen in der Schweiz auf die Strategie «Digitale Schweiz» zurück.[978] Sie hält fest, dass es 331

---

972 OK-DSG-Husi-Stämpfli, Art. 1 N 7, die festhält, dass das Datenschutzrecht «Persönlichkeitsschutz *avant tout*» sei und nicht den Schutz der Wirtschaftsteilnehmenden, der öffentlichen Sicherheit oder anderer Interessen bezwecke. Das Datenschutzrecht ist indes nach hier vertretener Ansicht als Teil einer zunehmenden Regulierung im Bereich Daten, als ein Datenrecht als Ganzes, zu betrachten. Insofern können solche Überlegungen, gerade beim Recht auf Datenportabilität durchaus einbezogen werden.

973 Botschaft DSG 2017, 6957 m.H.a. Bundesrat, Open-Government-Data-Strategie, 3493 ff.

974 Motion WBK-S 22.3890.

975 Bundesrat, Medienmitteilung vom 8. September 2025, 3; Bundesrat, Medienmitteilung vom 8. Dezember 2023.

976 Landolt, 339 ff. m.w.N.

977 Dies zeigt sich etwa daran, dass die Diskussionen – vorwiegend in der EU, aber mit etwas Verzögerung auch in der Schweiz – zunehmend auch zu Sachdaten geführt werden.

978 Dieser erschien zunächst als Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz im März 2012 und anschliessend als Strategie «Digitale Schweiz» in jeweils aktualisierter Form am 20. März 2016, am 5. September 2018, am 11. September 2020, am 16. Dezember 2022, am 8. Dezember 2023 und am 13. Dezember 2024. Die Strategie erscheint seit 2022 stark gekürzt und beschränkt sich auf eine kurze Skizzierung von einigen «Wirkungsbereichen» und «Fokusthemen».

neue und kooperative Formen der Datennutzung brauche, bei der die Einwohner und die Unternehmen eine grösstmögliche Kontrolle über ihre Daten ausüben können.[979] Die Schweizer Rechtsordnung müsse, so die Strategie, für die Datenwirtschaft optimal ausgestaltet sein und nur mittels zeitgemässer und kohärenter Rechtsgrundlagen könne das Potenzial der Daten ausgeschöpft werden.[980] Es sei deshalb eine international abgestimmte Datenpolitik zu entwickeln, «die unter anderem Fragen der Datensouveränität, des Zugangs zu Daten der Behörden, des internationalen Datenverkehrs, der Wettbewerbsordnung, des geistigen Eigentums, des Datenschutzes und des Umgangs mit Lokalisierungsvorschriften umfasst».[981] Die Schweiz müsse also über zeitgemässe und kohärente Rechtsgrundlagen bezüglich der Rechte an Daten und ihrer Nutzung verfügen.[982] Auch der Bundesrat hatte seine Überlegungen zur Datenportabilität in diese (übergeordnete) Strategie eingebettet.[983]

332 Auf dem Weg zu einer Datenpolitik des Bundes veranlasste er bereits 2017, dass das EJPD die Rechtslage für «eine Weiterverwendung von Personendaten, Sachdaten und anonymisierten Daten» analysiert.[984] Daraus gingen die Gutachten zur Datenportabilität von Weber/Thouvenin und des SIR hervor, auf welche in den Strategien «Digitale Schweiz» 2018 und 2020 verwiesen wurde.[985] Ein weiterer Auftrag zur Prüfung von sektoriellen Portabilitätsrechten erteilte der Bundesrat dem EJPD 2018.[986] Dieser wurde aber mit der Einführung des Portabilitätsrechts im DSG obsolet und folglich nicht mehr weiterverfolgt.[987]

333 Selbst in der Botschaft zum DSG verband der Bundesrat das (von ihm abgelehnte) Portabilitätsrecht ausdrücklich mit datenpolitischen Überlegungen. Er wollte «[i]m Rahmen der Datenpolitik […] verschiedene juristische Fragen im Zusammenhang mit der Wiederverwendung digitaler Daten» klären lassen, u.a. ob ein Portabilitätsrecht für Personendaten eingeführt werden sollte.[988]

---

979 Bundesrat, Strategie «Digitale Schweiz» 2020, 7620.
980 Bundesrat, Strategie «Digitale Schweiz» 2020, 7621.
981 Bundesrat, Strategie «Digitale Schweiz» 2020, 7621.
982 Bundesrat, Strategie «Digitale Schweiz» 2020, 7621.
983 Siehe etwa BJ, Erläuternder Bericht VE-DSG, 22, wonach die Frage nach der Einführung eines Rechts auf Datenportabilität im Rahmen der Strategie «Digitale Schweiz» weiter geprüft werden sollte; im Wortlaut identisch Botschaft DSG 2017, 6985.
984 BAKOM, Medienmitteilung vom 22. März 2017.
985 Bundesrat, Strategie «Digitale Schweiz» 2018, 5980; Bundesrat, Strategie «Digitale Schweiz» 2020, 7621 m.H.a. Weber/Thouvenin, *passim*; SIR, *passim*.
986 Siehe dazu BAKOM, Medienmitteilung vom 9. Mai 2018.
987 Dazu Rz. 101.
988 Botschaft DSG 2017, 6956.

Dabei verwies er ebenfalls auf die Strategie «Digitale Schweiz» mit welcher eine kohärente und zukunftsorientierte Datenpolitik entwickelt werden sollte.[989] Gleichzeitig stellte er klar, dass «die Kontrolle über diese Daten erhalten bleiben» soll.[990] Damit brachte der Bundesrat Handlungsbedarf zum Ausdruck, allerdings seiner Ansicht nach einstweilen eher *ausserhalb* des DSG.[991] Er wollte in der Folge die Einführung sektorspezifischer Datenportabilitätsrechte prüfen,[992] erachtete eine Regelung für Sachdaten anderenorts für nicht notwendig[993] und wollte im Wesentlichen die Erfahrungen in der EU abwarten und die Frage der Portabilitätsrechte im Rahmen der Strategie «Digitale Schweiz» weiter prüfen[994].

Der Bundesrat setzte sich also intensiv mit der Thematik auseinander, wurde jedoch auf halbem Weg von den Räten überholt.[995] Das Vorgehen des Bundesrats dürfte auf die holistische Digitalstrategie der EU zurückgehen, die auch – aber eben nicht nur – mit der DSGVO den digitalen Wandel regulatorisch abbilden wollte. Entsprechend sah der Bundesrat das Recht auf Datenportabilität ebenfalls als ein Instrument der Schweizer Datenpolitik schlechthin[996] und nicht bloss als ein solches mit einer daten*schutz*rechtlichen Relevanz. Er schien das Recht auf Datenportabilität ebenfalls – und anders als noch im Bericht Social Media[997] – holistisch zu denken. Dies scheint im Übrigen nach Erlass der nun verankerten Portabilitätsregelung weiterhin zu gelten. In einem 2022 erschienenen Bericht wird das Datenportabilitätsrecht im DSG als eine eigenständige wettbewerbliche und plattformregulierende Massnahme dargestellt. Trotz seiner Verankerung in Art. 28 DSG wird es dabei getrennt von der damaligen Revision des DSG beleuchtet.[998] 334

Ähnliche Ansätze liessen sich während der Gesetzesrevision des DSG bei den Räten erkennen. Diese entschieden sich zwar bekanntlich für eine Verankerung im DSG. Doch Ständerätin Bruderer stellte bereits zu Beginn der Beratungen zur DSG-Revision fest: «[Es braucht eine] Auseinandersetzung mit dem Anpassungsbedarf aufgrund der datenpolitischen Schutzbestimmungen der 335

989 Botschaft DSG 2017, 6956.
990 Botschaft DSG 2017, 6956.
991 In derselben Botschaft stand der Bundesrat einem datenschutzrechtlichen Portabilitätsrecht wie dargelegt kritisch gegenüber.
992 Siehe BAKOM, Medienmitteilung vom 9. Mai 2018.
993 UVEK, 22.
994 Botschaft DSG 2017, 6985.
995 Dazu Rz. 101.
996 Siehe BAKOM, Medienmitteilung vom 9. Mai 2018.
997 Dazu Rz. 97.
998 Bundesrat, Bericht Handlungsfelder, 37 f.

EU-DSGVO. Ich nenne es bewusst Datenpolitik. Ich möchte damit auch eine Brücke zur Strategie Digitale Schweiz schlagen. Die Erwartungen haben sich in vielerlei Hinsicht stark verändert: punkto Umgang mit Daten, punkto Schutz der Daten sowie Transparenz und punkto möglicher Mitsprache bei der Verwendung von personenspezifischen Daten.»[999] Dabei hob sie das Recht auf Datenportabilität ausdrücklich hervor. Es gehe bei der Revision des DSG «nicht einfach nur um den Datenschutz, sondern auch um weitere datenpolitische Fragen wie die Portabilität usw., mit denen wir uns dann [...] auseinanderzusetzen haben».[1000]

336 Insgesamt ist festzuhalten, dass das Recht auf Datenportabilität ein datenpolitisches Instrument darstellen sollte, das nicht von den (laufenden) datenpolitischen Entwicklungen in der Schweiz und Europa abstrahiert werden kann. Das Institut ist auf grundsätzliche datenpolitische Überlegungen zurückzuführen und ein auf einen freien Datenfluss im Zeitalter der Datenwirtschaft ausgerichtetes Rechtsinstitut, das zwar – wie nun geschehen – datenschutzrechtlich ausgestaltet sein kann, aber nicht notwendigerweise in einer engen Beziehung zum DSG stehen muss. Trotz dieser Erkenntnis ist die Regelung nach Art. 28 DSG weiterhin (vorwiegend) datenschutzrechtlich zu verstehen. Zu folgern ist jedoch, dass die Ausgestaltung des nunmehr geschaffenen Portabilitätsrechts nicht zwingend im datenschutzrechtlichen Gewand hätte erfolgen müssen.[1001] Vielmehr ist das Portabilitätsrecht *ein* Puzzlestück in der Digitalstrategie der Schweiz (und der EU) und daher in diesem grösseren Kontext zu verstehen.[1002]

6. Erkenntnisse

337 Das Recht auf Datenportabilität verfolgt mehrere wettbewerbsrechtliche Ziele, wobei die einzelnen Zielsetzungen verwoben sind und sich teilweise nicht trennscharf unterscheiden lassen. Besonders anspruchsvoll ist es, die Ziele –

999 Votum SR Bruderer, AB 2018 S 617.

1000 Votum SR Bruderer, AB 2018 S 617.

1001 So auch KRATZ, InTeR 2019, 30. Dazu bereits Rz. 243 und 373.

1002 Ähnlich auch LAUX, digma 2019, 166 und insb. 170, wonach die betroffene Person «Instrumente an die Hand bekommt, selber in die Datenwirtschaft einzugreifen». Siehe ferner Votum SR Bruderer, AB 2018 S 617; für die insofern nicht grundlegend andere Situation unter der DSGVO siehe BeckOK DSR-VON LEWINSKI, Art. 20 DSGVO N 15, der festhält, dass es um einen grösseren Kontext gehe und um die Frage der «Kompatibilität in und Interoperabilität von logischen Räumen». Es sei nicht bloss die Frage eines kommenden Datenmarktrechts, sondern «eine der informationellen Verfasstheit und Verfassung von Staat und Gesellschaft überhaupt».

dem breiten Anwendungsbereich entsprechend – ohne einen konkreten Anwendungsfall vor Augen zu analysieren und zu unterscheiden. Dennoch scheint bereits an dieser Stelle klar, dass trotz des weiten Anwendungsbereichs gerade die als «Mikroziele» verstandenen Zielsetzungen einer Senkung der Wechselkosten, Verhinderung eines Lock-In-Effekts und Verringerung der Markteintrittsschranken nur auf einzelne Sektoren zutreffen und sich nicht auf sämtliche möglichen Anwendungsbereiche übertragen lassen. Doch selbst in Bezug auf die im Gesetzgebungsprozess präsenten sozialen Netzwerke scheint die Verhinderung von Lock-In-Effekten, Wechselkosten und Markteintrittsschranken nicht immer zu passen. Gerade bei den sozialen Netzwerken wird in der Literatur jedenfalls bezweifelt, dass die gewünschten Effekte überhaupt erreichbar sind. Postuliert wird, dass vielmehr Netzwerkeffekte dafür verantwortlich seien, dass die Betroffenen nicht den Anbieter wechselten.[1003]

Von starken Netzwerkeffekten ist aufgrund der sozialen Komponente *gerade* bei sozialen Netzwerken auszugehen. Bei anderen Anwendungsfällen scheinen hingegen die kartellrechtlich gelagerten Ziele erreichbar, weil die Netzwerkeffekte geringer ausfallen und ein Wechsel eher möglich ist.[1004] Daneben trifft aber zu, dass sich aus dem Recht auf Datenportabilität keine Ansprüche für Wettbewerber, etwa entgegen dem Willen von Betroffenen, ableiten lässt. Das macht die wettbewerbsrechtliche Zielsetzung abhängig von der Ausübung des Rechts durch die betroffenen Personen. Dem Institut an sich kann damit nur begrenzt wettbewerbsrechtliche Wirkung zukommen. 338

Daraus lässt sich folgern, dass das Recht auf Datenportabilität in seiner ganzen Breite vorwiegend den generellen «Makrozielen» einer *ex ante*-Regulierung wie der allgemeinen Wettbewerbsförderung, Innovationsförderung und einem freien Datenfluss zuträglich sein sollte. Die kartellrechtlich gelagerten Mikroziele verfolgt es hingegen weniger. Denn namentlich andersartige Dienste können (als neue Verantwortliche) vom Recht auf Datenportabilität profitieren. Dies kann auch ökonomisch einen grösseren Mehrwert bieten als ein Wechsel unter gleichartigen Diensten, da beide andersartigen Verantwortlichen von neuen Usern profitieren können und die Qualität und Vielseitigkeit des Angebots potenziell zunimmt.[1005] Alte und neue Verantwortliche müssen dabei nicht unbedingt im Wettbewerb zueinander stehen, es sind keine Lock-In-Effekte zu verhindern und zumindest weniger Wechselkosten zu senken 339

1003 Fix, 79 f.
1004 Dazu § 4. Ausführlich zum Anwendungsfall soziale Netzwerke Rz. 404 ff.
1005 Engels, Internet Policy Review 2016, 8; Kratz, InTeR 2019, 29.

oder Markeintrittsschranken zu verringern. In diesen Makrozielen liegt nach hier vertretener Ansicht die primäre wettbewerbsrechtliche Zielsetzung, da nur sie geeignet sind, im gesamten Spektrum der Anwendungsfälle des Rechts auf Datenportabilität eine Wirkung zu entfalten.

340 Das Recht auf Datenportabilität beabsichtigt damit wettbewerbliche und innovationsfördernde Ziele und soll lediglich in einem engeren Bereich die Grundlagen für eine Erreichung spezifischerer Ziele schaffen und eben etwa Lock-In-Effekte verhindern und Wechselkosten reduzieren. Die Datenwirtschaft – in ihrer vorwiegenden Erscheinungsform im *World Wide Web* – soll so von proprietären Silos befreit werden, zwischen welchen die Betroffenen frei und ungehindert von wettbewerbsverzerrenden Hindernissen wechseln können. Für sie sollen möglichst wenig Hürden existieren, sodass sie sich für das für sie «beste» Angebot entscheiden können. Dies zielt auf einen funktionierenden Wettbewerb ab und stellt damit eine wettbewerbsrechtliche Zielsetzung des Instituts dar.[1006] Dieses Ziel deckt sich mit der Zielsetzung von Offenheit und Interkonnektivität des *Open Web*. Auch als diesen Zielen dienendes Institut ist das Portabilitätsrecht zu verstehen.

341 Die allgemeine Wettbewerbsförderung und die Förderung eines freien Datenflusses sind sodann zwei Zielsetzungen, die eng miteinander verwoben sind. Erstere soll ihrerseits auch einen freien Datenfluss bewirken.[1007] Diese Ziele sind als Ausdruck eines Paradigmenwechsels vom reinen Datenschutzrecht zu einem Datenrecht zu sehen, der mit dem Portabilitätsrecht angestossen wurde.

1006 Für die Schweiz im Besonderen SHK DSG-Baeriswyl, Art. 28 N 3; damit freilich begründend, weshalb auf eine entsprechende gesetzliche Regelung gerade zu verzichten sei Botschaft DSG 2017, 6984; so bereits BJ, Erläuternder Bericht VE-DSG, 22; BJ, Erläuternder Bericht DSV, 44; Götzinger/Vasella, SZW 2021, 41; Steiner, 125; Rosenthal, Jusletter 2020, Rz. 130, der jedoch von «Konsumentenschutz» spricht; noch vor der Revision des DSG aber mit Bezug auf die Entstehungsgeschichte unter der DSGVO und Mischformen gegenüber zumindest offen Thouvenin/Weber/Früh, 171 ff.; Toren, Jusletter IT 2019, Rz. 25 f.; Mischformen gegenüber offen zudem Weber/Thouvenin, 69 ff.; a.A. jedoch Laux, digma 2019, 170, der mit der wettbewerbsrechtlichen Wirkung insb. für Betroffene einverstanden scheint, i.E. aber nicht von wettbewerbspolitischen oder verbraucherschützerischen Zielen ausgeht.

1007 Ähnlich auch Fix, 100.

C. Konsumentenschutzrechtliche Ziele

Anzusprechen sind schliesslich mögliche konsumentenschutzrechtliche Ziele, die in der Literatur teilweise Erwähnung finden.[1008] Das DSG nimmt denn auch bereits im Ingress auf Art. 97 Abs. 1 BV Bezug, wonach dem Bund die Kompetenz zukommt, Massnahmen zum Schutz der Konsumentinnen zu treffen. Damit unterscheidet sich die verfassungsrechtliche Grundlage vom aDSG, welches (nur) auf die Art. 95, 122 und 173 Abs. 2 BV verwies. Allerdings führte schon der E-DSG die Bestimmung im Ingress auf, sah dabei jedoch kein Recht auf Datenportabilität vor. Gleichwohl enthielt bereits der E-DSG «einige Bestimmungen, die insbesondere die Transparenz der Datenbearbeitung, die Kontrolle durch die betroffenen Personen und das Aufsichtssystem des Beauftragten verbessern».[1009] Dadurch, so der Bundesrat, seien die Konsumentinnen besser geschützt.[1010] Diese Argumentation lässt sich auf das nun im DSG verankerten Recht auf Datenportabilität übertragen.[1011] Der Ingress zeigt auf, dass das DSG nicht (mehr) nur datenschutzrechtliche Zwecke i.e.S. verfolgt, sondern auch konsumentenschutzrechtliche Ziele. Dies dürfte u.a. daran liegen, dass in der Datenwirtschaft heute konsumentenschutzrechtliche Anliegen auf solche des Datenschutzes treffen.[1012] Entsprechend treffen viele Zielsetzungen des Datenschutzes – etwa der Schutz der liberalen Rechts- und Wirtschaftsordnung und die Selbstbestimmung des Einzelnen – auch auf den Konsumentenschutz zu.[1013] 342

Folglich stärkt das Recht auf Datenportabilität als Individualrecht die Betroffenen in ihrer Rolle als Konsumentinnen.[1014] Es erlaubt ihnen, über einen gewissen Zeitraum eine umfangreiche Sammlung von Angaben über sich selbst anzuhäufen und diese, wenn sie möchten, bspw. in einem PIMS zu verwalten und nach eigenem Gutdünken im Wirtschaftsverkehr einzusetzen.[1015] Dadurch, dass die Konsumentin auf Augenhöhe mit anderen Akteurinnen gebracht wird, 343

1008 PC LPD-Béguin, Art. 28 N 6; Rosenthal, Jusletter 2020, Rz. 130; Widmer/Egli, Rz. 18 f.; für die EU auch Fix, 102 m.w.N., der allerdings eine solche Zielsetzung selbst ablehnt.

1009 Botschaft DSG 2017, 7010.

1010 Botschaft DSG 2017, 7010.

1011 Siehe auch SHK DSG-Baeriswyl, Vorbemerkungen zu Art. 25–29 N 4, der sich ebenfalls auf den Ingress bezieht.

1012 Baeriswyl, Konsumentenschutz, 406; Hettich, 21.

1013 Baeriswyl, Konsumentenschutz, 406.

1014 Baeriswyl, Konsumentenschutz, 410; Jotterand, sic! 2025, 443; für die DSGVO Hennemann, PinG 2017, 6; Krause, PinG 2018, 239; Spiecker genannt Döhmann, 192.

1015 Siehe Laux, digma 2019, 166, der indes m.E. unzutreffenderweise von einer «vollständigen» Sammlung spricht; ähnlich Rosenthal, Jusletter 2020, Rz. 130.

sollen privatautonome Entscheide und damit eine funktionierende Wettbewerbswirtschaft ermöglicht werden.[1016] Allerdings ist nicht zwingend, dass die Betroffene in der Rolle einer Konsumentin auftreten muss. Die Geltendmachung des Portabilitätsrechts hängt jedenfalls nicht von einer solchen Eigenschaft ab.[1017]

344 Damit ist insgesamt von einer konsumentenschutzrechtlichen Zielsetzung des Rechts auf Datenportabilität auszugehen. Diese steht aber nicht im Vordergrund und wird inhaltlich von den wettbewerbsrechtlichen Zielen bereits abgedeckt.

1016 WIDMER/EGLI, Rz. 19.

1017 FIX, 103, auch darauf hinweisend, dass eine Betroffene auch in der Eigenschaft als Unternehmerin von ihrem Portabilitätsrecht Gebrauch machen kann.

IV. Abgrenzungen

Nachdem die Ziele des Portabilitätsrechts dargelegt wurden, sollen nachfolgend weitere, ähnlich ausgestaltete oder eine ähnliche Zielsetzung verfolgende Institute kurz vom Portabilitätsrecht abgegrenzt werden. 345

A. Zum datenschutzrechtlichen Auskunftsrecht

1. Unterschiede in der Zielsetzung

Im Zusammenhang mit der (datenschutzrechtlichen) Zielsetzung des Portabilitätsrechts wird oft das Auskunftsrecht herangezogen. Dieses wird als ein zentraler Bestandteil des Rechts auf informationelle Selbstbestimmung betrachtet[1018] und stellt «eine unentbehrliche Voraussetzung für die Verwirklichung des Schutzes der Privatsphäre» dar.[1019] Als Ausfluss dieser informationellen Selbstbestimmung werden der Betroffenen gewisse Einwilligungs-, Widerspruchs- und Überprüfungsmöglichkeiten gegenüber staatlichen und privaten Verantwortlichen zuerkannt; dem Auskunftsrecht wird dabei eine grundlegende Bedeutung zugemessen.[1020] Daraus folgt, dass sich die informationelle Selbstbestimmung nicht nur durch Abwehrrechte, sondern auch durch Gewährleistungs- und punktuelle Leistungsansprüche charakterisiert.[1021] 346

Insoweit ähneln sich das Auskunfts- und das Portabilitätsrecht. Mit dem Portabilitätsrecht werden der betroffenen Person ebenfalls datenschutzrechtliche Steuerungsbefugnisse zuteil, ihr wird ein positiver Rechtsanspruch und nicht bloss ein datenschutzrechtlicher Abwehranspruch vermittelt.[1022] Gewisse Autoren wollen den normativen Kern eines Rechts auf Datenportabilität denn auch aus dem datenschutzrechtlichen Auskunftsrecht ableiten.[1023] Es handle 347

1018 SHK DSG-Pärli/Flück, Art. 25 N 6; SGK BV-Schweizer/Striegel, Art. 13 N 101.

1019 BGE 144 I 126 E. 8.3.7; BGE 138 I 6 E. 7.5.2.

1020 SGK BV-Schweizer/Striegel, Art. 13 N 80.

1021 SGK BV-Schweizer/Striegel, Art. 13 N 80; von einem «positiven Element» in Abgrenzung zu den Abwehrrechten sprechend Jülicher/Röttgen/v. Schönfeld, ZD 2016, 361; zur Abgrenzung Rz. 354 ff.

1022 Weber/Thouvenin, 68; ähnlich auch Jülicher/Röttgen/v. Schönfeld, ZD 2016, 361.

1023 Noch vor der Revision des aDSG etwa Thouvenin/Weber/Früh, 12 f., 173 und 175; ähnlich wohl Charlet, 573; Landolt, 152; SGK BV-Schweizer/Striegel, Art. 13 N 109.

sich um eine «vergleichsweise geringfügige» Weiterentwicklung ebendieses Instituts.[1024] Nach dieser Ansicht hätte das Recht auf Datenportabilität also gesetzestechnisch als Weiterentwicklung des bereits bestehenden Auskunftsrechts gestützt auf das Recht auf informationelle Selbstbestimmung ausgestaltet werden können und zumindest im Grundsatz deckungsgleiche Ziele verfolgt. Dies war zu einem frühen Zeitpunkt im Gesetzgebungsprozess erwogen worden, wurde aber schliesslich verworfen.[1025]

348 Trotz gewisser Gemeinsamkeiten stellt das Recht auf Datenportabilität allerdings m.E. gerade bei teleologischer Betrachtung keine Weiterentwicklung oder Erweiterung des Auskunftsrechts dar und ist von diesem getrennt zu betrachten.[1026] Zwar dienen beide Institute der Verwirklichung des Persönlichkeitsschutzes. Die Stossrichtung ist jedoch verschieden, die Zielsetzung eine andere. Das Auskunftsrecht möchte den Persönlichkeitsschutz verwirklichen, indem die Betroffene erfahren kann, ob der Verantwortliche Daten über sie bearbeitet.[1027] Es soll ihr erlauben, die Einhaltung der Datenschutzgrundsätze zu überprüfen.[1028] Als reines Informationsrecht dient das Auskunftsrecht somit dazu, in einem zweiten Schritt die eigenen Rechte durchzusetzen.[1029]

349 Das Recht auf Datenportabilität soll hingegen die Herrschaft der betroffenen Person über «ihre» Personendaten sowie deren Weiterverwendung stärken.[1030] Das Institut ist, wie aufgezeigt,[1031] eine Reaktion auf die Datenwirtschaft. Die Betroffene soll Herrin über «ihre» Daten sein und entscheiden kön-

1024 Thouvenin/Weber/Früh, 172; ähnlich Husi-Stämpfli/Morand, 274.

1025 Husi-Stämpfli/Morand, 274, die konzeptionell im Recht auf Datenportabilität eine Erweiterung des Auskunftsanspruchs sehen; Thouvenin/Weber/Früh, 13 und 173; Weber/Thouvenin, 70; für die DSGVO siehe Europäisches Parlament, Bericht Albrecht, 100 ff. und die Begründung 236.

1026 Ebenso CR LPD-Benhamou, Art. 28 N 8; OFK DSG-Bieri/Heymann/Odermatt, Art. 28 N 5, die zwar einen datenschutzrechtlichen Zweck bejahen, bei der Abgrenzung vom Auskunftsrecht aber lediglich den einfacheren Wechsel zwischen Anbietern aufführen.

1027 BGE 144 I 126 E. 8.3.7; CR LPD-Benhamou, Art. 28 N 8; Botschaft DSG 1988, 433.

1028 SHK DSG-Pärli/Flück, Art. 25 N 6. Bisweilen wird in diesem Kontext auch von «kontrollieren» gesprochen, wobei dies nicht im herrschaftsrechtlichen Sinn zu verstehen ist.

1029 CR LPD-Benhamou, Art. 28 N 8; Götzinger/Vasella, SZW 2021, 42; ähnlich Jotterand, 27.

1030 BJ, Erläuternder Bericht DSV, 44; Jotterand, 27; Toren, Jusletter IT 2019, Rz. 27; a.A. jedoch Hennemann, PinG 2017, 8, der von einer Erweiterung des Auskunftsanspruchs spricht; ebenso Weber/Thouvenin, 70, die im Recht auf Datenportabilität nur eine vergleichsweise geringfügige Weiterentwicklung des datenschutzrechtlichen Auskunftsrechts sehen, bei welchem der Unterschied bloss darin liege, dass die betroffene Person beim Portabilitätsrecht auch direkt die Übertragung an Dritte verlangen kann.

1031 Dazu Rz. 258 ff.

nen, was mit diesen geschieht.[1032] In der Folge endet der Lebenszyklus der Daten nicht, nachdem die betroffene Person sie als Information zur Kenntnis genommen hat und allenfalls weitere Schritte unternimmt. Vielmehr soll die Betroffene oder eine neue Verantwortliche die Daten weiterverwenden können.

Vor diesem Hintergrund erscheint die Unterscheidung zwischen semantischen Informationen und Daten i.w.S. relevant:[1033] Beide Betroffenenrechte resultieren zwar in der Herausgabe von Personendaten. Im Kern zielt das Auskunftsrecht aber nur auf Informationen ab, welche in der Folge für weitere Zwecke, namentlich datenschutzrechtliche Ansprüche, genutzt werden können. Relevant ist für die Betroffene die Kenntnis der Information und nicht die Dispositionsfähigkeit über die Daten.[1034] 350

Dies zeigt sich auch bei einer Betrachtung von Art. 25 DSG: Nicht zufällig ist dort vom Erhalt von (semantischen) Informationen die Rede. Die zur Geltendmachung ihrer Rechte notwendigen Daten sind der Betroffenen zwar «schriftlich, oder in der Form, in der [sie] vorliegen» mitzuteilen (Art. 16 Abs. 2 DSV). Dies kann aber durchaus an Ort und Stelle geschehen oder mündlich erfolgen (Art. 16 Abs. 2 DSV) und dabei noch immer der Zielsetzung des Auskunftsrechts entsprechen. 351

Entsprechend bestimmt Art. 25 Abs. 2 DSG, welche *Informationen* der Betroffenen mitgeteilt werden müssen.[1035] Diese Terminologie wählte der Gesetzgeber wohl, um den gesamten Katalog von Abs. 2 lit. a–g zu umfassen, der mehr als nur Personendaten beinhaltet. Gerade dadurch wird jedoch deutlich, dass das Auskunftsrecht nicht auf eine Datenkontrolle oder gar -herrschaft abzielt. Dies kommt auch in der Aufzählung zum Ausdruck: Mitgeteilt werden müssen die bearbeiteten Personendaten *als solche* (Abs. 2 lit. b). Damit sind nicht ganze Dokumente vom Auskunftsrecht erfasst, sondern eben nur die isolierten Personendaten.[1036] 352

1032 WEBER/THOUVENIN, 68.

1033 Dazu Rz. 31 ff.

1034 Ähnlich auch für die DSGVO SCHRADER, 285.

1035 Ganz loslösen von Daten i.e.S. lässt sich die Information jedoch nicht. So hat das BGer festgehalten, dass es dem Gesetzgeber beim Auskunftsrecht darum ging, «schriftlich bzw. ‹physisch› vorhandene, und deshalb auf Dauer objektiv einsehbare Datensammlungen zu erfassen, nicht aber bloss im Gedächtnis abrufbare Daten», siehe BGE 147 III 139 E. 3.4.3.

1036 BÜHLER, 300, der das Verhältnis zwischen den beiden Instituten «noch ungeklärt» sieht, jedoch deutlich macht, dass das Auskunftsrecht keinem Editionsrecht gleichkommt und gleichzeitig keinen «solch einschränkenden Wortlaut» in das Portabilitätsrecht hineininterpretieren möchte; ROSENTHAL, Jusletter 2020, Rz. 120.

353 Das Recht auf Datenportabilität zielt hingegen auf Daten ab, welche Informationen über die Betroffene enthalten und in einem gängigen, elektronischen Format herauszugeben sind. Die Portierung soll die Informationen – in Form von Daten – verkehrsfähig[1037] machen. Erfasst sind damit i.d.R. ganze Datensätze und nicht nur Ausschnitte.[1038] Wie bereits erwähnt, möchte das BJ selbst Metadaten erfasst sehen.[1039] Damit lassen sich aus dem Auskunftsrecht keine Folgerungen über die Zielsetzung des Rechts auf Datenportabilität ableiten. Die Institute sind getrennt zu betrachten.[1040]

2. Unterschiede in der Ausgestaltung

354 Wie dargelegt, wurde im Gesetzgebungsprozess erwogen, das Portabilitätsrecht als Weiterentwicklung des Auskunftsrechts auszugestalten. Diese Forderung setzte sich politisch nicht durch. Allerdings finden sich in den nun geltenden, eigenständigen Regelungen noch immer gewisse Parallelen: So sind die beiden Institute die einzigen Betroffenenrechte, die das DSG kennt. Zudem verweisen die Einschränkungen des Rechts auf Datenportabilität (Art. 29 Abs. 1 DSG) und die Frist, Zuständigkeiten und Modalitäten der Portabilitätsregelung (Art. 22 DSV) auf das Auskunftsrecht. In der Literatur wird das Recht auf Datenportabilität entsprechend teils eng verwoben mit dem datenschutzrechtlichen Auskunftsrecht diskutiert.[1041] Auch vorliegend wurde in Bezug auf die Rechtsnatur auf das Auskunftsrecht zurückgegriffen.[1042]

355 Zumindest in zweierlei Hinsicht unterscheidet sich das Recht auf Datenportabilität jedoch auch in seiner Ausgestaltung vom datenschutzrechtlichen Auskunftsrecht und ist von diesem abzugrenzen. Einerseits ist der Anwendungsbereich des Auskunftsrechts weiter als derjenige des Rechts auf Datenportabilität.[1043] Das Auskunftsrecht umfasst gemäss Art. 25 DSG die Auskunft darüber, ob Personendaten über die Betroffene bearbeitet werden. Es erstreckt sich mithin auf alle vorhandenen Personendaten, die sich (ohne unverhältnismässig grossen Aufwand) der betroffenen Person zuordnen lassen.[1044] Somit können etwa Daten,

1037 Dieselbe Terminologie nutzend Ziegler/Vasella, digma 2019, 162. Siehe auch Art. 21 Abs. 1 DSV, wonach eine Weiterverwendung der portierten Daten ermöglicht werden soll.
1038 So wohl auch Rosenthal, Jusletter 2020, Rz. 135; Bühler, 300.
1039 Dazu Rz. 208.
1040 So auch Krämer/Senellart/De Streel, 19.
1041 SGK BV-Schweizer/Striegel, Art. 13 N 109; Ziegler/Vasella, digma 2019, 162.
1042 Dazu Rz. 217 f.
1043 PC LPD-Béguin, Art. 28 N 9; Schätzle, PinG 2016, 74.
1044 SHK DSG-Baeriswyl, Art. 28 N 6; CR LPD-Benhamou, Art. 28 N 8; SHK DSG-Pärli/Flück, Art. 25 N 12 f.

die gemäss Art. 28 Abs. 1 lit. a und b DSG oder Art. 20 Abs. 2 DSV vom Recht auf Datenportabilität ausgenommen sind, vom Auskunftsrecht umfasst sein.[1045] Als Normadressaten erfasst sind damit alle Verantwortlichen, während das Portabilitätsrecht faktisch vor allem Kunden des Verantwortlichen zur Auskunft berechtigt.[1046]

Andererseits ist der Anwendungsbereich des Auskunftsrechts aber auch enger. Mitgeteilt werden müssen lediglich die Personendaten *als solche*, während das Portabilitätsrecht einen Anspruch auf Herausgabe von Daten in einem gängigen elektronischen Format begründet, welches eine Weiterverwendung ermöglichen soll (Art. 21 Abs. 1 DSV). Grund dafür ist der eben erläuterte konzeptionelle Unterschied zwischen den beiden Instituten. 356

Folglich ist denkbar, dass ein Datensatz aus einer Portabilitätsanfrage dem Informationsanspruch einer betroffenen Person nicht gerecht wird, weil der Datensatz für eine Maschine, nicht aber für einen Menschen tatsächlich (aus-)lesbar ist.[1047] Umgekehrt können nicht weiterverwendbare Formate wie PDF einem Auskunftsanspruch gerecht werden, aber keine Portabilitätsanfrage rechtsgenüglich beantworten. Dies gilt insb. dann, wenn der aus der Portabilitätsanfrage herausgegebene Datensatz keine oder zu wenig sachdienliche Metadaten enthält.[1048] 357

B. Zu Datenzugang

Viele unterschiedliche Vorgänge werden in der Literatur als Datenzugang(srecht) bezeichnet.[1049] Ein gemeinsames oder allgemeines Verständnis lässt sich dabei nicht erkennen. Auch das Portabilitätsrecht wird teils als Datenzugangsrecht beschrieben,[1050] ebenso wie das Auskunftsrecht nach Art. 25 358

1045 SHK DSG-Baeriswyl, Art. 28 N 31; in Bezug auf abgeleitete Daten Cattaneo, 64; in diese Richtung für die Regelung in der DSGVO ebenfalls Graef/Husovec/Purtova, GLJ 2018, 1367; Lynskey, European Law Review 2017, 811.

1046 Rosenthal, Jusletter 2020, Rz. 132; dazu bereits Rz. 173.

1047 Li, 68; in diesem Sinn auch Tombal, 515.

1048 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 21.

1049 Siehe etwa Früh, digma 2019, 174, insb. Fn. 15, der verschiedene – zumeist im Gesetz als Auskunftsrecht bezeichnete – gesetzliche Regelungen im Familienrecht (Art. 170 ZGB), im Erbrecht (Art. 607 Abs. 3, Art. 610 Abs. 2 ZGB), im Auftragsrecht (Art. 400 OR) und im Aktienrecht (Art. 697 OR) aufzählt; dazu auch Rz. 368.

1050 Früh, digma 2019, 174, der das Portabilitätsrecht als eine Spielart eines Zugangsrechts bezeichnet; siehe auch Specker genannt Döhmann, 192 ff.

DSG. Letzteres wird in den lateinischen Sprachfassungen als «droit d'accès» resp. «diritto d'accesso» und damit wörtlich als Zugangsrecht bezeichnet.

359 Wird der Begriff technisch verstanden, so ist wesentlich, ob Daten nach Massgabe der neuen Verantwortlichen oder der Betroffenen eigenständig (aber unter technischer Ermöglichung des alten Verantwortlichen) «abgeholt» werden können («Pull»).[1051] Dies ist beim Portabilitätsrecht nicht notwendigerweise der Fall: Der alte Verantwortliche gibt die Daten i.d.R. vielmehr aktiv auf Anfrage hin heraus («Push»).[1052]

360 Unter einem Datenzugang wird damit eine kontinuierliche Anbindung an einen Datensatz in (mehr oder weniger) Echtzeit[1053] verstanden.[1054] Dieser wird oft über einen direkten Zugang zu einer API ermöglicht.[1055] Der Datenzugang kann aber auch auf anderem Wege gewährt werden, etwa über einen (S)FTP-Server. Möglich ist ferner eine Zugriffsinfrastruktur in Form einer über das Internet erreichbaren Website.[1056] Wesentlich ist, dass der alte Verantwortliche Zugriff auf seine Infrastruktur gewährt, wodurch Dritte «live» auf die Daten zugreifen können.[1057]

361 Auch hierin unterscheidet sich der Datenzugang vom Recht auf Datenportabilität, welches (zumeist) aus einem einmaligen oder zumindest nicht periodischen oder kontinuierlichen Vorgang besteht und bei welchem der alte Verantwortliche eine Kopie der bis zum Zeitpunkt des Gesuchs akkumulierten Daten herausgibt.[1058] Dies zeigt sich ferner an der 30-tägigen Frist für die Herausgabe bzw. Übertragung (Art. 22 i.V.m. Art. 18 Abs. 1 DSV). Daraus folgt, dass eine Portabilitätsanfrage beantwortet werden kann, indem der Verantwortli-

1051 Dazu OFK DSG-Bieri/Heymann/Odermatt, Art. 28 N 20; Landolt, 41, der dabei von Datenzugriff spricht.

1052 Dazu OFK DSG-Bieri/Heymann/Odermatt, Art. 28 N 20.

1053 Aus technischer Sicht ist nicht leichthin von einem Echtzeitzugang auszugehen, da sich die Anforderungen an einen Echtzeitzugang unterscheiden können. So kann eine Latenzzeit von einigen Sekunden beim Kommentieren eines Fotos auf einer anderen Plattform wohl noch als Echtzeit bezeichnet werden. Allerdings ist nicht mehr von Echtzeit auszugehen, wenn der Airbag eines smarten Fahrzeugs erst mit einer Latenzzeit von einigen Sekunden ausgelöst wird, weil zunächst eine Datenübertragung erfolgen muss.

1054 Siehe OECD, Mapping Initiatives, 40, die hierbei von «Datenportabilität 3.0» sprechen.

1055 Im Wesentlichen das gleiche Verständnis aufweisend Schallbruch et al., 39; Louven, K&R 2018, 230, nach welchem ein Datenzugangsverhältnis eine konkrete rechtliche Beziehung zwischen einem Anbieter und einem Nachfrager über den Zugang zu Daten beinhaltet.

1056 Landolt, 41 f.; Sattler, Personenbezug, 58 f.

1057 Schallbruch et al., 39.

1058 Crémer/De Montjoye/Schweitzer, 81.

che einen Datenzugang gewährt. Dies gilt aber umgekehrt nicht zwingend, da die Portierung per Mail oder gar per Post zulässig ist.[1059]

Die Unterscheidung ist besonders dann relevant, wenn eine Betroffene die Daten nicht primär von einem Verantwortlichen zu einer anderen transferieren, sondern wenn sie das Angebot mehrerer Verantwortlicher gleichzeitig nutzen möchte und dabei auf die Übertragung der Daten angewiesen ist. Dies kann namentlich dann der Fall sein, wenn eine Anbieterin komplementäre Dienste zum alten Verantwortlichen anbietet.[1060] Das Portabilitätsrecht ermöglicht ein solches *Multi-Homing* in seiner aktuellen Ausgestaltung nicht; ein Datenzugang kann dies jedoch ermöglichen.[1061] 362

Mit Blick auf die europäische Gesetzgebung fällt auf, dass gerade neuere, im Rahmen der europäischen Digitalstrategie erlassene Portabilitätsrechte nach diesem Verständnis eher als Datenzugangsrechte einzustufen sind, obwohl sie teilweise (wohl mit Blick auf die «Grundbestimmung» in Art. 20 DSGVO) noch als Portabilitätsrechte bezeichnet werden.[1062] Bereits vorwegzunehmen ist, dass in den einzelnen Sektoren teils ebenfalls Entwicklungen des Portabilitätsrechts in Richtung eines Datenzugangsrechts gefordert werden. 363

Die Gewährung eines Datenzugangs birgt allerdings andere Sicherheitsrisiken als eine Portierung. Dabei ist nach der Art des Datenzugangs zu unterscheiden. Möglich ist nämlich, dass trotz eines Datenzugangs die Daten beim alten Verantwortlichen verbleiben.[1063] Dies kann in Bezug auf den Datensatz Risiken minimieren – gerade wenn einzig ein Lesezugriff gewährt wird.[1064] Auch hierin ist ein Unterschied zum Portabilitätsrecht zu sehen, bei welchem ein Lesezugriff nicht ausreicht.[1065] Auf Seiten des alten Verantwortlichen birgt ein Daten- 364

1059 Dazu Rz. 212.

1060 Crémer/De Montjoye/Schweitzer, 81 f.; Graef/Husovec/Van den Boom, EuCML 2020, 13 f.

1061 Ähnlich wohl Landolt, 193.

1062 Siehe BJ, Erläuternder Bericht DSV, 48, nach welchem eine Übertragung im Abrufverfahren auch über eine API «denkbar» wäre. Diese Auffassung reiht sich wohl ein in die in Erw.G 68 DSGVO festgehaltene «Aufforderung», interoperable Formate zu entwickeln; dazu weiterführend Rz. 419 ff. (DMA) und 604 ff. (DV).

1063 Graef/Husovec/Van den Boom, EuCML 2020, 13; Landolt, 40, der von «Datenzugriff» spricht und dabei das Verbleiben im Kontrollbereich des alten Verantwortlichen als entscheidenden Unterschied zum «Datentransfer» sieht.

1064 Ein solcher Lesezugriff wird in der europäischen Literatur teils auch als in-situ-Zugang bezeichnet, siehe Eckardt/Kerber, 10 f.; Kerber, GRUR Int. 2023, 124; ebenfalls abgrenzend vom datenschutzrechtlichen Portabilitätsrecht Chao et al., CLSR 2025, 4; Schweitzer/Metzger, GRUR Int. 2023, 340.

1065 BeckOK IT-Recht-Steinrötter, Art. 20 DSGVO N 26.

zugang zudem neue Sicherheitsrisiken, weil durch die Anbindung und die damit einhergehende «Öffnung» gegen aussen neue Sicherheitslücken entstehen können.[1066]

C. Zu kartellrechtlichen Ansprüchen

365 Ein generelles Recht auf Datenportabilität vermittelt das Kartellrecht weder in der EU noch in der Schweiz.[1067] Dennoch werden Ansprüche auf eine Datenherausgabe – zumeist in der europäischen Literatur und vereinzelt in der Schweizer Lehre – auch unter kartellrechtlichen Gesichtspunkten diskutiert. Dabei wird die Herausgabe von Daten aufgrund von Art. 102 AEUV resp. Art. 7 KG diskutiert, teils unter Bezugnahme auf die sog. *essential facilities doctrine*.[1068] Nach dieser verhält sich ein Unternehmen unzulässig, wenn es sich weigert, Zugang zu einer von ihm kontrollierten Ressource zu gewähren, deren Nutzung unerlässlich ist, um auf einem vor- oder nachgelagerten Markt am Wettbewerb teilnehmen zu können, weil die Ressource aus rechtlichen oder anderen Gründen nicht innert nützlicher Frist dupliziert oder sonst wie beschafft werden kann.[1069] Liegt eine missbräuchliche Verhaltensweise in Form einer Verweigerung von Geschäftsbeziehungen vor,[1070] kann der Zugang zu den Daten möglicherweise gewährt werden.[1071] In der Schweiz lässt sich ein solches Verhalten unter Art. 7 Abs. 2 lit. a KG subsumieren.

366 Das Recht auf Datenportabilität unterscheidet sich in mehreren Belangen von solchen (möglichen) kartellrechtlichen Ansprüchen: Zunächst knüpft ein kartellrechtliches Zugangsrecht an eine missbräuchliche Verhaltensweise an, während das Recht auf Datenportabilität (im Rahmen der normativen Vorgaben von Art. 28 DSG) voraussetzungs- und hürdenlos anwendbar ist.[1072] Das

1066 Polański, EuCML 2018, 145 f. Siehe etwa die spezifischen Sicherheitsrisken, die sich bei APIs ergeben, https://perma.cc/J3DZ-MZXV.

1067 Alberini/Benhamou, Expert Focus 2017, 519.

1068 Schweitzer, GRUR 2019, 576 f.; für die Schweiz etwa Denoth/Kaufmann, sic! 2016, 510. Art. 102 AEUV entspricht dem Art. 7 KG, weshalb für dessen Auslegung auf die Literatur und Praxis zu Art. 102 AEUV zurückgegegriffen werden kann, siehe BGE 146 II 217 E. 4.3; Gohari, sic! 2019, 534 m.w.N.; ausführlich Landolt, 199 ff.; Savary, 236.

1069 Gohari, sic! 2019, 535.

1070 Gohari, sic! 2019, 539 f.

1071 Schweitzer, GRUR 2019, 576 f.

1072 Lynskey, European Law Review 2017, 801 f.; siehe auch Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 4, wonach das Institut keine Begrenzung auf Daten vorsieht, die «für den Anbieterwechsel notwendig oder nützlich sind».

Recht auf Datenportabilität ist sodann eine Form der *ex ante*-Regulierung,[1073] dies im Unterschied zu den kartellrechtlichen Tatbeständen, die grundsätzlich lediglich *ex post* wirken. Gerade die in der EU im DMA und in der DV neu geschaffenen Institute, die, wie noch aufgezeigt wird, hinsichtlich ihrer Zielsetzung teils Überschneidungen zum Recht auf Datenportabilität aufweisen, weichen diese Unterscheidung jedoch zunehmend auf. Als Regulierungsrecht ausgestaltet, stehen sie zwar dem Kartellrecht nahe, indem einen wirksamen Wettbewerb fördern sollen.[1074] Sie kommen jedoch – wie das Recht auf Datenportabilität – nicht erst nachträglich zur Anwendung, sondern müssen von den Marktteilnehmenden ohne Weiteres eingehalten werden.[1075] Ein Datenzugang gestützt auf das Kartellrecht ist damit nur fallweise möglich, während das Recht auf Datenportabilität grundsätzlich generell und insb. ohne das Zutun eines Konkurrenten anwendbar ist.[1076] Aufsichtsbehörden wie die WEKO oder der EDÖB müssen nicht aktiv werden. Wird ein Datenzugang in einem bestimmten wettbewerblichen Umfeld zum systematischen Problem, könnte das Kartellrecht angesichts der notwendigen Einzelfallprüfung überfordert sein.[1077] Dies kann eine *ex ante*-Regulierung notwendig machen.

Beim Portabilitätsrecht steht die Betroffene im Zentrum; sie muss eine Portierung initiieren.[1078] Damit unterscheidet sich das Institut von einem kartellrechtlichen Anspruch auf Zugang zu Daten, welcher das sich unzulässig verhaltende Unternehmen direkt verpflichtet.[1079] Wettbewerbsrechtlich würde die Situation so vereinfacht, da die betroffene Person nicht unmittelbar einzubinden wäre. Aus Sicht des Datenschutzrechts wäre ein Zugang aber heikel, gerade *weil* die betroffene Person nicht unmittelbar eingebunden würde.[1080] Notwendig wäre für die Zugangsgewährung wohl regelmässig deren Einwilligung.[1081] Festzuhalten ist ferner, dass das kartellrechtliche Zugangsrecht nur 367

1073 In diese Richtung Fix, 94; siehe auch Yan/He, JCLE 2022, 898 f.; dazu bereits Rz. 317.

1074 Heinemann, 226.

1075 Siehe grundlegend Heinemann, 226; vom DMA als einer «kartellrechtsnahen Regulierung» sprechend Heinemann/Meier, EuZ 2021, 88 f. Weiter in Bezug auf die neuen EU-Verordnungen siehe etwa Erw.G 5 DMA.

1076 CR LPD-Benhamou, Art. 28 N 11, der von einer Anwendung unabhängig vom Kontext spricht; ebenso Engels, Internet Policy Review 2016, 4; Graef/Verschakelen/Valcke, LJHSE 2013, 8.

1077 Schallbruch et al., 38.

1078 Dazu bereits Rz. 314.

1079 Graef/Verschakelen/Valcke, LJHSE 2013, 7.

1080 Savary, 253, nach welcher die diesbezüglichen Interessen der einzelnen Nutzer «zu beachten» wäre.

1081 Für das deutsche Recht Schallbruch et al., 38; Sperlich, 116 f.; auch Picht, IIC 2020, 955. Dies dürfte unter dem DSG nicht anders sein. Notwendig wäre angesichts der neuen Da-

gegenüber Unternehmen Anwendung finden kann, während das Recht auf Datenportabilität jegliche Verantwortlichen verpflichtet, auch solche die nicht wirtschaftlich tätig sind.[1082] Schliesslich wären unter einem kartellrechtlichen Zugangsrecht potenziell sämtliche Daten und damit insb. auch Sachdaten und abgeleitete Daten erfasst, was unter dem DSG nicht der Fall ist.[1083]

D. Weitere mögliche Institute

368 Denkbar wären überdies zahlreiche andere Institute, die eine Herausgabe oder eine Übertragung von Personendaten bewirken. So können etwa das Auftragsrecht (Art. 400 Abs. 1 OR), das Erbrecht (bspw. Art. 607 Abs. 3 ZGB) oder das Familienrecht (Art. 170 ZGB) zu einer Datenübertragung verpflichten.[1084] Solche Institute sind allerdings kaum an besondere Formen gebunden und erlauben regelmässig eine bloss mündliche Auskunft. Sie finden ihr Pendant daher eher im Auskunftsrecht. Dazu kommen zahlreiche sektorielle Institute, auf die vorliegend nur im Rahmen der sektoriellen Betrachtung eingegangen wird, soweit sie relevant sind. Entsprechend wird an dieser Stelle auf weitere Ausführungen verzichtet.

tenbearbeitung eine Rechtfertigung i.S.v. Art. 31 DSG. Dafür scheint nur die Einwilligung in Frage zu kommen. Es kann insb. bezweifelt werden, ob die kartellrechtlichen Interessen gegenüber den Persönlichkeitsschutz der betroffenen Personen ein überwiegendes Interesse darstellen könnte.

1082 Aus europäischer Sicht Lynskey, European Law Review 2017, 801. Zu beachten ist aber auch der eingeschränkte Geltungsbereich des DSG gemäss Art. 2 Abs. 2 lit. a DSG (sog. Haushaltsausnahme).

1083 Engels, Internet Policy Review 2016, 4; Graef/Verschakelen/Valcke, LJHSE 2013, 8; Lynskey, European Law Review 2017, 802.

1084 Weber/Thouvenin, 58; zum Auftrag Alberini/Benhamou, Expert Focus 2017, 519.

V. Synthese

A. Vereinbarkeit von datenschutz- und wettbewerbsrechtlichen Zielen

Nach der Untersuchung der einzelnen Ziele des Instituts und der Abgrenzung zu anderen Instituten, ist im Sinne einer Synthese zu diskutieren, ob die teils ähnlichen, teils unterschiedlichen Ziele miteinander vereinbar sind, oder ob Konflikte bestehen, die die Zielerreichung erschweren können. 369

Augenscheinlich sind die konzeptionellen Unterschiede zwischen den auf eine breite und nicht sektoriell eingeschränkte Anwendbarkeit angelegten datenschutzrechtlichen Zielen und den spezifischen und wohl primär auf soziale Netzwerke und Internetplattformen abzielenden wettbewerbsrechtlichen «Mikrozielen». Nicht alle Widersprüche zwischen diesen Zielen lassen sich aber auflösen. So bestehen etwa Zweifel, ob der weite Anwendungsbereich tatsächlich auf die Zielsetzung einer Verringerung von Markteintrittsschranken für Konkurrentinnen passt. Auch in Bezug auf (userinduzierte) Lock-In-Effekte überzeugt der weite Anwendungsbereich nicht. Das Institut weist kaum die erforderliche Bestimmtheit auf, um die Grundlage für eine Erreichung dieser Ziele zu schaffen.[1085] Der Grund für diesen Widerspruch liegt im bereits beschriebenen gesetzgeberischen Fokus auf die sozialen Netzwerke, der sich aber nicht einschränkend in der Regelung wiederfindet. Im besten Fall führt dies dazu, dass die Ziele nicht verwirklicht werden – und der Vorwurf eines überschiessenden Wettbewerbsrechts bis zu einem gewissen Grad zutrifft. Im ungünstigsten Fall können sich allerdings konträre Effekte einstellen, welche diese wettbewerbsrechtlichen Ziele unterlaufen und etwa die Marktstellung grosser Anbieterinnen verfestigen. Da eine Verallgemeinerung über alle Sektoren hinweg aber nicht möglich ist, sind diese Probleme bei der Untersuchung im nächsten Kapitel weitergehend zu adressieren. 370

Aus diesem Grund wird vorliegend postuliert, dass sich das Institut gerade wesentlich durch seine weitgehende Anwendbarkeit charakterisiert – dies in Abgrenzung zu einer möglichen sektoriellen Regelung, die nur spezifische Normadressatinnen kennt oder nur in einem eng definierten Sachbereich zur Anwendung kommt. In den Vordergrund treten damit in wettbewerbsrechtli- 371

1085 So auch LANDOLT, 345.

cher Hinsicht die Makroziele. Diese sind konzeptionell besser mit den datenschutzrechtlichen Zielen vereinbar: Sie sind ebenfalls auf eine breite Anwendbarkeit des Portabilitätsrechts innerhalb der Datenwirtschaft angelegt und versuchen als *ex ante*-Regulierung eine allgemeine Wettbewerbsförderung herbeizuführen.

372 Unter der europäischen Regelung wird die Vereinbarkeit dieser unterschiedlichen Ziele dadurch hergeleitet, dass das Recht auf Datenportabilität als Datenschutzregelung betrachtet wird, die der Wettbewerbsförderung diene.[1086] Dies sei kein Widerspruch, sondern Ausdruck der Tatsache, dass die Konzeption des Datenschutzes allein als Abwehrrecht gegenüber dem Staat überholt sei.[1087] Entsprechend soll es sich beim Portabilitätsrecht um einen verhaltenen Versuch handeln, die zunehmende Kommerzialisierung von Personendaten rechtlich abzubilden.[1088] Diese Ansicht trifft trotz der dargelegten Unterschiede hinsichtlich des datenschutzrechtlichen Verständnisses auch für die Schweizer Regelung zu: Im Kontext der Datenwirtschaft lässt sich die datenschutzrechtliche Zielsetzung des Instituts nicht mehr getrennt von der ökonomischen Bedeutung von Personendaten verstehen. Eine Regulierung der Rechte an und zum Umgang mit Daten zieht unweigerlich ökonomische Folgen nach sich. Dass diese «Folgen» in wettbewerblicher Hinsicht relevant sind und gesetzgeberisch gewollt sein können, versteht sich von selbst.

373 Nicht zielführend wäre es bei dieser Ausgangslage aber, dem Institut deswegen jegliche datenschutzrechtliche Komponente abzusprechen und es als rein wettbewerbsrechtlich gelagertes Institut zu verstehen.[1089] Zwar war die Normierung im DSG und damit die Tatsache, dass die Betroffene im Zentrum steht, ein gesetzgeberischer Entscheid, der auch anders hätte ausfallen können.[1090] Doch die nun erfolgte Verankerung im DSG erfordert eine Interpretation des Instituts vor diesem Hintergrund: Das Portabilitätsrecht adressiert die Verwertbarkeit von Personendaten und gibt der Betroffenen ein Mitspracherecht über den Datenfluss. Damit ist die Regelung im Datenschutzrecht nicht systemfremd, sondern vielmehr «systemschaffend»,[1091] weil sie Ausdruck eines

1086 So für die europäische Regelung Fix, 103.

1087 So für die europäische Regelung Fix, 103.

1088 Jülicher/Röttgen/v. Schönfeld, ZD 2016, 361.

1089 So aber Botschaft DSG 2017, 6984. In der deutschen Literatur war deutlicher von «Fremdkörper» die Rede, siehe Brüggemann, 11; BeckKomm-Herbst, Art. 20 DSGVO N 4.

1090 Ähnlich für die DSGVO-Regelung Kratz, InTeR 2019, 30; dazu bereits Rz. 243.

1091 Sperlich, 123 m.H.a. HK DSGVO-Sydow/Wilhelm-Robertson, Art. 20 N 4, die allerdings den zweiten Zweck der DSGVO – den freien Verkehr personenbezogener Daten – besonders hervorheben. Diese Zwecksetzung kann für die Schweiz, wie gezeigt, nicht so deutlich bejaht werden.

gesetzgeberischen Grundsatzentscheids ist, wonach eine Betroffene die Möglichkeit haben soll, über die sie betreffenden Daten in der Datenwirtschaft mitzubestimmen. Der Gesetzgeber stellte klar, dass der Fokus in Zukunft auf die Betroffene gelegt werden soll.[1092] Das Portabilitätsrecht ist somit in seiner Ausgestaltung im Kern ein grundrechtsbasiertes Betroffenenrecht, welches dieser grundrechtlichen Dimension folgend sektorübergreifend anwendbar ist.[1093] Ein mandatierter Zugang für allfällige Wettbewerberinnen ist konsequenterweise nicht vorgesehen[1094] und eine Datenübertragung gegen den Willen einer Betroffenen aus wettbewerbsrechtlichen Gründen wäre nicht mit den datenschutzrechtlichen Vorgaben vereinbar.[1095]

Es handelt sich folglich um ein datenschutzrechtliches Institut, das *auch* wett- 374
bewerbsfördernd wirken soll.[1096] Dass es sich jedenfalls nicht umgekehrt verhält, ergibt sich, wie gesehen, daraus, dass keinerlei wettbewerbsrechtliche Tatbestandsmerkmale vorliegen müssen, um die (potenziell sowohl wettbewerbsrechtliche als auch datenschutzrechtliche) Rechtsfolge herbeizuführen.[1097] Stattdessen müssen datenschutzrechtliche Merkmale vorliegen, um (datenschutzrechtliche und potenziell wettbewerbsrechtliche) Rechtsfolgen herbeizuführen.[1098] Das Portabilitätsrecht kann also datenschutzrechtliche Zwecke verfolgen, ohne dass eine wettbewerbliche Relevanz vorliegen muss, aber keine wettbewerbsrechtlichen Zwecke verfolgen, ohne dass eine datenschutzrechtliche Relevanz vorliegt. Somit wird versucht, das bestehende Spannungsverhältnis dadurch aufzulösen, dass das Portabilitätsrecht als datenschutzrechtliches Betroffenenrecht ausgestaltet ist und damit *by design* im

1092 Laux, digma 2019, 170.

1093 So für die europäische Regelung Kerber/Specht-Riemenschneider, 44. Freilich ist dabei vor allem eine Drittwirkung unter Privaten adressiert.

1094 Louven, ZWeR 2019, 171; Steffen/Wieworra/Kroon, 73 ff.; ferner Landolt, 187, der daraus einen nur einen geringfügigen Eingriff in die Privatautonomie des Verantwortlichen folgert.

1095 Zumindest scheint ein «überwiegendes Interesse» i.S.v. Art. 31 Abs. 1 und 2 DSG *de lege lata* nicht vorzuliegen. Der Rechtfertigungsgrund nach Art. 31 Abs. 2 lit. b DSG schliesst die Bekanntgabe an Dritte sogar ausdrücklich aus.

1096 Ähnlich von einer «Datenschutzregelung, die der Wettbewerbsförderung dient» sprechend auch Fix, 103; dazu eben Rz. 372.

1097 Es brauchen keinerlei wettbewerblichen Elemente vorzuliegen – weder ein Marktversagen, noch eine Marktmacht oder -missbrauch, ja nicht einmal ein Wettbewerb muss vorhanden oder ein Unternehmen tangiert sein. Ähnlich Duller, 309; Lynskey, European Law Review 2017, 801; Schweitzer/Welker, 120.

1098 So müssen Personendaten vorliegen, die rechtmässig bearbeitet werden, etwa weil eine Rechtfertigung vorliegt, dazu Rz. 196 ff.; ähnlich Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 4.

Einklang mit dem Datenschutzrecht steht.[1099] Ohnehin können auch wettbewerbsrechtliche Elemente einen Bezug zum Persönlichkeitsschutz haben, wenn sie auf die Autonomie über die einen selbst betreffenden Daten abzielen.[1100] Zugleich vermag eine datenschutzrechtliche Regelung auch Funktionen zu erfüllen, die ansonsten vom Wettbewerbsrecht zu gewährleisten sind.[1101]

375 Somit handelt es sich bei den Zielen um zwei Seiten derselben Medaille.[1102] Sie steht wiederum für ein sich in Entwicklung befindendes «Datenrecht» als Ganzes.[1103] Darin werden Daten als ökonomische Güter verstanden und nicht mehr einzig auf deren Personenbezug und das damit einhergehende Schutzbedürfnis reduziert. Die datenschutz- und wettbewerbsrechtlichen Zielsetzungen sind also grundsätzlich vereinbar, wobei in Bezug auf eine sinnvolle Vereinbarkeit die auf eine breite Anwendbarkeit angelegten datenschutzrechtlichen Ziele sowie in wettbewerbsrechtlicher Hinsicht die Makroziele im Vordergrund stehen.

1099 Landolt, 183 und 186, wobei nicht auf die angesichts der Mikroziele eigentlich erforderlichen unterschiedlichen Anwendungsbereiche eingegangen wird. Siehe auch a.a.O., 366 f., wo darauf hingewiesen wird, dass ein nutzerzentrierter Ansatz den wesentlichen Vorteil aufweise, dass eine gesonderte Prüfung der Datenschutzkonformität bei wettbewerbsrechtlich relevanten Konstellationen entfällt. Zwar bestünden gegenläufige Zielsetzungen, die «nur beschränkt in einen ausgemessenen Ausgleich» gebracht werden könnten, doch sei eine Annäherung von Datenschutz-, Wettbewerbs- und Konsumentenrecht zwingend, weshalb ein solcher nutzerzentrierter Ansatz zielführend sei. Darin ebenfalls einen Vorteil sehend Krämer, JCLE 2021, 276.

1100 Frei, Jusletter 2018, Rz. 57; siehe auch Elfering, 19, welche zwischen dem Zweck («purpose») und der Begründung («rationale») eines Rechts auf Datenportabilität unterscheidet: «While the purpose [...] is to strengthen data subjects' control and build trust in the digital environment, the underlying rationale is to avoid lock-in.»; kritisch Götzinger/Vasella, SZW 2021, 41; siehe grundlegend Kerber/Specht-Riemenschneider, 42 ff. und *passim*.

1101 Weber/Thouvenin, 71.

1102 Bijok, 199; Weber/Thouvenin, 69; die gleiche Metapher machend für das Datenschutzrecht und das Kartellrecht schlechthin Buchner, DuD 2008, 728; von zunehmender Verzahnung in Zeiten fortschreitender Digitalisierung sprechend KUKO DSGVO-Kamann/Braun, Art. 20 N 3; Kerber/Specht-Riemenschneider, 112, die mit Blick auf die grossen Unternehmen der Datenwirtschaft darauf hinweisen, dass die Ziele des Datenschutz- und des Wettbewerbsrechts nicht mehr unabhängig voneinander erreicht werden könnten.

1103 Siehe für die DSGVO auch BeckOK DSR-von Lewinski, Art. 20 DSGVO N 6, der von einer Frühform eines sich entwickelnden Datenmarkt- und Datenwirtschaftsrechts spricht; BeckOK IT-Recht-Steinrötter, Art. 20 DSGVO N 83, geht hingegen von einem «Baustein eines im Werden befindlichen Datenwirtschaftsrechts» aus. Nach Sperlich, 175, soll eine isolierte Betrachtung des Wettbewerbs- oder Datenschutzrechts an sich nicht mehr zeitgemäss sein, da deren Schutzziele in einem «untrennbaren Zusammenhang» stünden.

B. Notwendigkeit der Regulierung

Nach der rechtsdogmatischen Einordnung lassen sich zur Notwendigkeit des Portabilitätsrechts Aussagen machen. Denn wie alles staatliche Handeln, erfordert der Erlass eines neuartigen Rechts eine Rechtfertigung. Die Notwendigkeit kann sich aufgrund öffentlicher Interessen ergeben[1104] oder aufgrund von Interessen Privater angezeigt sein, namentlich zur Verhinderung eines Marktversagens.[1105] Aufgrund des Bezugs zu Personen(daten) ist auch eine rein persönlichkeits- bzw. datenschutzrechtliche Notwendigkeit denkbar. Im Zuge der Rechtfertigungsprüfung ist zudem ein besonderes Gewicht auf die Verhältnismässigkeit der Regulierung zu legen (Art. 5 Abs. 2 BV). Das Recht auf Datenportabilität muss hinsichtlich der Zielsetzungen geeignet, erforderlich und zumutbar sein.[1106] 376

Vertiefte Untersuchungen zur Rechtfertigung bzw. zur Notwendigkeit gesetzgeberisch tätig zu werden, finden sich zum Portabilitätsrecht, soweit ersichtlich, nicht. In der Botschaft zum revidierten DSG begnügte sich der Bundesrat damit, die Gesetzesrevision in allgemeiner Weise mit den bedeutenden technologischen und gesellschaftlichen Entwicklungen der letzten Jahre zu begründen.[1107] Diese hätten in der Bevölkerung Ängste ausgelöst und zu neuen Datenschutzrisiken geführt.[1108] Zudem müsse der Bund aufgrund internationalen Rechts tätig werden.[1109] Ein Datenportabilitätsrecht wollte der Bundesrat aber ohnehin nicht im DSG verankern, da dieses seiner Ansicht nach eher wettbewerbsrechtliche Ziele verfolgt.[1110] Daraus lässt sich jedoch folgern, dass er grundsätzlich von der Eignung hinsichtlich solcher wettbewerbsrechtlicher Ziele ausging, diese jedoch nicht im DSG umgesetzt sehen wollte. Seine ablehnende Haltung begründete der Bundesrat ferner mit hohen Implementierungskosten.[1111] Er erachtete ein solches Institut somit für (noch) unverhältnismässig, und sah mithin zumindest die Erforderlichkeit als nicht gegeben an. Dem gegenüber standen allerdings Stimmen in der Literatur und der Vernehmlassung, die ein Portabilitätsrecht forderten, und ein solches damit im- 377

1104 Siehe Thouvenin/Weber/Früh, 104 ff.

1105 Siehe Thouvenin/Weber/Früh, 125; für die EU einzig auf die Notwendigkeit eines Marktversagens eingehend Drexl, Connected Devices, 480.

1106 SGK BV-Schindler, Art. 5 N 53 ff., insb. 56.

1107 Botschaft DSG 2017, 6986.

1108 Botschaft DSG 2017, 6986.

1109 Botschaft DSG 2017, 6986.

1110 Botschaft DSG 2017, 6984 f.; dazu bereits Rz. 98.

1111 Botschaft DSG 2017, 6984 f. m.H.a. PricewaterhouseCoopers AG, 37; dazu auch PC LPD-Béguin, Art. 28 N 2; a.A. bezüglich der Kosten jedoch Weber/Thouvenin, 70.

plizit auch für verhältnismässig erachteten.[1112] Dieser Meinung war offenkundig auch das Parlament, welches von der Notwendigkeit der Regulierung ausging.

378 Die Frage der Notwendigkeit muss hier nicht beantwortet werden, da die Forschungsfrage das Portabilitätsrecht voraussetzt. Ohnehin hätte ein nicht notwendiges und damit verfassungswidriges Portabilitätsrecht in der Praxis keine Konsequenzen, da die Verfassungsgerichtsbarkeit in der Schweiz stark eingeschränkt ist und Bundesgesetze für die rechtsanwendenden Behörden massgebend sind (Art. 190 BV).[1113] Es handelt sich somit um eine gesetzgeberische Entscheidung, der Betroffenen zusätzliche Rechte zur Erreichung bestimmter Ziele einzuräumen. Allerdings kann die Verfassungsmässigkeit bei der Auslegung des Verordnungsrechts Berücksichtigung finden.[1114] Auf die Notwendigkeit ist jedoch zurückzukommen, denn in Abgrenzung zu sektoriellen Portabilitätsrechten wird zu prüfen sein, ob mit einem sektorübergreifenden Portabilitätsrecht das für eine Zielerreichung mildeste Mittel gewählt wurde.[1115]

C. Einschränkungen der Wirtschaftsfreiheit

379 Das Portabilitätsrecht darf die Grundrechte nicht in unzulässiger Weise einschränken (Art. 36 BV). Auch hier lässt sich der Vorbehalt der fehlenden Verfassungsgerichtsbarkeit anbringen; dennoch sind einige Punkte anzusprechen. Denn Portabilitätsverpflichtungen greifen in die in Art. 27 BV verankerte Wirtschaftsfreiheit derjenigen ein, die wegen eines solchen Portabilitätsrechts technische und organisatorische Vorkehrungen treffen müssen, die ansonsten möglicherweise nicht getroffen würden.[1116] Dem Bund ist es zwar grundsätzlich erlaubt, die privatwirtschaftliche Erwerbstätigkeit zu regeln (Art. 95 Abs. 1 BV). Er muss sich dabei aber an den Grundsatz der Wirtschaftsfreiheit halten (siehe Art. 94 Abs. 1 und ebenso Art. 27 BV).

380 Wird von diesem Grundsatz abgewichen, liegt eine Grundrechtseinschränkung nach Art. 36 BV vor. Sie muss über eine gesetzliche Grundlage verfügen,

---

1112 LAUX, digma 2019, *passim*; WEBER, Herausforderungen, 16; WEBER/THOUVENIN, 86, die Verhältnismässigkeit im Kontext der mit dem Institut eingehenden Grundrechtseinschränkung besprechend indes a.a.O., 64 ff.; siehe auch die Vernehmlassungsantworten bei BJ, Zusammenfassung Vernehmlassungsverfahren, 62.

1113 Dazu HÄFELIN et al., Rz. 2597 ff.

1114 HÄFELIN et al., Rz. 2604 ff., insb. 2613.

1115 Dazu Rz. 685 ff.

1116 WEBER/THOUVENIN, 64; ähnlich auch für die EU DREXL, Connected Devices, 480; ebenso DULLER, 308.

durch ein öffentliches Interesse gerechtfertigt und ausserdem verhältnismässig sein. Der Kerngehalt des tangierten Grundrechts muss dabei unangetastet bleiben. Letzteres ist beim Recht auf Datenportabilität anzunehmen, und mit der Normierung in Art. 28 DSG existiert auch eine ausreichende gesetzliche Grundlage. Die öffentlichen Interessen ergeben sich aus den in diesem Kapitel dargelegten datenschutz- und wettbewerbsrechtlichen Zielen.[1117]

Dem Verhältnismässigkeitsgrundsatz kommt bei der Einschränkung von 381
Grundrechten grosses Gewicht zu. Wie bereits bei der Verhältnismässigkeit als allgemeinem Grundprinzip ist eine Einschränkung der Grundrechte nur dann verhältnismässig, wenn sie mit Blick auf den Zweck der Regelung, d.h. das öffentliche Interesse und damit die datenschutz- und wettbewerbsrechtlichen Ziele, geeignet, erforderlich und zumutbar ist.[1118] Diese Erfordernisse wurden in der Literatur bislang nur selten ausdrücklich diskutiert und wenn, dann bejaht.[1119] Auch in dieser Hinsicht kann vorliegend eine vertiefte Untersuchung unterbleiben: Der Gesetzgeber hat Fakten geschaffen, die von der Forschungsfrage vorausgesetzt werden. Ohnehin wären die Verhältnismässigkeit und damit die konkreten Auswirkungen des Rechts auf Datenportabilität empirisch zu untersuchen, um belastbare Aussagen treffen zu können.[1120] An dieser Stelle ist daher einzig festzuhalten, dass die Schwelle für die Geeignetheit einer Massnahme tief anzusetzen ist. Sie ist namentlich bereits dann anzunehmen, wenn eine Massnahme in Bezug auf das verfolgte Ziel nicht wirkungslos oder gar kontraproduktiv ist.[1121] Darauf ist ebenfalls in § 5 zurückzukommen, wenn das Portabilitätsrecht möglichen sektoriellen Regelungen gegenübergestellt wird.

1117 So auch WEBER/THOUVENIN, 65.
1118 SGK BV-SCHWEIZER/KREBS, Art. 36 N 53.
1119 WEBER/THOUVENIN, 65 f.
1120 Dies ist abstrakt aber gar nicht möglich, siehe LYNSKEY, European Law Review 2017, 809; WEBER/THOUVENIN, 65. Empirische Untersuchungen gibt es bislang nur wenige, etwa KARASOY/TURGUT/DEGELING, *passim*; LUZSA/MAYR, *passim*; LUZSA et al., *passim*.
1121 WEBER/THOUVENIN, 65; ausführlich HOFSTETTER, 143 f.

VI. Zwischenfazit: Datenschutzrechtliches Instrument mit wettbewerbsrechtlichem Einschlag

382 Die rechtsdogmatische Einordnung bekräftigt die grundsätzliche Übereinstimmung der Regelungen in der EU und der Schweiz in systematischer und teleologischer Hinsicht. Das Recht auf Datenportabilität erweist sich als grösstenteils deckungsgleich. Es ist in der Schweiz ebenfalls als Betroffenenrecht im DSG verankert und verfolgt damit zunächst datenschutzrechtliche Ziele. Diese ergeben sich aus den neuen Schutzbedürfnissen der betroffenen Personen, die durch die technologischen Entwicklungen und die damit einhergehenden enormen Umwälzungen entstanden sind. Der Gesetzgeber hat es deswegen als nötig erachtet, den mit dem Aufkommen einer Datenwirtschaft entstandenen Ungleichgewichten entgegenzutreten. Das Institut ist also auf den Schutz der Persönlichkeit der von einer Datenbearbeitung betroffenen Person ausgerichtet, indem es ihr die Möglichkeit zur selbstbestimmten Datendisposition vermittelt. Die Betroffene soll autonom entscheiden, ob sie ihre Daten selbst verwalten oder an Dritte weitergeben will. Dafür benötigt sie ein rechtliches Mittel. Dies erklärt, weshalb das Portabilitätsrecht auf Personendaten generell anwendbar ist und dennoch gewisse Einschränkungen auf automatisierte Datenbearbeitungen und freiwillig bekanntgegebene Daten vorsieht: Das Portabilitätsrecht ist darauf angelegt, für Personendaten in der *ganzen* Datenwirtschaft, jedoch ohne sektorielle Einschränkung anwendbar zu sein.

383 Dieses *Empowerment* der Betroffenen in Form einer beschränkten Datenkontrolle kann sich zwar auf ein traditionell verstandenes Recht auf informationelle Selbstbestimmung abstützen. Überzeugender – und mit den wettbewerbsrechtlichen Zielen besser vereinbar – scheint es jedoch, die Etablierung einer Datenwirtschaft nicht nur in das Verständnis des Portabilitätsrechts einfliessen zu lassen, sondern dies auch als Anlass zu nehmen, das Verständnis des verfassungsrechtlichen Datenschutzes an die jüngsten Umwälzungen anzupassen.

384 Die veränderten Schutzbedürfnisse führen dazu, dass der verfassungsrechtliche Datenschutz nicht mehr einzig abwehrrechtlich verstanden werden kann. Der grundrechtliche Schutz soll mithin nicht mehr einen blossen Schutz der Betroffenen *vor* Datenbearbeitungen von Daten umfassen. Vielmehr ist der Schutz auch auf eine positive Seite der Persönlichkeit der Betroffenen auszu-

richten, denn Daten stellen längst eine Ware und eine Währung dar. Die Betroffene soll aktiv über die Verwendung ihrer Daten mitbestimmen und von ihnen profitieren können.

Entsprechend wird vertreten, dass der Gesetzgeber mit dem Recht auf Datenportabilität einen Aspekt von Art. 13 Abs. 2 BV in einem neuen Verständnis auch unter Privaten verwirklicht hat, wenn er in gewissen Konstellationen der betroffenen Person ein an die Datenwirtschaft angepasstes Mitspracherecht gibt. Es fand mithin eine Modernisierung des Verständnisses des verfassungsmässigen Datenschutzes statt – eine Entwicklung, welche in der Literatur teils als «dogmatische Neuausrichtung» oder «Paradigmenwechsel» bezeichnet wurde.[1122] 385

Daneben verfolgt das Recht auf Datenportabilität wettbewerbsrechtliche Ziele. Das Institut soll es Betroffenen in ihrer Rolle als Konsumentinnen ermöglichen, zu einem anderen Anbieter zu wechseln. Dies soll Wechselkosten senken und Lock-In-Effekte verhindern. Zudem soll Konkurrenten ein Markteintritt ermöglicht werden. Bei diesen Mikrozielen hatte der Gesetzgeber offenkundig die Internetplattformen und besonders die sozialen Netzwerke vor Augen. Wie sich jedoch zeigt, dürften in diesen vom Gesetzgeber anvisierten Fällen vor allem Netzwerkeffekte der Grund sein, weshalb eine Person nicht von einem Anbieter zu einem anderen wechselt. Die Möglichkeit einer Datenportierung beeinflusst einen solchen userinduzierten *Lock-In* hingegen nur in geringem Umfang, da das Institut Netzwerkeffekten kaum entgegenzutreten vermag. 386

Hervorzuheben ist bei den wettbewerbsrechtlichen Zielen zudem, dass die Regelung keine Einschränkung auf Internetplattformen vorsieht. Während in der EU eine sektorielle Regelung im Gesetzgebungsverfahren keine Mehrheit fand und bewusst verworfen wurde, fand in der Schweiz in den parlamentarischen Beratungen eine entsprechende Diskussion gar nie statt. Angesichts der nunmehr geltenden sektorübergreifenden Regelung ist das Portabilitätsrecht daher in seiner wettbewerbsrechtlichen Dimension breiter auszulegen. Es stellt nicht bloss eine *lex social media* oder gar eine dedizierte *lex facebook* dar. Vielmehr ist das Institut über die Internetplattformen hinaus als verschiedenen Makrozielen dienend zu verstehen. Solche Makroziele sind namentlich eine allgemeine Wettbewerbsförderung, die Förderung von Innovation und die Sicherstellung von freien Datenflüssen im ganzen Web. Mehr noch als ein Wechsel zwischen Konkurrenten dürfte als Ausfluss dieser allgemeinen Wettbewerbsförderung ein Wechsel zu andersartigen Anbietern von Dienstleistungen, also solchen, die 387

[1122] Dazu Rz. 247 ff. und 286.

nicht mit dem alten Verantwortlichen konkurrieren, vom Institut beabsichtigt sein. Denn das Institut ermöglicht mit seinem weiten Anwendungsbereich gerade eine Übertragung zwischen Sektoren. Dieses Verständnis wird von der historischen Betrachtungsweise untermauert, wonach die Ursprünge des Portabilitätsgedankens in der Förderung von Offenheit und Interkonnektivität im Internet, besonders im *Open Web*, liegen. Dem Portabilitätsrecht liegt die Idee zugrunde, dass der freie Austausch von Daten wesentlich dazu beigetragen hat, dass überhaupt neuartige innovative Angebote wie die sozialen Netzwerke entstehen konnten. Das Internet als *interconnected information space* soll damit bewahrt und der Freiraum, in dem solche innovativen Angebote geschaffen werden können, erhalten bleiben. Dabei wird *auch* auf die sozialen Netzwerke und heute dominanten Internetplattformen abgezielt, aber nur darum, weil sie aktuell diejenigen Akteure sind, die diese Makroziele am deutlichsten gefährden.

388 Auf einer solchen Makroebene sind auch die grundsätzlichen datenpolitischen Ziele des Portabilitätsrechts zu verstehen. Dabei ist zuzugestehen, dass das Portabilitätsrecht in dieser wettbewerbsrechtlichen Ausrichtung unter der DSGVO auf einem solideren Fundament steht. Bereits Art. 1 Abs. 1 DSGVO unterstreicht den freien Verkehr personenbezogener Daten. Eine solche Zielsetzung existiert unter dem DSG nicht ausdrücklich. Dennoch stellt das Portabilitätsrecht in der Schweiz das vorläufige Fazit der Diskussion um die Rechte an und den Umgang mit Daten dar, namentlich bezüglich eines möglichen «Dateneigentums». Das Portabilitätsrecht ist somit nur ein Teil eines sich erst im Entstehen befindlichen Datenrechts. Es handelt sich um ein Puzzlestück der Schweizer Digitalstrategie und ist in dessen grösserem Kontext zu verstehen: Datensilos sollen *generell* ab- und Datenzugänge vermehrt aufgebaut werden. Im Sinne eines Grundsatzentscheids legt das Portabilitätsrecht fest, dass der Betroffenen ein Mitspracherecht verbleiben und sie zukünftig im Zentrum stehen soll. Zu diesem Zweck muss ein übergeordnetes und übergreifendes Institut existieren, das nicht auf einzelne Sektoren beschränkt ist. Das Portabilitätsrecht ist daher mehr als die Summe seiner Teile, wenn diese aus zahlreichen sektoriellen Regelungen bestünden. Dies bedeutet im Übrigen, dass weitere Entwicklungen und andere Portabilitätsrechte denkbar sind, gerade in einzelnen Sektoren und mit Blick auf Entwicklungen in der EU.[1123]

389 Das Recht auf Datenportabilität ist zudem von anderen Instituten abzugrenzen, besonders vom Auskunftsrecht. Dabei sollte nicht von einer ähnlichen Konstruktion und der Tatsache, dass das Portabilitätsrecht punktuell auf das Auskunftsrecht verweist, geschlossen werden, dass diese Institute eine ähnli-

[1123] Siehe BAKOM, Medienmitteilung vom 9. Mai 2018.

che Zielsetzung verfolgen. Die Abgrenzung zeigt, dass das Portabilitätsrecht in seiner Zielsetzung und Ausgestaltung genuin neu ist und das Datenschutzrecht bis anhin keine vergleichbaren Institute kannte. Diese Aussage steht indes unter dem Vorbehalt der Untersuchung sektorieller Portabilitätsrechte (dazu § 4). Gleichzeitig zeigte die Abgrenzung, was das Portabilitätsrecht alles *nicht* ist.

Schliesslich wurde die Vereinbarkeit der datenschutz- und wettbewerbsrechtlichen Ziele diskutiert und bejaht. Das Portabilitätsrecht ist ein datenschutzrechtliches Instrument, das *auch* wettbewerbsfördernd wirken soll. Die Ziele widersprechen sich dabei nicht, sondern sind als zwei Seiten derselben Medaille zu sehen; diese bildet in der Schweiz ein Datenrecht. Damit tritt ein Paradigmenwechsel zutage. Die beabsichtigten Ziele vermögen die Regulierung zu rechtfertigen und auch die mit dem Institut einhergehenden Einschränkungen anderer Grundrechte, namentlich der Wirtschaftsfreiheit, sind zulässig. 390

Damit konnten die Ziele des Portabilitätsrechts erkannt und der erste Teil der Forschungsfrage beantwortet werden. Für den weiteren Gang der Untersuchung ist das Institut in drei Sektoren zu beleuchten. Dabei stehen die Anpassungsmöglichkeiten mit Blick auf die datenschutzrechtlichen und wettbewerbsrechtlichen Ziele im Vordergrund, um den zweiten Teil der Forschungsfrage zu beantworten. 391

§ 4 Fallbeispiele: Drei Datenökosysteme

I. Methode

A. Auswahl der Sektoren

392 Die digitale Transformation erfasst alle Wirtschafts- und Lebensbereiche.[1124] Folglich entfaltet das sektorübergreifend anwendbare Recht auf Datenportabilität potenziell Wirkung in der ganzen Datenwirtschaft. Im Einzelnen unterscheidet sich dessen Wirkung jedoch, da es in den Sektoren auf unterschiedliche rechtliche Grundlagen und tatsächliche Gegebenheiten trifft. Es lassen sich daher nicht sämtliche Anwendungsbereiche abdecken oder überhaupt antizipieren. Aus diesem Grund sind in diesem Kapitel zunächst drei Sektoren als Fallbeispiele zu wählen. Für diese ist anschliessend zu untersuchen, ob die mit dem Recht auf Datenportabilität beabsichtigten Ziele erreicht werden können und welche Veränderungen notwendig sind, um die Ziele (besser) zu erreichen. Damit folgt die Untersuchung einem induktiven Ansatz, um die Problembereiche, die mit dem Recht auf Datenportabilität einhergehen, in konkreten Sektoren darzustellen.[1125]

393 Die Auswahl geeigneter Sektoren ist dabei bis zu einem gewissen Grad arbiträr. Sie sollen, wie erwähnt, möglichst heterogen sein und zahlreiche Akteurinnen tangieren, um eine möglichst grosse Erkenntnistiefe erreichen zu können.[1126] Zu diesem Zweck wird an die bereits beschriebenen Begriffe «Datenökosystem» und «Datenraum» angeknüpft.[1127] Die laufenden Bestrebungen auf schweizerischer und europäischer Ebene zur Schaffung von Datenräumen in unterschiedlichen Sektoren zeigen, dass von einer datenschutzrechtlichen Relevanz auszugehen ist, wobei die Datenräume digitale Abbilder der ihnen zugrundeliegenden Datenökosysteme darstellen. Die dazugehörigen Sektoren stellen demnach jeweils eigenständige Datenökosysteme dar und bieten sich für eine Untersuchung an.

394 Der UVEK/EDA-Bericht nennt die Datenraumprojekte Mobilität, Energie, Finanzen, Gesundheit und Bildung.[1128] Er begründet die Anwendungsbeispiele nicht weiter, hält allerdings fest, dass es sich um Beispiele handle, die alle eine

---

1124 Europäische Kommission, Datenstrategie, 1; Expertengruppe Zukunft, 2; dazu Rz. 258 f.
1125 Zum induktiven Ansatz THOUVENIN/WEBER/FRÜH, 97.
1126 Dazu Rz. 26.
1127 Dazu Rz. 40 f. (Datenökosystem) und Rz. 42 f. (Datenraum).
1128 UVEK/EDA, 26 ff.

vertrauenswürdige Datennutzung beabsichtigten und somit eine Affinität zur digitalen Selbstbestimmung aufweisen.[1129] Dies sei nicht bei allen Datenraumprojekten in der Schweiz der Fall.[1130] Der Bericht nimmt daher eine Vorauswahl der Datenräume vor und beschränkt sich auf solche, die besonders *vertrauenswürdig* sind.

Die EU-Kommission nutzt in ihrer Datenstrategie die gleiche Terminologie und hält fest, dass Datenräume ein Ökosystem aus Unternehmen, Zivilgesellschaft und Einzelpersonen fördern sollen, welches neue Produkte und Dienstleistungen auf der Grundlage von mehr zugänglichen Daten hervorbringe.[1131] Konkret sei in strategischen Wirtschaftszweigen und Bereichen von öffentlichem Interesse die Entwicklung gemeinsamer europäischer Datenräume zu fördern.[1132] Sie führt neun sektorspezifische Datenräume auf: 395

- Industriedatenraum;
- Datenraum für den europäischen Grünen Deal;
- Mobilitätsdatenraum;
- Gesundheitsdatenraum;
- Finanzdatenraum;
- Energiedatenraum;
- Agrardatenraum;
- Datenräume für die öffentliche Verwaltung; und ein
- Kompetenzdatenraum.[1133]

Damit besteht in vier Sektoren Übereinstimmung zwischen der Schweiz und der EU: Im Mobilitäts-, Gesundheits-, Finanz- und im Energiesektor sind Datenräume geplant. Aus diesen sind die zu untersuchenden Sektoren auszuwählen, da nur so rechtsvergleichende Ausführungen möglich sind. 396

Datenraumprojekte in der Schweiz und der EU

Schweiz	**Europäische Union**
	Industriedatenraum
	Datenraum für den europäischen Grünen Deal

1129 UVEK/EDA, 26.
1130 UVEK/EDA, 26.
1131 Europäische Kommission, Datenstrategie, 6.
1132 Europäische Kommission, Datenstrategie, 25.
1133 Europäische Kommission, Datenstrategie, 26 f.

Schweiz	**Europäische Union**
Mobilitätsdatenraum	Mobilitätsdatenraum
Gesundheitsdatenraum	Gesundheitsdatenraum
Finanzdatenraum	Finanzdatenraum
Energiedatenraum	Energiedatenraum
	Agrardatenraum
	Datenräume für die öffentliche Verwaltung
	Kompetenzdatenraum
Bildungsdatenraum	
Geodatenraum	

397 In einem Energiedatenraum weisen viele Daten keinen Personenbezug auf, sondern sind Sachdaten.[1134] Das praktische Interesse an der Ausübung des Portabilitätsrechts dürfte bei allfälligen Betroffenen zudem gering sein. Höher ist der Anteil an Personendaten im Finanzdatenraum.[1135] Dieser ist jedoch bereits hochreguliert und wäre mit einem finanzmarktrechtlichen Fokus zu untersuchen.[1136] Vorliegend soll allerdings mit dem Gesundheitswesen ein anderer, sich derzeit stark wandelnder Sektor untersucht werden. Das Gesundheitswesen ist ebenfalls reguliert und in hohem Mass darauf angewiesen, Personendaten zu bearbeiten.[1137] Im Gesundheitsdatenökosystem kann das Recht auf Datenportabilität potenziell grosse Wirkung entfalten.

398 Der Sektor Mobilität ist heute digital wenig vernetzt.[1138] Bislang beherrschen ihn nicht einige wenige grosse Akteurinnen, sondern die Geschäftsmodelle und Akteurinnen scheinen sich eher zu erweitern.[1139] Daher fürchten die bestehenden Anbieterinnen einen Verlust ihres Wettbewerbsvorteils, wenn sie

1134 Vgl. die aufgezählten Datenarten bei UVEK/EDA, 28. Dies muss nicht immer der Fall sein. Die in einem Einfamilienhaus gemessenen Angaben zum Wasserverbrauch können etwa Personendaten darstellen, siehe BGE 147 I 346 E. 5.3.2.

1135 UVEK/EDA, 30.

1136 Siehe etwa De La Mano/Padilla, JCLE 2018, *passim*; Roth, SZW 2020, 677 f. und *passim*.

1137 Dies vor allem unter dem Stichwort «Big Data Analytics», siehe Thouvenin, Big Data, 28 ff.

1138 Dumauthioz/Löhrer/Singler, 4.

1139 Picht, IIC 2020, 947 f., auch auf die Datenportabilität im Mobilitätssektor eingehend.

Daten innerhalb des Sektors austauschen müssen.[1140] Dies macht das Portabilitätsrecht für diesen Sektor relevant.

Schliesslich sind viele Datenökosysteme nicht in Datenräumen abgebildet, weil keine «vertrauenswürdige Datennutzung»[1141] beabsichtigt ist. Ein solches Vorgehen entspricht dem amerikanischen Ansatz, wonach die Organisation von Datenräumen dem Privatsektor überlassen wird.[1142] Ein Beispiel dafür sind Onlineplattformen wie die sozialen Netzwerke.[1143] Diese treten oft als geschlossene Ökosysteme auf, wodurch sie Nutzerinnen an sich binden.[1144] Wie bereits aufgezeigt, ist die Entstehungsgeschichte des Portabilitätsrechts eng mit den sozialen Netzwerken verbunden. Daher ist es angebracht, diesen Sektor ebenfalls zu untersuchen. 399

B. Untersuchung der Sektoren

Für die Untersuchung der verschiedenen Sektoren werden diese als Datenökosysteme dargestellt. Die Betrachtung erfolgt dabei anhand der bereits genannten Eigenschaften, nach welchen sich ein Datenökosystem strukturieren lässt: Akteurinnen, Rollen, Beziehungen und Ressourcen.[1145] Akteurinnen sind Personen, denen im Datenökosystem eine oder mehrere Rollen zukommen, etwa natürliche Personen, Institutionen oder Unternehmen.[1146] Rollen sind die Funktionen, die Akteurinnen in einem Datenökosystem einnehmen, bspw. diejenige der Konsumentin, Produzentin oder Intermediärin.[1147] Aus datenschutzrechtlicher Sicht sind die Akteurinnen den Rollen als Verantwortliche, Betroffene oder Auftragsbearbeiterinnen zuzuordnen. 400

Die Beziehung beschreibt die Interaktion zwischen den Akteurinnen des Datenökosystems.[1148] Dabei steht ebenfalls die datenschutzrechtliche Betrachtung im Vordergrund, namentlich wer welche Daten bearbeitet und gestützt worauf. Die Beziehung kann auf einem gemeinsamen Interesse basieren, einem Geschäftsmodell folgen oder anderweitig ökonomisch, politisch, kulturell 401

1140 Dumauthioz/Löhrer/Singler, 21.
1141 UVEK/EDA, 26.
1142 Europäische Kommission, Datenstrategie, 4.
1143 Diese organisieren sich bislang selbst, etwa in der *Data Transfer Initiative*, hierzu Rz. 417 f.
1144 Collovà et al., 8.
1145 Dazu Rz. 40.
1146 Oliveira/Lóscio, dg.o 2018, 2 und 5.
1147 Oliveira/Lóscio, dg.o 2018, 5.
1148 Oliveira/Lóscio, dg.o 2018, 6.

und technologisch begründet sein.[1149] Denkbar ist zudem, dass eine Beziehung und damit eine Datenbearbeitung gesetzlich vorgegeben ist.

402 Die Ressourcen als letzte Eigenschaft eines Datenökosystems sind nicht zu vertiefen, da sie im datenschutzrechtlichen Kontext nicht relevant sind. Im Zentrum der Untersuchung stehen Daten als «Produkte» des Datenökosystems.[1150] Ressourcen sind dagegen nützliche oder wertvolle Produkte, ein Besitz oder eine Fähigkeit, die von Akteurinnen produziert, bereitgestellt, kuratiert oder verbraucht werden, wie Infrastruktur oder Software.[1151]

403 Nach der Bestimmung der relevanten Akteurinnen eines Sektors ist jeweils auf die möglichen Kombinationen der Beziehungen zwischen den Akteurinnen einzugehen. Dabei sind die datenschutzrechtlichen Rollen im Gefüge des Portabilitätsrechts darzulegen und es ist festzustellen, ob eine Beziehung denkbar ist. Im Einklang mit der induktiven Methode ist dabei nur auf diejenigen Akteurinnen einzugehen, die in Bezug auf das Datenportabilitätsrecht relevant erscheinen. Ebenso ist nur auf Beziehungen einzugehen, die relevant und plausibel erscheinen. Damit werden zahlreiche Akteurinnen und verschiedene Beziehungen der Akteurinnen untereinander nicht aufgeführt, weil von keiner datenschutz- bzw. portabilitätsrechtlichen Relevanz auszugehen ist, etwa weil eine Akteurin keine Personendaten bearbeitet oder nicht als Verantwortliche oder Betroffene in Frage kommt.

1149 Oliveira/Lóscio, dg.o 2018, 6.
1150 Oliveira/Lóscio, dg.o 2018, 4.
1151 Oliveira/Lóscio, dg.o 2018, 2.

II. Soziale Netzwerke

Internetplattformen und besonders soziale Netzwerke haben sich in kürzester Zeit zu einem integralen Bestandteil des modernen menschlichen Lebens entwickelt. Sie ermöglichen es, mit Freunden und Familie Informationen auszutauschen und in Kontakt zu bleiben. Dies hat sie in den Fokus des Gesetzgebers gerückt. Sowohl in den parlamentarischen Beratungen zum Portabilitätsrecht als auch bei den hier untersuchten Zielen spielten soziale Netzwerke eine grosse Rolle und sie sind als Anwendungsbeispiel nicht wegzudenken.[1152] Bisherige Untersuchungen beziehen sich denn auch zumeist auf die Datenportabilität bei Onlineplattformen.[1153] 404

Nachfolgend ist anhand der Akteure und deren Rollen und Beziehungen zu untersuchen, ob das Recht auf Datenportabilität in diesem Datenökosystem die Grundlagen schafft, damit die Ziele erreicht werden können. Dabei sind sowohl die datenschutzrechtlichen als auch die wettbewerbsrechtlichen Ziele zu untersuchen. 405

A. Strukturierung des Ökosystems

1. Akteure und deren Rollen

a. Private Nutzer

Natürliche Personen als private Nutzer verwenden soziale Netzwerke zu vielfältigen Zwecken. Sie sind dabei nicht nur Konsumenten, sondern auch Datenlieferanten.[1154] In datenschutzrechtlicher Hinsicht geben sie primär Personendaten bekannt oder es werden solche über sie erfasst. Sie sind diesbezüglich als betroffene Personen zu qualifizieren. Soweit sie mittels Beiträge oder Vi- 406

1152 Aufgrund ihrer zentralen Stellung wurden sie bereits begrifflich abgesteckt, siehe Rz. 46 ff.

1153 Mit der Begründung, dass sich an deren Marktverhalten die grundlegende Problematik der Datenökonomie besonders gut erkennen und darstellen lasse COLLOVÀ et al., 7; ENGELS, Internet Policy Review 2016, *passim*; ähnlich auch FIX, 78, der von Diensteanbietern im Internet spricht; von Social Media Plattformen sprechend PricewaterhouseCoopers AG, 36; STEINER, 125; einen anderen Fokus setzend hingegen etwa DURMUS/KAPLAN, DSB 2023, *passim*; SCHÄTZLE, PinG 2016, *passim*.

1154 BUCHNER, WRP 2019, 1245.

deos eine Datenbearbeitung initiieren, können sie allerdings auch Verantwortliche sein.[1155]

407 Die Abgrenzung kann in Einzelfällen schwerfallen. Ist es der Nutzer allein, der entscheidet, welche Daten Dritter er erhebt und auswählt, welchen Zweck er damit verfolgt, wo und wie weit die Daten verbreitet werden, wem sie zugänglich sind und wie lange sie auf seiner Seite verfügbar bleiben, so dürfte er Verantwortlicher sein.[1156] Eine Ausnahme ist allenfalls denkbar, wenn Daten ausschliesslich zum persönlichen Gebrauch bearbeitet werden und die Haushaltsausnahme greift (Art. 2 Abs. 2 lit. a DSG). Dabei ist jedoch zu berücksichtigen, dass Daten regelmässig auch mit dem Betreiber des sozialen Netzwerks geteilt werden, der diese (ebenfalls) auswertet.[1157]

b. Betreiber

408 Im Gegensatz zu anderen Arten von Plattformen veröffentlichen Betreiber sozialer Netzwerke keine eigenen Inhalte, sondern bieten nur die Grundlage dafür, dass Nutzer interagieren und selbst Inhalte in Form von Videos, Nachrichten und Fotos teilen können (sog. *user generated content*).[1158] Betreiber sind mehr oder weniger offene, interaktive und partizipative Intermediäre, die es Nutzern ermöglichen, untereinander zu kommunizieren.[1159] Sie können inhaltlich jeweils unterschiedliche Ausrichtungen haben. Gemeinsam ist ihnen jedoch, dass es in jedem Segment eine dominante Plattform gibt.[1160] In der Schweiz gehören Instagram (Meta), Facebook (Meta), LinkedIn (Microsoft), Snapchat (Snap Inc.) und TikTok (ByteDance) zu den populärsten sozialen Netzwerken.[1161] Je nach Betrachtungsweise und technischer Ausgestaltung (Kommentarfunktion oder die Möglichkeit, Inhalte zu teilen) können zudem Streamingdienste wie YouTube (Alphabet) oder Kommunikationsdienste wie

1155 Für das EU-Recht Artikel 29-Datenschutzgruppe, Stellungnahme Verantwortlicher/Auftragsverarbeiter, 26; HOFFMANN/SCHMIDT, GRUR 2021, 682.

1156 Für das deutsche Recht JANDT/ROSSNAGEL, ZD 2011, 161.

1157 Siehe JANDT/ROSSNAGEL, ZD 2011, 162. Ferner zur Haushaltsausnahme in der EU der Erw.G 18 DSGVO, der auch die Nutzung sozialer Netze ausdrücklich erwähnt.

1158 GRAEF, 12 f.; LICHTNECKER, GRUR 2013, 135.

1159 Bundesrat, Bericht Social Media, 7.

1160 CLEMENT et al., 239. Bspw. YouTube für Videoclips, WhatsApp für Kurznachrichten oder LinkedIn für die Pflege des geschäftlichen Netzwerks.

1161 Quellen gibt es für die Schweiz nur wenige, etwa die Angaben der Interessengemeinschaft Elektronische Medien, siehe https://perma.cc/LS37-T5C5. Auch zahlreiche Marketingagenturen machen ähnliche Angaben, ohne jedoch auf ihre Methodologie hinzuweisen, etwa https://perma.cc/945J-AEGA. Für die Nutzung bei Jugendlichen im Besonderen siehe die JAMES-Studie KÜLLING-KNECHT et al., *passim*.

WhatsApp (Meta), die in der Schweiz ebenfalls verbreitet sind, soziale Netzwerke darstellen.[1162]

Betreiber stellen eine Infrastruktur bereit, administrieren die Server und beeinflussen damit massgeblich, welche Daten gespeichert werden und in welchem Umfang dies geschieht.[1163] Sie verfolgen dabei zumeist ein kommerzielles Erlösmodell. Dieses besteht darin, dass sie Nutzungsgebühren verlangen oder Werbung schalten.[1164] Bei Letzterem handelt es sich vor allem um Werbeanzeigen, die den Nutzern dynamisch und zielgruppengerecht angezeigt werden.[1165] Für das grösste soziale Netzwerk der Welt (Facebook von Meta) sind Werbeeinnahmen die mit Abstand wichtigste Einkommensquelle.[1166] 409

Datenschutzrechtlich fungieren soziale Netzwerke als Verantwortliche. Diese Qualifikation dürfte regelmässig unbestritten sein, denn soziale Netzwerke entscheiden (ggf. mit anderen Beteiligten) über den Zweck und die Mittel der Datenbearbeitung.[1167] 410

c. Kommerzielle Nutzer

Neben privaten Nutzern, die soziale Netzwerke primär für den Austausch privater Mitteilungen in einem kleineren Kreis nutzen, gibt es kommerzielle Nutzer, für die eine professionell betriebene, publizistische Kommunikation im Vordergrund steht.[1168] Sie haben zum Ziel, das Kaufverhalten von Konsumenten oder die öffentliche Meinungsbildung zu beeinflussen.[1169] Im Gegensatz zu konventionellen Werbemethoden kommen auf sozialen Netzwerken die natürlichen Personen auf die Unternehmen zu.[1170] Kommerzielle Nutzer bezahlen dabei u.U. – aber nicht immer – für die Nutzung des sozialen Netzwerks. Sie können etwa Fansites betreiben, diese administrieren und dabei die gleichen Funktionen nutzen wie private Nutzer.[1171] Sie können auch ausschliesslich als 411

1162 Vertiefend auch BKartA, Beschluss B6-22/16 vom 6. Februar 2019, Rz. 170 ff.
1163 Golland, 124.
1164 Bundesrat, Bericht Social Media, 9; ausführlich auch Golland, 20 ff.
1165 Bundesrat, Bericht Social Media, 9; ähnlich auch Lichtnecker, GRUR 2013, 135.
1166 Siehe beispielhaft die Quartalszahlen im Q1/2025 von Meta Platforms Inc., in welchen $ 41,392 Mia. Werbeeinnahmen lediglich $ 510 Mio. «anderer Einnahmen» gegenüberstehen, abrufbar unter: https://perma.cc/YZ9S-VKSF.
1167 Artikel 29-Datenschutzgruppe, Stellungnahme Verantwortlicher/Auftragsverarbeiter, 26; ferner EuGH C-210/16 vom 5. Juni 2018, Rz. 30.
1168 Bundesrat, Bericht Social Media, 7.
1169 Bundesrat, Bericht Social Media, 7.
1170 Lichtnecker, GRUR 2013, 136.
1171 Golland, 18.

Werbetreibende auftreten, wenn sie entgeltlich nutzerdatenbasierte zielgerichtete Werbung schalten.[1172] Eine weitere Erscheinungsform der kommerziellen Nutzer sind Entwickler (*Publisher*). Deren Webangebote (Webseiten oder Apps) lassen sich mit dem sozialen Netzwerk integrieren, sodass sie die Nutzerbasis erhöhen und ihren Dienst monetarisieren können.[1173] Dies stellt eine Plattformisierung dar.[1174]

412 Datenschutzrechtlich variiert die Qualifikation der kommerziellen Nutzer: Sie können nach der Rechtsprechung des EuGH zusammen mit einem Betreiber eines sozialen Netzwerks als gemeinsame Verantwortliche gelten, etwa wenn sie eine Fanpage betreiben.[1175] Dabei reicht die Möglichkeit aus, die konkrete Umsetzung eines vom sozialen Netzwerk bereitgestellten Tools zu beeinflussen, etwa wenn Kriterien definiert werden können, auf deren Grundlage Besucherstatistiken erstellt werden.[1176] Ist dies nicht der Fall, so kommt kommerziellen Nutzern grundsätzlich keine eigenständige Rolle zu, die über die Rolle privater Nutzer hinausgeht. Da kommerzielle Nutzer zumeist juristische Personen sind, dürften sie jedenfalls nur selten betroffene Personen darstellen.

2. Relevante Beziehungen

a. Private Nutzer und (mehrere) Betreiber

aa. Allgemein

413 Private Nutzer schliessen mit einem Betreiber einen Vertrag über die Nutzung des Angebots des sozialen Netzwerks ab. Hierfür müssen sie sich zumeist online registrieren und dabei den Nutzungsbedingungen des Betreibers zustimmen.[1177] Grundlage ist ein Innominatvertrag, der jeweils angesichts der konkre-

1172 BKartA, Beschluss B6-22/16 vom 6. Februar 2019, Rz. 216, dort am Beispiel Facebook.

1173 BKartA, Beschluss B6-22/16 vom 6. Februar 2019, Rz. 226, dort am Beispiel Facebook.

1174 Dazu Rz. 53 ff.

1175 EuGH C-210/16 vom 5. Juni 2018. Dieser Entscheid erging noch unter der DSRL, welche – anders als die DSGVO – zum Schengen Besitzstand gehörte und entsprechend auch durch die Schweiz angewendet wurde, siehe Anhang B des Abkommens zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands vom 26. Oktober 2004 (SR 0.362.31).

1176 EuGH C-210/16 vom 5. Juni 2018, Rz. 57.

1177 Dumermuth, 137; Staffelbach, 18 ff.; anschaulich am Beispiel von Facebook der EuGH, siehe EuGH C-252/21 vom 4. Juli 2023, Rz. 28; zur besonderen Thematik der sog. «Schattenprofile», die von Nutzern, die gerade nicht registriert sind, angelegt werden Golland, 180.

ten Umstände zu beurteilen ist.[1178] Dem Betreiber geben private Nutzer Personendaten bekannt, etwa indem sie bei der Registrierung oder anschliessend Angaben über sich machen, Fotos veröffentlichen oder anderweitig am sozialen Netzwerk partizipieren.[1179] Sie können – je nach sozialem Netzwerk – unterschiedliche Informationen wie Name oder Wohnort, Interessen, Hobbys, beruflichen Hintergrund oder politische Vorlieben preisgeben.[1180] Teils verlangen soziale Netzwerke bestimmte Angaben auch zwingend.[1181] Darüber hinaus werden Daten über das Nutzungsverhalten der privaten Nutzer erhoben und gestützt auf andere Rechtfertigungsgründe als die Einwilligung bzw. den Vertrag bearbeitet.[1182]

Der Betreiber bestimmt bis zu einem gewissen Grad eigenständig, welche Daten der Nutzer er erhebt, welche Ansprüche er an ausgetauschten Daten erwirbt und wie er diese ökonomisch verwertet.[1183] Im Bereich des *user generated content* sind es hingegen grundsätzlich die privaten Nutzer, die darüber bestimmen, welche Inhalte sie teilen möchten: Denkbar sind Urlaubsfotos, Konzertkritiken, Angaben über die Jobsuche oder den Beziehungsstatus, um nur einige zu nennen. Wiederum ist es aber der Betreiber, der über die ökonomische Verwertung dieser Angaben bestimmen kann, *wenn* private Nutzer sich dazu entscheiden, etwas zu teilen. 414

Verbreitet ist eine Verwertung in Form von personalisierter Werbung. In Bezug auf Facebook hat der EuGH festgehalten, dass auf die Einwilligung abzustellen ist und die anderen in Art. 6 DSGVO aufgeführten Rechtmässigkeitsbedingungen eng auszulegen sind, wenn Personendaten von privaten Nutzern, die ausserhalb der eigentlichen Plattform gesammelt werden, zu Werbezwe- 415

1178 Dumermuth, 136 f.; zur Rechtslage in Deutschland Bräutigam/Richter, 85.

1179 Weitergehend zur Funktionsweise und den erfassten Daten natürlicher Personen Golland, 13 ff.

1180 Zum Personenbezug der einzelnen Daten ausführlich Golland, 66 ff.; siehe auch die Angaben bei Lichtnecker, GRUR 2013, 135.

1181 So verlangt etwa Facebook in Ziff. 3.1 seiner Nutzungsbedingungen, dass für das Konto derselbe Name angegeben wird, der auch im täglichen Leben verwendet wird, siehe https://perma.cc/5APT-W4RM.

1182 Dies sind bei Facebook etwa berechtigte Interessen von Facebook bzw. von Dritten, die Erfüllung einer rechtlichen Verpflichtung, der Schutz lebenswichtiger Interessen der betroffenen oder einer anderen Person und im öffentlichen Interesse durchgeführte Aufgaben. Facebook bezeichnet nur Daten, die in dem für die Erfüllung ihrer Verträge mit der Betroffenen erforderlichen Mass verarbeitet werden als portabilitätsberechtigt und nennt die Einwilligung als eine «andere Rechtsgrundlage», siehe hierzu https://www.facebook.com/about/privacy/legal_bases.

1183 Bundesrat, Bericht Social Media, 11.

cken verwendet werden sollen.[1184] In der Folge führte Facebook in Europa, einschliesslich der Schweiz, ein Bezahlmodell ein, wenn private Nutzer nicht einwilligten, dass die sie betreffenden Daten auch für Werbung genutzt werden dürfen.[1185]

416 Die vorhandenen Daten fallen damit grundsätzlich unter das Portabilitätsrecht und private Nutzer können sie nach Massgabe von Art. 28 DSG herausverlangen. Dabei ist neben der Herausgabe insb. eine Übertragung denkbar, wenn private Nutzer zwischen zwei Betreibern wechseln. Die Betreiber können untereinander in einem Wettbewerbsverhältnis stehen, wenn sie gleichartige Dienstleistungen erbringen und ein neuer Betreiber aus Sicht der privaten Nutzer geeignet ist, den alten zu ersetzen.[1186] Betreiber können aber auch andersartige Dienstleistungen erbringen und somit in keinem Wettbewerbsverhältnis zueinander stehen.[1187] Denkbar ist ferner, dass ein privater Nutzer die ihn betreffenden Daten nicht an einen anderen Betreiber, sondern an eine ganz andere Verantwortliche übertragen möchte (etwa an einen Arzt).

bb. Data Transfer Initiative

417 Im Juli 2018 riefen Google, Microsoft, Twitter und Facebook und damit namhafte Betreiber sozialer Netzwerke gemeinsam das *Data Transfer Project* ins Leben. Die Initiative zielt darauf ab, Tools zu entwickeln, die es Nutzern ermöglichen, ihre Daten direkt zwischen Betreibern zu übertragen, ohne sie herunterladen und erneut hochladen zu müssen.[1188] Im Kern wird damit die Funktionsweise des Rechts auf Datenübertragung angestrebt. Die Initiative schliesst an die bereits 2010 durch Facebook und 2011 durch Google eingeführte Produkte *Download Your Information* und *Google Takeout* an, welche es Nutzern erlaubten, eine Kopie ihrer Daten in unterschiedlichen standardisier-

1184 EuGH C-252/21 vom 4. Juli 2023, Rz. 26 ff. und 93.

1185 Nach dem EuGH muss den privaten Nutzern die Freiheit bleiben, bestimmte Datenbearbeitungsvorgänge, die für die Erfüllung des Vertrags nicht erforderlich sind, einzeln zu verweigern. Dafür muss ihnen, ggf. gegen Entgelt, eine Alternative geboten werden, siehe EuGH C-252/21 vom 4. Juli 2023, Rz. 150. Dazu auch SRF Online, «Bezahlen für keine Werbung: Meta führt ein Bezahlmodell ein» vom 1. November 2023, abrufbar unter: https://perma.cc/QA59-CHDU.

1186 Siehe Engels, Internet Policy Review 2016, 6 ff.

1187 Siehe Engels, Internet Policy Review 2016, 8 ff.

1188 Google Open Source Blog, «Introducing Data Transfer Project: an open source platform promoting universal data portability» vom 20. Juli 2018, abrufbar unter: https://perma.cc/5T9Q-2ECH. Nunmehr heisst das Projekt *Data Transfer Initiative*, siehe https://perma.cc/DN9D-XFDE.

ten Formaten herunterzuladen.[1189] Nunmehr sollen aber innerhalb des ganzen Ökosystems der partizipierenden Akteure Daten von individuellen, proprietären Formaten in sog. kanonische und damit einheitliche Formate umgewandelt und anschliessend zwischen den Akteuren transferiert werden können.[1190] Ziel ist es, eine Datenübertragung zu ermöglichen, während Autorisierungsmechanismen beibehalten und die Sicherheit der Dienste gewährleistet werden.[1191] Gleichzeitig sollen Betreiber neue Nutzer gewinnen und eine Nutzerbasis für neue Produkte aufbauen können, indem sie die einfache Import- und Exportfähigkeit von Daten unterstützen.[1192] Für die Umwandlung der Daten sind laut *Data Transfer Initiative* zwei Arten von «Adaptern» vorgesehen: Datenadapter[1193] und Authentifizierungsadapter[1194]. Sie befinden sich ausserhalb der Kerninfrastruktur des Betreibers und können von diesem selbst oder von Dritten geschrieben werden.[1195] Die Architektur soll dabei auf bestehenden Standards (wie OAuth und REST[1196]) aufbauen, um die Umsetzung möglichst einfach zu halten.[1197] Für den Datentransfer sollen anschliessend Datenmodelle bestehend aus standardisierten branchenüblichen Formaten gewählt und mit Metadaten versehen werden, die einen Import bei anderen Betreibern ermöglichen.[1198]

Der Quellcode dieses Open Source-Projekts ist öffentlich,[1199] entsprechend 418
können sich auch andere Betreiber (oder Dritte in anderen Sektoren) dem Projekt anschliessen, indem sie eine Schnittstelle nach der genannten Architektur aufbauen. Tatsächlich ist es heute möglich, Fotos, Videos oder weitere Anga-

1189 Nicholas/Weinberg, 5.
1190 Willard et al., 6; siehe auch Fix, 319 ff.
1191 Willard et al., 6.
1192 Willard et al., 6.
1193 Dabei handelt es sich nach Willard et al., 10, um einen Quellcode, der die APIs eines bestimmten Betreibers in die verwendeten Datenmodelle übersetzt. Solche Datenadapter können paarweise existieren: Es kann einen *Exporter* geben, der von der API des Betreibers in das Datenmodell übersetzt und einen *Importer*, der vom Datenmodell in die API des Betreibers übersetzt.
1194 Dabei handelt es sich gemäss Willard et al., 11, um Quellcode, der es Nutzerinnen ermöglicht, ihre Konten zu authentifizieren, bevor sie Daten von einem anderen Betreiber oder zu einem anderen Betreiber übertragen, bspw. OAuth.
1195 Willard et al., 10.
1196 Mit dem Protokoll OAuth wird eine sichere API-Autorisierung ermöglicht, siehe https://perma.cc/L3S6-33DJ. Mit dem Architekturstil REST sollen Ressourcen (bspw. ein Dokument) über eine anerkannte, sprachunabhängige und zuverlässig standardisierte Client/Server-Interaktion übertragen werden, siehe https://perma.cc/HXX3-BWEY.
1197 Willard et al., 8.
1198 Willard et al., 9; Fix, 320.
1199 Siehe https://perma.cc/U3FR-5W9G.

ben, die ein Nutzer bei einem Betreiber hinterlegt hat (einmalig oder periodisch) an einen anderen Betreiber zu übertragen.[1200] Auch wenn die *Data Transfer Initiative* keinen ausdrücklichen Bezug zum Datenschutzrecht herstellt, so ist es doch naheliegend, dass der Ansatz in seiner im Juli 2018 veröffentlichten Form als Reaktion auf die Vorgaben des europäischen Gesetzgebers zu werten ist.[1201] Praktisch ist die Bedeutung des Projekts bislang allerdings bescheiden und eine nennenswerte Fortentwicklung war in letzter Zeit nicht zu beobachten.[1202]

cc. *Europäischer Digital Markets Act (DMA)*

419 Die EU hat für digitale Dienste wie die sozialen Netzwerke spezielle Regelungen geschaffen. Namentlich hat sie mit dem DSA und dem DMA zwei Verordnungen erlassen, welche zum «reibungslosen Funktionieren des Binnenmarkts» beitragen sollen (Art. 1 Abs. 1 DSA und Art. 1 Abs. 1 DMA). Diese sehen für «Vermittlungsdienste» (DSA) resp. «zentrale Plattformdienste» (DMA) unterschiedliche Verpflichtungen vor. Nur der DMA enthält allerdings Vorgaben zur Portabilität von Daten, weshalb nachfolgend nur auf diesen einzugehen ist.

420 Der DMA nimmt Onlineplattformen und soziale Netzwerke gegenüber den privaten Nutzern in die Pflicht. Er gilt nur sehr eingeschränkt für sog. Torwächter (oft Englisch als «Gatekeeper» bezeichnet), welche zentrale Plattformdienste bereitstellen oder anbieten (Art. 1 Abs. 2 DMA). Die zentralen Plattformdienste umfassen, wie bereits erläutert, die Onlinedienste sozialer Netzwerke (Art. 2 Ziff. 2 lit. c DMA).[1203] Torwächter sind nach Art. 2 Ziff. 1 DMA diejenigen Unternehmen, die solche zentralen Plattformdienste bereitstellen und überdies nach Art. 3 DMA förmlich benannt worden sind. Eine Benennung durch die EU-Kommission erfolgt u.a., wenn ein Unternehmen gewisse Schwellenwerte erreicht und daher davon auszugehen ist, dass es erheblichen Einfluss auf den Binnenmarkt hat (Art. 3 Abs. 1 lit. a und Abs. 2 DMA).[1204] Daneben kann die EU-

1200 Siehe bspw. https://facebook.com/tyi. Die Funktion ist nur mit einem Konto zugänglich. Eine direkte Übertragung ist von Facebook an Google Photos, Dropbox, Google Docs, Koofr, Photobucket, Google Calendar, Daybook, Blogger, WordPress.com/Jetpack und Backblaze B2 möglich.

1201 FIX, 321; KRATZ, InTeR 2019, 29.

1202 FIX, 321.

1203 Dazu Rz. 47.

1204 Gegenwärtig sind die Unternehmen Alphabet, Amazon, Apple, Booking, ByteDance, Meta und Microsoft als Torwächter benannt, wobei deren Produkte TikTok, Facebook, Instagram und LinkedIn als Onlinedienste sozialer Netzwerke eingestuft werden, siehe https://perma.cc/36FH-6789.

Kommission unter den Voraussetzungen von Art. 3 Abs. 8 DMA weitere Unternehmen als Torwächter benennen und somit Nischenmärkte erfassen.[1205]

Der DMA ist eine neue Art «gatekeeper-spezifischer» Regulierung.[1206] Wie diese einzuordnen ist, ist umstritten. Vertreten wird, dass es sich beim DMA um eine neue Form von Regulierungsrecht handle, welche nicht mehr darauf abziele, einen Wettbewerb zu ermöglichen, sondern Unternehmen für die Erreichung bestimmter gesellschaftlicher Ziele in die Pflicht nehme.[1207] Folglich wird im DMA eine sektorspezifische Regulierung des (freilich unbestimmten) «digitalen Sektors» gesehen (siehe Art. 1 Abs. 1 DMA), der – in den Worten des EuGH – die zentralen Plattformdienste «in die Nähe einer wesentlichen Einrichtung» (*essential facility*) rücke.[1208] Zudem würden nicht nur solche Plattformen dem DMA unterstellt, die einer Monopolstellung zumindest nahe kommen, wie Betriebssysteme oder Suchmaschinen, sondern auch Dienste wie Video-Sharing-Plattformen oder Werbeservices. Eine solche breite Herangehensweise berücksichtige die vernetzte Natur der digitalen Märkte, in der Plattformdienste ein digitales Ökosystem und *walled gardens* bildeten.[1209] Eine isolierte Betrachtung einzelner Dienste würde die durch Daten getriebene Marktkonvergenz ignorieren, weshalb ein regulatorischer Ansatz das komplexe Netzwerk von Ökosystemen insgesamt erfassen müsse.[1210] Dieser Ansatz wirkt *ex ante*. Entsprechend wurde auch auf die kartellrechtliche Voraussetzung der Marktmacht verzichtet, da eine solche Analyse die Vielfalt der plattformbasierten Geschäftsmodelle nur unzureichend erfassen würde und die *bottleneck*-Wirkung der Unternehmen gerade auf deren Diversität zurückzuführen sei.[1211] Die Behörden beziehen sich stattdessen auf die im DMA festgelegten Schwellenwerte, wodurch eine aufwändige Einzelfallanalyse entfällt.[1212] 421

Der DMA will u.a. verhindern, dass Torwächter – und nur diese – die Bestreitbarkeit der zentralen Plattformdienste oder das Innovationspotenzial des dynamischen digitalen Sektors untergraben, indem sie einen Wechsel des Betreibers oder die Parallelverwendung mehrerer Dienste beschränken (Erw.G 59 422

1205 Magnin, Rz. 698.

1206 Podszun, Economics 2023, 2; siehe auch Mendelsohn/Budzinski, Rz. 19.

1207 Podszun, Economics 2023, 6.

1208 Podszun, Economics 2023, 7 m.H.a. EuGH T-612/17 vom 10. November 2021, Rz. 224; einen eigenständigen regulierungsrechtlichen Ansatz sieht hingegen Magnin, Rz. 704. Zur *essential facilities doctrine* Rz. 365.

1209 Podszun, Economics 2023, 7.

1210 Podszun, Economics 2023, 7.

1211 Europäische Kommission, DMA Impact Assessment Report, 47.

1212 Yildiz, Rz. 543.

DMA). Der DMA soll mithin Wechselkosten senken und Lock-In-Effekte verringern und einen Plattformwechsel ohne grossen Aufwand ermöglichen.[1213] Um dies zu erreichen, setzt der DMA nicht auf Generalklauseln und allgemeine Verbotsformeln, sondern auf einen grossen und in seinem Detailgrad variierenden Katalog aus unterschiedlichen Verboten und Pflichten für Torwächter.[1214] Im Zuge dessen ist auch ein unmittelbarer Zugang zu den Daten, die Endnutzer bereitgestellt haben oder die durch deren Tätigkeit im Zusammenhang mit den relevanten zentralen Plattformdiensten des Torwächters generiert wurden, vorgesehen (Erw.G 59 DMA): Art. 6 Abs. 9 DMA sieht eine Portabilität für Sach- und Personendaten vor. Torwächter sind verpflichtet, diese Daten kostenlos zu übertragen, können ihrerseits eine Übertragung aber nicht beantragen. Dank des weiten Geltungsbereichs kann die oft aufwändige Abgrenzung von Personen- und Sachdaten unterbleiben.[1215] Vom Recht umfasst ist auch der Echtzeitzugang zu den Daten, den u.a. APIs sicherstellen sollen.[1216] Zudem stellt der Wortlaut klar, dass auch beobachtete Daten erfasst sind, was unter der DSGVO, anders als unter dem DSG, nicht unbestritten ist.[1217] Begünstigt sind nur private Nutzer als Endnutzer, nicht aber die gewerblichen oder kommerziellen Nutzer oder andere Betreiber. Allerdings kann ein Endnutzer solche als Dritte beauftragen, woraufhin eine Übertragung möglich ist. Vom Begriff des Endnutzers umfasst sind zudem, anders als im Datenschutzrecht, auch juristische Personen, soweit sie nicht als gewerbliche Nutzer auftreten (Art. 2 Ziff. 20 DMA).

423 Der DMA enthält überdies Portabilitätsrechte für gewerbliche Nutzer und von diesen zugelassene Dritte. Nach Art. 6 Abs. 10 DMA muss der Torwächter diesen auf ihren Antrag hin kostenlos einen effektiven, hochwertigen und permanenten Echtzeitzugang zu aggregierten und nichtaggregierten Nutzungsdaten gewähren und deren Nutzung ermöglichen. Darunter fallen bestimmte Daten, die im Zusammenhang mit der Nutzung der zentralen Plattformdienste oder von bestimmten anderen Diensten bereitgestellt oder generiert werden (Art. 6 Abs. 10 DMA). Dies umfasst auch personenbezogene Daten. Der Zugang zu diesen darf jedoch nur dann gewährt oder ermöglicht werden, wenn sie unmittelbar mit der Nutzung der vom betreffenden gewerblichen Nutzer über den betreffenden zentralen Plattformdienst angebotenen Produkte oder Dienst-

1213 Yildiz, Rz. 937 m.w.N.
1214 Mendelsohn/Budzinski, Rz. 13.
1215 Duller, 168.
1216 Dazu Lazarotto, EJLT 2024, 8 f.
1217 Duller, 168; zur DSGVO Rz. 127.

leistungen durch die Endnutzer im Zusammenhang stehen und sofern der Endnutzer einer solchen Weitergabe zustimmt (Art. 6 Abs. 10 DMA).

Welche Daten unter dem DMA vom Portabilitätsrecht umfasst sind, ist noch unklar. Eine Praxis hat sich bislang nicht etabliert. Gefordert wird, dass zwischen den Interessen der Parteien abzuwägen sei und dabei namentlich auch die Innovationsanreize der Torwächter gebührend zu berücksichtigen seien.[1218] Erw.G 65 DMA hält hierzu fest, dass Verpflichtungen nach dem DMA auf das Mass beschränkt sein sollen, das erforderlich ist, um die Bestreitbarkeit zu gewährleisten und den schädlichen Auswirkungen der unfairen Praktiken von Torwächtern zu begegnen.[1219] Wie im Datenschutzrecht stellt sich zudem die Frage, ob abgeleitete Daten erfasst sind. Mit Blick auf etwaige negative Auswirkungen auf die Innovationsanreize und die Tatsache, dass diese Daten kaum «im Zusammenhang mit der Nutzung» des zentralen Plattformdienstes generiert werden, ist dies eher abzulehnen.[1220] 424

Bestimmte «nummernunabhängige interpersonelle Kommunikationsdienste» muss der Torwächter schliesslich interoperabel ausgestalten, sofern er diese Funktionen für die eigenen privaten Nutzer selbst bereitstellt (Art. 7 DMA). Darunter fallen Messengerdienste wie Signal oder WhatsApp. 425

Aufgrund der sich teilweise überschneidenden Anwendungsbereiche können sowohl die Portabilitätsrechte nach dem DMA als auch nach der DSGVO anwendbar sein. Der DMA hält dazu fest, dass dieser «unbeschadet der Vorschriften gelten [soll], die sich aus anderen Rechtsakten der Union zur Regelung bestimmter Aspekte der unter diese Verordnung fallenden Dienstleistungen ergeben, insbesondere der [DSGVO]» (Erw.G 12 DMA). Dies lässt darauf schliessen, dass die Portabilitätsrechte nach dem DMA keine *lex specialis* sein sollen.[1221] Erw.G 59 DMA hält ausdrücklich fest, dass die Verpflichtungen des Torwächters nach dem DMA das Recht auf Datenportabilität nach der DSGVO «ergänzen» sollen. 426

1218 Noch in Bezug auf den Vorschlag eines DMA siehe Monopolkommission, 45.

1219 Siehe Brandt/Grewe, MMR 2023, 930.

1220 Brandt/Grewe, MMR 2023, 930; gerade unter Einbezug des Wortlauts von Art. 20 DSGVO wohl eher befürwortend Duller, 169 ff.; ebenfalls befürwortend, gerade mit Blick auf den Wettbewerb Lazarotto, EJLT 2024, 8.

1221 Brandt/Grewe, MMR 2023, 931; siehe auch Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 8 f.

dd. Rechtslage in der Schweiz

427 In der Schweiz wurden spezialgesetzliche Vorgaben bei sozialen Netzwerken bislang abgelehnt. Der Bundesrat begründete dies 2013 damit, dass viele der auf verbreiteten sozialen Netzwerken vorhandenen Kundendaten bereits mitgenommen werden könnten und eine spezielle Pflicht «noch nicht» erforderlich sei.[1222] Er wollte die Entwicklung der sozialen Netzwerke jedoch beobachten und behielt sich vor, ein Recht zur Datenmitnahme einzuführen.[1223] In Betracht gezogen wurde gar eine Interoperabilitätsverpflichtung. So war der Bundesrat der Ansicht, dass es sich als sinnvoll erweisen könnte, die Schnittstellen zwischen verschiedenen sozialen Netzwerken zu regulieren und damit den grossen Plattformen vorzuschreiben, dass Nutzer auch mit Nutzern anderer Plattformen Daten und Nachrichten austauschen können müssen.[1224] In seiner erneuten Standortbestimmung 2017 sah er allerdings keinen Anlass für eine sektorielle Lösung und sprach sich gegen das datenschutzrechtliche Portabilitätsrecht aus.[1225] Dieses fügte, wie bereits ausgeführt, erst das Parlament in das DSG ein.

428 Der Bundesrat hat inzwischen erneut bekräftigt, dass er spezialgesetzliche Vorgaben als nicht notwendig erachtet, namentlich soll eine Umsetzung des DMA in der Schweiz nicht nötig sein.[1226] Der wirksame Wettbewerb werde auch auf digitalen Märkten primär mit dem geltenden kartellrechtlichen Rahmen sichergestellt und die gesetzlichen Bestimmungen liessen eine plattformspezifische Anwendung zu, weshalb der Bundesrat keinen unmittelbaren Handlungsbedarf sieht.[1227] Dies begründet er auch damit, dass zu erwarten sei, dass die grossen Onlineplattformen die neuen EU-Regeln in der Schweiz ebenfalls anwenden werden.[1228] Auch die Bundesverwaltung geht davon aus, dass die Bestimmungen des DMA grundsätzlich bereits durch die kartellrechtliche Missbrauchskontrolle nach Art. 7 KG abgedeckt werden können.[1229] Dennoch hat der Bundesrat jüngst eine gewisse Regulierung für Betreiber vorgeschlagen. Am 29. Oktober 2025 schickte er eine lange erwartete Vorlage für ein Bundesgesetz über Kommunikationsplattformen und Suchmaschinen in die

1222 Bundesrat, Bericht Social Media, 36.
1223 Bundesrat, Bericht Social Media, 75.
1224 Bundesrat, Bericht Social Media, 75.
1225 Bundesrat, Nachfolgebericht Social Media, 29 f.
1226 Motion Marti 23.3069, Stellungnahme Bundesrat.
1227 Motion Marti 23.3069, Stellungnahme Bundesrat.
1228 Motion Marti 23.3069, Stellungnahme Bundesrat.
1229 IK-EUDP, 11.

Vernehmlassung.[1230] Das neue Gesetz soll die Rechte der Nutzer von Kommunikationsplattformen und von Suchmaschinen stärken (Art. 1 VE-KomPG). Zudem soll es die Transparenz bezüglich deren Funktionsweise und Risiken fördern (Art. 1 VE-KomPG). Da sich die Vorlage inhaltlich am DSA orientiert,[1231] enthält sie jedoch keine Rechte der Nutzer zur Portierung ihrer Daten. Die Bearbeitung von Personendaten soll «nicht im Vordergrund des Vorentwurfs» stehen, wird aber auch nicht ausgeschlossen.[1232] Immerhin ist im VE-KomPG ein Datenzugang für Forschende vorgesehen. Diese sollen Zugang zu Daten beantragen können, wenn sich damit systemische Risiken erforschen lassen, die mit dem Betrieb von Kommunikationsplattformen und Suchmaschinen einhergehen (Art. 26 VE-KomPG). Es bleibt abzuwarten, ob die Räte weitergehenden Handlungsbedarf sehen.

b. Private und kommerzielle Nutzer

Kommerzielle Nutzer erhalten von privaten Nutzern eine unmittelbare Rückmeldung. Stellen Betreiber Analysetools bereit, können sie wichtige Informationen sammeln, etwa die Zahl der erreichten Nutzer, die Zahl der Interaktionen oder die Beliebtheit eines Beitrags.[1233] Betreiber ermöglichen zudem eine direkte Interaktion zwischen privaten und kommerziellen Nutzern, etwa in Form eines sog. Werbefolgekontakts, wenn private Nutzer eine Werbung weiter verfolgen (bspw. durch einen Klick auf die Werbung).[1234] Dabei kommt es zu (positiven) indirekten Netzwerkeffekten zwischen den beiden Akteuren, wobei diese asymmetrisch ausgestaltet sind, da intensivierte Werbung für private Nutzer nicht zwingend einen Vorteil darstellt.[1235] 429

Insofern können kommerzielle Nutzer als Verantwortliche durchaus Personendaten privater Nutzer bearbeiten. Diese fallen grundsätzlich unter das Recht auf Datenportabilität. Dennoch ist anzumerken, dass kommerzielle Nutzer nach der Rechtsprechung des EuGH Verantwortliche darstellen können, ohne dass sie Zugang zu den betreffenden Personendaten haben müssen.[1236] 430

1230 Bundesrat, Medienmitteilung vom 29. Oktober 2025.

1231 Das BAKOM verweist jedenfalls bezüglich der Rechtslage in der EU einzig auf den DSA, siehe BAKOM, Bericht Vernehmlassung VE-KomPG, 5; siehe bereits Bundesrat, Medienmitteilung vom 5. April 2023.

1232 BAKOM, Bericht Vernehmlassung VE-KomPG, 50.

1233 Golland, 13.

1234 BKartA, Beschluss B6-22/16 vom 6. Februar 2019, Rz. 220, dort am Beispiel Facebook.

1235 BKartA, Beschluss B6-22/16 vom 6. Februar 2019, Rz. 220 f. und 442, dort am Beispiel Facebook.

1236 EuGH C-210/16 vom 5. Juni 2018, Rz. 38.

In diesem Fall können sie einem Portabilitätsbegehren jedoch nicht nachkommen und müssen dies auch nicht, da die Daten nicht ihnen bekanntgegeben wurden.

3. Erkenntnisse und Überleitung

431 Das Feld der unterschiedlichen Akteure und relevanten Beziehungen ist bei sozialen Netzwerken überschaubar. In Bezug auf das Recht auf Datenportabilität sind es private Nutzer, die primär gegenüber Betreibern in der Rolle als Betroffene auftreten. Ebendiese Betreiber sind alte und potenziell neue Verantwortliche, wobei Übertragungen an andersartige Verantwortliche in weiteren Sektoren ebenfalls plausibel (und, wie gezeigt wird, wünschenswert) erscheinen.

432 Das Aufkommen von Internetplattformen und die Plattformisierung an sich führten im Sektor der sozialen Netzwerke zu besonderen wettbewerblichen Dynamiken. Gerade Betreiber nehmen daher in diesem Datenökosystem eine besondere Stellung ein. Wie in allgemeiner Weise bereits gezeigt, versucht das Recht auf Datenportabilität auf diese Dynamiken einzuwirken. Daher sind in einem nächsten Schritt die datenschutz- und wettbewerbsrechtlichen Ziele des Instituts im Kontext der sozialen Netzwerke zu würdigen.

B. Kritische Würdigung der Datenportabilität

1. Datenschutzrechtliche Ziele: Die Krux mehrerer betroffener Personen

433 Das Recht auf Datenportabilität wird der datenschutzrechtlichen Zielsetzung bei sozialen Netzwerken weitgehend gerecht. Die Betroffene kann in die Datenwirtschaft eingreifen und über die Zuordnung der sie betreffenden Daten (mit)entscheiden. Auch bei Annahme eines traditionellen Verständnisses des Rechts auf informationelle Selbstbestimmung wird der Betroffenen mit dem Recht auf Datenportabilität eine (eingeschränkte) Herrschaft über ihre Daten ermöglicht. Dies gilt auch für die sozialen Netzwerke.

434 Allerdings zeigen sich in diesem Sektor Unzulänglichkeiten bezüglich der Daten, die vom Recht auf Datenportabilität umfasst sind und von den Betroffenen herausverlangt werden können. Denn gerade bei sozialen Netzwerken gibt es regelmässig mehrere betroffene Personen. Dies kann die Ausübung des Rechts

auf Datenportabilität erschweren, da es einer Betroffenen einzig erlaubt, die *sie betreffenden* Personendaten herauszuverlangen.

Zwar ist das Recht nach hier vertretener Ansicht mit Blick auf die *ratio legis* und die von Beginn weg anvisierten sozialen Netzwerke extensiv auszulegen. Umfasst sind damit auch Daten mit Doppelbezug[1237] und dabei auch solche, die von Dritten bekanntgegeben wurden, sich aber nicht sinnvoll von der Betroffenen trennen lassen[1238]. Problematisch ist jedoch selbst dann, dass Inhalte in sozialen Netzwerken in besonderem Mass in einen Kontext eingebettet sind, der aus anderen Inhalten besteht und auf diese reagiert (bspw. «Gefällt mir»-Button) und mit ihnen interagiert (bspw. eine Kommentarfunktion).[1239] Die dem Portabilitätsrecht unterliegenden Daten lassen sich kaum sinnvoll herauslösen, ohne dass sie für die Betroffene an Wert verlieren.[1240] Da entsprechende Anreize fehlen, üben Betroffene ihr Recht weniger aus. Denn selbst bei einem extensiven Verständnis der Datenportabilität sind die herauszugebenden Daten für Betroffene kaum weiterverwendbar, da bei der neuen Verantwortlichen die wichtige kontextuelle Einbettung i.d.R. fehlt. 435

Zurecht wird daher bezweifelt, ob Personendaten mit einem Bezug zu Drittpersonen der Betroffenen überhaupt einen Vorteil bringen, wenn sie diese überträgt.[1241] Die Drittperson müsste im Fall von sozialen Netzwerken ebenfalls bei der neuen Verantwortlichen registriert sein, und überdies müsste deren Angebot technisch genügend kompatibel sein, um aufgrund der portierten Daten den Bezug zu dieser Drittperson abzubilden.[1242] Dies wäre etwa dann der Fall, wenn eine umfassende Interoperabilität zwischen Betreibern vorläge.[1243] Damit erscheint der Vorbehalt der Direktübertragung an eine neue Verantwortliche bei Unverhältnismässigkeit, d.h. einer technischen Unmöglichkeit (Art. 21 Abs. 3 DSV), ebenfalls in einem neuen Licht, da in solchen Fällen möglicherweise nicht der Übertragungsvorgang, sondern die anschliessende Darstellung bei der neuen Verantwortlichen technisch unmöglich ist.[1244] 436

Insgesamt können die portierten Daten der Betroffenen in den überwiegenden Fällen der sozialen Netzwerke nur, aber immerhin, für eine Archivierung die- 437

1237 Dazu Rz. 185 ff.
1238 Dazu Rz. 191 ff.
1239 Dazu am Beispiel Facebook BKartA, Beschluss B6-22/16 vom 6. Februar 2019, Rz. 472.
1240 Ähnlich auch Steffen/Wieworra/Kroon, 72.
1241 Füllsack/Kirschke-Biller, Rz. 239.
1242 Füllsack/Kirschke-Biller, Rz. 239.
1243 Dazu Rz. 457 ff.
1244 Ebenso für die im Wesentlichen gleiche Lage unter der DSGVO Füllsack/Kirschke-Biller, Rz. 239.

nen.[1245] Dies gilt selbst dann, wenn die Daten gestützt auf Art. 28 Abs. 2 DSG direkt an eine neue Verantwortliche (bspw. einen Archivdienst oder eine Cloud) übertragen werden. Dieses Ergebnis reicht in Bezug auf die persönlichkeitsbezogene, rein datenschutzrechtliche Perspektive jedoch aus, um davon auszugehen, dass die Grundlagen für eine datenschutzrechtliche Zielerreichung des Portabilitätsrechts geschaffen werden. Die Betroffene ist im Vergleich zur Situation ohne Portabilitätsrecht in einer Position der Stärke: Sie ist «diejenige, die eine 360-Grad-Sicht über sich selbst hat und alle Daten hat, die irgendwelche Leute über sie gesammelt haben».[1246]

2. Wettbewerbsrechtliche Ziele

a. Netzwerkeffekte und Lock-In bei gleichartigen Betreibern

438 Hinsichtlich der wettbewerbsrechtlichen Ziele sind Zweifel angebracht, ob Lock-In-Effekte und die hohen Wechselkosten tatsächlich darauf beruhen, dass private Nutzer ohne Portabilitätsrecht nur darum nicht den Betreiber wechseln, weil sie keinen Zugang zu den sie betreffenden Daten haben.[1247] Dies wurde bereits bei den wettbewerbsrechtlichen Zielen allgemein festgestellt, trifft aber besonders auf den im Gesetzgebungsprozess präsenten Anwendungsfall der sozialen Netzwerke zu.[1248] Für diesen wird vorgebracht, dass Netzwerkeffekte dafür verantwortlich seien, dass Nutzer nicht wechselten.[1249] Dabei ist ein Wechsel zwischen zwei gleichartigen Betreibern von einem Wechsel von einem Betreiber zu einem andersartigen Anbieter zu unterscheiden. Nachfolgend wird zunächst die Situation zwischen gleichartigen Betreibern geschildert.

439 Gerade bei diesen verhindert eine erleichterte Übertragung von Daten einen *Lock-In* nur begrenzt. Deutlich äusserte sich hierzu das BKartA in seinem Be-

1245 So das BKartA, Beschluss B6-22/16 vom 6. Februar 2019, Rz. 472.

1246 Votum NR Glättli AB 2019 N 1815, noch im Kontext einer vorgeschlagenen weiterreichenden Datenportabilität, die sämtliche Personendaten der betroffenen Person umfasst hätte.

1247 Dieses Problem akzentuiert sich, wenn davon ausgegangen wird, dass Daten mit Doppelbezug nicht unter das Recht auf Datenportabilität fallen oder die enge Auslegung vertreten wird, wonach nur die die portabilitätsanfragende Person betreffenden Daten herausgegeben werden müssen, unter Entfernung jeglichen Kontexts.

1248 Dazu Rz. 306; in diese Richtung auch BKartA, Beschluss B6-22/16 vom 6. Februar 2019, Rz. 448, dort konkret am Beispiel Facebook; ähnlich auch THOUVENIN/WEBER/FRÜH, 173.

1249 FIX, 79 f.; KRATZ, InTeR 2019, 29; ZSCHOCH, 271.

schluss zu Facebook: Wenn ein Nutzer auf Aktivitäten anderer Nutzer reagiert habe, etwa durch Teilen oder Kommentieren von Inhalten, lasse sich die Aktivität des Nutzers nicht sinnvoll von den Inhalten trennen, auf die sich die Aktivität bezogen hat oder die sich auf die Aktivität beziehen.[1250] Aus diesem Grund sei ein Extrahieren der Aktivitäten des Nutzers «mit der Grundidee eines sozialen Netzwerks, das ja gerade die Interaktionen zwischen den Nutzern ermöglicht, kaum vereinbar».[1251] Es liege damit an der Grundkonstruktion eines sozialen Netzwerks, dass die Mitnahme der eigenen Aktivitäten von einem sozialen Netzwerk zu einem anderen sozialen Netzwerk nur eingeschränkt möglich sei.[1252] Der Lock-In-Effekt beruht also nicht nur auf den einen selbst betreffenden Personendaten. Diese Unzulänglichkeit nahmen die Gesetzgeber jedoch sowohl in der EU als auch in der Schweiz in Kauf und mit ihr das Risiko, dass für den Nutzer als betroffene Person relevante Daten nicht vom Recht auf Datenportabilität umfasst sind.

Ein Nutzer verbleibt primär aufgrund der Netzwerkeffekte auf einem sozialen Netzwerk. Deren Wirkung vermag das Recht auf Datenportabilität allerdings kaum zu beeinflussen.[1253] Zwar zeigt eine Erhebung, dass ein möglicher Datenverlust Nutzer sozialer Netzwerke durchaus an einem Wechsel hindern kann.[1254] In der gleichen Erhebung gaben aber weniger als 10 % der Befragten an, dass sie bei vergangenen Wechseln eines sozialen Netzwerks gerne Daten mitgenommen hätten.[1255] Es ist daher davon auszugehen, dass das Recht auf Datenportabilität einzig diejenigen (zusätzlichen) Netzwerkeffekte, die dadurch entstehen, dass die Daten bereits bei einem Anbieter sind, beeinflusst.[1256] Den überwiegenden Teil der Netzwerkeffekte, die in einem userinduzierten *Lock-In* resultieren, dürfte das Portabilitätsrecht aber kaum berühren.[1257] 440

1250 BKartA, Beschluss B6-22/16 vom 6. Februar 2019, Rz. 470.

1251 BKartA, Beschluss B6-22/16 vom 6. Februar 2019, Rz. 470.

1252 BKartA, Beschluss B6-22/16 vom 6. Februar 2019, Rz. 470.

1253 Fix, 80; Weber/Thouvenin, 65; ähnlich auch Götzinger/Vasella, SZW 2021, 45; darauf hinweisend, dass mit der Ausübung des Rechts auf Datenportabilität zumindest durch den Datentransfer Netzwerkeffekte reduziert werden, die durch den Datensatz beim alten Verantwortlichen ansonsten wirkten Martinelli, 139; Krämer/Senellart/De Streel, 9, nach welchen nur mit interoperablen Diensten der Lock-In-Effekt verringert würde.

1254 Luzsa et al., 19 und 22. Dieser Faktor wurde von den 445 befragten Personen leicht weniger wichtig bewertet wie der mögliche Verlust von Kontakten, wenig Wissen über alternative Dienste und wenig Wechselerfahrung.

1255 Luzsa et al., 23. Konkret lag der Anteil bei nur 8.6 % und damit deutlich tiefer als etwa beim Wechsel einer Cloud (16.0 %) aber in der gleichen Grössenordnung wie bei Streaminganbietern (6.8 %).

1256 Martinelli, 139.

1257 Dies kann aber ausreichen, da die Schwelle für die Geeignetheit einer Massnahme äusserst tief anzusetzen ist, namentlich bereits dann, wenn sie in Bezug auf das verfolgte Ziel nicht

441 Damit ist festzuhalten, dass das Recht auf Datenportabilität einen Wechsel sozialer Netzwerke insgesamt zwar etwas erleichtert (und nicht etwa erschwert). Private Nutzer werden aber eher nicht von einem Betreiber zu einem anderen (gleichartigen) Betreiber wechseln, solange alle Kontakte beim alten Betreiber sind.[1258] Möchten sie es trotzdem tun, so erleichtern ihr die rechtlichen Vorgaben immerhin die Datenmitnahme.[1259] Für private Nutzer senkt dies die Wechselkosten. Bei einer Gesamtbetrachtung schafft das Recht auf Datenportabilität zwischen gleichartigen Betreibern jedoch nicht die Grundlagen dafür, dass ein *Lock-In* der privaten Nutzer ausbleibt.[1260] Dafür scheinen die Netzwerkeffekte zu stark.

b. Weniger Netzwerkeffekte und Lock-In bei andersartigen Betreibern

442 Geht man allerdings der Idee eines *Open Web* folgend davon aus, dass das Recht auf Datenportabilität nicht nur auf gleichartige, sondern zumindest *auch* auf andersartige Anbieter ausgerichtet ist,[1261] so ergibt sich gerade für plattformbasierte soziale Netzwerke eine neue Sichtweise, da im Verhältnis zwischen Betreibern und andersartigen Anbietern (z.B. einem sozialen Netzwerk und einer Datingapp oder einem auf Sport fokussierten sozialen Netzwerk und einem Hausarzt) Netzwerkeffekte nur eine untergeordnete Rolle spielen. Aus diesem Blickwinkel ist es unproblematisch, dass zwischen gleichartigen sozialen Netzwerken starke Netzwerkeffekte einen Wechsel beeinflussen, da das Recht auf Datenportabilität nicht zwingend auf diese Beziehung abzielt. Zwischen andersartigen Anbietern dürfte ein Lock-In-Effekt kaum auf

---

wirkungslos oder gar kontraproduktiv ist, siehe dazu WEBER/THOUVENIN, 65; ausführlich HOFSTETTER, 143 f.

1258 Dazu allgemein Rz. 306, wobei freilich bereits eine «allgemeine» Betrachtung oft die sozialen Netzwerke im Blick hat.

1259 Auf Plattformen allgemein bezogen ENGELS, Internet Policy Review 2016, 7; ähnlich FIX, 80; siehe auch die Anmerkungen des BKartA, wonach zumindest bei Facebook die extrahierbaren Daten «praktisch nicht nutzbar» seien, weil es auch an einer Importmöglichkeit an andere Netzwerke fehle. Die exportierten Daten dienten somit eher der Archivierung als der Portabilität, BKartA, Beschluss B6-22/16 vom 6. Februar 2019, Rz. 472.

1260 Ähnlich DURCHHOLZ, PinG 2024, 210; ZSCHOCH, 271. Diese Sichtweise wird dadurch gestützt, dass sich bislang faktisch keine anderen Betreiber auf dem Markt etablieren konnten, obwohl bereits seit 2010 einzelne soziale Netzwerke die Möglichkeit der Datenmitnahme anbieten, siehe NICHOLAS/WEINBERG, 1. Entsprechend gibt es keine Indikatoren, dass eine Senkung der Wechselkosten die Markteintrittsschranke für gleichartige Betreiber verringern würde.

1261 So KRATZ, InTeR 2019, 29; ebenfalls Votum NR Glättli, AB 2019 N 1815; dazu ausführlich bereits Rz. 86 ff. sowie Rz. 320 ff.

Netzwerkeffekte zurückzuführen sein.[1262] Stattdessen kann ein Wechsel durchaus davon abhängen, ob die Betroffene ihre Daten mitnehmen kann. Der *Lock-In* ist mithin daten- und nicht userinduziert. Die vom Recht auf Datenportabilität vorgesehene Möglichkeit zur Datenmitnahme senkt daher die Wechselkosten.[1263]

c. Besondere Relevanz von «winner-takes-it-all»-Märkten

Womöglich ist allerdings gerade bei den sozialen Netzwerken nicht die Unterscheidung zwischen gleichartigen Betreibern und andersartigen Anbietern wichtig, sondern vielmehr, dass viele der Unternehmen, welche von starken Netzwerk- und Lock-In-Effekten profitieren, auf einem «winner-takes-it-all»-Markt tätig sind und in diesem die «Gewinner» darstellen. Kippt ein Markt irreversibel, wächst einem Akteur der gesamte Markt zu und es liegt ein Gewinnermarkt vor.[1264] Diese Konstellation ist in der Datenwirtschaft häufig[1265] und betrifft zumeist Plattformen, oft soziale Netzwerke. Ausschlaggebend für das Kippen und einen Gewinnermarkt können zwar durchaus Netzwerk- oder Lock-In-Effekte sein, welche dazu beitragen, dass Wettbewerber von einem Markteintritt absehen.[1266] Legt man den Fokus jedoch nicht bloss auf diese Effekte, sondern auf den daraus resultierenden Gewinnermarkt, liesse sich mit einer darauf ausgerichteten Ausgestaltung des Portabilitätsrechts dort ansetzen, wo dies aus wettbewerblicher Sicht erforderlich erscheint. 443

Soll das Portabilitätsrecht jedoch der Entstehung eines Gewinnermarkts vorbeugen, so bleibt vom Recht auf Datenportabilität, wie es *de lege lata* existiert, nur noch wenig übrig. Es müsste gewichtige Präzisierungen aufweisen, die es kaum noch erlaubten, das Institut im DSG zu verankern. Namentlich könnte es nicht mehr auf sämtliche Marktteilnehmende anwendbar sein und damit parallel andere – datenschutzrechtliche – Zielsetzungen adressieren. Vielmehr wäre stets vorab zu prüfen, ob tatsächlich eine «winner-takes-it-all»-Konstellation bei einem Akteur vorliegt, d.h. ob die portabilitätsverpflichtete Person bestimmte Eigenschaften auf dem Markt erfüllt. Die EU wählte eine solche Lösung mit dem DMA, welcher an die Gatekeeper-Eigenschaft von Unterneh- 444

1262 Ähnlich auch Fix, 80 f.
1263 Engels, Internet Policy Review 2016, 8, die von «complementary platforms» spricht.
1264 Heinemann, ius.full 2021, 178.
1265 Furman et al., 56; Picht, IIC 2020, 946.
1266 Furman et al., 35.

men, die zentrale Plattformdienste bereitstellen, anknüpft und eine Portabilitätsverpflichtung nur dieser Gatekeeper vorsieht (Art. 6 Abs. 9 DMA).[1267]

445 Diese Lösung hängt direkt mit den vom datenschutzrechtlichen Portabilitätsrecht beabsichtigten Zielen zusammen. Wie im Mobilitätssektor ebenfalls zu diskutieren sein wird,[1268] hat die deutsche Kommission Wettbewerbsrecht 4.0 bereits in der Vergangenheit eine auf marktbeherrschende Unternehmen beschränkte Stärkung der Nutzerrechte auf Datenportabilität vorgeschlagen, namentlich um zu verhindern, dass kleinere Wettbewerber aufgrund der starken Netzwerkeffekte von «Gewinnern» verdrängt werden.[1269] Aus diesem Grund schlug sie auch eine Pflicht zur Verwendung interoperabler Datenformate und zur Gewährleistung einer Echtzeitübertragung von Daten vor.[1270] Auch der sog. Furman-Report, der als wegweisend für den DMA gilt, sprach sich für Verpflichtungen für Unternehmen mit einem «strategischen Marktstatus» aus.[1271] Ein weiterer Bericht zuhanden der EU-Kommission gab zu bedenken, dass aus wettbewerbspolitischer Sicht strengere Portabilitätsvorgaben für marktbeherrschende Unternehmen angezeigt sein könnten.[1272] Diese Vorschläge wurden in der EU im Wesentlichen im DMA umgesetzt, was insb. bedeutet, dass nicht nur Personendaten von der Regelung umfasst sind. Damit setzt der Unionsgesetzgeber gerade für die in der Datenwirtschaft wichtigen plattformbasierten sozialen Netzwerke dort an, wo eine Wirkung erhofft wird, nämlich bei den marktmächtigen Internetplattformen. Damit lassen sich umgekehrt nachteilige Auswirkungen verhindern, die sich bei einer generellen Verpflichtung von nicht marktbeherrschenden Unternehmen ebenfalls ergeben können.[1273]

d. Allgemeine Wettbewerbs- und Innovationsförderung

446 Gerade bei andersartigen Anbietern und besonders solchen, die in einem anderen Sektor tätig sind (etwa der Mobilität oder dem Gesundheitswesen), ist zudem die Zielsetzung der allgemeinen Wettbewerbs- und Innovationsförderung bedeutsam. Dabei handelt es sich nach hier vertretener Ansicht um das primäre wettbewerbsrechtliche Ziel.[1274] Während ein Wechsel zwischen

1267 Dazu Rz. 419 ff.
1268 Dazu Rz. 667 ff., insb. 671.
1269 Schallbruch et al., 41 und 52 ff., insb. 54.
1270 Schallbruch et al., 41.
1271 Furman et al., 5.
1272 Crémer/De Montjoye/Schweitzer, 58 und 82.
1273 Schallbruch et al., 55. So besteht die Gefahr, dass grössere Betreiber Zugang zu Datenpools kleinerer Anbieter erhalten und somit ihre Marktstellung verfestigen können.
1274 Dazu Rz. 320 ff.

gleichartigen Betreibern (zumindest theoretisch) kaum an der Mitnahmemöglichkeit der Betroffenen scheitert, kann dies bei andersartigen Anbietern durchaus der Fall sein. Auch wenn – oder eben gerade, *weil* – kein Wettbewerbsverhältnis existiert, profitieren andersartige Anbieter besonders von der Ausübung des Rechts auf Datenportabilität.[1275] Betroffene Personen können dadurch sie betreffende Daten weitgehend hindernisfrei an andere Anbieter übertragen (lassen), ohne dass Netzwerkeffekte ein Wechselhindernis darstellen.[1276] Dies schafft die Grundlagen, um den Wettbewerb und die Innovation zu fördern. Denn neue Verantwortliche haben weniger hohe Hürden zu überwinden und sind imstande auf Datensätze zuzugreifen, die ihnen sonst versperrt blieben. Diese Datensätze können Ausgangspunkt für neue Angebote sein oder ein bestehendes Angebot effizienter machen. Dieser Zugang zu grösseren Datenpools sollte in der Schweiz gerade kleineren einheimischen Unternehmen zugutekommen.[1277]

Das Gesagte kann, anders als bei einem Wechsel zwischen gleichartigen Betreibern, auch für Nutzungsdaten gelten: Gerade andersartige Anbieter können ihr Angebot auf den Nutzungsdaten eines oder mehrerer Betreiber aufbauen. Dies gilt selbst dann, wenn die Daten dem privaten Nutzer zuvor nicht bekannt waren. Dabei kann von Belang sein, dass private Nutzer bei einem Wechsel datenschutzfreundlichere Betreiber bevorzugen[1278] und umgekehrt Betreiber den Standort Schweiz als datenschutzfreundlich und damit attraktiv wahrnehmen.[1279] Insgesamt schafft das Recht auf Datenportabilität also bei andersartigen Anbietern die Grundlagen dafür, dass Lock-In-Effekte verringert, Wechselkosten gesenkt und eine allgemeine Wettbewerbs- und Innovationsförderung angeregt werden können. Relativierend ist indes daran zu erinnern, dass bislang keine Angebote ersichtlich sind, welche sich aus der bereits seit 447

1275 Siehe Krämer/Senellart/De Streel, 9.

1276 Etwa an die erwähnte Ärztin, dazu Rz. 416.

1277 Dies hängt allerdings von der betroffenen Person ab. Weitergehend Rz. 322.

1278 Luzsa et al., 21. In Bezug auf Social Media nannten 73.2 % der befragten Personen Sorgen um Datenschutz und Privatsphäre. 77.1 % gaben ferner an, dass wenig Vertrauen in den aktuellen Anbieter ein Motiv für den Wechselwunsch sei.

1279 So wirbt die Firma Proton, die u.a. über einen Mailservice verfügt und Cloudlösungen anbietet etwa besonders mit ihrem Schweizer Standort, siehe https://perma.cc/Y3PN-3FWN. Der Schweizer Messengerdienst Threema wirbt ebenfalls damit, dass die Anforderungen der DSGVO und dem DSG eingehalten würden. Zudem wird hervorgehoben, dass US-amerikanische Gesetze keine Anwendung fänden, siehe https://perma.cc/HH79-DBG7.

längerem bestehenden Möglichkeit zur Datenmitnahme ergeben hätten.[1280] Von praktischer Bedeutung erscheint vielmehr das Phänomen der Plattformisierung.

e. In Bezug auf die Plattformisierung

448 Die Plattformisierung ermöglicht es Betreibern, in andere Teile des Netzes zu expandieren und weitere Daten zu beschaffen.[1281] Das Recht auf Datenportabilität wollte dieser Entwicklung Einhalt gebieten, was sich in den wettbewerbsrechtlichen Zielsetzungen zeigt.

449 Es ist jedoch unklar, ob das Recht auf Datenportabilität als Gegengewicht zur zunehmenden Plattformisierung bei sozialen Netzwerken funktionieren kann. Diese ist bei sozialen Netzwerken heute in Form von API-Anbindungen gängige Praxis. So stellt es eine Form von Plattformisierung dar, wenn sich ein privater Nutzer mit seinem Account, den er bei einem Betreiber angelegt hat, bei einem Drittanbieter anmeldet.[1282] Die Plattformisierung senkt zwar die Wechselkosten, ist dabei aber einseitig auf die Interessen der Betreiber ausgerichtet und dient primär diesen.[1283] Zudem wirkt sie vorwiegend für andersartige Anbieter und damit komplementäre Angebote.

450 Daneben fördern Ansätze wie die *Data Transfer Initiative* eine standardisierte Datenportabilität, die ohne proprietäre Formate auskommt und grundsätzlich allen Interessierten offenstehen soll. Mit ihr soll auch der Wechsel zwischen gleichartigen Betreibern möglich sein. Bei dieser Open-Source-Lösung handelt es sich um einen ersten Schritt in Richtung Interoperabilität.[1284] Ob sie der Plattformisierung jedoch noch zusätzlich Vorschub leistet oder die Grundlagen für die Erreichung der wettbewerbsrechtlichen Ziele des Datenportabilitätsrechts schaffen kann, hängt von der konkreten und vor allem dauerhaften Umsetzung durch die Betreiber ab. Solange Dritte auf den Goodwill des Betreibers eines sozialen Netzwerks angewiesen sind, ist davon auszugehen, dass

---

1280 Kritisch hierzu auch NICHOLAS/WEINBERG, 5 f. und 12 ff. In ihrer Studie führten sie einen Datenexport bei Facebook durch und befragten anschliessend Softwareentwickler und Produktmanager, welche neuen Produkte oder Angebote aus dem Datensatz entstehen könnten. Diese befanden den Wert des Datensatzes für gering.

1281 Dazu Rz. 53 ff.

1282 Siehe https://developers.tiktok.com/ (TikTok), https://learn.microsoft.com/en-us/linkedin/ (LinkedIn), https://developers.facebook.com/docs/instagram-platform/instagram-api-with-facebook-login (Instagram), https://developers.facebook.com/docs/graph-api/ (Facebook).

1283 NICHOLAS, MTLR 2021, 274.

1284 BeckKomm-HERBST, Art. 20 DSGVO N 20.

die Plattformisierung weiter fortschreitet.[1285] Auch wenn namhafte soziale Netzwerke und andere grosse Unternehmen an der Initiative teilnehmen und eigene Schnittstellen zur Verfügung stellen, so funktioniert dies nur so lange, wie sich die beteiligten Unternehmen von ihrer Teilnahme einen höheren Nutzen versprechen als von einer Geheimhaltung.[1286] Freilich ist einzuräumen, dass die existierenden Anbindungen rege genutzt werden und die Basis für zahlreiche Angebote darstellen. So ist eine automatisierte periodische Übertragung möglich und die auf wenigen Klicks basierende Umsetzung erscheint intuitiv und benutzerfreundlich.

Dies ist beim Portabilitätsrecht nicht der Fall. Es vermag der Expansion und Datenbeschaffung (grosser) Betreiber bislang kaum etwas entgegenzusetzen. Denn Betreiber sind aufgrund des Rechts auf Datenportabilität nicht gehalten, ihr Verhalten anzupassen. Vielmehr erhalten sie sogar die rechtliche Möglichkeit, bei Portabilitätsanfragen als neue Verantwortliche auf der Empfängerseite zu stehen, wenn Betroffene eine Übertragung an sie wünschen, was aufgrund der direkten Netzwerkeffekte bei grossen Betreibern oft der Fall sein dürfte. Immerhin lässt sich einwenden, dass die Entscheidung über den Zugang zu bestimmten Personendaten und die Übertragung ebendieser zu Dritten unter dem Portabilitätsrecht nur der betroffenen Person zusteht.[1287] 451

Womöglich könnte der Plattformisierung aber insofern entgegengetreten werden, als ein Dritter, der bislang zur Erbringung einer eigenen Dienstleistung die Personendaten seiner Kunden über eine API-Anbindung an die Plattform eines Betreibers erhalten hatte, nun die alternative Möglichkeit hat, solche Daten auf Wunsch der Betroffenen an ihn übertragen zu lassen und anschliessend entkoppelt vom Betreiber zu nutzen. Damit könnten Dritte vermehrt in einen Markt eintreten, ohne dabei an einen Plattformbetreiber gebunden und von diesem, wie gezeigt,[1288] abhängig zu sein. 452

Das Recht auf Datenportabilität vermag die Vorzüge, welche die Plattformisierung Dritten bietet, kaum umfassend zu kompensieren. Denn für Dritte entsteht bei einer Plattformisierung wenig Aufwand. Sie müssen ihr Angebot lediglich in die API des Betreibers einbinden. Dieser übernimmt einen grossen Teil der technischen Umsetzung: Er stellt das erforderliche infrastrukturelle Modell und einen umfassenden technologischen Rahmen bereit, auf dem 453

1285 Dazu Rz. 55.

1286 Fix, 321.

1287 Wobei auch eine stellvertretende Ausübung durch die neue Verantwortliche zulässig wäre, siehe Rz. 218.

1288 Zur problematischen Abhängigkeit zu einem Plattformbetreiber Rz. 55 f.

Dritte ihr Angebot aufbauen können.[1289] Dadurch können Dritte neuartige Angebote schaffen oder solche durch die Kombination mehrerer Angebote als API-Mashup kreieren.[1290]

454 So weit geht das Recht auf Datenportabilität nicht: Es muss keine direkte Einbindung in die Infrastruktur des alten Verantwortlichen erfolgen und ein Zugang zu dessen Plattform wird nicht gewährt. Womöglich wäre dies aber nötig, um der Plattformisierung entgegenzutreten. Vielfach dürfte ein Echtzeitzugang zu den Daten notwendig sein. Denn besonders komplementäre datengetriebene Angebote sind regelmässig auf einen Echtzeitzugang zu den Daten angewiesen, um ihr Angebot zu ermöglichen.[1291]

f. Förderung des freien Datenflusses

455 Das Portabilitätsrecht verfolgt schliesslich bei sozialen Netzwerken ebenfalls datenpolitische Ziele, namentlich soll es einen freien Datenfluss fördern. Dies gilt sowohl für den Datenfluss zwischen gleichartigen Betreibern als auch zu andersartigen Anbietern. Das Institut vereinfacht generell die Möglichkeit, Daten auszutauschen. Dies war gerade für Internetplattformen wie soziale Netzwerke beabsichtigt, die besonders als Datensilos oder *walled gardens* wahrgenommen wurden, welche über viele Daten verfügten, diese aber kaum zur Verfügung stellten.[1292] Damit trägt das Institut zudem der Zielsetzung des *Open Web* Rechnung. Abgesehen davon, dass die sozialen Netzwerke im Gesetzgebungsprozess besonders im Fokus standen, wirkt sich diese Zielsetzung aber nicht besonders auf sie aus: Der Förderung des freien Datenflusses ist inhärent, dass sie für sämtliche Akteure des (digitalisierten) Wirtschaftslebens gilt und nicht bloss sektoriell.

3. Mögliche Handlungsspielräume

456 Nach dem Gesagten drängen sich mit Blick auf die datenschutz- und wettbewerbsrechtlichen Ziele und Unzulänglichkeiten zwei Handlungsspielräume auf. Möglich wäre einerseits, das Portabilitätsrecht hin zu einer Echtzeitübertragung und in Richtung einer Interoperabilität weiterzuentwickeln. Anderer-

1289 Helmond, SM+S 2015, 8.

1290 Dazu Rz. 55.

1291 Schweitzer, GRUR 2019, 574.

1292 Votum NR Glättli, AB 2019 N 1813, der davon sprach, dass neue, auch kleinere Unternehmen die Möglichkeit haben sollten, eine neue Datenwirtschaft zum Wohle aller zu schaffen.

seits liessen sich spezifische Portabilitätsrechte umsetzen. Diese könnten beschränkt sein auf einzelne Betreiber, welche bestimmte (wettbewerbsrechtliche) Voraussetzungen erfüllen. Da die europäische Gesetzgebung mit dem DMA bereits eine spezialgesetzliche Umsetzung liefert, liegt es nahe, dass entsprechende Anpassungen in der Schweiz ebenso auf spezialgesetzlichem Weg erfolgen würden. Zunächst sind jedoch lediglich die für diesen Sektor denkbaren Handlungsspielräume aufzuzeigen.

a. Fortentwicklung der datenschutzrechtlichen Portabilität in Richtung Interoperabilität

Die Problematik mehrerer betroffener Personen liesse sich in datenschutzrechtlicher Hinsicht dadurch beheben, dass zwischen sozialen Netzwerken eine umfassende Interoperabilität angestrebt wird.[1293] Eine Bildkommentierung Dritter verlöre ihre soziale Einbettung nicht, wenn das dazugehörige Bild auf ein anderes soziales Netzwerk übertragen würde. Dabei ist Interoperabilität ein Zielzustand, auf welchen hinzuarbeiten ist, etwa durch Vorgaben zur Anbindung an APIs oder durch einen Echtzeitzugang zu Daten auf sozialen Netzwerken. Ähnliche Regelungen sehen sowohl die DV[1294] als auch der DMA bereits vor. 457

Gleichzeitig könnten solche Vorgaben hinsichtlich der wettbewerbsrechtlichen Ziele eine Veränderung bewirken. So würden damit die Wechselkosten weiter gesenkt – mehr zumindest als dies aktuell bei einer Einmalübertragung der Fall ist.[1295] Eine Interoperabilität könnte *Multi-Homing* ermöglichen und einen (userinduzierten) Lock-In-Effekt verhindern, weil ein Wechsel für Nutzer gar nicht mehr nötig wäre.[1296] Dies hätte auch Auswirkungen auf die Netzwerkeffekte, die bislang dafür sorgten, dass Nutzer kein Interesse an einem Betreiberwechsel hatten und so den userinduzierten *Lock-In* erst verursachten.[1297] Netzwerkeffekte könnten dadurch marktweit zur Geltung kommen und somit für einzelne Betreiber relativierend wirken.[1298] Eine solche Annäherung an eine Interoperabilität verspricht zudem niedrigere Markteintrittshürden 458

1293 Europäische Kommission, Free Flow, 48; Graef, Telecommunications Policy 2015, 509 und *passim*.

1294 Ausführlich dazu am Beispiel des Mobilitätssektors Rz. 604 ff.

1295 Nicholas, MTLR 2021, 273.

1296 Zschoch, 272.

1297 Graef, Telecommunications Policy 2015, 510; Kerber/Schweitzer, JIPITEC 2017, 52.

1298 Graef, Telecommunications Policy 2015, 510; Kühling/Hildebrandt/Bulowski, K&R 2022, 673; kritisch aber bezüglich des Einflusses einer API-Anbindung auf die Netzwerkeffekte Nicholas, MTLR 2021, 281.

für andere Betreiber[1299] und wäre für komplementäre Anbieter innovationsfördernd.[1300]

459 Im Gegensatz zu einer Herausgabe oder einer Übertragung liesse sich bei einem API-Zugang sodann spezifizieren, welche Daten die neue Verantwortliche tatsächlich benötigt.[1301] Eine Übertragung sämtlicher dem Portabilitätsrecht unterliegenden Daten wäre nicht nötig, was angesichts immer grösser werdender Datenmengen einen Effizienzgewinn darstellt. Die angestrebte Interoperabilität könnte damit im Ergebnis von einem Wettbewerb «um den Markt» («winner-takes-it-all») zu einem Wettbewerb «auf dem Markt» führen.[1302]

460 Der Plattformisierung liesse sich so ebenfalls entgegentreten. Von einer API-Anbindung oder einem Echtzeitportabilitätsrecht wären voraussichtlich mehr Daten umfasst, als dies bei der heute gängigen Plattformisierung und der *Data Transfer Initiative* der Fall ist. Ein zuverlässiger Zugang wäre dabei zwingend (rechtlich) sicherzustellen, da andere Betreiber auf eine Anbindung an die API oder den kontinuierlichen Erhalt von Daten angewiesen sein können. Müssen sie einen Ausschluss von der Anbindung befürchten, werden sie kaum auf die Datensätze zugreifen wollen, da in diesem Fall ihre Produkte nicht mehr funktionieren.[1303] In dieser Hinsicht dürfte eine (einmalige) Datenübertragung verlässlicher sein, da die neue Verantwortliche nach der Übertragung die Daten kontrollieren kann.

461 Dies spricht gegen eine solche Fortentwicklung des Portabilitätsrechts. Denn dessen Zielsetzung sieht nicht vor, dass der alte Verantwortliche als Akteur weiterhin präsent ist. Die Betroffene kann sich nicht von ihm lösen, wenn er weiterhin beteiligt ist, weil er die Infrastruktur bereitstellt. Der alte Verantwortliche ist – und bleibt – bei einer Schnittstellenanbindung das Nadelöhr, durch das die Daten fliessen. Eine API ermöglicht es Dritten zwar, Anwendungen und Dienste «auf» einer Plattform zu entwickeln, doch kann ein Betreiber je nach Ausgestaltung die infrastrukturelle Kontrolle über diese Anwendungen und Dienste beibehalten und somit seine Grösse und Reichweite vergrössern und seine Machtposition innerhalb des Ökosystems noch konsolidieren.[1304]

1299 BKartA, Sektoruntersuchung, 46; Kerber/Schweitzer, JIPITEC 2017, 52; Palfrey/Gasser, 120.

1300 BKartA, Sektoruntersuchung, 46; am Beispiel des Mobilitätssektors Kerber, JCLE 2019, 386.

1301 OECD, Enhancing Access, 32.

1302 BKartA, Sektoruntersuchung, 45; Kühling/Hildebrandt/Bulowski, K&R 2022, 673.

1303 Nicholas, MTLR 2021, 281 f.

1304 Van Der Vlist et al., SM+S 2022, 17. Wird der Idee der «Schöpferischen Zerstörung» nach Schumpeter gefolgt, so muss dies nicht zwingend problematisch sein, da die Innovation

Eine weitere Kehrseite der umfassenden Interoperabilität ist die innovationshemmende Wirkung, wenn Betreiber einmal geschaffene interoperable Produkte kaum noch weiterentwickeln.[1305] Befürchtet wird, dass sie ihre Innovationen allen anderen Wettbewerbern verfügbar machen müssen, wodurch die Anreize, neue Entwicklungen voranzutreiben, beeinträchtigt würden.[1306] Ferner bestehen Datenschutzrisiken, weil das Datenschutzniveau vereinheitlicht und dadurch womöglich gesenkt würde.[1307] Gerade datenschutzfreundliche Betreiber würden so ausgebremst und wichtige Differenzierungsmöglichkeiten im Wettbewerb entfallen.[1308] Denkbar wäre daher, dass nur Basisfunktionen interoperabel gemacht werden müssen.[1309] Denn direkte Netzwerkeffekte und die daraus resultierenden (hohen) Wechselkosten sowie Lock-In-Effekte machen es für Betreiber attraktiv, in einen Markt einzutreten, da diese Faktoren dafür sorgen, dass der Betreiber die anfangs gewonnenen Nutzer auch halten kann.[1310] Fallen diese Anreize weg, könnte dies Markteintrittsschranken eher erhöhen als senken, weil der Eintritt in den Markt riskanter, der langfristige Erfolg des angebotenen Diensts weniger wahrscheinlich und die erzielbaren Gewinne damit als geringer eingeschätzt werden.[1311] Daneben könnten hohe Implementierungskosten gerade kleinere Unternehmen davon abhalten, in den Markt einzutreten.[1312] 462

Schliesslich bestehen Zweifel, dass Interoperabilitätsvorgaben bei sozialen Netzwerken tatsächlich dem Konsumenteninteresse entsprechen. Eine deutsche Untersuchung mit 2000 Konsumenten deutet zumindest darauf hin, dass diese je nach Beziehungsnähe zu anderen Personen unterschiedliche Kommunikationsdienste nutzen wollen und eine Interoperabilitätsverpflichtung nicht im Einklang mit ihren Interessen stünde.[1313] Diese Sichtweise ist nachvollziehbar: Viele Menschen dürften eine Vermischung ihrer Urlaubsfotos (bspw. auf Instagram), mit beruflichen Updates (etwa auf LinkedIn), sowie insb. die Vermischung der jeweils unterschiedlichen Adressatenkreise kaum als Mehrwert 463

und der Wettbewerb insgesamt dennoch gefördert werden könnten, siehe dazu NICHOLAS, MTLR 2021, 285 f.

1305 BKartA, Sektoruntersuchung, 45 f.

1306 BKartA, Sektoruntersuchung, 46; KÜHLING/HILDEBRANDT/BULOWSKI, K&R 2022, 673.

1307 KÜHLING/HILDEBRANDT/BULOWSKI, K&R 2022, 673.

1308 KÜHLING/HILDEBRANDT/BULOWSKI, K&R 2022, 673.

1309 BKartA, Sektoruntersuchung, 46; KÜHLING/HILDEBRANDT/BULOWSKI, K&R 2022, 673.

1310 ZSCHOCH, 273.

1311 ENGELS, Internet Policy Review 2016, 9; SWIRE/LAGOS, Maryland Law Review 2013, 352 f.; ZSCHOCH, 273.

1312 ZSCHOCH, 272 f.

1313 ARNOLD/SCHNEIDER/LENNARTZ, Telecommunications Policy 2020, *passim*; dazu auch BKartA, Sektoruntersuchung, 51.

verstehen. Folglich ist eine weitgehende Interoperabilität zwischen den Betreibern auch praktisch oftmals wenig wünschenswert.

464 Interoperabilitätsvorgaben für soziale Netzwerke hielt der Bundesrat 2013 aber zumindest noch für möglich. «Allenfalls» könnte es sich laut Bundesrat als sinnvoll erweisen, die Schnittstellen zwischen verschiedenen sozialen Netzwerken zu regulieren und etwa den grössten Plattformen vorzuschreiben, dass die privaten Nutzer auch mit jenen anderer Plattformen Daten austauschen können müssen.[1314] Im jüngst veröffentlichten VE-KomPG greift der Bundesrat das Thema jedoch nicht auf. Dies ist zwar nicht überraschend, weil sich die Vorlage am DSA und nicht am DMA orientiert. Dennoch wäre eine erneute Positionierung des Bundesrates zu begrüssen, zumal sich die Ausgangslage angesichts der Entwicklungen in der EU und des technologischen Fortschritts seit 2013 erheblich verändert hat.

b. Spezifisches Portabilitätsrecht gegenüber einzelnen Betreibern

465 Das EU-Recht sieht Portabilitätsrechte gegenüber einzelnen Betreibern vor, soweit diese als Torwächter benannt wurden. In der Schweiz wären spezifische Regelungen für die sozialen Netzwerke ebenfalls denkbar. Solche existieren bislang nicht und sind nach heutigem Stand auch nicht beabsichtigt. Rechtlich unbefriedigend ist jedenfalls die Annahme, dass die neuen EU-Regeln ohnehin in der Schweiz angewendet werden.[1315]

466 Ein spezifischer Anwendungsbereich für einzelne Normen wäre dem Datenschutzrecht nicht fremd und vereinbar mit dem risikobasierten Ansatz[1316]. Unternehmen und andere privatrechtliche Organisationen sind etwa davon befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, wenn sie weniger als 250 Mitarbeitende beschäftigen (Art. 24 DSV). Grössere Unternehmen trifft hingegen eine entsprechende Pflicht. Anders als bei einer bloss sektoriell wirkenden Regelung könnte die Anknüpfung an konkrete Unternehmenskennzahlen verhindern,

1314 Bundesrat, Bericht Social Media, 75.

1315 So aber der Bundesrat in Motion Marti 23.3069, Stellungnahme Bundesrat. Dass dies nicht zwingend ist, zeigte Apples Entscheid, die vom DMA vorgeschriebene Öffnung ihres App Stores nicht auf die Schweiz auszudehnen, siehe Swiss IT Magazine, «Apple erlaubt alternative App Stores in der EU – Schweiz bleibt aussen vor» vom 26. Januar 2024, abrufbar unter: https://perma.cc/7SHV-QG3V. Siehe auch die empirische Untersuchung von Picht et al., sic! 2025, 14 und *passim*, wonach Apple und Google (Alphabet) die spezifischen Vorgaben des DMA derzeit für die Schweiz nicht übernehmen, während Facebook und LinkedIn die Verpflichtungen aus dem DMA auch für die Schweiz anzuwenden scheinen.

1316 Siehe dazu Botschaft DSG 2017, 6970 f.

dass ein Unternehmen in andere, unregulierte Sektoren vorstösst und so die wettbewerbsrechtliche Zielsetzung unterläuft. Denn die strukturellen Vorteile einzelner Unternehmen liegen unabhängig vom Sektor u.a. im Zugang zu grossen Datenmengen (siehe Erw.G 3 DMA). Entsprechend wird befürchtet, dass gerade grosse Internetplattformen sektorielle Regelungen dazu nützen könnten, Zugang zu Daten zu erhalten, ohne dass sie ihre Datensätze herausgeben müssten, da die sektoriellen Regelungen die Internetplattformen nicht erfassen.[1317] Diese Bedenken wurden auch in der parlamentarischen Beratung zum Portabilitätsrecht geäussert.[1318]

Spezifische Vorgaben könnten Datensilos und der zunehmenden Plattformisierung des Webs entgegentreten und die anderen Ziele des Rechts auf Datenportabilität unterstützen. Die Monopolkommission sieht die im DMA gewählte Lösung jedenfalls als geeignet an, um die Datenportabilität zu erleichtern, Wechselkosten der privaten Nutzer zu senken und somit den Wettbewerb um zentrale Plattformmärkte zu fördern.[1319] Auch andere Autoren sprechen sich aus Gründen des Konsumentenschutzes für eine asymmetrische Regulierung aus, die weitergehende Vorschriften für einzelne Anbieter vorsehen würde.[1320] Vertreten wird ferner, dass es sich bei der Datenportabilität nach Art. 6 Abs. 9 DMA um eine «machtabhängige» Konkretisierung von Art. 20 DSGVO handle, die darauf abziele, den Betreiberwechsel und ein *Multi-Homing* zu erleichtern, den Markteintritt von Konkurrenten zu ermöglichen und die Bestreitbarkeit der Gatekeeperposition zu steigern.[1321] 467

Postuliert man demnach, dass diese Konkretisierung der DSGVO infolge der Transformation von einer Warenwirtschaft zu einer Datenwirtschaft notwendig geworden ist,[1322] und dass sich in der Schweiz das Recht auf Datenportabi- 468

1317 Illustriert am Beispiel der PSD2 OECD, Mapping Initiatives, 13.

1318 Votum NR Glättli, AB 2019 N 1814: «[Die Plattformen] wollen nicht nur einen Marktanteil haben, der in bestimmten Teilen immer stärker in Richtung Monopol geht, sondern sie wollen einen möglichst grossen Kundenanteil haben. Das heisst, dass diese Plattformen ganz vielen, zum Teil absolut unrentablen wirtschaftlichen Tätigkeiten nachgehen, um über jeden Einzelnen, den sie kennen, möglichst viel zu wissen, und das in möglichst vielen Lebensbereichen – eben mit einem möglichst grossen Kundenanteil». Dazu weitergehend Rz. 102.

1319 Monopolkommission, 45, die sich noch auf den Vorschlag der EU-Kommission bezieht.

1320 Kerber/Specht-Riemenschneider, 109 f., die dabei auf eine weiterführende Studie verweisen.

1321 Metzger/Schweitzer/Wagner, ZfPW 2023, 253.

1322 So Metzger/Schweitzer/Wagner, ZfPW 2023, 255, die dann aber ausdrücklich offenlassen, ob die wettbewerblichen Probleme zutreffend erfasst und effektiv bewältigt werden können.

lität nach dem DSG ebenfalls nicht isoliert betrachten lässt,[1323] so könnte sich auch hierzulande eine entsprechende Regelung als notwendig erweisen. Dies vor dem Hintergrund, dass sich die Funktionsweise von Plattformen und sozialen Netzwerken in der Schweiz nicht grundlegend von derjenigen in der EU unterscheidet.

469 Allerdings sind es nicht ausschliesslich die Portabilitätsvorgaben im DMA, die den wettbewerbsrechtlichen Zielen förderlich sind. Vielmehr ist es der DMA als Ganzes, der solche Ziele verfolgt. Folglich spiegeln sich die Ziele im gesamten Erlass wider; dieser wäre gesamthaft zu betrachten. So untersagt Art. 6 Abs. 2 DMA dem Torwächter etwa im Wettbewerb mit gewerblichen Nutzern, gewisse nicht öffentlich zugängliche Daten der gewerblichen Nutzer zu verwenden. Damit existiert eine umfassend auf Plattformen zugeschnittene Regulierung, die nicht einzig die Datenportabilität als Mittel zur wettbewerbsrechtlichen Zielerreichung einsetzt. Nur diese wird vorliegend jedoch untersucht.

470 Die Regelung im DMA könnte allerdings in seiner Ausgestaltung in Art. 6 Abs. 9 in Bezug auf die hier besprochenen wettbewerbsrechtlichen *und* datenschutzrechtlichen Zielsetzungen durchaus als Vorlage dienen, da die Regelung den Endnutzern die Übertragbarkeit bestimmter Daten an sie (oder einen von ihnen beauftragten Dritten) ermöglicht. Dies kann neben der wettbewerbsrechtlichen Zielsetzung auch eine persönlichkeitsrechtliche Komponente enthalten. Der DMA gewährt den Endnutzern das Recht über bestimmte Daten – die anders als im Datenschutzrecht nicht notwendigerweise Personendaten sein müssen – zu verfügen und wirtschaftlich davon zu profitieren.[1324] Im Unterschied zur datenschutzrechtlichen Portabilität muss der Zugang dabei permanent und in Echtzeit erfolgen, was die Wirksamkeit des Instituts hinsichtlich der wettbewerbsrechtlichen Ziele erhöht und insb. *Multi-Homing* ermöglicht.

471 Damit erscheint ein Portabilitätsrecht nach dem Vorbild des DMA auch bei isolierter Betrachtung förderlich hinsichtlich der wettbewerbsrechtlichen Ziele, da es sich um eine Regulierung handelt, die – anders als das breite und stark persönlichkeitsrechtlich gefärbte Recht nach Art. 28 DSG – auf die ökonomischen und wettbewerblichen Gegebenheiten der sozialen Netzwerke zugeschnitten ist und besser auf diese reagiert. Damit kann die Grundlage für

1323 Dazu Rz. 328 ff., insb. 334 f.

1324 Siehe dazu Europäische Kommission, Datenstrategie, 1, die ausdrücklich auch bei nicht personenbezogenen Daten davon spricht, dass «alle von der digitalen Dividende profitieren» sollen.

eine wettbewerbsrechtliche Zielerreichung geschaffen werden.[1325] Eine an den DMA angelehnte Lösung könnte die bestehenden Unzulänglichkeiten des datenschutzrechtlichen Portabilitätsrechts adressieren, insbesondere in Bezug auf den Echtzeitzugang und den Umfang der erfassten Daten.

Es wäre damit zwar naheliegend, eine solche Regelung in einem spezialgesetzlichen Erlass nach Vorbild des DMA vorzusehen. Denkbar wäre aber auch, das datenschutzrechtliche Portabilitätsrecht lediglich in diesem Sinn zu ergänzen. Dies gilt allerdings nur eingeschränkt und soweit lediglich Personendaten der Portierung unterliegen sollen. Sollte eine Regulierung mit ausschliesslich wettbewerbsrechtlichem Bezug erfolgen und nicht personenbezogene Daten ebenfalls erfassen, könnte eine Regelung in einem anderen Erlass in Betracht kommen.[1326] 472

Ob ein solches Portabilitätsrecht in seiner Anwendung allerdings tatsächlich wirksam wäre, hängt massgeblich von seiner Umsetzung ab. Dazu wäre ein offener und partizipativer Standardisierungsprozess für die Entwicklung von Datenformaten und offenen Schnittstellen sicherzustellen, der alle Interessengruppen miteinbezieht.[1327] In dieser Hinsicht könnten die Vorarbeiten der *Data Transfer Initiative*, die viele relevante Akteure vereint und an einer Branchenüblichkeit ansetzt, als Vorbild dienen. Zudem wird angeregt, dass die Funktionsfähigkeit und Auswirkungen der Standards überwacht und flexibel angepasst werden können müssen.[1328] Dies schliesst der DMA nicht aus.[1329] Entsprechende Überlegungen aus dem DMA lassen sich daher für die Schweiz übernehmen: Konkret müssen Torwächter gemäss Art. 11 DMA der EU-Kommission Bericht erstatten über die getroffenen Massnahmen zur Einhaltung der Verpflichtungen nach Art. 6 DMA, wodurch die EU-Kommission über die Umsetzung im Bild bleibt. 473

Gemäss Art. 8 Abs. 2 UAbs. 2 DMA kann die EU-Kommission zudem Durchführungsakte erlassen, in denen der Torwächter zu ergreifende Massnahmen festlegt, um den Portabilitätsverpflichtungen nachzukommen. Art. 46 Abs. 1 lit. b DMA ermächtigt die EU-Kommission sodann detaillierte Regelungen für die Anwendung von Form, Inhalt und sonstigen Einzelheiten der technischen Massnahmen zu erlassen, die von den Torwächtern durchzuführen sind, um 474

1325 So noch basierend auf dem Vorschlagstext KERBER/SPECHT-RIEMENSCHNEIDER, 82 f.

1326 Siehe etwa HEINEMANN, ZWeR 2022, 315, der am Beispiel des Geoblockingverbots aufführt, dass der Gesetzgeber gerne Spezialregeln als Beispieltatbestand in das UWG aufnimmt.

1327 SCHWEITZER et al., 207 und 307.

1328 SCHWEITZER et al., 30.

1329 Siehe zu den Möglichkeiten SCHWEITZER et al., 267.

die Einhaltung der Portabilitätsverpflichtungen zu gewährleisten. Sie kann zudem die Portabilitätsvorgaben anpassen: Art. 12 Abs. 1 DMA überträgt der EU-Kommission die Befugnis, delegierte Rechtsakte zu erlassen, um die Verpflichtungen nach Art. 6 DMA «zu ergänzen», wobei einige Beschränkungen in Abs. 2 zu beachten sind. Mit der Festlegung von Normen kann die EU-Kommission die europäischen Normungsgremien beauftragen (Art. 48 DMA). Spätestens dann dürfte ein Einfluss auf die Schweiz – und insb. auf Schweizer Unternehmen – faktisch nicht zu vermeiden sein.[1330]

475 Ohnehin dürfte ein alleiniges Vorpreschen der Schweiz kaum erfolgversprechend sein. Denn bei den zu regulierenden Torwächtern und sozialen Netzwerken handelt es sich um weltweit tätige Unternehmen mit globalen Geschäftsmodellen. Bereits innerhalb der EU wurde es als unbefriedigend betrachtet, wenn mehrere unterschiedliche Regulierungen anwendbar wären.[1331] Der DMA sollte vor allem eine einheitliche Regulierung schaffen, um einer Zersplitterung der rechtlichen Vorgaben in Europa zuvorzukommen. Dies wäre auch für die Schweiz zu berücksichtigen, denn hohe Umsetzungskosten für Unternehmen könnten dazu führen, dass sich Gatekeeper aus der Schweiz zurückziehen. Auch KMU könnten auf Schwierigkeiten stossen, weil es deren Skalierbarkeit hemmt, wenn sie für die Schweiz neue und andere Vorgaben befolgen müssen.[1332] Zudem ist zu bezweifeln, dass die Schweiz überhaupt die notwendigen Ressourcen für eine solche *ex ante*-Regulierung aufzubringen vermag, da kleine und mittelgrosse Länder kaum über die erforderlichen Mittel verfügen.[1333]

4. Erkenntnisse

476 Das Recht auf Datenportabilität kann die Grundlagen schaffen, um die datenschutzrechtlichen Ziele zu erreichen. Dies gilt allerdings vor allem dann, wenn Autonomie und Möglichkeit zur Datendisposition so verstanden werden, dass die Betroffene ihre Daten an einem von ihr gewählten Ort archivieren kann. Dies entspricht indes kaum dem Willen des Gesetzgebers, der ein wirkungsvolles Instrument für einen Wechsel (auch) zwischen Betreibern sozialer Netzwerke im DSG verankern wollte.

1330 Die Schweizerische Normen-Vereinigung gibt an, dass von rund 26'000 Normen im Schweizer Normenwerk rund 25'000 europäische oder internationale Normen sind, die in das Schweizer Normenwerk übernommen wurden, siehe https://perma.cc/KBD8-SP4Z.

1331 Europäische Kommission, DMA Impact Assessment Report, 8.

1332 Europäische Kommission, DMA Impact Assessment Report, 8.

1333 Heinemann, ZWeR 2022, 309.

Unzulänglichkeiten zeigen sich, sobald der Doppelbezug von Daten und die «soziale» Komponente der sozialen Netzwerke berücksichtigt werden: Das Portabilitätsrecht ermöglicht keine sinnvolle Herauslösung der zu portierenden Daten, ohne dass diese für die Betroffene an Wert verlieren. Denn Daten sind in sozialen Netzwerken regelmässig in einen Kontext eingebettet und dieser Kontext stellt für die Betroffene den Mehrwert dar. Daher bietet der reine Erhalt von Daten, zumal nur solchen mit einem Bezug zur Betroffenen, faktisch kaum einen Vorteil. 477

Auch in wettbewerbsrechtlicher Hinsicht bestehen Unzulänglichkeiten bei einem Wechsel zwischen sozialen Netzwerken: Das Portabilitätsrecht schafft kaum die Voraussetzungen, um einen *Lock-In* zu verhindern. Grund dafür sind die starken Netzwerkeffekte, die in diesem Sektor besonders wirken, aber vom Institut nicht spezifisch adressiert werden. Dies ist insofern bemerkenswert, als ein Wechsel zwischen zwei sozialen Netzwerken im Gesetzgebungsprozess das Musterbeispiel für die Anwendung des Portabilitätsrechts war. 478

Anders verhält es sich, wenn Betroffene von einem Betreiber eines sozialen Netzwerks zu einem andersartigen Anbieter wechseln. Netzwerkeffekte hindern sie in diesem Fall kaum daran. Zudem besteht die Möglichkeit, dass kleinere Anbieter von den Datensätzen profitieren und dadurch in einen Markt eintreten können. Damit tritt auch das Ziel der allgemeinen Wettbewerbs- und Innovationsförderung in den Vordergrund: Das Portabilitätsrecht baut Hürden für neue und innovative Angebote ab. 479

Im untersuchten Sektor zeigen sich weitere Besonderheiten. So sind datenbasierte Märkte wie der vorliegende oft Gewinnermärkte, weshalb für die Erreichung der wettbewerbsrechtlichen Ziele vor allem der Entstehung eines solchen Marktes vorzubeugen wäre. Diesem Anspruch wird das Portabilitätsrecht jedoch *de lege lata* nicht gerecht. Auch *de lege ferenda* scheint eine derartige Ausgestaltung im DSG nicht denkbar, da die dafür notwendigen Anpassungen nicht im DSG erfolgen können und das Portabilitätsrecht nicht als datenschutzrechtliches Instrument auszugestalten wäre. Zudem wirkt die Plattformisierung bei sozialen Netzwerken besonders ausgeprägt. Sie verfügt über eine hohe Funktionalität, weshalb die Nutzung von Schnittstellen durch andersartige Anbieter verbreitet ist. Problematisch ist jedoch, dass die Plattformisierung *walled gardens* fördert und sich der Zugang zu den Daten jederzeit einseitig beschränken lässt. Das Portabilitätsrecht stellt allerdings keine taugliche Alternative zur Plattformisierung dar und vermag dieser gegenwärtig kaum etwas entgegenzusetzen. Dafür fehlt es insb. an einem Echtzeitzugang zu den Daten und an verpflichtenden Schnittstellen. 480

481 Mit der *Data Transfer Initiative* existiert bereits ein unternehmensübergreifendes Portabilitätsprojekt, das eine Alternative zum Recht auf Datenportabilität ist. Die Initiative überzeugt durch ihre hohe Funktionalität und steht aufgrund ihres Open Source-Ansatzes allen offen. Namentlich ermöglicht sie auch den Wechsel zwischen zwei gleichartigen Betreibern. Da die Initiative auf die grossen Betreiber sozialer Netzwerke zurückgeht, erscheint die Umsetzung ausgereift und nahe an den Bedürfnissen des Sektors. Es lässt sich allerdings einwenden, dass Betreiber den Zugang jederzeit einseitig sperren können, wodurch die Betroffene von deren Goodwill abhängig bleibt.

482 Insgesamt zeigt sich, dass ein Echtzeitzugang zu den Daten und in einem nächsten Schritt das Ideal einer umfassenden Interoperabilität vielversprechende Ansätze sind, die sowohl die datenschutz- als auch wettbewerbsrechtlichen Ziele berücksichtigen. Allerdings wäre es womöglich gerade mit Blick auf den bereits vom Gesetzgeber zugestandenen Fokus auf die sozialen Netzwerke überzeugender, wenn spezifische Portabilitätsrechte gegenüber bestimmten Betreibern erlassen würden. Der europäische Gesetzgeber hat sich für diesen Weg entschieden und Portabilitätsrechte gegenüber designierten Torwächtern verankert. Diese Regelung muss sich nun bewähren. Ob die Schweiz einen ähnlichen Weg gehen möchte, steht noch nicht fest. Eine Übernahme des DMA ist bislang nicht geplant.

483 Bemerkenswert ist allerdings, dass gerade bei Zielen, die sektorübergreifend wirken sollen – also sowohl die persönlichkeitsrechtlichen Ziele als auch die wettbewerbsrechtlichen Makroziele – eine spezifische Regulierung bestimmter Betreiber vielversprechender erscheint. Diese Regulierung erfolgt zwar in der EU bewusst nicht im eigentlichen Sinn sektorspezifisch. Dennoch erhofft man sich von den Vorgaben für Torwächter im DMA und besonders von den darin enthaltenen Portabilitätsverpflichtungen eine Wirkung, die das datenschutzrechtliche Portabilitätsrecht bislang nicht zu zeigen vermochte. Die spezifische Regulierung einzelner Betreiber ist also gerade darauf ausgelegt, sektorübergreifend zu wirken. Damit zeigt sich für den Sektor der sozialen Netzwerke unterschiedlicher Handlungsbedarf. Dieser wird bei der sektorübergreifenden Betrachtung zu würdigen sein.

III. Gesundheitswesen

Die Datenflüsse des Gesundheitswesens waren lange Zeit analog geprägt und noch heute stockt die Digitalisierung dieses Sektors.[1334] Allerdings gibt es in keinem anderen auf Informationstechnologien basierenden Sektor mehr Teilnehmende, mehr Geld und mehr Probleme.[1335] Denn das Datenökosystem besteht aus zahlreichen unterschiedlichen Akteurinnen mit oftmals entgegengesetzten Interessen. Dabei ist bereits unklar, was und wer alles zum Gesundheitswesen gehört. Nach dem Historischen Lexikon der Schweiz umfasst das Gesundheitswesen die Gesamtheit der Normen und Werte, der gelebten Praxis und der betroffenen Personen – wie Behandelnde oder Behandelte – im Zusammenhang mit der körperlichen und seelischen Gesundheit bzw. Krankheit.[1336] In einem engeren Sinn sind damit vor allem die institutionell fassbaren Prozesse und Einrichtungen gemeint.[1337] 484

Kaum vereinfachend wirkt, dass das Gesundheitswesen in der Schweiz grundsätzlich in die Kompetenz der Kantone fällt.[1338] Dies führt trotz zunehmender Vernetzung zu einer Fragmentierung der geltenden Vorschriften.[1339] In datenschutzrechtlicher Hinsicht kommt hinzu, dass im Gesundheitsdatenökosystem vorwiegend Daten mit Personenbezug bearbeitet werden, die damit unter das Datenschutzrecht fallen. Sie sind zudem regelmässig als besonders schützenswert zu qualifizieren (Art. 5 lit. c Ziff. 2 DSG). Ferner ist der Sektor seit jeher von umfassenden Reformbestrebungen geprägt; in jüngster Zeit sind auch gesetzgeberische Bestrebungen zu einer Digitalisierung und einer Regulierung von Datenflüssen im Gesundheitswesen zu beobachten.[1340] 485

Im Gesundheitswesen spielen auch wettbewerbsrechtliche Ziele eine Rolle. Zahlreiche Akteurinnen stehen zueinander im Wettbewerb und die Innovation und Förderung der Datenflüsse ist gerade für die medizinische Forschung elementar. Dennoch sind diese Ziele, wie noch gezeigt wird, nicht ohne Weiteres 486

1334 Beispielhaft etwa die zu einem geflügelten Wort verkommenen Faxgeräte des BAG im Zuge der Covid-19-Pandemie, siehe VON MATT RAFAEL, «Langsame Datenübermittlung: Fast jeder fünfte Arzt nutzt noch Fax», SRF Online vom 28. Februar 2024, abrufbar unter: https://perma.cc/SPN9-8989. Zu den Entwicklungen Rz. 495 und 520 ff.

1335 PALFREY/GASSER, 195.

1336 BRÄNDLI, 1.

1337 BRÄNDLI, 1.

1338 Botschaft BV, 332; SPRECHER, Digitalisierung, 36.

1339 Ähnlich SPRECHER, Digitalisierung, 36.

1340 Dazu Rz. 495.

auf das Gesundheitswesen übertragbar. Gleichzeitig lässt sich beobachten, dass gerade die vom Portabilitätsrecht anvisierten Internetplattformen zunehmend in den Gesundheitssektor drängen.[1341] Dennoch stehen in diesem Sektor – mit der Patientin im Zentrum – die datenschutzrechtlichen Ziele im Vordergrund. In diesem Kapitel ist daher primär zu untersuchen, ob das Recht auf Datenportabilität die Grundlagen schafft, damit die datenschutzrechtlichen Ziele erreicht werden können. Die wettbewerbsrechtlichen Ziele werden nur in geringerem Masse angesprochen. Dafür ist das Gesundheitsdatenökosystem zu strukturieren und das Portabilitätsrecht in diesem Kontext zu untersuchen.

A. Strukturierung des Ökosystems

1. Akteurinnen und deren Rollen

a. Natürliche Personen

487 Im Zentrum des Gesundheitsdatenökosystems stehen natürliche Personen, die keine einheitliche Rolle einnehmen: Sie sind Versicherte, Probandinnen oder Patientinnen. Die jeweilige Bezeichnung unterstellt allerdings bereits eine Beziehung zu anderen Akteurinnen, weshalb im Folgenden zunächst neutral von natürlichen Personen die Rede ist. Von ihnen werden in datenschutzrechtlicher Hinsicht primär Daten *erfasst*. Sie sind damit in ihrer datenschutzrechtlichen Rolle als betroffene Personen zu qualifizieren.

b. Leistungserbringerinnen

488 Im Gesundheitswesen sind zahlreiche Leistungserbringerinnen tätig. Unter diesen aus dem Krankenversicherungsrecht stammenden Oberbegriff fallen Ärztinnen, Apothekerinnen, Chiropraktorinnen, Hebammen, Personen, die auf Anordnung oder im Auftrag einer Ärztin Leistungen erbringen sowie Organisationen, die solche Personen beschäftigen, Laboratorien, Abgabestellen für Mittel und Gegenstände, die der Untersuchung oder Behandlung dienen, Spitäler, Geburtshäuser, Pflegeheime, Heilbäder, Transport- und Rettungsunternehmen sowie Einrichtungen, die der ambulanten Krankenpflege durch Ärztinnen dienen (Art. 35 Abs. 2 KVG). Sie erbringen gesundheitsrelevante

1341 STEFFEN/WIEWORRA/KROON, 34 m.w.N.; siehe grundlegend etwa WASILEWSKI, *passim*.

Leistungen und bearbeiten dabei regelmässig Personendaten. Sie nehmen i.d.R. die datenschutzrechtliche Rolle einer Verantwortlichen ein.[1342]

Dabei ist zu beachten, dass viele Leistungserbringerinnen kantonale öffentliche Organe sind, etwa Kantons- oder Universitätsspitäler. Auf Datenbearbeitungen ist in diesen Fällen das kantonale Datenschutzrecht anwendbar, nicht das DSG.[1343] Dies gilt auch für Private, die eine (kantonale) öffentliche Aufgabe wahrnehmen und dabei aufgrund eines Leistungsauftrags handeln, wie etwa die sog. Listenspitäler im Bereich der obligatorischen Krankenpflege, bei welchen der Kanton einen Anteil von mind. 55 % an die stationären Leistungen bezahlt (Art. 49*a* Abs. 2 und 2ter KVG).[1344] Da diesen Listenspitälern ein Teil einer öffentlichen Aufgabe – die Gesundheitsversorgung – übertragen wird, unterstehen sie in diesem Umfang dem kantonalen Datenschutzrecht.[1345] Dies gilt selbst dann, wenn sie mit anderen Spitälern im Wettbewerb stehen, da es sich dabei nicht um privatwirtschaftlichen Wettbewerb handelt, sondern um Wettbewerb zwischen Trägern öffentlicher Aufgaben.[1346] 489

c. Versicherungsunternehmen

Im Gesundheitswesen sind Versicherungsunternehmen vorwiegend als Krankenkassen tätig. Bei diesen handelt es sich um juristische Personen des privaten oder öffentlichen Rechts, die keinen Erwerbszweck verfolgen und die soziale Krankenversicherung nach dem KVG durchführen (Art. 2 Abs. 1 KVAG). Als 490

1342 Rosenthal, Jusletter 2019, Anhang, dort 7, der innerhalb der Kategorie der Leistungserbringerinnen weiter differenziert, etwa im Verhältnis zwischen Belegärztin, freiberuflicher Ärztin und Spital. Auf dieser Ebene kann die Rollenzuteilung in der Praxis äusserst komplex sein, gerade wenn auch eine gemeinsame Verantwortlichkeit oder eine Auftragsbearbeitung in Frage kommt, siehe George, Gesundheitswesen, Rz. 2176 f.; für die DSGVO und besonders im Kontext einer Datenübermittlung Schrader, 158 ff., insb. 159.

1343 Bundesrat, Bericht Patientenrechte, 20 f.; PK IDG/BS-Rudin, § 3 N 7; dazu Rz. 173.

1344 PK IDG/BS-Rudin, § 3 N 10; ausführlich hierzu Rütsche, 34 ff., 41 und 51 f.; Widmer/Egli, Rz. 41 ff.

1345 PK IDG/BS-Rudin, § 3 N 10; Widmer/Egli, Rz. 41. Siehe exemplarisch § 9 a des Spitalplanungs- und -finanzierungsgesetz des Kantons Zürich (Ordnungsnummer 813.20), welcher vorsieht, dass Listenspitäler die einwandfreie Erfüllung des Leistungsauftrags sicherzustellen haben. Siehe jedoch die Einwände von Aebi-Müller et al., Arztrecht 2016, § 2 Rz. 17 ff., nach welchen die Unterscheidung zwischen ambulanter und stationärer Behandlung «teilweise absurde Konsequenzen» hätte. Dieser Einwand dürfte sich mit der Änderung des KVG vom 22. Dezember 2023 (BBl 2024 31), welche eine einheitliche Finanzierung der Leistungen vorsieht, erledigt haben. Nachdem die Stimmbevölkerung der Änderung am 24. November 2024 zugestimmt hat, wird sie voraussichtlich am 1. Januar 2028 in Kraft treten, siehe https://perma.cc/6E6P-NU6E.

1346 Rütsche, digma 2012, 180.

Durchführungsorgan der sozialen Krankenversicherung stellen sie in diesem Bereich ein Bundesorgan dar.[1347] Gleiches gilt für die Durchführung der obligatorischen Unfallversicherung.[1348]

491 Krankenkassen können allerdings daneben Zusatzversicherungen anbieten und weitere Versicherungsarten betreiben (Art. 2 Abs. 2 KVAG). In diesem Bereich gelten sie datenschutzrechtlich i.d.R. als Private[1349] und werden nachfolgend als Versicherungsunternehmen bezeichnet. Versicherungsunternehmen, einschliesslich Krankenkassen, bearbeiten eine Vielzahl an Personendaten, für welche sie i.d.R. als Verantwortliche zu qualifizieren sind.

d. Forschende

492 Eine grosse Rolle für das Gesundheitswesen spielt die Forschung. Sie zielt darauf ab, methodengeleitet zu verallgemeinerbaren Erkenntnissen zu gelangen (Art. 3 lit. a HFG; ähnlich auch Art. 2 lit. a FIFG) und hat so einen unverzichtbaren Anteil an der Fortentwicklung und Verbesserung des Gesundheitswesens. Da Forschung zunehmend datengestützt ist, ist der Zugang zum Gesundheitsdatenökosystem für sie wichtig. Der Bundesrat versteht den Begriff der Forschung in diesem Zusammenhang weit und unterscheidet verschiedene Arten von Datennutzung: die akademische Forschung durch Hochschulen und private und staatliche Forschungsstätten, die privatwirtschaftliche Forschung durch die Industrie, die Ressortforschung durch von der Bundesverwaltung beauftragte wissenschaftlich tätige Einrichtungen und die Datennutzung zum Zweck der Information des Gesundheitssystems durch Gesundheitsbehörden, Leistungserbringerinnen, Versicherer und andere Akteurinnen.[1350] Dabei ist wie bei den Leistungserbringerinnen zu berücksichtigen, dass öffentliche Organe wie kantonale Universitäten, Fachhochschulen oder öffentliche Spitäler auch im Forschungsbereich unter die kantonale Datenschutzgesetzgebung fallen. Nur Forschung durch Private oder durch Bundesbehörden (etwa im ETH-Bereich) fällt unter das DSG (Art. 2 Abs. 1 DSG).

493 An konkreten Forschungsvorhaben sind regelmässig mehrere Akteurinnen beteiligt, etwa ein Sponsor, eine Prüfperson (*investigator*) oder ein Auftragsfor-

1347 BGE 131 II 413 E. 2.2; Gehring, HAVE 2023, 224; Guillod, 422; Vasella/Ziegler, digma 2020, 81.

1348 Dal Molin, Rz. 10.

1349 Urteil des BVGer A-3548/2018 vom 19. März 2019 E. 4.5.5; Vasella/Ziegler, digma 2020, 80; siehe aber Rütsche, Rz. 54.

1350 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 13 ff.; siehe auch die Aufzählung aus deutscher Perspektive bei Drepper/Schlünder/Buckow, 180.

schungsinstitut (sog. *contract research organization*).[1351] Dies wirft in der Praxis die Frage nach der datenschutzrechtlichen Rolle der jeweiligen Akteurinnen auf. Dies ist vorliegend jedoch nicht zu vertiefen, da die Forschung an sich als «Akteurin» des Gesundheitswesens und deren (datenschutzrechtliche) Beziehung zu anderen Akteurinnen von Interesse ist. In diesem Kontext bearbeiten Forschende Personendaten i.d.R. als Verantwortliche, ohne dass eine weitere Aufschlüsselung der Rollenverteilung nötig ist.

e. Staat

Im Zusammenhang mit dem Gesundheitswesen bearbeiten unterschiedliche staatliche Stellen Personendaten. Bereits aufgezeigt wurde die Rolle von Leistungserbringerinnen, Forschenden oder privaten Versicherungsunternehmen, die punktuell öffentliche Organe darstellen. Darüber hinaus existieren jedoch öffentlich-rechtliche Anstalten des Bundes, die eine Rolle im Gesundheitswesen einnehmen, und als Bundesorgane dem DSG unterstehen, etwa die Suva oder die Militärversicherung.[1352] Auf kantonalem Recht basierende Organisationen, wie kantonale Ausgleichskassen oder IV-Stellen, die im Sozialversicherungsbereich eine Bundesaufgabe durchführen, unterliegen gleichwohl dem kantonalen Datenschutzrecht.[1353] Staatliche Stellen bearbeiten Daten i.d.R. als Verantwortliche und handeln dabei hoheitlich und gestützt auf eine gesetzliche Grundlage (Art. 34 Abs. 1 DSG),[1354] weshalb das Portabilitätsrecht nicht in Frage kommt und auf weitere Ausführungen verzichtet wird. 494

Daneben übernimmt der Staat – und trotz der grundsätzlichen kantonalen Kompetenz zunehmend der Bund – eine weitere Rolle im Gesundheitsdatenökosystem: diejenige eines Koordinators.[1355] Er will eine bessere Nutzung von Gesundheitsdaten für eine qualitativ hochstehende und effiziente Gesundheitsversorgung ermöglichen,[1356] Datenstrategien in der Krankenversicherung entwickeln[1357] oder einen dedizierten Gesundheitsdatenraum schaffen[1358]. Mit dem EPDG wurde eine gesundheitspolitische Vision bereits gesetzlich geregelt, wenngleich dessen Wirkung bislang gering ist und eine umfassende 495

1351 Siehe dazu Isler, digma 2020, 68 und *passim*.
1352 Gehring, HAVE 2023, 224.
1353 Gehring, HAVE 2023, 225.
1354 Dazu Guillod, 414.
1355 Siehe https://perma.cc/MQ7Q-MB6P.
1356 Bundesrat, Bericht Nutzung von Gesundheitsdaten, *passim*.
1357 Bundesrat, Bericht Kohärente Datenstrategie für das Gesundheitswesen, *passim*.
1358 UVEK/EDA, 28 f.; siehe zur Sekundärnutzung Motion WBK-S 22.3890.

Überarbeitung erfordert.[1359] Zur Förderung der digitalen Transformation im Gesundheitswesen haben die eidgenössischen Räte ausserdem bis zum Jahr 2035 einen Verpflichtungskredit in Höhe von knapp CHF 400 Mio. gesprochen.[1360]

f. Herstellerinnen von Medizinprodukten

496 Medizinprodukte sind Produkte, die für die medizinische Verwendung bestimmt sind oder angepriesen werden und deren Hauptwirkung nicht durch ein Arzneimittel erreicht wird (Art. 4 Abs. 1 lit. b HMG). Beispielhaft können als Medizinprodukte u.a. Apparate, Geräte und Software genannt werden. Sie sind besonders reguliert und dürfen nur gemäss den Vorgaben nach Art. 45 ff. HMG sowie der gestützt darauf erlassenen MepV in Verkehr gebracht werden. Diese Vorgaben sind wiederum stark an den europäischen Vorschriften angelehnt und verweisen auf diese.[1361] Kein Medizinprodukt stellt allerdings Software dar, welche sich bei der Verarbeitung von medizinischen Daten auf die Speicherung, Archivierung, einfache Suche, Kommunikation oder verlustfreie Kompression beschränkt.[1362]

497 Medizinprodukte können Personendaten erfassen und bearbeiten. Zu denken ist etwa an Computertomografen (CT), Röntgengeräte, Herzfrequenzmessgeräte oder Bildanalysesoftware. Welche datenschutzrechtliche Rolle deren Herstellerinnen einnehmen, ist im Einzelfall zu beurteilen. Möglich ist, dass sie als Verantwortliche auftreten. Denkbar ist aber auch, dass eine Leistungserbringerin ein Medizinprodukt verwendet und die (alleinige) Verantwortliche ist. Dies kann dazu führen, dass die Herstellerinnen als Auftragsbearbeiterinnen zu qualifizieren sind. Möglich ist zudem eine gemeinsame Verantwortlichkeit.[1363] Da sich die rechtliche Situation im ersten und dritten Fall analog zu den Leistungserbringerinnen verhält und die Betroffene im zweiten Fall das Portabilitätsrecht gegenüber dem Verantwortlichen geltend machen muss,

1359 Siehe hierzu https://perma.cc/GQ6F-WE2Z. Vernichtende Kritik ist teilweise von Seiten der Ärzteschaft zu vernehmen, siehe Huber, SÄZ 2022, 175, der von einem «Monster» spricht, das nie funktionieren werde. Es handle sich um ein «chaotisches Archiv an PDF-Dokumenten», welches nutzlos sei und den Aufwand nicht rechtfertige.

1360 Siehe Bundesbeschluss zum Verpflichtungskredit für ein Programm zur Förderung der digitalen Transformation im Gesundheitswesen für die Jahre 2025–2034 vom 29. Mai 2024, BBl 2024 1033.

1361 Leins-Zurmühle, LSR 2021, 138.

1362 Swissmedic, 5 f.; Weber/Thouvenin, 73 f.

1363 Siehe zu den in dieser Hinsicht vergleichbaren digitalen Gesundheitsanwendungen in Deutschland Schrader, 323 ff.

wird nachfolgend auf weitere Ausführungen zu den Herstellerinnen von Medizinprodukten verzichtet.

g. Anbieterinnen von gesundheitsrelevanten Anwendungen

Neben den (regulierten) Herstellerinnen von Medizinprodukten gibt es weitere Anbieterinnen von gesundheitsrelevanten Anwendungen. Diese gehören nicht im eigentlichen Sinn zum Gesundheitssektor. Vermehrt drängen jedoch grosse Technologieunternehmen durch unabhängig entwickelte Anwendungen oder durch entsprechende Akquisitionsbemühungen in den datengesteuerten Gesundheitssektor.[1364] Sie sind in der Lage, kundenorientierte Dienstleistungsplattformen aufzubauen und können die dahinterliegende Cloud-Technologie und die Logistikprozesse gleich mitanbieten, wodurch sie die gesamte Wertschöpfungskette abdecken und ihre Marge maximieren.[1365] 498

Anders als die medizinischen Anwendungen, die unter das Medizinprodukterecht fallen, unterliegen Gesundheitsanwendungen, die blosse «Lifestyleprodukte» darstellen, keiner besonderen Regulierung.[1366] Die Abgrenzung kann im Einzelfall allerdings schwierig sein. Wird bspw. ein Fitnesstracker nicht einzig zur Aufzeichnung und Visualisierung von Nutzerdaten, sondern auch zu Diagnose- oder Behandlungszwecken (wie bspw. zur Unterstützung der Stressbewältigung) vorgesehen oder verwendet, dürfte er eher ein Medizinprodukt und kein Lifestyleprodukt mehr darstellen.[1367] 499

Viele Apps, Fitnesstracker, Smartwatches, smarte Kleidungsstücke, Pulsgurte, Smartringe usw. sind heute als gesundheitsrelevante Anwendungen verfügbar und erfassen zahlreiche Daten. Die Anbieterinnen solcher Anwendungen sind i.d.R. als Verantwortliche einzustufen. 500

1364 Hierbei von «datenreichen etablierten Unternehmen» sprechend Steffen/Wieworra/Kroon, 34; siehe für einen umfassenden Überblick Wasilewski, *passim*. Teilweise stellen die Technologieunternehmen auch Herstellerinnen von Medizinprodukten dar, was jedoch im Einzelfall zu beurteilen ist. Siehe etwa die softwaregestützte App für die Apple Watch, mit der ein einkanaliges Elektrokardiogramm aufgezeichnet werden kann und welche ein Medizinprodukt darstellt, https://perma.cc/K6XE-RQWM.

1365 Wasilewski, 42.

1366 Gordon, digma 2016, 70.

1367 Leins-Zurmühle, LSR 2021, 140.

2. Relevante Beziehungen

a. Natürliche Person (Patientin) und Leistungserbringerin

aa. Rechtsnatur des Behandlungsverhältnisses

501 Liegt eine Beziehung zwischen einer natürlichen Person und einer Leistungserbringerin vor, handelt es sich in aller Regel um ein Behandlungsverhältnis, d.h. die natürliche Person ist als Patientin einzuordnen. Die rechtliche Qualifikation dieses Behandlungsverhältnisses hängt davon ab, ob es privatrechtlicher oder öffentlich-rechtlicher Natur ist. Ist es privatrechtlicher Natur, so stellt etwa das klassische Verhältnis zwischen einer Ärztin und einer Patientin einen Auftrag nach Art. 394 ff. OR dar.[1368] Daneben kann im Rahmen des sog. Behandlungsvertrags bei einer Behandlung in einem Privatspital ein totaler oder ein gespaltener Spitalaufnahmevertrag vorliegen: Bei ersterem wird das Rechtsverhältnis zwischen dem Spital und der Patientin gänzlich abgedeckt (also einschliesslich Unterkunft, Verpflegung, pflegerische und ärztliche Behandlung usw.).[1369] Bei zweiterem beschränkt sich die Leistung des Spitals darauf, Unterkunft, Verpflegung und Pflege zu gewähren, während die ärztliche Leistung Gegenstand eines eigenständigen Vertrags zwischen Ärztin und Patientin ist.[1370]

502 Handelt es sich um ein öffentliches Spital, untersteht das Rechtsverhältnis dem (kantonalen) öffentlichen Recht.[1371] So wird bspw. mit der Aufnahme in ein als öffentlich-rechtliche Anstalt organisiertes Spital ein Anstaltsverhältnis zur Trägerin des Spitals begründet.[1372] Das öffentlich-rechtliche Behandlungsverhältnis ist in den kantonalen Erlassen geregelt, etwa in Gesundheitsgesetzen, Vollzugsverordnungen und Spitalreglementen.[1373] Die Leistungserbringerin ist in diesem Fall mit obrigkeitlicher Gewalt ausgestattet und die Rechte und Pflichten aller Beteiligten sind gesetzlich vorgegeben.[1374] Dies gilt auch, wenn ein Spital zwar über privatrechtliche Strukturen verfügt, aber dennoch öffentliche Aufgaben erfüllt: Das Privatrecht dient dann zwar als rechtliches Gestaltungsmittel, vermag dabei jedoch nicht das Rechtsverhältnis zur Patientin den

1368 Aebi-Müller, Jusletter 2020, Rz. 32; Fellmann, 106 m.w.N.
1369 Aebi-Müller et al., Arztrecht 2024, Rz. 174 ff.; Fellmann, 106 f.
1370 Fellmann, 107.
1371 Fellmann, 108.
1372 Fellmann, 108.
1373 Aebi-Müller et al., Arztrecht 2024, Rz. 182.
1374 Fellmann, 108; Payllier, 167 f.

Wirkungen des öffentlichen Rechts zu entziehen.[1375] Umgekehrt – und kaum vereinfachend – kann eine Ärztin (in beschränktem Rahmen) auch in einem öffentlichen Spital einer privatärztlichen Tätigkeit nachgehen und in eigenem Namen und auf eigene Rechnung tätig sein, wodurch sie wiederum dem Privatrecht untersteht.[1376] Alle diese Umstände beeinflussen die Anwendbarkeit des Portabilitätsrechts.

bb. Dokumentationspflichten der Leistungserbringerin

503 Für Leistungserbringerinnen existieren weitreichende Dokumentationspflichten. Diese lassen sich bei privaten Leistungserbringerinnen aus dem Rechtsverhältnis ableiten (Art. 400 Abs. 1 OR), sie sind aber auch kantonalrechtlich explizit für den Gesundheitsbereich vorgesehen, und zwar unabhängig davon, ob eine Leistungserbringerin öffentlich-rechtlicher oder privatrechtlicher Natur ist. Nach § 13 Abs. 1 GesG/ZH muss etwa «[w]er einen Beruf des Gesundheitswesens ausübt» über jede Patientin eine Patientendokumentation anlegen und diese laufend nachführen. Sie muss Auskunft über die Aufklärung und Behandlung einer Patientin geben. Als Behandlung gelten dabei insb. Untersuchungen, Diagnosen, Therapie und Pflege (§ 13 Abs. 1 GesG/ZH; ähnlich auch § 17 Abs. 1 PatG/ZH).[1377] Daneben hält das zürcherische Recht fest, dass die Patientendokumentation «Eigentum» der Institution ist (§ 18 Abs. 1 PatG/ZH), wobei der Patientin gemäss der einschlägigen Datenschutzgesetzgebung Einsicht gewährt wird (§ 19 Abs. 1 und 3 PatG/ZH). § 13 Abs. 4 GesG/ZH sieht ferner einen Anspruch auf Herausgabe der Patientendokumentation in Kopie vor. Im Kanton Basel-Stadt umfasst die Dokumentation gemäss § 29 Abs. 1 GesG/BS Angaben über die diagnostischen Abklärungen, Untersuchungen und Ergebnisse sowie die therapeutischen und pflegerischen Massnahmen. Nach Abs. 3 hat die Patientin das Recht auf eine Kopie der Dokumentation, soweit keine schutzwürdigen Interessen Dritter entgegenstehen. Diese gesetzlichen Pflichten können sich auf die Anwendbarkeit des Portabilitätsrechts auswirken.

1375 Fellmann, 109.

1376 Aebi-Müller et al., Arztrecht 2016, § 2 Rz. 170; auch Payllier, 174 ff.; Rütsche, 14.

1377 Siehe jedoch die vom BGer vorgenommene Relativierung des Umfangs der Dokumentationspflichten in BGE 141 III 363. Demnach dient die Dokumentationspflicht primär der Erfüllung des Behandlungsauftrags und nicht der Beweissicherung, weshalb Kontrolluntersuchungen dann nicht dokumentationspflichtig sind, «wenn es medizinisch üblich ist, bei Ausbleiben eines positiven Befundes keine Aufzeichnungen vorzunehmen» (E. 5.1). Das BGer leitet die Dokumentationspflicht indes nur auftragsrechtlich her.

cc. Datenbearbeitungen in dieser Beziehung

504 Die durch die Leistungserbringerin erhobenen und bearbeiteten Daten, zumal solche die der Dokumentationspflicht unterliegen, sind regelmässig personenbezogen. Sie hängen direkt oder indirekt[1378] mit dem Gesundheitszustand der Patientin zusammen und werden in aller Regel bei der Patientin selbst erhoben, durch Befragung, körperliche oder apparative Untersuchung, Fragebogen oder per Telefon oder App.[1379] Gelegentlich werden ergänzende Fragen auch an Angehörige gestellt und Daten aus vergangenen Erhebungen eingeholt, etwa von anderen Ärztinnen, Labors oder Praxen.[1380] Solche Gesundheitsdaten sind durch das DSG besonders geschützt und vielfach aus Sicht der Patientin besonders intim. Entsprechend muss eine Patientin darauf vertrauen können, dass eine Leistungserbringerin ihre Daten vertraulich behandelt, ansonsten sie ihr diese kaum bekanntgibt.[1381] Aus diesem Grund existiert eine berufliche Schweigepflicht, welche u.a. Leistungserbringerinnen strafbewehrt dazu verpflichtet, Daten vertraulich zu behandeln (Art. 62 DSG, siehe ferner Art. 321 StGB). Daraus lässt sich folgern, dass entsprechende Daten nicht in grossem Umfang übertragen werden sollen.

505 Die Tätigkeit der Leistungserbringerinnen befindet sich, wie der gesamte Sektor, aufgrund von Digitalisierungsbestrebungen im Umbruch. Sie bedienen sich zunehmend elektronischer Hilfsmittel, um Daten zu erheben, oder beziehen bereits erhobene Informationen, etwa zu Gesundheitsdeterminanten, aus anderen Kontexten wie bspw. einer Smartwatch.[1382] Dennoch dürfte gerade die ärztliche Anamnese noch öfter als Datenerhebungen in anderen Sektoren rein

1378 Mit den zunehmenden Verknüpfungsmöglichkeiten lassen sich auch aus «gewöhnlichen» Daten u.U. gesundheitliche Folgerungen ziehen, siehe dazu SCHNEBLE/ELGER/SHAW, JMIR 2020, *passim*; insoweit von «Gesundheitsdeterminanten» sprechend Bundesrat, Bericht Nutzung von Gesundheitsdaten, 11; siehe zur umstrittenen Frage ob solche Daten «Gesundheitsdaten» i.S.v. Art. 5 lit. c Ziff. 2 DSG darstellen BSK DSG-BLECHTA/DAL MOLIN/WESIAK-SCHMIDT, Art. 5 N 57; siehe auch bereits Botschaft DSG 1988, 446, welche festhielt, dass nur medizinische Befunde, welche sich für die Betroffenen negativ auswirken könnten, erfasst sind; dazu ferner GEORGE, Gesundheitswesen, Rz. 2166 f. m.w.H.

1379 GERBER, 51; WIDMER/EGLI, Rz. 191.

1380 GERBER, 51.

1381 Ähnlich WIDMER/EGLI, Rz. 156.

1382 Während eine Leistungserbringerin gewisse Angaben durch Befragungen oder Untersuchungen feststellen kann, lassen sich andere Angaben auf anderem Weg u.U. besser und objektiver einholen, siehe dazu Rz. 549.

analog erfolgen, etwa durch das Ausfüllen eines Anamneseformulars oder durch handschriftliche Notizen der behandelnden Ärztin.[1383]

dd. Folgerungen

Nach dem Gesagten ist die Ausübung des Portabilitätsrechts in der Beziehung zwischen Patientin und Leistungserbringerin grundsätzlich möglich. Dennoch schränken mehrere Punkte dessen Anwendbarkeit ein. So ist kein Portabilitätsrecht möglich, wenn Leistungserbringerinnen, öffentliche Organe sind oder im Umgang mit der Patientin eine öffentliche Aufgabe wahrnehmen. Sie unterliegen kantonalem Datenschutzrecht und sind von Art. 28 DSG nicht erfasst. Dies dürfte praktisch viele Fälle betreffen und viele Datenbearbeitungen vom Portabilitätsrecht ausschliessen. 506

Unterliegen Leistungserbringerinnen allerdings dem DSG, ist prinzipiell eine Geltendmachung des Portabilitätsrechts möglich. Die erhobenen Daten und einzelnen Schritte einer Datenbearbeitung sind jedoch im Hinblick auf die Einschränkung gemäss Art. 28 Abs. 1 lit. b DSG genau zu unterscheiden. Denn obwohl sich eine medizinische Behandlung regelmässig auf eine informierte Einwilligung stützt,[1384] muss die damit einhergehende Datenbearbeitung nicht zwingend auf einer Einwilligung basieren[1385]. Vielmehr können Private auch Daten im Einklang mit den Grundsätzen des DSG erheben (siehe Art. 30 Abs. 2 lit. a DSG). In diesen Fällen liegt keine Persönlichkeitsverletzung vor, weshalb eine Rechtfertigung, etwa eine Einwilligung, nicht notwendig ist.[1386] In anderen Fällen lassen sich Datenbearbeitungen aus anderen Gründen rechtfertigen, namentlich aufgrund einer gesetzlichen Verpflichtung (siehe Art. 31 Abs. 1 DSG).[1387] Dies trifft bspw. auf ein beim Eintritt in ein Spital angelegtes Falldos- 507

1383 Noch 2014 gaben etwa erst 62 % der befragten Praxisärztinnen an, über ein elektronisches System zur Speicherung und Verwaltung von Patientendaten zu verfügen. 2024 waren es hingegen bereits 84 %, siehe GOLDER et al.

1384 Sog. «informed consent», siehe bspw. § 20 PatG/ZH; grundlegend dazu GUILLOD, 295 ff.

1385 WIDMER/EGLI, Rz. 192; grundlegend und durchaus kritisch zur datenschutzrechtlichen Einwilligung im medizinischen Kontext ERARD/DI TRIA, Jusletter 2024, Rz. 12 ff., 29 ff. und *passim*; dazu auch SCHRADER, 129.

1386 Ebenso WIDMER/EGLI, Rz. 193 f.; dazu im Kontext des Portabilitätsrechts Rz. 194 f.

1387 PC LPD-GENECAND, Art. 31 N 46; ERARD/DI TRIA, Jusletter 2024, Rz. 21, 27 und 29; weniger deutlich indes AEBI-MÜLLER et al., Arztrecht 2024, Rz. 1344 f., die zwar die Datenerhebung als vertragliche Pflicht bezeichnen, eine Datenerhebung jedoch nur ausnahmsweise als ohne Einwilligung zulässig erachten. Siehe auch AEBI-MÜLLER, Jusletter 2020, Rz. 10, nach welcher nur in seltenen Fällen andere Rechtfertigungsgründe als die Einwilligung in Betracht kommen. Sie bezieht sich dabei allerdings nur auf eine Offenbarung an Dritte, nicht auf initiale Erhebung.

sier zu, welches die Leistungserbringerin gestützt auf die erwähnten Dokumentationspflichten erstellt.[1388] Eine Patientin wird in diesem Fall nicht um ihre Einwilligung gefragt und sie kann das Anlegen eines solchen Dossiers nicht verhindern.[1389] Ebenfalls nicht verhindern kann sie hernach die Aufbewahrung nach Massgabe der einschlägigen Dokumentationspflichten.

508 Die initiale Beschaffung[1390] resp. Erhebung von Gesundheitsdaten, zumal solchen die von der Patientin bekanntgegeben und nicht bei Dritten eingeholt wurden, erfolgt jedoch in aller Regel gestützt auf einen Behandlungsvertrag[1391] oder eine Einwilligung[1392]. Eine solche Einwilligung muss bei Gesundheitsdaten ausdrücklich erfolgen (siehe Art. 6 Abs. 7 lit. a DSG). In beiden Fällen ist damit für Gesundheitsdaten, die eine Patientin anlässlich eines Gesprächs dem Arzt offenbart, oder deren Erhebung sie zulässt,[1393] die Voraussetzung nach Art. 28 Abs. 1 lit. b DSG erfüllt, auch wenn Leistungserbringerinnen über eine gesetzliche Grundlage verfügen und zur Dokumentation verpflichtet sind. Im hier interessierenden privatrechtlichen Verhältnis zwischen Leistungserbringerin und Patientin führt einzig ein abgeschlossener Behandlungsvertrag dazu, dass die Patientin die Daten bekanntgibt, und dies wohl regelmässig gestützt auf eine Einwilligung.[1394] Eine Erhebung ist kaum denkbar, ohne dass die

1388 Waldmeier, 143, welche den konkreten Datenfluss am Beispiel des (öffentlich-rechtlichen) Universitätsspitals Basel erläutert. Als Rechtfertigung führt sie einerseits § 3 Abs. 1 des Gesetzes über die öffentlichen Spitäler des Kantons Basel-Stadt auf und andererseits die Dokumentationspflichten nach § 29 GesG/BS, die auch für Private Anwendung finden; die kantonalgesetzliche Grundlage kann dabei auch eine Datenbearbeitung nach dem DSG rechtfertigen Erard/di Tria, Jusletter 2024, Rz. 19 m.w.N.; dazu bereits Rz. 503.

1389 Waldmeier, 143.

1390 So die Terminologie des DSG in Art. 5 lit. d. Die von der DSGVO verwendete Terminologie, die von einer Erhebung bzw. einer Erfassung spricht, scheint im medizinischen Kontext indes angebrachter und wird auch im Humanforschungsrecht verwendet (vgl. Art. 17 HFG).

1391 Siehe für das europäische Recht Dierks, 230 f., der sich auf die Verarbeitungsgrundlage nach Art. 9 Abs. 2 lit. h DSGVO bezieht. Diese wurde im DSG jedoch nicht übernommen. M.E. lässt sich aber die Rechtfertigung im Schweizer Recht auf Art. 31 Abs. 2 lit. a DSG abstützen, die auch für besonders schützenswerte Personendaten gilt. Ebenso Schrader, 129 m.w.N., nach welcher es «zumeist» nicht notwendig ist, eine Einwilligung einzuholen.

1392 Aebi-Müller et al., Arztrecht 2024, Rz. 1347; ähnlich bereits Aebi-Müller et al., Arztrecht 2016, § 9 Rz. 4; PC LPD-Genecand, Art. 31 N 46; siehe hierzu jedoch Erard/di Tria, Jusletter 2024, Rz. 21, die gerade mit Blick auf die Dokumentationspflicht auch eine gesetzliche Grundlage für die Beschaffung («*collecte*») aufführen.

1393 Namentlich durch apparative Untersuchungen wie Röntgenaufnahmen, Ultraschall oder Kernspintomographie oder eine Blutabnahme, in welche die Patientin einwilligt. Siehe auch Rosenthal, Jusletter 2020, Rz. 134.

1394 Vereinzelte Ausnahmen scheinen die Regel zu bestätigen, siehe die in Art. 34 Abs. 2 EpG verankerte Pflicht, der zuständigen Ärztin Auskunft über den eigenen Gesundheitszustand und über Kontakte zu anderen Personen zu geben. Ähnlich sind auch die Pflichten

Patientin mitwirkt. Daran ändern Dokumentationspflichten – die erst greifen, wenn eine Beziehung zwischen Leistungserbringerin und Patientin überhaupt erst existiert – nichts. Die Daten werden freiwillig[1395] einer Leistungserbringerin bekanntgegeben und fallen somit unter Art. 28 Abs. 1 lit. b DSG.[1396] Andere Daten, die eine private Leistungserbringerin gestützt auf andere Rechtfertigungsgründe erhebt und bearbeitet, fallen hingegen nicht unter das Portabilitätsrecht. Zu denken ist etwa an Daten, die die Leistungserbringerin im Zusammenhang mit der Abrechnung der obligatorischen Krankenversicherung erfasst.[1397]

Einschränkend wirkt zudem die Voraussetzung nach Art. 28 Abs. 1 lit. a DSG. Dies ist dann relevant, wenn eine Leistungserbringerin Patientendaten nicht automatisiert bearbeitet, sondern Fallakten rein physisch aufbewahrt. Wie bereits erläutert, ist eine Verantwortliche nicht verpflichtet, Daten entsprechend aufzubereiten.[1398] Allerdings dürfte diese Einschränkung gerade mit Blick auf die zunehmende Digitalisierung des Gesundheitswesens gegenwärtig stark an Bedeutung verlieren. 509

Ferner ist darauf hinzuweisen, dass besonders in der Beziehung zwischen Patientin und Leistungserbringerin die Abgrenzung zwischen beobachteten und abgeleiteten Daten praktisch schwierig ist und die Daten technisch oft nur schwer trennbar sind.[1399] Bereits eine Diagnose kann ein abgeleitetes Datum darstellen, welches sich etwa aus den Aussagen einer Patientin und einer durchgeführten Messung ergibt.[1400] Zudem muss in dieser Beziehung der Datensicherheit besonderes Gewicht zukommen, weil Gesundheitsdaten heikel sein können und Betroffene i.d.R. keine Voraussetzungen für sichere Kommunikationswege mitbringen.[1401] Damit unterscheiden sie sich von anderen Leistungserbringerinnen. Ebenfalls problematisch ist die vielfach sehr grosse Da- 510

zur ärztlichen Untersuchung resp. Behandlung nach Art. 36 f. EpG. Allerdings wäre in diesen Fällen noch zu untersuchen, ob die Ärztin überhaupt dem DSG für Private untersteht.

1395 Dazu Rz. 196 ff. Damit liegt auch ein Unterschied zu den in Fn. 1394 genannten Fällen vor. Folglich ist die Ausübung des Portabilitätsrechts auch dann möglich, wenn gar keine Persönlichkeitsverletzung vorliegt.

1396 Bühler, Rz. 161; siehe auch Schrader, 286, wonach unter der DSGVO bei einer Patientenbehandlung Datenverarbeitungen, die sich auf Art. 9 Abs. 2 lit. h DSGVO stützten aufgrund von Erw.G 68 Satz 3 DSGVO trotzdem der Portierung unterliegen sollten; ebenso BeckOK DSR-von Lewinski, Art. 20 DSGVO N 33.

1397 CR LPD-Benhamou, Art. 28 N 29.

1398 Dazu Rz. 198.

1399 Drepper/Schlünder/Buckow, 190.

1400 Li/Quinn, CLSR 2024, 7; Schrader, 287.

1401 Drepper/Schlünder/Buckow, 191 f.

tenmenge im medizinischen Bereich, etwa Daten, die aus modernen Bildgebungsverfahren stammen oder bei einer Sequenzierung des Genoms anfallen.[1402] Dies kann eine Herausgabe an die Patientin erschweren.

511 Schliesslich ist klarzustellen, dass das Berufsgeheimnis nach Art. 321 StGB vorliegend nicht von Belang ist. Da das Portabilitätsrecht nur auf Initiative der Betroffenen und damit mit deren Einwilligung eine Datenübertragung an Dritte vorsieht, wird das Berufsgeheimnis nicht verletzt (siehe Art. 321 Ziff. 2 StGB).[1403]

ee. Bundesorgane als Leistungserbringer

512 Bislang war von kantonalen öffentlichen Organen die Rede oder von privaten Verantwortlichen, die unter das DSG fallen. Tatsächlich gibt es für Bundesorgane im Gesundheitsbereich nur wenige Anwendungsbeispiele[1404] und von der Verpflichtung zur Datenportierung sind sie meist ausgenommen.[1405] Sie unterstehen nicht dem Rechtfertigungsregime von Art. 31 DSG, sondern müssen, wie kantonale Organe, i.d.R.[1406] für sämtliche Datenbearbeitungen über eine Rechtsgrundlage verfügen.[1407] Bundesorgane sollten aber bei der Voraussetzung nach Art. 28 Abs. 1 lit. b DSG ebenfalls primär an das Kriterium der Freiwilligkeit der Datenbearbeitung anknüpfen. Findet diese aus Sicht der Betroffenen freiwillig statt, ist m.E. mit Blick auf die Zielsetzungen des Portabilitätsrechts auch eine Bundesbehörde zur Portierung verpflichtet. Mit Blick auf die aufgeführten Beispiele[1408] wäre eine Patientin also nach einer (hoheitlich durchgeführten) sanitarischen Untersuchung am Zoll gestützt auf Art. 36 EpG nicht portabilitätsberechtigt, ein in einem Bundesasylzentrum ärztlich betreuter Flüchtling hingegen schon.

1402 Drepper/Schlünder/Buckow, 189 f.

1403 Dazu Erard/di Tria, Jusletter 2024, Rz. 18.

1404 Schweizer, digma 2020, 206 nennt sanitarische Untersuchungen an der Zollgrenze oder die gesundheitliche Betreuung von Flüchtlingen in Bundesasylzentren. Zu nennen wäre ferner die Tätigkeit des sog. militärischen Gesundheitswesens gestützt auf Art. 34*a* MG.

1405 Dazu Rz. 494.

1406 Siehe Art. 34 Abs. 4 DSG, der u.a. eine Einwilligung im Einzelfall vorsieht.

1407 Auf kantonaler Ebene etwa anschaulich das vom Universitätsspital Basel gestützt auf das IDG/BS veröffentlichte «Verzeichnis der Verfahren mit Personendaten», welches über sämtliche Datenbearbeitungsverfahren, deren Zweck und deren Rechtsgrundlage Aufschluss gibt, abrufbar unter: https://perma.cc/UH6J-8YDW.

1408 Dazu Fn. 1404.

ff. Europäischer Raum für Gesundheitsdaten (EHDS)

Die EU regelt die Beziehungen zwischen den Akteurinnen des Gesundheitswesens künftig spezialgesetzlich durch die EHDS-VO. Dabei handelt es sich um die erste Umsetzung eines sektorspezifischen gemeinsamen europäischen Datenraums.[1409] In der EHDS-VO finden sich Vorgaben für die Beziehung zwischen natürlichen Personen (darunter Patientinnen) und Gesundheitsdienstleisterinnen, welche im Wesentlichen der Rolle der Leistungserbringerinnen entsprechen.[1410] Der Gesundheitsdatenraum (EHDS) soll erstmals gemeinsame Vorschriften, Standards und Infrastrukturen sowie einen Governance-Rahmen schaffen und so den Zugang zu elektronischen Gesundheitsdaten erleichtern (Art. 1 Abs. 1 EHDS-VO). Die Verordnung trat am 26. März 2025 in Kraft und gilt grundsätzlich ab dem 26. März 2027, wobei gerade die hier besprochenen Bestimmungen teils erst später gelten (siehe Art. 105 EHDS-VO). 513

Die EHDS-VO baut u.a. auf den Betroffenenrechten der DSGVO auf und soll sie präzisieren und ergänzen (Art. 1 Abs. 2 lit. a sowie Erw.G 8 EHDS-VO). Die Verordnung unterscheidet zwischen einer Primärnutzung und einer Sekundärnutzung von elektronischen Gesundheitsdaten, wobei im Kontext der Leistungserbringerinnen die Primärnutzung in Kapitel II von Interesse ist. Sie umfasst die Verarbeitung elektronischer Gesundheitsdaten für die Gesundheitsversorgung zur Beurteilung, Erhaltung oder Wiederherstellung des Gesundheitszustands einer natürlichen Person, einschliesslich der Verschreibung, Abgabe und Bereitstellung von Arzneimitteln und Medizinprodukten, sowie für die einschlägigen Sozialleistungen und für die einschlägigen Dienste der Verwaltung oder Kostenerstattung (so Art. 2 Abs. 2 lit. d EHDS-VO). 514

Hinsichtlich einer solchen Primärnutzung ist in Art. 7 EHDS-VO ein «Recht natürlicher Personen auf Datenübertragbarkeit» vorgesehen. Es verpflichtet die Gesundheitsdienstleisterinnen, einer Betroffenen ganz oder teilweise Zugang zu ihren personenbezogenen elektronischen Gesundheitsdaten zu gewähren oder diese an eine andere Gesundheitsdienstleisterin zu übermitteln (Abs. 1). Dies hat unverzüglich, kostenlos und ungehindert zu erfolgen (Abs. 1). Nach Abs. 3 hat die Betroffene ferner das Recht, die Übermittlung ihrer Daten an eine eindeutig bestimmte Empfängerin aus dem Bereich der sozialen Sicherheit oder der Erstattungsdienste zu verlangen. 515

1409 Europäische Kommission, Vorschlag EHDS, 1; siehe auch Rz. 395 f.

1410 Art. 2 Abs. 1 lit. b EHDS-VO verweist dabei auf Art. 3 lit. g der RL 2011/24/EU, welche Gesundheitsdienstleister definiert als jede natürliche oder juristische Person oder sonstige Einrichtung, die im Hoheitsgebiet eines Mitgliedstaats rechtmässig Gesundheitsdienstleistungen erbringt.

516 Damit ist in der EHDS-VO ein Recht auf Datenportabilität verankert. Dieses unterscheidet sich jedoch verschiedentlich vom datenschutzrechtlichen Portabilitätsrecht. Zunächst schränkt die sektorspezifische Regelung den Kreis der Normadressatinnen auf Gesundheitsdienstleisterinnen ein, ebenso wie den Kreis der zulässigen Datenempfängerinnen. Eine Übermittlung ist also nur innerhalb des Gesundheitswesens möglich. Dies überzeugt, geht es doch gerade um den Aufbau eines Gesundheitsdatenraums, welcher den Austausch der – oftmals heiklen – Daten *innerhalb* des Gesundheitsdatenökosystems ermöglichen soll.

517 Weiter sind unter der EHDS-VO sämtliche personenbezogenen elektronischen Gesundheitsdaten (siehe dazu Art. 2 Abs. 2 lit. a i.V.m. Art. 2 Abs. 1 lit. a EHDS-VO) von der Portabilitätspflicht umfasst. Dies beinhaltet auch abgeleitete Daten (siehe Erw.G 6 und 15 EHDS-VO). Da, wie gesehen, bereits Diagnosen im medizinischen Kontext u.U. als abgeleitete Daten zu qualifizieren sind, erscheint dies sinnvoll.[1411] Zudem dürften mit Blick auf die (medizinische) Selbstbestimmung der Betroffenen die Interessen der Patientin gegenüber allfälligen Geschäftsinteressen von Gesundheitsdienstleistern überwiegen.[1412] Die Daten sind zudem unabhängig von der Rechtsgrundlage, aufgrund welcher sie verarbeitet werden, vom sektorspezifischen Recht erfasst (Erw.G 15 EHDS-VO). Eine Einschränkung wie unter der DSGVO resp. dem DSG ist nicht vorgesehen.

518 Schliesslich kann eine Gesundheitsdienstleisterin nicht auswählen, in welchem Format sie die Daten übermitteln möchte: Art. 15 EHDS-VO sieht ein einheitliches europäisches Austauschformat für die Sammlung elektronischer Gesundheitsdaten (*electronic health record* oder EHR) vor. Die entsprechenden technischen Spezifikationen, welche ein gängiges, maschinenlesbares und die Übertragung personenbezogener elektronischer Gesundheitsdaten zwischen verschiedenen Softwareanwendungen, Geräten und Gesundheitsdienstleistern ermöglichendes Format vorsehen müssen, legt die EU-Kommission fest (Art. 15 Abs. 1 EHDS-VO). Damit wird das Gesundheitswesen im Bereich der Primärnutzung faktisch durch die EU-Kommission standardisiert und eine Interoperabilität im Geltungsbereich des EHDS angestrebt.

519 Um die Ausübung des Rechts auf Datenübertragbarkeit und weiterer in Kapitel II vorgesehener Rechte zu ermöglichen, müssen die Mitgliedstaaten sog. Zugangsdienste für elektronische Gesundheitsdaten einrichten (Art. 4

1411 Dazu Rz. 510.

1412 Dies kann bei der Sekundärnutzung anders sein und wird in Art. 52 EHDS-VO berücksichtigt. Zur Beziehung der Probandin mit Forschenden Rz. 535 ff.

EHDS-VO). Dabei handelt es sich um einen Onlinedienst (etwa ein Portal oder eine App) mit welchem Patientinnen Zugang zu ihren eigenen elektronischen Gesundheitsdaten erhalten können (Art. 2 Abs. 2 lit. h EHDS-VO). Dieser ist für die Patientin kostenlos und ermöglicht es ihr, eigenständig Daten in ihr EHR einzugeben oder unrichtige Einträge online zu berichtigen (Art. 4 ff. EHDS-VO).

gg. Rechtslage in der Schweiz

In der Schweiz existiert bislang kein mit dem EHDS vergleichbares Gesetzgebungsprojekt. Im Zusammenhang mit der gesundheitspolitischen Strategie 2020–2030 des Bundesrates («Gesundheit2030») wird jedoch generell angestrebt, dem technologischen und digitalen Wandel vermehrt Rechnung zu tragen. So soll ein von Bund, Kantonen, Wissenschaft und weiteren Interessenkreisen der Gesellschaft getragener nationaler Rahmen für die Verwaltung digitaler Gesundheitsdaten geschaffen werden.[1413] Ausfluss daraus ist das Programm zur Förderung der digitalen Transformation im Gesundheitswesen («DigiSanté»). Da die eidgenössischen Räte bislang erst den bereits erwähnten Verpflichtungskredit für die Jahre 2025–2034 gesprochen haben, sind lediglich grobe Konzepte bekannt; konkrete Auswirkungen und Ausgestaltungen sind noch nicht abschätzbar. Erklärtes Ziel ist es allerdings, dass Systeme nahtlos zusammenarbeiten können und Informationen nicht mehrfach erhoben werden müssen (sog. Once-Only-Prinzip).[1414] Ferner soll DigiSanté klare Regeln für den Datenzugang schaffen und die Mehrfachnutzung durch verschiedene Akteurinnen ermöglichen.[1415] Im Kern sollen also die Datenflüsse des Gesundheitswesens im Sinne dieser Grundlagen optimiert werden. Ob dabei, wie unter dem EHDS, auf eine an das Portabilitätsrecht angelehnte Regelung gesetzt wird, ist noch offen. 520

Bereits heute positivrechtlich verankert sind ähnliche Regelungen jedoch in der Gesetzgebung zum elektronischen Patientendossier. Das EPDG soll in der Schweiz die Qualität der medizinischen Behandlung stärken, die Behandlungsprozesse verbessern, die Patientensicherheit erhöhen, die Effizienz des Gesundheitssystems steigern und die Gesundheitskompetenz der Patientinnen fördern (Art. 1 Abs. 3 EPDG). Das EPDG sieht u.a. Zugangsrechte zum Patientendossier vor, für die Patientin einerseits (Art. 8 EPDG) und für Gesundheitsfachpersonen andererseits, soweit diese über entsprechende Zugriffsrechte 521

1413 Bundesrat, Bericht Gesundheit2030, 15.
1414 Botschaft Verpflichtungskredit, 13.
1415 Botschaft Verpflichtungskredit, 13.

verfügen (Art. 9 EPDG). Eine Patientin kann zudem die Anbieterin des Patientendossiers (sog. Stammgemeinschaft) wechseln. Die Stammgemeinschaft muss dafür nach Art. 17 Abs. 1 lit. e EPDV einen Prozess zum Wechsel vorsehen, was einem sachlich eng begrenzten Portabilitätsrecht gleichkommt.[1416] Das EPD gilt allerdings weitgehend als gescheitert; Fachkreise bemängeln, dass hinterlegte Daten nicht interoperabel abgelegt werden und somit lediglich ein «PDF-Friedhof» entstehe.[1417] Nachdem ein Vorentwurf für eine umfassende Revision des EPDG im Vernehmlassungsverfahren kritisiert wurde,[1418] hat der Bundesrat jüngst eine grundlegende Neuausrichtung beschlossen: Er möchte das EPD durch ein elektronisches Gesundheitsdossier (EGD) ersetzen.[1419] Am 5. November 2025 hat der Bundesrat die Botschaft für ein entsprechendes Gesetz (E-EGDG) an das Parlament überwiesen.[1420]

522 Das EGD soll sicherstellen, dass Personen mittels eines elektronischen Gesundheitsdossiers auf ihre behandlungsrelevanten Daten zugreifen und diese Daten Gesundheitsfachpersonen und Gesundheitseinrichtungen zugänglich machen können (Art. 1 E-EGDG). Die neue Terminologie unterstreicht, dass das EGD die Schweizer Bevölkerung durch alle Lebensphasen begleiten soll und nicht nur durch solche der Krankheit.[1421] Materiell ist die wesentlichste Änderung jedoch ein neu geschaffenes Informationssystem, das der Bund betreibt. Dieses soll künftig sämtliche Daten, einschliesslich der Gesundheitsdossiers, zentral aufbewahren (Art. 5 ff. E-EGDG). Eine weitere Neuerung ist ein Opt-Out-Modell für die Bevölkerung.[1422] Zudem sollen nicht nur stationäre, sondern auch ambulante Leistungserbringerinnen verpflichtet sein, sich dem EGD anzuschliessen und alle behandlungsrelevanten Daten einzutragen.[1423] Dadurch soll die breite Bevölkerung das EGD verwenden und einen Nutzen daraus ziehen, anders als dies beim EPD der Fall ist.

523 Die Art. 11 ff. E-EGDG legen fest, wer Zugang zu den Daten erhält. Inhaberinnen eines EGD können Daten in ihrem Gesundheitsdossier einsehen und sie in

1416 Siehe dazu Weber/Thouvenin, 62 f.

1417 So bspw. Urech Marcel, «EPD: Es droht der PDF-Friedhof», Netzwoche vom 16. September 2019, abrufbar unter: https://perma.cc/2E7U-3SGE.

1418 Botschaft EGDG, 24 ff., wobei der Bundesrat hervorhob, dass die überwiegende Mehrheit die Zielsetzungen und Stossrichtungen des VE-EPDG unterstützt habe.

1419 Bundesrat, Medienmitteilung vom 5. November 2025.

1420 Bundesrat, Medienmitteilung vom 5. November 2025.

1421 Botschaft EGDG, 8.

1422 Botschaft EGDG, 14 f.; dies sah bereits der VE-EPDG vor, siehe Bundesrat, Bericht Vernehmlassung EPDG, 10.

1423 Botschaft EGDG, 14; dies sah bereits der VE-EPDG vor, siehe Bundesrat, Bericht Vernehmlassung EPDG, 27.

einem gängigen elektronischen Format beziehen (Art. 11 Abs. 1 lit. a E-EGDG). Zudem können sie Gesundheitsfachpersonen und Gesundheitseinrichtungen Einsicht in ihre Gesundheitsdaten gewähren und ihnen erlauben, diese Daten in ihren Systemen zu speichern (Art. 11 Abs. 2 lit. a E-EGDG). Dies gilt auch für digitale Gesundheitsanwendungen, wenn die Inhaberin eines EGD die entsprechende Berechtigung erteilt (Art. 11 Abs. 2 lit. c E-EGDG). Die Gesundheitsanwendungen müssen allerdings durch das EDI zugelassen sein und zwingende Anforderungen an Sicherheit und Datenschutz erfüllen.[1424] Entgegen dem vorliegenden Verständnis von gesundheitsrelevanten Anwendungen muss es sich dabei nicht zwingend um Lifestyleprodukte handeln. Gemäss Bundesrat können auch Medizinprodukte digitale Gesundheitsanwendungen i.S.d. EGDG darstellen.[1425]

Anders als im Vorentwurf sind neu klare technische Vorgaben geplant.[1426] Nach Art. 7 E-EGDG hat der Bundesrat die Datenübermittlung zwischen unterschiedlichen Systemen im Ausführungsrecht zu regeln. Er muss dabei anerkannte internationale Normen sowie den aktuellen Stand der Technik berücksichtigen und Datenformate und Vorgaben für die technische Anbindung festlegen (Art. 7 E-EGDG). Der Bundesrat legt m.a.W. die zu verwendenden Normen, Standards, Datenformate und Integrationsprofile verpflichtend fest.[1427] Gängige und verbreitete Standards für strukturierte Gesundheitsdaten (etwa FHIR), sollen es ermöglichen, Daten zwischen verschiedenen Anwendungen und Systemen interoperabel auszutauschen.[1428] Gesundheitsfachpersonen und Gesundheitseinrichtungen müssen die Formate nach einer Übergangsfrist zwingend verwenden.[1429] 524

Das EGDG enthält künftig ein auf Gesundheitsdaten beschränktes Recht auf Datenherausgabe, mit welchem die Inhaberinnen des EGD ihre Daten herunterladen und auf einem persönlichen Datenträger speichern können (Art. 11 E-EGDG).[1430] Ebenfalls bedeutend ist, dass der Bund eine umfassende Infrastruktur schafft, die über alle Leistungserbringerinnen hinweg die Möglichkeit zur Datenübertragung vorsieht. Anders als unter dem gescheiterten EPD macht der Bundesrat hierbei zwingende Vorgaben, um eine Interoperabilität zu ermöglichen. Dabei stehen die Inhaberinnen des EGD weiterhin im Zentrum. Sie 525

1424 Botschaft EGDG, 34 und 50.
1425 Der Bundesrat wird die Details im Ausführungsrecht regeln, siehe Botschaft EGDG, 61 f.
1426 Zurückhaltender noch Bundesrat, Bericht Vernehmlassung EPDG, 42.
1427 Botschaft EGDG, 45.
1428 Botschaft EGDG, 45.
1429 Botschaft EGDG, 45.
1430 Botschaft EGDG, 50.

können der Nutzung des EGD umfassend widersprechen oder die Zugriffsberechtigung auf ihre Gesundheitsdaten steuern.

526 Damit ist mit dem EGD ein zentralisierter Gesundheitsdatenraum für die Beziehung zwischen Patientin und Leistungserbringerin geplant.[1431] Dieses soll eng verbunden sein mit einem im Rahmen von DigiSanté noch zu entwickelnden Swiss Health Data Space (SwissHDS).[1432] Aktuell ist das EPD bzw. das künftige EGD jedoch die einzige technische Möglichkeit, behandlungsrelevante Daten schweizweit und sicher den Leistungserbringerinnen bereitzustellen.[1433] Dies gilt jedoch nur innerhalb der engen Grenzen des Gesundheitswesens. So enthält das EGD keine Möglichkeit, Daten der Forschung zur Verfügung zu stellen.[1434] Dies war im VE-EPDG noch vorgesehen, wurde aber aus der Vorlage entfernt, ohne dies weiter zu begründen.[1435] Allerdings möchte der Bundesrat bei der Schaffung von Rechtsgrundlagen für einen SwissHDS auch das EGDG erneut prüfen und gegebenenfalls erneut anpassen.[1436] Es ist damit weiter zu beobachten, ob der Gesetzgeber die Betroffene in ihrer Rolle als Patientin einzig mit dem EGD «digital selbstbestimmen»[1437] lassen möchte, oder ob er auch weitergehende Datenübertragungen ermöglichen wird.

b. Natürliche Person (Versicherte) und Versicherungsunternehmen

527 Krankenkassen bearbeiten als Bundesorgane Daten der natürlichen Personen, die in der Rolle als Versicherte auftreten. Gleiches gilt für Versicherungsunternehmen im Bereich der obligatorischen Unfallsversicherung. Sie bearbeiten Daten gestützt auf eine gesetzliche Grundlage nach Art. 84 KVG resp. Art. 96 UVG. Die gesetzliche Grundlage im KVG erlaubt es Krankenkassen und weiteren Akteurinnen, sämtliche Personendaten zu bearbeiten, die sie für ihre Aufgaben benötigen (Art. 84 Abs. 1 KVG). Eine parallele Bestimmung findet sich in Art. 96 Abs. 1 UVG für die Unfallversicherung. Versicherungsunternehmen bearbeiten Daten damit weder gestützt auf eine Einwilligung noch in unmittelbarem Zusammenhang mit einem Vertrag, selbst wenn ein solcher zwischen der Versicherten und der Krankenkasse resp. der Unfallversicherung existiert.

1431 Dazu Botschaft EGDG, 13. Aufgrund der geänderten Terminologie ist davon auszugehen, dass das EGD zukünftig auch weitere Rollen natürlicher Personen erfasst.
1432 Botschaft EGDG, 13 und 18 ff., Botschaft Verpflichtungskredit, 18 f.
1433 Botschaft EGDG, 19.
1434 Botschaft EGDG, 26.
1435 So noch Bundesrat, Bericht Vernehmlassung EPDG, 29 f.
1436 Botschaft EGDG, 21, die pauschal die Sekundärnutzung von Gesundheitsdaten aufführt.
1437 So UVEK/EDA, 13, allerdings noch zum EPD.

Daten werden somit nicht freiwillig und nach Massgabe der Versicherten bearbeitet, sondern vielmehr zwingend gestützt auf die gesetzliche Grundlage, um etwa für die Einhaltung der Versicherungspflicht zu sorgen, Leistungsansprüche zu beurteilen oder Leistungen zu berechnen, zu gewähren oder mit Leistungen anderer Sozialversicherungen zu koordinieren (siehe beispielhaft Art. 84 Abs. 1 lit. a–i KVG; ähnlich Art. 96 Abs. 1 lit. a–g UVG).[1438] Aus der Beziehung zwischen Versicherter und Krankenkasse resp. Unfallversicherung entstehen damit keine Portabilitätsansprüche und ein solches Versicherungsunternehmen muss gestützt auf Art. 28 DSG Daten weder herausgeben noch übertragen.[1439]

Demgegenüber sind Versicherungsunternehmen für andere Versicherungsarten (bspw. Zusatzversicherungen) als Private einzuordnen.[1440] Sie stehen in einer vertraglichen Beziehung zur Versicherten (siehe Art. 1 ff. VVG) und stützen Datenbearbeitungen primär auf den Vertrag oder eine Einwilligung. Aus diesem Grund ist die Ausübung des Datenportabilitätsrechts grundsätzlich denkbar, wobei ein besonderes Augenmerk auf das Kriterium der Bekanntgabe zu legen ist: Daten, die das Versicherungsunternehmen bei Dritten einholt (etwa bei Laboren oder Ärztinnen), fallen nicht unter das Portabilitätsrecht. 528

Oft nehmen Versicherungsunternehmen eine Doppelrolle als Bundesorgan (für die obligatorische Krankenversicherung) und Privatperson (für die Zusatzversicherung) ein. In diesen Fällen sind Behandlungen, die von der Grundversicherung abgedeckt und darüber hinaus mit zusatzversicherten Leistungen verbunden sind, als sog. Leistungen mit Sockelbeitrag aus der Grundversicherung ebenfalls als öffentliche Aufgabe zu qualifizieren (bspw. ein Einzelzimmer im Spital).[1441] Ein Anspruch auf Portierung besteht dann ebenfalls nicht. 529

c. Natürliche Person (Probandin) und Forschende

aa. Allgemein

Eine natürliche Person kann in der Rolle einer Probandin an einem Forschungsprojekt teilnehmen. Forschende unterstehen dabei unterschiedlichen rechtlichen Vorgaben. Für kantonale öffentliche Organe scheidet ein Portabi- 530

1438 Ausführlich dazu WIDMER/EGLI, Rz. 313 ff.

1439 Siehe CR LPD-BENHAMOU, Art. 28 N 24 und 29; BSK DSG-LAUX/STEINER, Art. 28 N 42; a.A. hinsichtlich der Kundendaten bei einem Wechsel der Versicherung BÜHLER, Rz. 162.

1440 WIDMER/EGLI, Rz. 34 und 355 f.

1441 GEORGE, Gesundheitswesen, 642; RÜTSCHE, Rz. 54 und 111; RÜTSCHE, digma 2012, 181.

litätsrecht von vornherein aus, weil für sie der Geltungsbereich des DSG nicht eröffnet ist.[1442] Handelt es sich bei den Forschenden um Private oder Bundesorgane, sind die Bestimmungen des DSG anwendbar. Im ersten Fall begründet ein Vertrag das Rechtsverhältnis zwischen den Akteurinnen.[1443] Im zweiten Fall verhält es sich analog zur Situation bei den Leistungserbringerinnen und das Rechtsverhältnis untersteht dem öffentlichen Recht, weil die Forschungstätigkeit als öffentliche Aufgabe erbracht wird.[1444] Das Verhältnis wird dann grundsätzlich durch eine Verfügung und durch gesetzliche Vorgaben geregelt, u.U. auch durch einen verwaltungsrechtlichen Vertrag.[1445]

531 Der Einwilligung kommt bei der Datenerhebung im Forschungsbereich in jedem Fall eine besondere Bedeutung zu. Dies gilt für Private wie öffentliche Organe. Grund dafür sind spezialgesetzliche Vorgaben im HFG, die gerade im hier untersuchten Gesundheitsbereich regelmässig gelten. Das HFG kommt für sämtliche Forschung im Humanbereich zur Anwendung, d.h. für Forschung zu Krankheiten des Menschen sowie zu Aufbau und Funktion des menschlichen Körpers (Art. 2 Abs. 1 HFG). Dies gilt nicht nur, wenn mit Personen interagiert oder mit biologischem Material geforscht wird, sondern bereits, wenn entsprechende Forschung mit personenbezogenen Gesundheitsdaten durchgeführt wird (Art. 2 Abs. 1 lit. e HFG). Eine Probandin darf dabei – unabhängig vom Rechtsverhältnis zu den Forschenden – nur in ein Forschungsprojekt einbezogen werden, wenn sie nach hinreichender Aufklärung eingewilligt hat (Art. 16 Abs. 1 HFG). In der Humanforschung stützt sich eine Datenerhebung damit regelmässig auf eine Einwilligung, wobei für die blosse Weiterverwendung von Gesundheitsdaten besondere Vorgaben gelten.[1446] Die erhobenen Daten unterliegen damit potenziell dem Portabilitätsrecht, sofern sie nicht von Beginn weg anonym erhoben wurden und solange sie nicht anonymisiert wurden und damit nicht (mehr) dem DSG unterliegen.

1442 Dazu Rz. 492.

1443 Grundlegend zum Vertragsverhältnis GRÜNIG, 81 ff.

1444 Ebenso GRÜNIG, 78 f.

1445 GRÜNIG, 79 m.w.N.

1446 Siehe auch BAERISWYL, digma 2020, 65. Zwar können Personendaten für die Forschung u.U. auch ohne Einwilligung der Probandin weiterverwendet werden, etwa in den Fällen von Art. 32 ff. HFG. Bei der initialen Erhebung von Personendaten durch Forschende in einem Humanforschungskontext führt indes kein Weg an der Einwilligung vorbei. Dies gilt selbst dann, wenn die Daten anonym erhoben werden und das HFG eigentlich keine Anwendung finden würde (Art. 2 Abs. 2 lit. c HFG), weil für die Erhebung eine (wenn auch anonyme) Interaktion mit der Probandin stattfinden muss, die dem HFG unterliegt (Art. 2 Abs. 1 lit. a HFG). Siehe dazu weiterführend SHK HFG-VAN SPYK, Art. 2 N 27.

bb. Sekundärnutzung für die Forschung

Die Beziehung zwischen Probandin und Forschenden ist besonders mit Blick auf eine Sekundärnutzung von Gesundheitsdaten relevant. Bei einer Sekundärnutzung treten Forschende nicht zwingend als alte, sondern eher als neue Verantwortliche auf und können so unmittelbar von einer Ausübung des Portabilitätsrechts profitieren.[1447] Sie ermöglicht die effiziente Verwendung von bereits erhobenen Daten zu neuen (Forschungs-)Zwecken und dies ohne eine Probandin durch eine (erneute) Erhebung zu belasten oder auch nur (zeitlich) zu beanspruchen. Grosse Hoffnungen ruhen daher gerade im Gesundheitsbereich auf der Sekundärnutzung von Daten und zahlreiche Register speichern bereits heute unterschiedliche Gesundheitsdaten zu diesem Zweck.[1448] 532

Die Daten für die Sekundärnutzung stammen aus unterschiedlichen Quellen. Vielfach wurden sie anlässlich eines vergangenen Forschungsprojekts erhoben und lassen sich anschliessend für ein neues Forschungsprojekt durch andere Forschende verwenden. In diesen Fällen kann das HFG bereits bei der Erhebung anwendbar sein. Die Daten können aber auch in einem anderen Kontext erhoben worden sein, etwa aufgrund einer gesetzlichen Verpflichtung oder als sog. *real world data* durch die Probandinnen selbst. Die Daten lassen sich dann nach Massgabe des HFG für ein entsprechendes Forschungsprojekt weiterverwenden. Denkbar ist, dass Probandinnen in diesen Fällen ihre Daten spenden, indem sie bspw. Behandlungsdaten bereitstellen oder einen Zugriff auf ihre Smartwatch erlauben und so zu Erkenntnissen in der Forschung beitragen. 533

Handelt es sich um ein Forschungsprojekt ausserhalb des Anwendungsbereichs des HFG, so sehen das DSG und die meisten kantonalen Datenschutzgesetze Privilegierungen für die Sekundärnutzung zu nicht personenbezogenen Zwecken vor, etwa für die Forschung.[1449] In diesen Fällen ist es erlaubt, Personendaten ohne Einwilligung der Probandin zu Forschungszwecken weiterzuverwenden, wenn dabei gewisse Voraussetzungen eingehalten werden. Sowohl das DSG als auch kantonale Datenschutzgesetze stehen also einer Weiterverwendung durch Forschende in der Rolle als neue Verantwortliche gegenüber offen. 534

1447 Ähnlich auch ROSENTHAL, Jusletter 2020, Rz. 134, der davon ausgeht, dass eine Patientin die Daten herausverlangt, um sie der Forschung zur Verfügung zu stellen.

1448 Siehe etwa eine Übersicht unter https://register-schweiz.fmh.ch/.

1449 Siehe Art. 31 Abs. 2 lit. e und Art. 39 DSG (für Private und Bundesorgane). Für die Kantone Zürich und Basel-Stadt etwa §§ 9 Abs. 2 und 18 IDG/ZH sowie §§ 10 und 22 IDG/BS.

cc. Europäischer Raum für Gesundheitsdaten (EHDS)

535 Die EHDS-VO regelt nicht nur die Primärnutzung von elektronischen Gesundheitsdaten,[1450] sondern in Kapitel IV auch deren Sekundärnutzung. Für welche Daten eine Sekundärnutzung zulässig ist, legt Art. 51 Abs. 1 EHDS-VO abschliessend fest: Erfasst sind u.a. elektronische Gesundheitsdaten aus dem EHR (lit. a), Verwaltungsdaten zur Gesundheitsversorgung (lit. e), automatisch durch Medizinprodukte generierte personenbezogene elektronische Gesundheitsdaten (lit. h) sowie Daten aus Wellness-Anwendungen (lit. i). Die Gesundheitsdateninhaberinnen müssen diese Daten zur Verfügung stellen, wobei nach Art. 50 Abs. 1 EHDS-VO Ausnahmen für Kleinstunternehmen[1451] und einzelne Forschende resp. natürliche Personen gelten. Sie müssen die Daten selbst dann zur Sekundärnutzung zur Verfügung stellen, wenn sie durch Immaterialgüterrechte geschützt werden oder Geschäftsgeheimnisse beinhalten, wobei ebenfalls gewisse Einschränkungen gelten (Art. 52 EHDS-VO). Da sämtliche elektronischen Gesundheitsdaten erfasst sind, ist ein Personenbezug nicht zwingend notwendig; auch nicht personenbezogene Daten sind zur Verfügung zu stellen.

536 Die Sekundärnutzung findet über sog. Zugangsstellen[1452] für Gesundheitsdaten statt. Sie werden von den Mitgliedstaaten benannt und übernehmen die Rolle einer Intermediärin zwischen den unterschiedlichen Akteurinnen im Bereich der Sekundärnutzung (Art. 55 Abs. 1 EHDS-VO). Art. 53 EHDS-VO gibt einen *numerus clausus* der zulässigen Zwecke der Sekundärnutzung vor. Erlaubt ist namentlich die wissenschaftliche Forschung im Gesundheits- oder Pflegesektor, worunter auch Entwicklungs- und Innovationstätigkeiten für Produkte oder Dienstleistungen und das Trainieren, Testen und Bewerten von Algorithmen gehört (Art. 53 Abs. 1 lit. e EHDS-VO). Zu diesen Zwecken kann jede natürliche oder juristische Person (sog. Gesundheitsdatennutzerin) bei einer Zugangsstelle einen Antrag auf Datenzugang stellen (Art. 67 Abs. 1 EHDS-VO). Die Zugangsstelle prüft diesen anschliessend. Dient der Antrag einem zulässigen Zweck und sind die verlangten Daten für diesen Zweck erforderlich, angemessen und verhältnismässig und sind auch alle weiteren Anforderungen nach Kapitel IV erfüllt, stellt die Zugangsstelle eine Datengenehmigung aus (Art. 68 EHDS-VO). Anschliessend hat die Zugangsstelle die elektronischen Gesundheitsdaten anzufordern und innerhalb von zwei Monaten nach Erhalt von den

1450 Dazu Rz. 513 ff.

1451 Siehe hierzu Art. 2 des Anhangs der Empfehlung 2003/361/EG.

1452 Nicht zu verwechseln mit den bei der Primärnutzung relevanten Zugangsdiensten für Gesundheitsdaten.

Gesundheitsdateninhaberinnen den Gesundheitsdatennutzerinnen bereitzustellen (Art. 68 Abs. 7 EHDS-VO).

Neben dem eben geschilderten Datenzugang ist eine sog. Gesundheitsdatenanfrage möglich. Bei dieser erhält die anfragende Person die Daten nur in einem anonymisierten und statistischen Format, ohne dass ihr ein Datenzugang zu den zugrundeliegenden Daten gewährt würde (Art. 69 Abs. 1 EHDS-VO). 537

Die Sekundärnutzung ist ohne Einwilligung der Probandinnen möglich. Art. 71 EHDS-VO sieht jedoch ein Widerspruchsrecht für Probandinnen vor («Opt-Out»). Demnach können diese nach Abs. 1 einer Verarbeitung der sie betreffenden personenbezogenen elektronischen Gesundheitsdaten für die Sekundärnutzung jederzeit und ohne Angabe von Gründen widersprechen. 538

Zusammenfassend lässt sich festhalten, dass der EHDS für die Sekundärnutzung kein Recht auf Datenübertragbarkeit der Betroffenen vorsieht. Vielmehr schafft er ein neuartiges System basierend auf Intermediärinnen, welche die Interessen der Betroffenen dadurch schützen sollen, dass sie die Voraussetzungen für eine Sekundärnutzung inhaltlich überprüfen und den Zugang zu Daten kontrollieren. Die Betroffene nimmt dabei keine zentrale Rolle ein; lediglich ein Widerspruchsrecht steht ihr zu. Dies ist insofern nicht überraschend, als dass es sich nicht zwingend um Personendaten handeln muss, sondern die Sekundärnutzung deutlich weiter gefasst wird. Das Vorgehen ist aber auch für Personendaten folgerichtig, da das europäische Datenschutzrecht für Personendaten ebenfalls Privilegierungen von Datenbearbeitungen zu Forschungszwecken vorsieht (siehe Art. 5 Abs. 1 lit. b und Art. 89 DSGVO). 539

dd. Rechtslage in der Schweiz

Mit einem 2022 veröffentlichten Bericht hat der Bundesrat in Erfüllung eines Postulats in der Schweiz die Schaffung von gesetzlichen Grundlagen für eine qualitativ hochstehende und effiziente Gesundheitsversorgung angestossen.[1453] Er schlägt darin ein System zur Weiterentwicklung des Datenmanagements im Gesundheitswesen vor, wobei er den Fokus auf die mehrfache Nutzung und die Verknüpfung von Gesundheitsdaten zu Forschungszwecken legt.[1454] Der Bundesrat greift verschiedene strategische Schwerpunkte des Berichts Datenräume und des Berichts Gesundheit2030 auf, etwa dass das Potenzial von Gesundheitsdaten besser genutzt und neue Formen der gemeinsa- 540

[1453] Bundesrat, Bericht Nutzung von Gesundheitsdaten, *passim*.
[1454] Bundesrat, Bericht Nutzung von Gesundheitsdaten, 8.

men Nutzung von Daten ermöglicht werden sollen.[1455] Trotz des breit gefassten Titels zielt der Bericht einzig – und anders als die EHDS-VO – auf die Nutzung zu Forschungszwecken ab.[1456] Eine Primärnutzung steht nicht im Zentrum.[1457]

541 Geschaffen werden soll ein Datenraum für Gesundheitsdaten bzw. ein «Nationales System zur Weiterverwendung und Verknüpfung von Gesundheitsdaten».[1458] Der Bund soll eine Dienstleistung anbieten, die den Austausch von qualitativ hochwertigen Gesundheitsdaten für die Weiterverwendung mit oder ohne Verknüpfung[1459] zwischen «Datenproduzentinnen» und «Datennutzerinnen» vermittelt und für diese abwickelt.[1460] Eine «Nationale Datenkoordinationsstelle» (NDKS) soll zu diesem Zweck errichtet werden und diese treuhänderische Aufgabe für den Bund übernehmen.[1461]

542 Der Bericht stösst die Entwicklung in der Schweiz erst an. Zahlreiche Detailfragen sind noch ungeklärt und werden gegenwärtig erst vertieft untersucht. Allerdings erscheint absehbar, dass Gesetzesanpassungen, wohl in Form einer Rahmengesetzgebung, zur Schaffung der notwendigen Strukturen und Prozesse unumgänglich sind.[1462] Aktuell prüft das EDI die Vorschläge des Berichts auf ihre Plausibilität und Praktikabilität und wird anschliessend gesetzliche Anpassungen vorschlagen, «insbesondere mit Blick auf die Konformität mit dem Datenschutz».[1463] In Bezug auf die Mechanismen, die das Teilen von Gesundheitsdaten ermöglichen sollen, bleibt der Bundesrat im Bericht äusserst vage.[1464] Er stellt zwar fest, dass den Datenproduzentinnen und -nutzerinnen u.a. Anreize zur Förderung der mehrfachen Datennutzung gesetzt werden

1455 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 15 f.

1456 Kritisch hierzu SPRECHER, MedR 2022, 836.

1457 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 13. Dies gilt sowohl für die Primärnutzung für die Forschung, welche der Bundesrat wohl bereits durch das geltende Recht abgedeckt sieht, als auch für die Primärnutzung in anderen Bereichen, etwa durch Leistungserbringerinnen.

1458 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 35 ff.

1459 Für die Verknüpfung werden Einzeldaten derselben Personen aus mindestens zwei Datensätzen mithilfe einer oder mehrerer sog. Verknüpfungsvariablen zusammengeführt. Eine solche könnte etwa die (eineindeutige) Sozialversicherungsnummer AHVN13 sein, siehe hierzu Bundesrat, Bericht Nutzung von Gesundheitsdaten, 12.

1460 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 37.

1461 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 37.

1462 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 44.

1463 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 45.

1464 Der Bundesrat räumt allerdings ein, dass der Bericht keine fundierte datenschutzrechtliche Abhandlung zur Weiterverwendung und verknüpften Auswertung von Gesundheitsdaten sei, siehe Bundesrat, Bericht Nutzung von Gesundheitsdaten, 8.

müssten.[1465] Folglich seien in der von Wettbewerb gekennzeichneten Schweizer Forschungslandschaft Grundlagen und Anreizmechanismen zu prüfen, damit Datenproduzentinnen überhaupt Dritten den Zugang zu den von ihnen verwalteten Daten gewährten.[1466] Auf mögliche Lösungen geht der Bericht indes nicht ein. Allerdings lässt sich ihm entnehmen, dass die Akteurinnen «auf der Grundlage von gesetzlich festgehaltenen Datenrechten und ethischen Prinzipien, vertrauenswürdigen Prozessen und Infrastrukturen fair und selbstbestimmt zusammenarbeiten» sollen.[1467] Zunächst sei jedoch die Beziehung zwischen den Datenakteurinnen und deren Beziehung zu den Daten zu klären.[1468] Dabei sollen die Kontroll- und Nutzungsrechte über die Daten im Zentrum der Diskussion stehen.[1469] Immerhin hält der Bericht als Anforderung fest, dass die Einwilligung oder eine andere Form des adäquaten Einbezugs der Betroffenen zur primären und sekundären Datennutzung vorliegen müsse.[1470] Dies lässt darauf schliessen, dass die Probandin weiterhin miteinbezogen werden soll.

Eine Verpflichtung zum Teilen von Daten sieht das Nationale System zur Weiterverwendung und Verknüpfung von Gesundheitsdaten zu Forschungszwecken, soweit ersichtlich, nicht vor. Ausführlich behandelt der Bericht einzig die Notwendigkeit einer Einwilligung resp. eines Widerspruchsrechts der Probandin mit Blick auf die gesetzlichen Vorgaben im HFG und DSG.[1471] Denkbar seien neue Einwilligungsverfahren, etwa dynamische und interaktive Verfahren zur zweckgebundenen Einwilligung zur primären Erhebung und Nutzung von Daten resp. ein Widerspruchsrecht bezüglich der Sekundärnutzung von Daten.[1472] Ebenfalls erwogen wird ein Ausbau des Generalkonsents,[1473] womit eine Nutzung von Gesundheitsdaten zu Zwecken, die über die rein medizinische Forschung hinausgehen, erlaubt würde.[1474] 543

1465 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 37.
1466 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 29.
1467 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 26.
1468 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 26.
1469 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 26, wobei er anfügt, dass dies gelte, solange fraglich sei, ob es ein «Dateneigentum» gebe.
1470 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 35.
1471 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 33 f., 35, 40 f.
1472 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 40 f.
1473 Der Generalkonsent ist eine in Art. 32 f. HFG verankerte Art der Einwilligung, welche sich nicht auf ein konkretes Forschungsprojekt bezieht, sondern für noch unbestimmte Forschungszwecke abgegeben wird, siehe dazu SPRECHER, ZBJV 2018, Teil 2, 526 ff.
1474 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 41.

544 Einen vollständigen Rechtsrahmen für eine mehrfache Datennutzung würde dies noch nicht schaffen, denn Änderungen am Einwilligungsverfahren betreffen bloss die Berechtigung, nicht aber eine Verpflichtung zur Weitergabe von Gesundheitsdaten. Für Datenproduzentinnen kann es aufwändig sein, Daten zu teilen und eine u.U. kostspielige Infrastruktur für deren Weitergabe zu entwickeln. Daher lässt sich nicht folgern, dass die Daten in jedem Fall der Forschung offenstehen. Ausgehend von den bislang verfügbaren Informationen könnte das Portabilitätsrecht im Sinne eines Mittelwegs in dieser Beziehung eine Lücke füllen. Denn wenn ein Datensatz dem Portabilitätsrecht unterliegt, existiert ein rechtlicher Anspruch auf eine Übertragung an Forschende auch entgegen dem Willen der Datenproduzentin.[1475] Dabei steht die Probandin als Betroffene im Zentrum und kann selbstbestimmt entscheiden, ob sie gewisse Daten der Forschung zugänglich machen möchte.[1476] Daneben kann die neue Verantwortliche resp. die potenzielle Datennutzerin Anreize setzen, dass eine Probandin die Daten überträgt.

545 Die Schweizer Lösung scheint auf den ersten Blick in vielen Belangen mit dem EHDS übereinzustimmen. Dies ist angesichts der grossen Bedeutung von Forschungskooperationen über Landesgrenzen hinaus zu begrüssen. Die NDKS findet ihr Pendant in den Zugangsstellen und die Schweiz scheint im Wesentlichen ebenfalls eine Opt-Out-Lösung für die Sekundärnutzung anzustreben.[1477] Die Probandin kann damit bei der Weiterverwendung von Gesundheitsdaten eine entscheidende Rolle einnehmen. Wie sich jedoch Anreize schaffen lassen, damit Forschende an die notwendigen Daten gelangen, ist bislang nicht geklärt. Das Portabilitätsrecht könnte damit – gerade, weil absehbar ist, dass die Probandin miteinbezogen werden soll – an dieser Schnittstelle eine entscheidende Rolle übernehmen. Gleichzeitig führt die Fragmentierung der Rechtsgrundlagen in der Forschung dazu, dass das Portabilitätsrecht in vielen Anwendungsfällen ausscheiden dürfte.

546 Zahlreiche Fragen sind zudem derzeit noch offen, etwa das Verhältnis zum neuen EGD. Vieles deutet darauf hin, dass der im Rahmen von DigiSanté entwickelte SwissHDS als Schnittstelle dienen könnte. Der Bundesrat hielt in der

1475 Bspw. können Forschende die erhobenen Daten als ihr Eigentum betrachten und deshalb nicht herausgeben wollen, siehe Sprecher, ZBJV 2018, Teil 2, 529.

1476 Ähnlich auch Li/Quinn, CLSR 2024, 10, die sich wohl aber auf die Portabilität nach dem EHDS beziehen.

1477 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 40 f., wo einerseits von einem dynamischen, interaktiven Verfahren mit einem jederzeitigen Widerspruchsrecht und andererseits sogar von einer freiwilligen Datenspende zur freien nicht spezifizierten Weiterverwendung ohne Widerruf die Rede ist.

Botschaft zum EGDG fest, dass die «potenzielle Nutzbarmachung» von Daten aus dem EGD, sofern von den Betroffenen erwünscht, nicht als proprietäre Lösung über das EGDG umgesetzt würde, sondern über den SwissHDS.[1478] Der Bundesrat behält sich dabei vor, die rechtlichen Grundlagen des EGD erneut anzupassen.[1479] So könnten zukünftig Regelungen entstehen, die eine «konzeptgerechte Datenweitergabe» von Daten aus dem EGD in den SwissHDS – und umgekehrt – ermöglichen.[1480] Darunter könnten auch Daten für die Forschung fallen. Derzeit ist allerdings unklar, wie sich diese Pläne in das Nationale System zur Weiterverwendung und Verknüpfung von Gesundheitsdaten einfügen. Es bleibt daher die Entwicklung der zahlreichen Gesetzgebungsprojekte abzuwarten.

d. Natürliche Person und Anbieterinnen von gesundheitsrelevanten Anwendungen

Natürliche Personen treten als Konsumentinnen gegenüber Anbieterinnen von gesundheitsrelevanten Anwendungen auf. Sie schliessen einen Vertrag mit den Anbieterinnen ab und willigen in die Erfassung derjenigen Daten ein, die sie erheben und auswerten lassen möchten. Die Art der erhobenen Daten verändert sich dabei laufend mit der technologischen Entwicklung: Bewegung (etwa in Form von Schritten oder Treppenstufen), Herzfrequenz, Körpertemperatur, Schlafrhythmus oder Blutdruck können über die in Mobiltelefonen oder anderen Geräten verbauten Sensoren erfasst werden.[1481] Aus diesen und anderen Daten lassen sich Erkenntnisse zu Stoffwechsel, Sportlichkeit, dem Gemüts- und Gesundheitszustand oder zu Krankheitssymptomen und vielem mehr gewinnen.[1482] 547

Solche bei Anbieterinnen von gesundheitsrelevanten Anwendungen gespeicherten Daten können unter das Portabilitätsrecht fallen, wenn sie bekanntgegebene, oft beobachtete Daten darstellen. Für abgeleitete Daten in Form eigener Auswertungen der Anbieterinnen ist dies indes nicht der Fall.[1483] Gerade im Gesundheitsbereich, und besonders bei Wearables, dürfte die Abgrenzung allerdings nicht immer leicht sein: Denn beobachten bedeutet in diesem Kon- 548

1478 Botschaft EGDG, 21.

1479 Dazu bereits Rz. 526.

1480 Botschaft EGDG, 21.

1481 Ciortuz/Wiedekopf/Fudickar, 324; Isler, digma 2016, 64.

1482 Isler, digma 2016, 64; siehe zum Weg zu solchen Erkenntnissen die «Datenverarbeitungs-Pipeline» bei Ciortuz/Wiedekopf/Fudickar, 328 f.

1483 Anders jedoch unter der EHDS-VO, welche gemäss Erw.G 15 ausdrücklich auch aufbauend auf Art. 20 DSGVO abgeleitete Daten unter dem EHDS erfassen soll.

text stets messen und einer simplen Messung (wie etwa der Herzaktivität) liegt rasch eine komplexe Technologie zugrunde, die nach wissenschaftlichen Methoden vorgeht.[1484] Der Übergang vom reinen Beobachten zum Ableiten ist damit fliessend. Folglich ist für einzelne Daten jeweils individuell zu prüfen, ob sie dem Portabilitätsrecht unterliegen.

549 Die Daten können auch für Leistungserbringerinnen oder Forschende nützlich sein. Während sich gewisse Angaben durch Befragungen oder Untersuchungen feststellen lassen (etwa zur Familiengeschichte oder zum Körpergewicht), können andere Angaben durch eine gesundheitsrelevante Anwendung möglicherweise besser und objektiver eingeholt werden. Patientinnen können Leistungserbringerinnen bspw. einen Echtzeitzugriff auf Daten ihrer Smartwatch erteilen, was eine bidirektionale Kommunikation und eine benutzerfreundliche Oberfläche zur Visualisierung des individuellen Fortschritts der Patientin und die Verfolgung von Zielen ermöglicht.[1485] Für die Forschung können solche Daten interessant sein, weil Studien in der «natürlichen» Umgebung der Probandinnen durchgeführt werden und somit tatsächliche Erfahrungen und Erlebnisse widerspiegeln.[1486] Durch «digitale Phänotypisierung» sollen Daten von Smartphones oder anderen Geräten (bspw. aus Bewegungssensoren oder dem Bedienungsverhalten) den Gesundheitszustand quantifizieren und womöglich vorhersagen können.[1487] Dies kann sowohl für die Behandlung einer Patientin dienlich sein, als auch in der Forschung wertvolle Impulse liefern, zumal eine Datenerhebung durch ein Alltagsgerät wie eine Smartwatch, ein Fitnesstracker oder ein Hörgerät in vielen Fällen verlässlichere Resultate liefern dürfte.[1488] Zumindest in der Forschung ist aus Gründen der Wissenschaftlichkeit indes primär der Rohdatensatz bedeutend und kaum abgeleitete Analysen einzelner, womöglich unterschiedlicher Anbieterinnen.[1489]

550 Stammen Daten aus Wellness-Anwendungen, können sie als personenbezogene elektronische Gesundheitsdaten unter die Primärnutzung nach der

1484 Drepper/Schlünder/Buckow, 183.

1485 Ciortuz/Wiedekopf/Fudickar, 325 m.w.N.

1486 Torous et al., JMIR Mental Health 2016, 2; ähnlich aber auch auf mögliche Probleme bezüglich Datenqualität und Interoperabilität hinweisend Li/Quinn, CLSR 2024, 7; ebenso Weber/Thouvenin, 76.

1487 Am Beispiel der psychischen Gesundheit Birk/Samuel, CPR 2022, 524 und *passim*. Siehe etwa die «Apple Heart Study» an welcher über 400'000 Personen mit einer Apple Watch teilnahmen, https://perma.cc/9J6J-KJ5T.

1488 Hooke et al., Pediatric Blood & Cancer 2016, *passim*, wobei die teilnehmenden Kinder extra mit Fitnesstrackern ausgestattet wurden.

1489 Torous et al., JMIR Mental Health 2016, 2; anders jedoch die Bedürfnisse in der Privatwirtschaft, siehe dazu IGE, 19.

EHDS-VO fallen und sind auch für die Sekundärnutzung unter der EHDS-VO zur Verfügung zu stellen (siehe Art. 51 Abs. 1 lit. i EHDS-VO; für die Definition siehe Art. 2 Abs. 1 lit. ab EHDS-VO).[1490] In der Schweiz gibt es bislang keine solchen spezifischen Regelungen. Unter dem EGDG sind digitale Gesundheitsanwendungen jedoch künftig an das Informationssystem EGD anschliessbar (Art. 16 E-EGDG).[1491]

3. Erkenntnisse und Überleitung

Nur wenige Autorinnen diskutieren das Recht auf Datenportabilität im Kontext des Gesundheitswesens. Vermehrt werden allerdings in diesem Sektor «Zugangsrechte» diskutiert und gesetzlich verankert. Sie entsprechen im Ergebnis oft einem spezialgesetzlichen Portabilitätsrecht. Aus der Untersuchung der Akteurinnen und deren Beziehung untereinander geht hervor, dass das Portabilitätsrecht vor allem zwischen natürlicher Person und Leistungserbringerinnen, Forschenden und Anbieterinnen von gesundheitsrelevanten Anwendungen relevant sein kann. Dabei bestehen teilweise wesentliche Einschränkungen. Es fällt für das Gesundheitswesen besonders auf, dass Daten aus anderen Sektoren in das Gesundheitsdatenökosystem integriert werden können, um die Gesundheitsversorgung zu optimieren. Umgekehrt gilt das jedoch nicht. Zudem vermischen sich die Akteurinnen und deren Beziehungen, etwa wenn eine natürliche Person Daten aus einer gesundheitsrelevanten Anwendung für ein Forschungsprojekt bereitstellen möchte. Die Beziehungen sind nachfolgend kritisch hinsichtlich der Zielsetzungen des Portabilitätsrechts zu würdigen. 551

B. Kritische Würdigung der Datenportabilität

1. Allgemein

Das Portabilitätsrecht ist nicht auf das Gesundheitswesen ausgerichtet, in diesem Sektor aber anwendbar.[1492] Die vorstehenden Ausführungen deuten darauf hin, dass die Ziele des Instituts im Gesundheitswesen anders zu bewerten 552

1490 Kritisch EDSA/EDSB, 26. So sei namentlich die Datenqualität nicht zwingend hoch genug.

1491 Dazu bereits Rz. 523.

1492 So ausdrücklich eHealth Suisse, Interoperabilität, 16; Weber/Thouvenin, 83 und auch 87, wo die Autoren anklingen lassen, dass womöglich konkrete Negativeffekte mit der allgemeinen Regelung des Portabilitätsrechts einhergehen könnten, welche eine Ausnahme für gewisse Branchen erforderlich machen könnten; für die DSGVO NomosKomm-Dix, Art. 20 DSGVO N 15; Drepper/Schlünder/Buckow, 194 f.; Schrader, 285 f.

sind als in anderen Sektoren. Namentlich unterscheidet sich die Interessenlage von derjenigen in anderen Sektoren. Zumindest im Bereich der Grundversicherung ist das Gesundheitswesen in ein sozialversicherungsrechtliches System eingebettet, welches eine ausreichende, allen zugängliche sowie qualitativ hochstehende medizinische Versorgung zu möglichst günstigen Kosten sicherstellen soll (siehe Art. 117*a* Abs. 1 BV und Art. 43 Abs. 6 KVG).[1493] Damit steht die Gesundheit der Betroffenen im Vordergrund. Dies beeinflusst, wie das Portabilitätsrecht zu würdigen ist. Denn Daten sollen auch in diesem Sektor vor allem neue Erkenntnisse liefern, die Qualität von Behandlungen verbessern sowie durch Effizienzsteigerungen Erträge sichern und Kosten einsparen.[1494] Zudem ist im Gesundheitswesen aufgrund der oft heiklen Gesundheitsdaten ein besonderes Gewicht auf die Datensicherheit zu legen.

553 Entsprechend scheinen die wettbewerbsrechtlichen Ziele des Instituts nicht umfassend auf die Situation im Gesundheitswesen zuzutreffen. Gesundheitsdaten sollen kaum je in andere Sektoren oder Datenökosysteme übertragen werden. Mit Blick auf die Sensitivität der Daten sind *walled gardens* daher im Gesundheitsdatenökosystem angebracht und bieten einen gewissen Schutz.[1495] Allerdings möchte der Gesetzgeber *innerhalb* des Gesundheitssektors Datensilos ebenfalls umfassend abbauen. Er strebt zudem – anders als in anderen Sektoren – grundsätzlich eine umfassende Interoperabilität zwischen den Akteuren an.[1496]

554 Trotz der *walled gardens* sollen Daten aber aus anderen Sektoren in das Gesundheitswesen fliessen. Eine Übertragung in eine Richtung, etwa von *real world data*, ist erwünscht. Dies gilt besonders dann, wenn es sich dabei lediglich um Gesundheitsdeterminanten handelt, die erst durch weitergehende

1493 Rütsche, SZKW 2025, 45.

1494 Sprecher, ZBJV 2018, Teil 2, 520.

1495 So auch Palfrey/Gasser, 198: «There is security in distribution». Beispielhaft ist auch die Verpflichtung von Google, die angesichts der Akquisition von FitBit, einer Herstellerin von Fitnesstrackern, erhaltenen Nutzerdaten auf technischem Weg getrennt von anderen Daten zu halten. Konkret muss Google die Daten in einem Datensilo speichern, «das von allen anderen Google-Daten, die für Werbezwecke verwendet werden, getrennt ist», siehe Europäische Kommission, Medienmitteilung vom 17. Dezember 2020.

1496 Bundesrat, Strategie «Digitale Schweiz» 2020, 7626; Botschaft EPDG, 5331, wonach ohne Koordination und Steuerung der Digitalisierung des Gesundheitswesens das Risiko bestehe, dass Lösungen «nicht ein notwendiges Mass an Interoperabilität» erreichten; eHealth Suisse, Strategie, 35, wonach eine technische und semantische Interoperabilität angestrebt wird. Es soll ein «lückenlose[r] Informationsfluss zwischen den Gesundheitseinrichtungen und Gesundheitsfachpersonen sowie von diesen zu Drittsystemen» hergestellt werden. Lovis, 18; siehe auch mit Blick auf eine «public health crisis» Thouvenin et al., Jusletter 2022, Rz. 11; grundlegend auch Palfrey/Gasser, 193 ff.

Analysen einen gesundheitsrelevanten Aspekt beleuchten. Zu nennen sind exemplarisch die Standortdaten eines Mobiltelefons verbunden mit Angaben über Luftschadstoffe in einer Region und dem Gesundheitszustand einer Person. Weiter drängen im Gesundheitsbereich neuartige Anbieterinnen in den Sektor. Diese Entwicklung wird zwar durch besondere Regulierungen wie die MepV teilweise noch abgefedert, da die regulatorischen Vorgaben Hürden darstellen. Dennoch zeigt sich, dass die einzelnen Datenökosysteme zunehmend verschmelzen.

2. Datenschutzrechtliche Ziele

a. Im Regelfall mit Einschränkungen erreicht

Das Portabilitätsrecht schafft in unterschiedlicher Weise die Grundlagen für eine datenschutzrechtliche Zielerreichung. So hatten sich Anbieterinnen von gesundheitsrelevanten Anwendungen bislang zumeist alle Rechte an den erhobenen Daten über ihre allgemeinen Geschäftsbedingungen gesichert.[1497] Während das Portabilitätsrecht allein daran nichts ändert, verbessert sich doch die Rechtsstellung der Betroffenen, wenn sie Daten nunmehr in jedem Fall übertragen lassen können. Damit erhalten sie die Möglichkeit, die Daten zu verwerten – kommerziell oder anderweitig. Auch bei der Übertragung zwischen unterschiedlichen Leistungserbringerinnen, etwa Ärztinnen oder Spitälern, ist das Institut hilfreich. In diesen Fällen dürften indes weniger kommerzielle und vielmehr praktische Gründe für eine Übertragung sprechen. Die Betroffene soll nicht an eine Akteurin gebunden sein und die Möglichkeit erhalten, die Daten zwischen unterschiedlichen Leistungserbringerinnen zu transferieren. Das Institut ermöglicht der Betroffenen somit in jedem Fall, über die Weiterverwendung der sie betreffenden Daten mitzubestimmen. 555

Mehr als in anderen Sektoren wollen Betroffene im Gesundheitsbereich ihre Daten selbst nutzen oder verwalten (Art. 28 Abs. 1 DSG).[1498] Dies liegt daran, dass sich Patientinnen heute mehr für ihren eigenen Gesundheitszustand interessieren und entsprechend an aussagekräftigen Daten interessiert sind.[1499] Damit ist die Herausgabe von Daten durch Leistungserbringerinnen oder Anbieterinnen von gesundheitsrelevanten Anwendungen an die Betroffene för- 556

1497 Siehe dazu Gordon, digma 2016, 71.

1498 Drepper/Schlünder/Buckow, 178.

1499 Drepper/Schlünder/Buckow, 178; exemplarisch ist hier die sog. *Quantified Self* Bewegung zu nennen, dazu Gordon, digma 2016, *passim*.

derlich, um die datenschutzrechtlichen Ziele zu erreichen. Hierbei sind einige Besonderheiten des Gesundheitswesens zu berücksichtigen, etwa das Recht auf Nichtwissen oder das therapeutische Privileg.[1500] Der Verantwortliche sollte diese auch beim (weitgehenden) Anspruch aus Art. 28 DSG im Interesse der Betroffenen beachten, weshalb es sich nicht aufdrängt, die Daten kommentarlos herauszugeben. Stattdessen dürfte regelmässig eine Einordnung der Daten durch eine Fachperson angezeigt sein. Die pauschale Herausgabe eines *data dumps* wäre kaum mit den Berufspflichten der Leistungserbringerinnen vereinbar.

557 Gegenüber anderen Akteurinnen führt die Fragmentierung der datenschutzrechtlichen Zuständigkeiten im Gesundheitswesen allerdings zu unbefriedigenden Ergebnissen, da der Betroffenen der Zugang zum Recht auf Datenportabilität verwehrt wird, wenn ein kantonales Organ die Daten bearbeitet und das DSG nicht anwendbar ist. Diesbezüglich scheint das Portabilitätsrecht die Grundlage für die Erreichung der datenschutzrechtlichen Ziele nicht zu schaffen.

b. Besondere Interessenlage in der Forschung

558 Die anders geneigte Interessenlage in der Forschung führt zu einer besonderen Ausprägung der datenschutzrechtlichen Ziele im Gesundheitswesen. Zwar kann eine Probandin die sie betreffenden Daten von den vielfach kantonalem Recht unterstehenden Forschenden nicht herausverlangen, weil das DSG sie nicht erfasst. Zumeist strebt sie aber gar nicht die Herausgabe der Daten *von* der Forschung an, sondern vielmehr deren Übertragung *an* die Forschung. Die Schweizer Bevölkerung ist dem Erfassen und Teilen von Personendaten gegenüber zwar grundsätzlich eher kritisch eingestellt,[1501] eine Mehrheit zeigt aber die Bereitschaft, an einer Gesundheitsstudie teilzunehmen und dabei Gesundheitsdaten bereitzustellen.[1502] Werden die Daten in einem Spital erhoben

1500 Unter dem therapeutischen Privileg kann eine Information im Interesse der Patientin u.U. zurückbehalten werden. Als Ausfluss ihres Selbstbestimmungsrechts hat eine Patientin zudem ein Recht auf Nichtwissen bezüglich der Angaben über ihre Gesundheit Aebi-Müller et al., Arztrecht 2024, Rz. 1380 ff. Ausdrücklich auch etwa Erw.G 10 EHDS-VO.

1501 73 % der Befragten in einer Studie gaben an, dass sie es nicht mögen, wenn ihre Daten gesammelt werden und sie sie deshalb geheim halten oder dass sie es nicht mögen, wenn ihre Daten gesammelt werden, sie aber manchmal gezwungen seien, sie anzugeben. Bei chronisch kranken Befragten gaben 35 % eine dieser Antworten, siehe Pletscher/Mändli Lerch/Glinz, SMW 2022, 5.

1502 Gemäss Brall et al., PLoS ONE 2021, 5 f. sind 53.6 % der Befragten dazu bereit an einer solchen hypothetischen Studie teilzunehmen.

und vor der Weiterverwendung für die medizinische Forschung anonymisiert, ist die Bereitschaft noch höher.[1503] Ein mögliches Entgelt spielt dabei nur eine untergeordnete Rolle.[1504] Probandinnen haben in der Forschung also hauptsächlich altruistische Beweggründe.[1505] Diese lassen sich vorliegend als datenschutzrechtliche Ziele verstehen, da das Portabilitätsrecht Probandinnen erlaubt, ihre Daten selbstbestimmt der Forschung bereitzustellen.

559 Gerade wenn die Schweiz – anders als die EU – keinen umfassenden Rechtsrahmen für die Datenweitergabe für die Forschung implementieren sollte, kann das Portabilitätsrecht somit sicherstellen, dass eine Probandin selbstbestimmt die Herausgabe und die Übertragung der sie betreffenden Daten an die Forschung veranlassen kann. Dies könnte etwa über PIMS[1506] oder den geplanten Gesundheitsdatenraum geschehen.[1507] Das Portabilitätsrecht scheint damit geeignet, aktuelle Entwicklungen im Forschungsumfeld zu unterstützen und die Betroffenen zu aktiven und gestaltenden Akteurinnen in diesem von intensiver Datennutzung geprägten Umfeld zu machen.[1508] Das Portabilitätsrecht schafft damit die Grundlagen, um die datenschutzrechtlichen Ziele in der Forschung zu erreichen.

3. Wettbewerbsrechtliche Ziele

560 Das Recht auf Datenportabilität und dessen wettbewerbsrechtliche Ziele treffen im Gesundheitswesen auf einen komplexen, fragmentierten Markt, auf welchem für Leistungserbringerinnen ein «regulierter Wettbewerb»[1509] und damit eine teilweise andere Ausgangslage als in den anderen Sektoren herrscht. Obwohl ein regulierter Wettbewerb bestehen soll, werden im Umgang mit Daten im Gesundheitswesen Intransparenz und Monopolisierungs-

1503 Werden die Befragten im Rahmen von Untersuchungen im Spital gefragt, wären 71 % der Befragten bereit, Daten unter diesen Bedingungen zu teilen. Bei chronisch Kranken ist die Zustimmung noch höher, Pletscher/Mändli Lerch/Glinz, SMW 2022, 5. Dabei handelt es sich um eine andere Studie mit einem anderen Studiendesign, weshalb die Daten nur mit Vorsicht verglichen werden sollten. Zudem ist denkbar, dass der Zeitpunkt dieser Studie – nach Beginn der Covid-19-Pandemie – die Bereitschaft eher erhöht haben dürfte.

1504 Pletscher/Mändli Lerch/Glinz, SMW 2022, 5 f.

1505 Siehe auch Drepper/Schlünder/Buckow, 179, die das Interesse einer Betroffenen an der Forschung zu ihrer eigenen Krankheit aufführen.

1506 Dazu Rz. 566.

1507 Ähnlich auch Drepper/Schlünder/Buckow, 180, die im deutschen Kontext das Potenzial von «Datenintegrationszentren» aufführen.

1508 Drepper/Schlünder/Buckow, 180.

1509 Siehe Interpellation Dittli 20.3220, sowie die dazugehörige Stellungnahme des Bundesrates vom 1. Juli 2020.

tendenzen und damit Informationsvorsprünge und Machtgefälle verortet.[1510] Insofern kann das Portabilitätsrecht tatsächlich die Grundlagen für die Erreichung gewisser wettbewerbsrechtlicher Ziele schaffen.[1511] Diesbezüglich ist zunächst das Verhältnis zwischen Anbieterinnen von gesundheitsrelevanten Anwendungen und natürlichen Personen zu nennen. Bei diesen handelt es sich um diejenigen Akteurinnen, die der Gesetzgeber beim Erlass des Instituts vor Augen hatte. Das Portabilitätsrecht dürfte also mögliche Lock-In-Effekte senken und Wechselkosten verringern, zumal gerade Wearables stärker daten- und weniger gemeinschaftszentriert sind, was einen userinduzierten *Lock-In* bei einer Akteurin unwahrscheinlich macht.

561 Die wettbewerbsrechtlichen Ziele können sich aber in beschränktem Mass auch auf die Beziehung zwischen Leistungserbringerin und Patientin und damit auf Teile des «regulierten Wettbewerbs» auswirken: Die einfachere Mitnahme von Gesundheitsdaten zu einer neuen Leistungserbringerin schafft die Grundlagen, um allfällige Lock-In-Effekte zu verringern und Wechselkosten zwischen Leistungserbringerinnen zu senken. Diese Möglichkeit der Datenmitnahme kann Anreize schaffen, um die Übertragung von Gesundheitsdaten zwischen Leistungserbringerinnen und weiteren Akteurinnen und deren unterschiedlichen Systemen anzuregen. Dies ist heute oft nicht möglich, weil die Systeme untereinander nicht kompatibel sind.[1512]

562 Im Gesundheitssektor lässt sich das Portabilitätsrecht punktuell als Umsetzung der datenpolitischen Bestrebungen nach einem freien Datenfluss verstehen. Die sektorübergreifenden Makroziele, die einen Abbau von Datensilos und die Übertragung über Sektoren hinweg vorsehen, sind eingeschränkt auf den Gesundheitsbereich übertragbar. Aufgrund der besonderen Sensitivität der Daten ist eine Übertragung zwar vielfach gerade nicht gewünscht und wird gesetzgeberisch eher unterbunden als gefördert.[1513] Dennoch kann das Portabilitätsrecht zu einem freien Datenfluss im Gesundheitswesen beitragen, etwa um Daten aus unterschiedlichen Quellen an Forschende zu übermitteln, oder indem es eine Grundlage dafür schafft, dass unterschiedliche Leistungserbringerinnen kostengünstig und effizient Daten austauschen können. Dies gilt angesichts des weiten Verständnisses von Gesundheit bzw. gesundheitsrelevan-

1510 Sprecher, ZBJV 2018, Teil 2, 537; ähnlich Rütsche, SZKW 2025, 45.

1511 In diesem Sinn wohl Sprecher, ZBJV 2018, Teil 2, 542 f.; ähnlich auch Brauchbar, Bioethica Forum 2015, 55.

1512 Botschaft EPDG, 5403. Dieses Problem soll das EPD bzw. künftig das EGD angehen und – wenn die Implementierung für Akteurinnen zwingend wird – letztlich auch forcieren. Die eidgenössischen Räte üben ebenfalls Druck aus, siehe etwa Postulat Wyss 24.3013.

1513 Dazu ferner Rz. 553.

ten Daten auch für Personendaten, die in den Gesundheitssektor eingebracht werden – und damit sektorübergreifend. Folglich wirkt das Portabilitätsrecht innovationsfördernd, während es die Entscheidungsfreiheit über die Verwendung der heiklen Gesundheitsdaten bei der Betroffenen belässt.

4. Spezialgesetzliche Vorgaben verdrängen das Portabilitätsrecht

563 Ungeachtet der Zielsetzung gibt es in der Schweiz mit dem EPD bereits Vorgaben für den Datenzugang und -zugriff im Gesundheitssektor. Das Portabilitätsrecht ermöglicht im Wesentlichen, was das EPD spezifischer vorsieht.[1514] So sind unter dem EPD etwa unterschiedliche Zugriffsrechte und Vertraulichkeitsstufen für medizinische Daten vorgesehen (Art. 1 ff. EPDV). Zudem legen die Ausführungsbestimmungen konkrete Vorgaben zu Metadaten oder Austauschformaten fest (siehe Art. 10 Abs. 3 EPDV sowie Anhang 3 und 4 EPDV-EDI). Damit wird der Bereich des elektronischen Patientendossiers in hohem Mass verbindlich standardisiert. Das Portabilitätsrecht geht allerdings heute insofern noch weiter, als es ein weiterverwendbares Format zwingend vorschreibt (Art. 21 Abs. 1 DSV). Dies ist unter dem EPD derzeit nicht der Fall,[1515] wird sich jedoch voraussichtlich mit dem EGD ändern. Neu wird der Bundesrat verbindliche technische Vorgaben machen, um eine Interoperabilität im Gesundheitswesen weitgehend zu ermöglichen. Dies beinhaltet auch Vorgaben zum Datenformat. Inhaberinnen eines EGD können dann ihre Gesundheitsdaten gestützt auf das EGDG in einem gängigen elektronischen Format beziehen. Damit gehen die neuen Vorgaben voraussichtlich über das Recht in Art. 28 DSG hinaus, bei welchem der Verantwortliche das (gängige elektronische) Format selbst wählen kann.

564 Darüber hinaus sehen sowohl das bestehende Patienten- als auch das künftige Gesundheitsdossier nicht nur Kontrollrechte für die Betroffenen vor, sondern adressieren auch organisatorische Aspekte für ein Datenmanagement im Gesundheitswesen, wie Zuständigkeiten, Datensicherheit oder die genannten

1514 Noch vor der DSG-Revision mit dem Hinweis, dass selbst ohne EPD umfassende Auskunfts- und Herausgaberechte bestanden Sprecher/Hofer, 69.

1515 Unter dem EPD finden sich zwar detaillierte Vorgaben hinsichtlich Standardisierung, doch können, wie aufgeführt, auch etwa PDF-Dokumente im EPD abgelegt und übertragen werden, siehe Botschaft EPDG, 5373. Siehe auch die Standards zur Dokumentenablage in Ziff. 2.4 lit. c des Anhangs 2 EPDV-EDI, auf Ziff. 2.13 des Anhangs 3 der EPDV-EDI verweisend. Dort ebenfalls aufgeführt – und damit erlaubt – sind indes auch weiterverwendbare Formate wie FHIR (JSON, XML) oder DICOM.

Standards. Dies dürfte denn auch der bisherige Verdienst des EPD im föderal geprägten und stark arbeitsteiligen Schweizer Gesundheitswesen sein, in welchem solche Bestrebungen bislang stets scheiterten.[1516] Daran knüpft das EGD an. Wenngleich sich das Patientendossier in seiner jetzigen Form noch nicht durchgesetzt hat und weitere Gesetzgebungsprojekte erst anlaufen, so stellt sich doch die Frage, ob das Datenportabilitätsrecht im Gesundheitswesen notwendig ist und ihm im Gesundheitswesen überhaupt eine eigenständige Bedeutung zukommt. Im weitgehend regulierten und mit heiklen Daten operierenden Gesundheitsbereich könnten sektorspezifische Vorgaben zu bevorzugen sein.[1517]

565 Tatsächlich dürfte das Portabilitätsrecht im Gesundheitswesen kaum mehr relevant sein, wenn ein Recht auf Datenherausgabe im EGDG verankert wird (Art. 11 Abs. 1 lit. a E-EGDG). Einzig in (seltenen) Fällen, in welchen Betroffene ihre Daten, etwa *real world data*, aus einem anderen Sektor in das Gesundheitsdatenökosystem übertragen möchten, könnte das Portabilitätsrecht dann noch hilfreich sein. Dies gilt allerdings nur, wenn es sich beim Verantwortlichen nicht ohnehin um eine zugelassene Anbieterin von gesundheitsrelevanten Anwendungen handelt, die vom EGDG erfasst wird.

5. PIMS als Bindeglied zwischen den Akteurinnen

566 Denkbar wäre der Einsatz von PIMS als Bindeglied zwischen den Akteurinnen. Diesen wird bei gesundheitsrelevanten Daten das grösste Potenzial zugeschrieben.[1518] PIMS könnten gerade für die Forschung eine tragende Rolle spielen, weil dort vergleichbare Daten vieler Personen nötig sind und das *consent management* wesentlich ist, also das Verwalten der Nutzung und Freigabepräferenzen der Daten.[1519] Da Personendaten mehrfach und für unterschiedliche (Forschungs-)Zwecke nutzbar sind, könnten PIMS den Einwilligungsprozess vereinfachen und dynamisieren und Betroffene weiterhin die Kontrolle über sie betreffende Daten behalten. Entsprechend helfen PIMS Betroffenen, selbstbestimmt über die Daten zu verfügen und diese ggf. zu monetarisieren, wenn ein Entgelt für die Bereitstellung der Daten erbracht wird.[1520] Zudem können Nutzerinnen aus altruistischen Motiven Daten an PIMS übertragen.

1516 Sprecher/Hofer, 79.

1517 Cichocki, Jusletter IT 2015, Rz. 51, der sich dabei auf die Regulierung von Big Data im Allgemeinen bezieht.

1518 Weber/Thouvenin, 43.

1519 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 20.

1520 Weber/Thouvenin, 16. Siehe etwa https://perma.cc/R6FV-7D93.

Beispiele von operativ tätigen PIMS-Anbieterinnen aus dem Gesundheitsbereich gibt es bereits, etwa die Genossenschaft MIDATA. Diese Plattform ermöglicht es teilnehmenden Personen, ein Datenkonto zu eröffnen und anschliessend autonom und selektiv Zugriff auf die eigenen Daten für die medizinische Forschung und klinische Studien zu gewähren.[1521] MIDATA möchte eine umfassende Interoperabilität erreichen, indem sie an eine FHIR-API anknüpft.[1522] Der Vorteil solcher PIMS-Anbieterinnen besteht darin, dass sie die Datensätze mehrerer Betroffener bündeln und so, nach Bedarf, von Beginn weg aggregiert an Forschende bekanntgeben können. Wenn ein entsprechender Datensatz bereits verfügbar ist, kann eine aufwendige Datenerhebung durch Forschende deshalb unterbleiben. 567

6. Mögliche Handlungsspielräume

a. Partielle Anwendbarkeit auch für öffentliche Organe

Mit Blick auf die Kompetenzaufteilung zwischen Bund und Kantonen ist es zwar überzeugend, dass kantonale öffentliche Organe vom persönlichen Geltungsbereich des DSG nicht erfasst sind. Gerade im Gesundheitsbereich zeigen sich aber Unzulänglichkeiten. Für eine Patientin dürfte es kaum eine Rolle spielen, ob sie in einem öffentlichen oder einem privaten Spital behandelt wurde, wenn sie die sie betreffenden Daten herausverlangen oder übertragen möchte. Ein klassisch hoheitliches Verhältnis zwischen Staat und Betroffener liegt jedenfalls nicht vor und es wäre überholt, ein solches angesichts der Tendenz zur Abkehr von paternalistischen Behandlungsmethoden anzunehmen.[1523] Dies muss auch für die damit einhergehenden Datenbearbeitungen gelten. Mit Blick auf die datenschutzrechtliche Zielsetzung ist die heute geltende Differenzierung nicht angebracht.[1524] 568

1521 Siehe https://perma.cc/YU67-9EFJ.

1522 Siehe https://perma.cc/7JLT-3JQF.

1523 Siehe dazu Bundesrat, Bericht Patientenrechte, 1 und ebenso 21, wonach die grundlegenden materiellen Patientenrechte ungeachtet der Rechtsnatur des Behandlungsverhältnisses gewährleistet seien.

1524 Ähnlich RÜTSCHE/D'AMICO/SCHLÄPFER, 32, nach welchen ein Vereinheitlichungsbedarf in Bezug auf Rechtsgebiete besteht, die nach privater und öffentlicher Rechtsnatur von Behandlungsverhältnissen unterscheiden. Sie erachten eine einheitliche Regelung gerade auch des Datenschutzes aus rechtsstaatlichen Gründen und im Interesse der Patientinnen als wünschenswert.

569 Das Portabilitätsrecht sollte sich damit auf alle Leistungserbringerinnen beziehen, unabhängig von dem der Beziehung zugrundeliegenden Rechtsverhältnis. Faktisch ist eine solche Vereinheitlichung derzeit allerdings nicht realisierbar: Der Bund hat keine Kompetenz, um Datenbearbeitungen kantonaler Organe zu regeln und eine einheitliche Regelung in den einzelnen Kantonen erscheint unwahrscheinlich, zumal die meisten Datenbearbeitungen kantonaler öffentlicher Organe zurecht nicht vom Portabilitätsrecht erfasst sind.[1525]

b. Erweiterung des Portabilitätsrechts auf abgeleitete Daten

570 Denkbar wäre zudem, abgeleitete Daten ebenfalls durch das Portabilitätsrecht zu erfassen. Dies erscheint für Gesundheitsdaten angebracht, da gerade abgeleitete Daten für die Betroffene wichtig sind, etwa die Ergebnisse bestimmter Analysen oder ganze Diagnosen. Zwar besteht dabei die Gefahr, dass es aus wettbewerbsrechtlicher Sicht zu einer Fehlallokation von Ressourcen kommt.[1526] Allerdings ist im Gesundheitswesen bei den Leistungserbringerinnen ohnehin nicht von einem freien, sondern von einem «regulierten Wettbewerb» auszugehen. Zudem dürften durch immer komplexere Verarbeitungsvorgänge abgeleitete Daten im Gesundheitsbereich vermehrt die Norm werden.[1527] Auch die Abgrenzung dürfte sich gerade im Gesundheitsbereich zunehmend schwierig gestalten. Dazu kommt, dass neue Behandlungsmöglichkeiten und andere Innovationen nur dann gefördert werden können, wenn der Zugang zu den relevanten Daten gegeben ist.

571 Insgesamt kann m.E. der im Gesetzgebungsprozess vorgebrachte Schutz der Eigenleistung des Verantwortlichen bei abgeleiteten Daten gegenüber den Gesundheitsinteressen der Betroffenen nicht überwiegen. Das Portabilitätsrecht sollte Betroffenen im Gesundheitsbereich zu einem vollständigen Bild über sie verhelfen. Entsprechend sollten abgeleitete Daten umfasst sein. Dies entspräche einem Gleichlauf mit der EHDS-VO, die ebenfalls keine Einschränkung enthält (Erw.G 15 EHDS-VO).[1528]

1525 Jüngst gibt es jedoch für das Gesundheitswesen politische Bestrebungen in diese Richtung, siehe Interpellation Hässig 25.3836; ähnlich der Vorschlag der Schweizerische Akademie der Medizinischen Wissenschaften (SAMW) zur Schaffung einer Bundeskompetenz im Gesundheitsbereich und zum Erlass eines «Bundesgesetzes über die Gesundheit», siehe https://perma.cc/Y2D7-VPFF.

1526 Dies aufwerfend Weber/Thouvenin, 73.

1527 Li/Quinn, CLSR 2024, 4.

1528 Li/Quinn, CLSR 2024, 6.

c. Interoperabilitätsvorgaben

Erklärtes Ziel im Gesundheitswesen ist eine umfassende Interoperabilität.[1529] 572
Dass die natürliche Person – als Patientin, Probandin oder in einer anderen Rolle – dabei im Zentrum stehen soll, wird kaum bestritten. Das Portabilitätsrecht kann als datenschutzrechtliches Betroffenenrecht Ausgangspunkt für solche Bestrebungen sein. Das BJ sieht bereits heute die Verantwortlichen in der Pflicht, die zu portierenden Daten in einem interoperablen Format bereitzustellen und sie mit geeigneten Metadaten für die Betroffene und die neue Verantwortliche verständlich zu beschreiben, um ihre Weiterverwendung zu ermöglichen.[1530] Es wurde jedoch bereits dargelegt, dass sich aus Art. 28 DSG und aus der DSV keine Verpflichtung zur Interoperabilität und keine Pflicht zur Aufbereitung (neuer) Metadaten ableiten lässt.[1531]

Denkbar wäre aber die Schaffung von Interoperabilitätsvorgaben. Solche sollten 573
jedoch mit Blick auf die hohe Komplexität des Gesundheitssektors nicht pauschal durch den Staat vorgeschrieben werden.[1532] Aus diesem Grund dürfte ein gemischter Ansatz zu präferieren sein, der die verschiedenen Akteurinnen des Gesundheitswesens miteinbezieht und berücksichtigt und gleichzeitig, wo nötig, eine Vereinheitlichung durchzusetzen vermag.[1533] Denn gerade im innovativen Gesundheitsbereich droht die Gefahr eines *Lock-In*, wenn verfrüht Standards verpflichtend gemacht werden, diese aber technologisch rasch überholt sind.[1534] Die Kompetenz- und Koordinationsstelle von Bund und Kantonen für den Gesundheitsbereich (eHealth Suisse) hat bereits eine Interoperabilitätsstrategie ausgearbeitet. Sie misst dem Portabilitätsrecht eine grosse Bedeutung bei und empfiehlt die Schaffung einer Interoperabilitäts-Schnittstelle für die Datenportabilität, die alle Akteurinnen des Gesundheitswesens verbindlich implementieren müssen.[1535] Um dies zu garantieren, wird die Verankerung einer solchen Schnittstelle als Kriterium für die Vergütung nach dem KVG vorgeschlagen.[1536] Wie gesehen, ist unter der EHDS-VO ebenfalls ein Trend zur Standardisierung und Schaffung einer Interoperabilität zu erken-

1529 Dazu Rz. 553.
1530 BJ, Erläuternder Bericht DSV, 47.
1531 Siehe Rz. 208.
1532 Palfrey/Gasser, 195.
1533 So Palfrey/Gasser, 195, jedoch den US-amerikanischen Gesundheitssektor beleuchtend.
1534 Palfrey/Gasser, 200, die insgesamt aber mehr Vor- als Nachteile der Interoperabilität sehen, besonders «if we get its design right».
1535 Vgl. eHealth Suisse, Interoperabilität, 47.
1536 Dazu eHealth Suisse, Interoperabilität, 47.

nen. Der E-EGDG weist mit seinen umfassenden und verbindlichen Standards ebenfalls in Richtung einer Interoperabilität.

574 In technischer Hinsicht könnten zur Sicherstellung der semantischen Dateninteroperabilität im Gesundheitswesen bewährte semantische Standards eingesetzt werden, etwa die Klassifikation ICD[1537] oder die Nomenklatur SNOMED CT.[1538] Auch für die syntaktische Interoperabilität stehen bewährte Standards bereit, namentlich die von HL7 entwickelten Standards wie FHIR.[1539] Dabei handelt es sich um eine objektorientierte, datenzentrierte Spezifikation, die auf einer webbasierten Architektur aufbaut und relevante Behandlungsdaten als «Ressourcen» repräsentiert.[1540] Die Ressourcen sind Datenobjekte, die jeweils eine Information abbilden und miteinander verknüpft werden können.[1541] FHIR spezifiziert für den Austausch von und den Zugriff auf unterschiedliche Informationsobjekte eine API für datenbanktypische Interaktionen wie *Create*, *Read*, *Update* oder *Delete* auf jede Ressource.[1542] Ein Datensatz, der auf FHIR basiert, beinhaltet demnach unterschiedliche Ressourcen, die jeweils auf eine konkrete Ressource des Typs «Patientin» verlinken und sich dadurch auf die natürliche Person bezieht.[1543]

575 Gleichwohl zeichnet sich ab, dass solche Interoperabilitätsvorgaben kaum alle Sektoren gleichermassen betreffen und sich eine sektorielle Regelung aufdrängen dürfte, etwa im Ausführungsrecht zum EGDG oder in den gesetzlichen Grundlagen zu einem SwissHDS. Dies wird in § 5 zu besprechen sein.

7. Erkenntnisse

576 Das Portabilitätsrecht ist im Gesundheitswesen in vielen Fällen anwendbar und kann die Grundlage schaffen, um einige der anvisierten Ziele zu erreichen. Es lässt sich damit namentlich in datenschutzrechtlicher Hinsicht ein *Empowerment* der Betroffenen bewirken, weil diese über ihre Gesundheitsdaten verfügen kann. In einigen Anwendungsfällen ist das Institut allerdings unge-

1537 Siehe dazu https://perma.cc/KS8Y-PVY8.
1538 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 28; eHealth Suisse, Interoperabilität, 17; zu SNOMED CT siehe https://browser.ihtsdotools.org; dazu allgemein Rz. 113 f.
1539 Bundesrat, Bericht Nutzung von Gesundheitsdaten, 28; siehe Botschaft EGDG, 21, wonach das EPD, das EGD und der SwissHDS auf FHIR setzen; Fix, 314 ff.; weitergehend zu FHIR, siehe https://perma.cc/2QML-KANL.
1540 Daumke et al., 466.
1541 Daumke et al., 466.
1542 Daumke et al., 466.
1543 Daumke et al., 466.

nügend auf die Begebenheiten des Gesundheitswesens zugeschnitten, weshalb auch Unzulänglichkeiten bestehen.

So offenbart sich die nur punktuelle Anwendbarkeit des DSG im Gesundheitswesen als Schwäche. Dem Institut sind unter dem DSG bereits aufgrund des eingeschränkten persönlichen Geltungsbereichs Grenzen gesetzt, anders als das europäische Rechtsinstitut, das grundsätzlich für sämtliche Verantwortlichen anwendbar ist. Dies lässt sich in den untersuchten Anwendungsfällen auch nicht dadurch rechtfertigen, dass es sich bei den Datenbearbeitungen um eine öffentliche Aufgabe im Sinne einer hoheitlichen Tätigkeit handeln würde. Entsprechend verfügen Betroffene in zahlreichen Konstellationen über kein Recht auf Datenportabilität, weil der Verantwortliche datenschutzrechtlich als kantonales Organ einzustufen ist. 577

In wettbewerbsrechtlicher Hinsicht schafft das Portabilitätsrecht die Grundlagen für eine Zielerreichung nur bis zu einem gewissen Grad. Angesichts des «regulierten Wettbewerbs» im Gesundheitswesen gilt es einige Unterschiede zu beachten. So sind die Interessen in diesem Sektor vielfach anders gelagert und auf die Gesundheit der Betroffenen ausgerichtet. Auch ein weitgehend freier Datenfluss ist nicht zwingend gewünscht und *walled gardens* werden womöglich sogar begrüsst. Allerdings lässt sich beobachten, wie Technologieunternehmen mit neuartigen Gesundheitsanwendungen in den nicht regulierten Bereich des Gesundheitswesens eintreten. 578

Ausgehend davon zeigen sich gewisse Handlungsspielräume. So wäre wünschenswert, dass kantonale Organe ebenfalls vom Portabilitätsrecht erfasst sind, damit nicht zahlreiche Datenbearbeitungen im Gesundheitssektor von einer Portierung ausgenommen sind. Ferner sollten abgeleitete Daten aufgrund ihrer hohen Relevanz im Gesundheitswesen ebenfalls unter das Portabilitätsrecht fallen, da die gesetzgeberische Interessenabwägung zugunsten des Verantwortlichen im untersuchten Sektor nicht überzeugt. Schliesslich werden Interoperabilitätsvorgaben angeregt. Anerkanntermassen strebt das Gesundheitswesen eine umfassende Interoperabilität zwischen den Akteurinnen an. Aus diesem Grund könnten hinsichtlich der vom Portabilitätsrecht beabsichtigten Ziele Anpassungen, die in Richtung einer solchen Interoperabilität wirken, erforderlich sein. 579

Die diskutierten Handlungsspielräume weisen vielfach einen engen Bezug zum Gesundheitswesen auf und dürften primär sektoriell zu adressieren sein. Dies ist in der EU mit der EHDS-VO bereits umfassend geschehen, und auch die Gesetzgebung zum Patienten- bzw. zum Gesundheitsdossier verfolgt u.a. die vom Portabilitätsrecht verfolgten Ziele. Dies führt zur Frage, ob diesbezüglich 580

eine sektorielle Regelung nicht zielführender wäre, zumal, wie gesehen, das Gesundheitswesen gewisse *walled gardens* durchaus begrüsst. Dies wird in § 5 in sektorübergreifender Weise vertieft.

IV. Mobilität

Mit der enormen Zunahme der mobilen digitalen Kommunikation[1544] ist der Mobilitätsbereich zu einem datengetriebenen Sektor geworden: Moderne Fahrzeuge sind dabei als Docking-Stationen zu verstehen,[1545] die rund 25 Gigabyte Daten pro Stunde erzeugen.[1546] Oft ist in diesem Zusammenhang von «smarter Mobilität» die Rede.[1547] Sie soll eine «intelligente» Möglichkeit der Ortsveränderung ermöglichen, die – je nach Fokus – energieeffizienter, emissionsärmer, sicherer, kostengünstiger oder komfortabler ist.[1548] Bei smarter Mobilität soll also das vorhandene Angebot durch den Einsatz von Informations- und Kommunikationstechnologien optimal genutzt werden.[1549] Nach diesem Verständnis wird die Mobilität nachfolgend nur mit Blick auf datenschutz- und portabilitätsrechtliche Gesichtspunkte beleuchtet. Dies bedeutet, dass nur diejenige Formen von Mobilität untersucht werden, mit denen eine Bearbeitung von (Personen-)Daten einhergeht und bei welchen die Betroffene im Zentrum steht.[1550] 581

Erhoben werden im Mobilitätsdatenökosystem Daten über Fahrzeuge und deren Komponenten, Daten für vernetzte Verkehrssysteme, Daten, die in einem allfälligen Unfalldatenspeicher abgelegt werden, oder Daten für Medien- und Kommunikationsdienste wie Landkarten oder Wetterprognosen.[1551] Die Vernetzung wird dabei zunehmend zum Standard und vielfach gesetzlich vorgegeben. So müssen seit einigen Jahren sämtliche neu gebauten Fahrzeuge der Klassen M1 und N1[1552] mit einem Notrufsystem ausgestattet sein, welches auf 582

1544 So hat sich das mobile Datenvolumen der Netzanbieterin Swisscom etwa zwischen 2010 und 2020 um den Faktor 200 vergrössert, siehe BOSSHARDT/HERMANN, 5 f.

1545 So VIEWEG CHRISTOF, «Das Auto ist nur die Docking-Station», Zeit Online vom 13. Oktober 2015, abrufbar unter: https://perma.cc/D6SR-KDLX.

1546 Europäische Kommission, Datenstrategie, 32.

1547 FLÜGGE, *passim*, sowie die weiteren Beiträge dieses Buchs; FRÜH/BRAUN BINDER/SCHIBLI, sui generis 2022, *passim*.

1548 WOLTER, 528.

1549 WOLTER, 528.

1550 Ein im Wesentlichen identisches Verständnis aufweisend etwa SACKMANN, 25. Aus diesem Grund werden die Diskussionen rund um eine umfassende Mobilitätsdateninfrastruktur in der Schweiz ausgeklammert. Für diese sollen Personendaten nur am Rande eine Rolle spielen, siehe FRÜH/SCHIBLI/BRAUN BINDER, SZW 2023, 74 f. Zudem stehen Betroffene nicht im Zentrum, sondern andere Akteure, siehe Botschaft MODIG, 13.

1551 METZGER, GRUR 2019, 130.

1552 Entsprechend nur solche Kraftfahrzeuge, die für die Beförderung von Fahrgästen und deren Gepäck ausgelegt sind und höchstens neun Sitzplätze aufweisen sowie für den Gü-

Knopfdruck oder automatisch – etwa bei Auslösen des Airbags – die zuständigen Notrufbehörden alarmiert.[1553] Diese Vorgaben, die in der europäischen eCallVO festgehalten sind, sind auch in der Schweiz verbindlich (Anhang 2 Ziff. 112 VTS) und bedingen, dass moderne Fahrzeuge gewisse Daten über das Mobilfunknetz an die Notrufbehörden übermitteln können.[1554] Grundsätzlich sind alle Daten, die ein vernetztes Fahrzeug aussendet, zumindest potenziell personenbezogen, da der Fahrer über einen Account, über Zertifikate oder über Standortdaten identifizierbar ist.[1555]

583 Die Plattformisierung macht vor dem Mobilitätssektor nicht halt.[1556] Parallel zu den klassischen Geschäftsmodellen, die eine vertikale Struktur aufweisen – also etwa die Entwicklung und Produktion von Fahrzeugen und deren Absatz über geschützte Kanäle – bilden sich digitale Geschäftsmodelle heraus, die auf plattformbasierten Mobilitätsdienstleistungen beruhen.[1557] Fahrzeughersteller erweitern ihre Geschäftsmodelle, angetrieben durch die Entwicklung hin zum autonomen Fahren, sowohl durch den Betrieb eigener digitaler Plattformen für Mobilitätsdienstleistungen als auch durch die Bereitstellung ihrer Dienstleistungen auf von anderen betriebenen digitalen Plattformen.[1558] Sie entwickeln sich damit von produktorientierten zu datengetriebenen Unternehmen.[1559]

584 In diesem Kapitel ist zu untersuchen, ob das Recht auf Datenportabilität im Mobilitätssektor die Grundlagen schaffen kann, damit seine datenschutz- und wettbewerbsrechtlichen Ziele erreicht werden. Zu diesem Zweck soll zunächst der Mobilitätssektor strukturiert und anschliessend das Recht auf Datenportabilität in diesem Kontext untersucht werden.

---

terverkehr ausgelegte und gebaute Kraftfahrzeuge bis 3,5 Tonnen (Art. 2 Abs. 1 eCallVO, der auf Anhang II Teil A 1. der mittlerweile aufgehobenen RL 2007/46/EG verweist. Diese wurde durch die TypgenehmigungsVO ersetzt). Siehe zur Klasseneinteilung nach EU-Recht die Schweizer Übernahme in Art. 12 VTS.

1553 Siehe dazu ASTRA, 2.

1554 Bislang scheint sich das System indes nicht etabliert zu haben. Im März 2021 – also drei Jahre nach Inkrafttreten – waren nur vereinzelt Notrufzentralen mit entsprechenden Empfängern ausgestattet, siehe dazu Cetojevic Darko, «eCall: Ein Notruf, den fast niemand hört», K-Tipp vom 7. März 2021, abrufbar unter: https://perma.cc/D9YM-YGBP.

1555 Metzger, GRUR 2019, 131. Dazu ausführlich Rz. 602 f.

1556 Grundlegend dazu Rz. 53 ff.

1557 Kortus-Schultes, 97.

1558 Kortus-Schultes, 97 f.

1559 Siehe allgemein Pflaum/Klötzer, 58 ff.

A. Strukturierung des Ökosystems

1. Akteure und deren Rollen

a. Mobile Personen

Sämtliche mobilen Personen sind Akteure des Mobilitätsdatenökosystems.[1560] Sie können als Fussgänger, Teilnehmende im Individualverkehr (als Halter, Fahrer oder Insassen eines Fahrzeugs)[1561] oder als Nutzer von öffentlichen Verkehrsmitteln am Mobilitätsdatenökosystem teilnehmen. 585

In datenschutzrechtlicher Hinsicht werden von mobilen Personen primär Daten *erfasst*. Sie sind damit in der datenschutzrechtlichen Rolle einer betroffenen Person. In gewissen Konstellationen kann eine mobile Person jedoch auch Verantwortliche sein, etwa dann, wenn sie einer anderen mobilen Person ihr Fahrzeug ausleiht und sie in der Folge herausfinden kann, wo sich die Entlehnerin befindet.[1562] 586

b. Fahrzeughersteller

Weitere Akteure sind die Hersteller von Fahrzeugen, etwa Automobilhersteller sowie Hersteller von Motorrädern, E-Scootern, (E-)Fahrrädern, Flugzeugen usw.[1563] 587

Im Automobilbereich stammen die Hersteller aus dem Ausland; seit 1975 werden in der Schweiz keine Personenwagen mehr serienmässig produziert.[1564] Entsprechend vertreten Importgesellschaften die ausländischen Hersteller. Diese Importgesellschaften erhalten das ausschliessliche Recht, Fahrzeuge und Originalersatzteile des betreffenden Herstellers zu beziehen und diese zu vertreiben.[1565] Folglich existiert gerade bei Automobilen oft ein ganzes Netzwerk aus «offiziellen» Händlern, die vertraglich das exklusive Vertriebsrecht 588

1560 Otto/Burmann, Informatik Spektrum 2021, 288; unter der Begrifflichkeit «Kunde», die jedoch bereits eine Rolle bzw. Beziehung unterstellt ebenso Expertengruppe Zukunft, 98.
1561 Klink-Straub/Straub, ZD 2018, 460.
1562 Siehe das entsprechende Beispiel bei Rosenthal, Jusletter 2019, Rz. 27.
1563 Otto/Burmann, Informatik Spektrum 2021, 288.
1564 Kindler, 21.
1565 Kindler, 21 f.

innehaben.[1566] Solche Händler übernehmen (exklusiv) Reparatur- und weitere Leistungen für die Hersteller, die auch als Erstausrüster oder *original equipment manufacturer* (OEM) bezeichnet werden. Sie bilden den sog. OEM-*Aftermarket*. In dieser Untersuchung werden diese Akteure den Herstellern zugeordnet: Unter Fahrzeugherstellern wird also neben dem Primärmarkt der ganze OEM-*Aftermarket*, bestehend aus sämtlichen eigenen und gebundenen Händlern, Teilzulieferern und gebundenen Werkstätten, erfasst, da diese in datenschutzrechtlicher Hinsicht nicht als vom OEM unabhängig betrachtet werden können.[1567]

589 Fahrzeughersteller sind an nutzungsbezogenen Daten interessiert, um ihre Produkte weiterzuentwickeln und sie für Kunden attraktiver zu machen.[1568] Bei smarten Fahrzeugen stehen Apps zur Verfügung, die viele Funktionen ermöglichen und dazu in grossem Umfang Daten bearbeiten.[1569] Ob die erfassten Daten einen Personenbezug aufweisen, ist jeweils individuell zu bestimmen. Soweit jedoch Personendaten bearbeitet werden, handelt der Hersteller in der Rolle als Verantwortlicher.[1570]

c. Anbieter von Dienstleistungen

590 Im Mobilitätsdatenökosystem können bei verschiedenen Anbietern Dienstleistungen bezogen werden, etwa bei Taxibetrieben oder Vermietern von Mietautos.[1571] Darüber hinaus existieren Fernbusanbieter und Transportunternehmen wie Nahverkehrsbetriebe, Zugbetreiber oder Luftfahrtunternehmen, bei wel-

1566 MARTENS/MUELLER-LANGER, JCLE 2020, 119 m.w.N.; siehe ferner ausführlich das Vertriebssystem für Motorradprodukte der Herstellerin Yamaha, das Alleinbezugsverpflichtungen von ihren Vertragspartnern vorsieht, WEKO, Yamaha, 12 ff.

1567 Diese Akteure ebenfalls zusammenfassend METZGER, GRUR 2019, 130; ähnlich auch HAWKER, The Antitrust Bulletin 2011, 60. Dies in Abgrenzung zu den freien, ungebundenen Händlern, die als Anbieter von Dienstleistungen (Rz. 590 ff.) oder Fahrzeughändler (Rz. 596 f.) qualifiziert werden.

1568 KLINK-STRAUB/STRAUB, ZD 2018, 460.

1569 So verlangen etwa die Autohersteller Tesla, Audi und Toyota Zugriff auf den Kalender der Nutzer ihrer Android App, siehe mit weiteren Beispielen METERE et al., ArXiv 2022, 5.

1570 So auch ROSENTHAL, Jusletter 2019, Rz. 27; siehe ebenfalls KARIKARI, 114 f., der sich zudem zur Möglichkeit der Verantwortlichkeit des Herstellers aufgrund einer Zweckveranlassung äussert. Die Zuweisung der datenschutzrechtlichen Rolle kann gerade in grossen Konzernverhältnissen, wie sie Automobilhersteller aufweisen, Schwierigkeiten bereiten. So kann ein Fahrzeughersteller Verantwortlicher für den Datenbearbeitungsprozess sein, im Konzernverhältnis jedoch gleichzeitig Auftragsbearbeiter oder gemeinsamer Verantwortlicher, siehe dazu ALPMANN, 16 f. Dies braucht vorliegend indes nicht weiter thematisiert zu werden, da die Fahrzeughersteller für die hiesigen Zwecke als Einheit behandelt werden.

1571 Expertengruppe Zukunft, 98.

chen regelmässig Daten anfallen.[1572] Ferner hat sich in den letzten Jahren mit der sog. Sharing Economy ein neues, besonders datenintensives Servicemodell etabliert.[1573] Es sind dies Car-Sharing-Plattformen und Vermittlungsdienste wie Uber oder Mobility,[1574] Velo-[1575] und Scooterverleihe[1576].

Indirekt mit dem Mobilitätssektor verbundene private Dienstleistungen können zudem durch Versicherer, Autogaragen oder Anbieter von datenbasierten Zusatzdiensten erbracht werden.[1577] In Abgrenzung zu den Fahrzeugherstellern bilden sie den unabhängigen oder freien Sekundärmarkt (*independent aftermarket*).[1578] Sie werden auch als unabhängige Wirtschaftsakteure bezeichnet.[1579] Gerade datenbasierte Zusatzdienste haben in jüngster Zeit einen enormen Wandel erfahren, denn grosse Akteure wie Google oder Apple drängen, teils als Fahrzeughersteller – vor allem aber auch als Anbieter von Dienstleistungen – in den Mobilitätssektor.[1580] 591

Die Anbieter können für ihre Dienstleistungen selbstständig Daten erfassen oder sie benötigen solche teilweise von anderen Akteuren. Diese Daten bearbeiten sie in der Rolle als Verantwortliche. 592

d. Staat

Staatliche Behörden unterstehen dem Legalitätsprinzip und dürfen Daten regelmässig nur gestützt auf eine gesetzliche Grundlage bearbeiten.[1581] Dies gilt auch im Mobilitätssektor. Handelt eine Behörde jedoch privatrechtlich, etwa im Bereich der Bedarfsverwaltung, gelten für sie die Datenschutzbestimmungen für private Personen (Art. 40 DSG).[1582] Das ist insb. der Fall, wenn die Behörde am wirtschaftlichen Wettbewerb teilnimmt.[1583] Sie soll dann der privaten Konkurrenz datenschutzrechtlich gleichgestellt sein.[1584] 593

1572 Otto/Burmann, Informatik Spektrum 2021, 288.
1573 Grundlegend dazu Abegg/Bernauer, 1 ff.
1574 Expertengruppe Zukunft, 98.
1575 Etwa «Publibike», siehe https://perma.cc/CK9D-KCHB.
1576 Etwa «Lime» oder «Bird», siehe https://www.li.me und https://www.bird.co/de/.
1577 In diesem Sinn Klink-Straub/Straub, ZD 2018, 459 ff.
1578 Metzger, GRUR 2019, 130 ff.
1579 Siehe Art. 3 Abs. 45 TypgenehmigungsVO; dazu weitergehend Rz. 640 ff.
1580 Kerber, JIPITEC 2018, 324.
1581 Dazu bereits Rz. 196 f. und im Gesundheitssektor Rz. 494.
1582 Zur privatrechtlichen Natur SHK DSG-Rudin, Art. 2 N 16; für das Recht auf Datenportabilität BJ, Erläuternder Bericht DSV, 45.
1583 Botschaft DSG 1988, 474; ebenso unter dem neuen DSG, siehe Botschaft DSG 2017, 8083.
1584 Botschaft DSG 1988, 474; ebenso unter dem neuen DSG, siehe Botschaft DSG 2017, 8083.

594 Wichtigstes Beispiel des Mobilitätsdatenökosystems sind konzessionierte Transportunternehmen, wie etwa die als spezialgesetzliche öffentlich-rechtliche Aktiengesellschaft[1585] organisierten SBB. Sie verfügen über eine gesetzliche Grundlage für das Bearbeiten von Personendaten (Art. 54 Abs. 1 PBG) und gelten grundsätzlich als Bundesorgane, für welche die Bestimmungen nach Art. 33 ff. DSG anwendbar sind.[1586] Für Mobilitätsangebote, welche auch Beförderungsleistungen umfassen, die nicht dem PBG unterstehen (Variante 1) oder wesentliche andere Dienstleistungen wie touristische oder kulturelle Angebote umfassen (Variante 2), sind allerdings die Art. 30–32 DSG massgebend (Art. 54 Abs. 5 PBG). In Spezialfällen sollen damit jeweils die gleichen Bestimmungen des Datenschutzrechts anwendbar sein; eine Fragmentierung soll verhindert werden.[1587] Diese Regelung gilt nach Art. 54 Abs. 6 PBG auch für Dritte, die Fahrausweise nach dem PBG verkaufen.

595 Behörden bearbeiten Daten in der Rolle der Verantwortlichen. Fallen ihre Datenbearbeitungen in Einzelfällen unter die besonderen Bestimmungen des DSG für private Personen, ist eine Portabilitätspflicht möglich. Auf kantonale und kommunale Behörden findet das DSG hingegen gar keine Anwendung (Art. 2 Abs. 1 DSG *e contrario*).[1588] Ihnen kommt im hier relevanten Bereich keine Rolle zu.

e. Fahrzeughändler

596 Fahrzeughändler, etwa Autogaragen als Verkäufer oder Leasinggeber, sind weitere relevante Akteure.[1589] Sie stellen Fahrzeuge nicht selbst her, vertreiben sie aber frei an Abnehmer – als Neuwagen oder Occasionsfahrzeuge. In Abgrenzung zum OEM-*Aftermarket* sind Fahrzeughändler nur diejenigen Akteure, die frei und nicht gebunden an einen Fahrzeughersteller Fahrzeuge, Accessoires und Ersatzteile vertreiben. Soweit sie Daten bearbeiten – bspw. nach der Rückgabe eines geleasten Fahrzeugs – sind sie in der Rolle des Verantwortlichen.

597 Fahrzeughändler erbringen neben dem Handel mit Fahrzeugen und Ersatzteilen oft auch weitere Dienstleistungen wie Reparaturen. Vorliegend sind solche Tätigkeiten unter der Rolle des Anbieters von Dienstleistungen erfasst.[1590]

1585 BGE 132 III 470 E. 3.3.
1586 Botschaft PBG, 44.
1587 Botschaft PBG, 44.
1588 Dazu bereits Rz. 173.
1589 SCHÄTZLE, PinG 2016, 72.
1590 Dazu Rz. 590 ff.

2. Relevante Beziehungen

a. Mobile Personen und Fahrzeughersteller

aa. Allgemein

Mobile Personen schliessen mit Fahrzeugherstellern einen Vertrag ab und erwerben von diesen ein Fahrzeug. Zudem willigen die mobilen Personen im Vertrag regelmässig in gewisse Datenbearbeitungen ein.[1591] Damit ist die Voraussetzung in Art. 28 Abs. 1 lit. b DSG i.d.R. erfüllt. 598

Wie einleitend bemerkt, sind moderne Fahrzeuge fahrende Computer. Sie bearbeiten Daten automatisiert i.S.v. Art. 28 Abs. 1 lit. a DSG. Neben dem Fahrzeug an sich sind heute regelmässig auch zu erbringende Nebenleistungen wie bspw. Softwareupdates Vertragsbestandteil zwischen den Akteuren.[1592] Damit handelt es sich bei einem Fahrzeugkauf oft um ein Dauerschuldverhältnis, das sich mitunter über Jahre erstrecken kann.[1593] Von einem solchen Vertragsverhältnis sind andere mobile Personen, etwa andere (Mit-)Fahrer, nicht erfasst.[1594] Dies kann in Bezug auf das Portabilitätsrecht in Einzelfällen zu Abgrenzungsproblemen führen, weil Art. 28 Abs. 1 lit. b DSG nicht zutrifft. Von solchen Ausnahmefällen abgesehen, findet das Recht auf Datenportabilität jedoch Anwendung auf diese Beziehung zwischen den Akteuren. 599

Gerade smarte Fahrzeuge erfassen zahlreiche Daten und übertragen diese teilweise sogleich auf die Server der Fahrzeughersteller.[1595] Die mobilen Personen können die erhobenen Daten dabei nur beschränkt kontrollieren: Es sind massgeblich die Fahrzeughersteller, die den Umfang des Datenzugangs 600

1591 Kerber/Gill, 86; Metzger, GRUR 2019, 130; Schweitzer, GRUR 2019, 573. Siehe beispielhaft auch die Datenschutzerklärung des Herstellers Tesla: «Die Kriterien zur Speicherung von Daten können die Berücksichtigung ihrer Verwendung, unsere Beziehung zu Ihnen, die Existenz eines Dienstleistungsvertrags, Ihre Einwilligung oder die gesetzliche Aufbewahrungspflicht für bestimmte Daten beinhalten.», abrufbar unter: https://www.tesla.com/de_ch/legal/privacy > «Zu diesen Zwecken können wir Ihre Informationen verwenden».

1592 Kerber, JIPITEC 2018, 323. Zu den Dienstleistungen, die Fahrzeughersteller ebenfalls erbringen können, siehe auch die Rolle des Anbieters von Dienstleistungen.

1593 Kerber, JIPITEC 2018, 323.

1594 Metzger, GRUR 2019, 134.

1595 Während früher Daten lokal im Fahrzeug gespeichert wurden und nur dann auswertbar waren, wenn eine Verbindung zum Fahrzeug bestand, etwa im Rahmen der OBD-Systeme, senden Fahrzeuge die Daten heute immer öfter unmittelbar an Server, siehe Van den Boom, EBLR 2023, 159.

und damit die Wertschöpfungskette der Daten kontrollieren.[1596] Welche Daten dies genau sind, lässt sich nicht abschliessend bestimmen. Hinweise geben aber Datenschutzerklärungen und unabhängige Untersuchungen. Fahrzeuge des Herstellers Tesla erfassen bspw. Fahrzeugtyp und Fahrzeugdaten,[1597] Diagnosedaten,[1598] Daten des Infotainment-Systems, Daten zum Kundensupport, Informationen zum Verlauf von Service- und Reparaturarbeiten[1599] sowie zahlreiche weitere Angaben.[1600] Auch im Zusammenhang mit der Bestellung und der Finanzierung des Autos erfasst der Hersteller Daten.[1601] Gewisse Erhebungen sind nach der hier gewählten Vorgehensweise allerdings den Anbietern von Dienstleistungen zuzuordnen.[1602]

601 Eine Untersuchung des ADAC zu vier unterschiedlichen Fahrzeugmodellen ergab, dass bei sämtlichen untersuchten Modellen zahlreiche Daten erfasst werden, etwa solche, die Rückschlüsse auf das Nutzungsprofil, die Intensität der Nutzung oder die Anzahl der Fahrer und den Fahrstil erlaubten.[1603] Darunter waren die Anzahl einzelner Fahrtstrecken, aufgeschlüsselt nach Kilometern, GPS-Daten, Zahl der elektromotorischen Gurtstraffungen,[1604] Einträge für zu hohe Motordrehzahl oder -temperatur[1605] und die Zahl der Verstellvorgänge des elektrischen Fahrersitzes.[1606] Eine weitere Untersuchung der Daten-

1596 Van den Boom, EBLR 2023, 158.

1597 Konkret Baujahr, Marke, Modell, Fahrgestellnummer (FIN), Fahrzeugkonfiguration, Telemetriedaten zu Performance, Nutzung, Betrieb und Zustand, in Anspruch genommene Ladestation, Auslastung, Ladegeschwindigkeit, Batterieanalytik und Performance.

1598 Konkret Protokolle zur Identifizierung und Behebung unerwarteter Software- oder Konnektivitätsprobleme sowie andere Debugging-Protokollberichte.

1599 Konkret Serviceeinrichtung, Datum, Kilometerstand, durchgeführte Reparaturen, Kostenvoranschlag und Kosten, Details zu Teilen und andere vergleichbare Informationen.

1600 Siehe https://www.tesla.com/de_ch/legal/privacy > «Welche Informationen wir erfassen» > «Wenn Sie Tesla-Kunde sind».

1601 Siehe https://www.tesla.com/de_ch/legal/privacy > «Welche Informationen wir erfassen» > «Wenn Sie vor dem Kauf mit uns interagieren» / «Wenn Sie Tesla-Kunde sind» > «Informationen von Ihren oder über Ihre Tesla-Energieprodukte».

1602 Dazu Rz. 623.

1603 Wieler Jochen/Kroher Thomas/Henn Christof, «Daten im Auto: Fluch oder Segen?», ADAC vom 15. Januar 2024, abrufbar unter: https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/assistenzsysteme/daten-modernes-auto/#diese-fahrzeugdaten-werden-gesammelt.

1604 Zur Überprüfung der Fahrweise anhand der Anzahl und Intensität von Bremsmanövern.

1605 Zur Überprüfung der Fahrweise anhand der Geschwindigkeit.

1606 Zur Überprüfung der Anzahl der unterschiedlichen Fahrer, siehe Wieler Jochen/Kroher Thomas/Henn Christof, «Daten im Auto: Fluch oder Segen?», ADAC vom 15. Januar 2024, abrufbar unter: https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/assistenzsysteme/daten-modernes-auto/#diese-fahrzeugdaten-werden-gesammelt.

schutzerklärungen von 25 Fahrzeugherstellern konnte nachweisen, dass diese potenziell Daten über sexuelle Aktivitäten, Einwanderungsstatus, Ethnie, Gesichtsausdruck, Gewicht, Gesundheit oder Genetik einer betroffenen Person erheben.[1607]

Auch wenn davon auszugehen ist, dass Fahrzeugdaten aller Art einen Personenbezug aufweisen können,[1608] ist nicht immer ohne Weiteres klar, ob sie in einer konkreten Situation Personendaten darstellen. Bauteile, die Sensoren enthalten, bearbeiten etwa grundsätzlich keine Personendaten.[1609] Da solche Daten jedoch gemeinsam mit Standortdaten oder der sog. FIN im Fahrzeug gesammelt und in einem Datensatz gespeichert werden, sind sie in der Praxis personenbezogen.[1610] 602

Nach übereinstimmender Ansicht der deutschen Datenschutzbehörden und des VDA sind Fahrzeugdaten jedenfalls dann personenbezogen, wenn eine Verknüpfung mit der FIN oder dem Kfz-Kennzeichen vorliegt.[1611] In diese Richtung deutet auch die Rechtsprechung des EuGH zur DSGVO. Denn die sog. Zulassungsbescheinigung eines Fahrzeugs muss neben der FIN auch den Namen und die Anschrift des Inhabers dieser Zulassungsbescheinigung enthalten.[1612] Daher handle es sich um ein Personendatum «der in der Zulassungsbescheinigung ausgewiesenen Person, sofern derjenige, der Zugang zur FIN hat, über Mittel verfügen könnte, die es ihm ermöglichen, die FIN zur Identifizierung des Halters des Fahrzeugs, auf das sich die FIN bezieht, oder zur Identifizierung der Person, die auf Grund eines anderen Rechtstitels denn als Halter über 603

1607 Siehe Mozilla Foundation, «‹Privacy Nightmare on Wheels›: Every Car Brand Reviewed By Mozilla – Including Ford, Volkswagen and Toyota – Flunks Privacy Test» vom 6. September 2023, abrufbar unter: https://perma.cc/QF76-Y998.

1608 Für Fahrzeugdaten mit Fokus auf Motorfahrzeugversicherungen Blumer, 99 ff.; für Daten, die von C-ITS-Diensten ausgesendet werden Europäische Kommission, Intelligente Verkehrssysteme, 9; EY/FIA Region I, 22 m.w.N., nach welchen ein Grossteil, wenn nicht sogar alle Daten, Personendaten darstellen; Früh/Braun Binder/Schibli, sui generis 2022, 20; Gill/Metzger, EDPL 2022, 226; ausführlich zu einem möglichen Personenbezug anhand unterschiedlicher Beispiele Karikari, 76 ff.; Sackmann, 80 ff.; ferner Van den Boom, EBLR 2023, 160, die von einem Konsens in der Literatur dahingehend ausgeht, dass Fahrzeugdaten Personendaten seien, «especially in combination with other data»; technische Daten, die sich auf ein Fahrzeug beziehen hingegen nicht als mögliche Personendaten sehend Charlet, 574; ähnlich davon ausgehend, dass zumindest Teile der relevanten Mobilitätsdaten keinen Personenbezug aufweisen Picht, IIC 2020, 950 f.

1609 Alpmann, 17.

1610 Alpmann, 17. Bei der FIN handelt es sich um eine international genormte, eindeutige Seriennummer für Fahrzeuge, siehe https://perma.cc/6HRX-JVPF.

1611 DSK/VDA, 1.

1612 EuGH C-319/22 vom 9. November 2023, Rz. 47.

das betreffende Fahrzeug verfügen kann, zu nutzen».[1613] Nach dem EuGH soll die FIN sogar mittelbar für Fahrzeughersteller ein Personendatum darstellen, wenn Anbieter von Dienstleistungen[1614] «bei vernünftiger Betrachtung über Mittel verfügen können, die es ermöglichen, die FIN einer identifizierten oder identifizierbaren natürlichen Person zuzuordnen».[1615] Dies soll selbst dann gelten, wenn die FIN für sich genommen für die Fahrzeughersteller kein persönliches Datum darstellt.[1616]

bb. Europäische Datenverordnung (DV)

(1) Grundlagen

604 In der EU wurde mit der DV (oft «Data Act» oder «DA») ein harmonisierter Rahmen für die Nutzung von vernetzten Produkten und verbundenen Diensten – dem sog. Internet der Dinge oder Internet of Things (IoT) – geschaffen (siehe Erw.G 4 DV). Dieser erfasst die Beziehung zwischen mobilen Personen und Fahrzeugherstellern.

605 Als horizontaler Erlass ist die DV allerdings nicht auf den Mobilitätssektor beschränkt, sondern grundsätzlich sektorübergreifend anwendbar (siehe Erw.G 42 DV). Sie gründet denn auch auf dem Gedanken, dass datengetriebene Technologien eine transformative Wirkung auf alle Wirtschaftssektoren gehabt und die Verbreitung von Produkten, die mit dem Internet vernetzt sind, den Umfang und den potenziellen Wert von Daten für Verbraucher, Unternehmen und Gesellschaft erhöht hätten (Erw.G 1 DV).

606 Die DV reguliert das IoT als Ganzes, weil sie davon ausgeht, dass das IoT digitale Ökosysteme schafft, die sich, zumindest was die Daten anbelangt, nicht mehr nach einzelnen Märkten auftrennen lassen.[1617] Dabei verunmöglichten heute jedoch Hindernisse bei der Datenweitergabe, dass Daten zum Nutzen

---

1613 EuGH C-319/22 vom 9. November 2023, Rz. 48.

1614 Der EuGH spricht von «unabhängigen Wirtschaftsakteuren», was der Terminologie der TypgenehmigungsVO entspricht, um die es im Entscheid ging, siehe Rz. 640 ff.

1615 EuGH C-319/22 vom 9. November 2023, Rz. 49.

1616 EuGH C-319/22 vom 9. November 2023, Rz. 49; weitergehend zu einer solchen – überraschenden – Rechtsfigur eines «mittelbaren» Personenbezugs Hanloser, ZD 2024, *passim*, insb. 186; siehe aber Weller, GRUR-Prax 2023, 761, nach welchem der EuGH wohl kaum die Zurechnung der Identifizierungsmöglichkeiten meinte, sondern lediglich habe klarstellen wollen, dass für den Fahrzeughersteller aus dem ursprünglichen Sachdatum ein personenbezogenes Datum werde, wenn und soweit ein Zugriff des Herstellers auf die bei dem Anbieter von Dienstleistungen vorliegenden identifizierenden Informationen möglich sei.

1617 Schweitzer/Metzger, GRUR Int. 2023, 345.

der Gesellschaft optimal verteilt würden (Erw.G 2 DV). Als Hindernisse nennt Erw.G 2 DV einen Mangel an Anreizen für Dateninhaber, freiwillig Vereinbarungen über die Datenweitergabe einzugehen, Unsicherheiten in Bezug auf Rechte und Pflichten in Verbindung mit Daten, sowie den Missbrauch vertraglicher Ungleichgewichte hinsichtlich Datenzugang und -nutzung.

607 Die DV macht aus diesem Grund u.a. Vorgaben für die Bereitstellung von Produktdaten und verbundenen Dienstdaten für Nutzer eines vernetzten Produkts oder verbundenen Diensts (Art. 1 Abs. 1 lit. a DV), von Daten durch Dateninhaber für Datenempfänger (lit. b), sowie von Daten durch Dateninhaber für öffentliche Stellen (lit. c).[1618] Vernetzte Produkte kommen u.a. im Mobilitätssektor und dort besonders in Fahrzeugen vor, wobei die DV ausdrücklich auch Nutzern ermöglichen soll, datenbasierte Dienste auf *Aftermarkets* zu nutzen (Erw.G 14 und 16 DV).

608 Kapitel II regelt zu diesem Zweck in den Art. 3–7 DV die Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen. Art. 3 DV sieht vor, dass Produktdaten und verbundene Dienstdaten für den Nutzer zugänglich gemacht werden müssen. Dazu müssen nach Abs. 1 vernetzte Produkte bereits so konzipiert und hergestellt und verbundene Dienste so konzipiert und erbracht werden, dass Produktdaten und verbundene Dienstdaten, einschliesslich Metadaten, standardmässig einfach, sicher, unentgeltlich, in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, direkt zugänglich sind.

609 Art. 4 DV enthält sodann ein Recht auf Datenherausgabe an den Nutzer, soweit er nicht direkt vom vernetzten Produkt oder dem verbundenen Dienst aus auf die Daten zugreifen kann. In diesem Fall müssen die Dateninhaber (dazu Art. 2 Ziff. 13 DV), die nicht notwendigerweise auch Vertragspartner sein müssen, die «ohne Weiteres verfügbaren Daten» (dazu Art. 2 Ziff. 17 DV), einschliesslich Metadaten unverzüglich, einfach, sicher, unentgeltlich, in einem umfassenden, strukturierten,[1619] gängigen und maschinenlesbaren Format und – falls relevant und technisch durchführbar – in der gleichen Qualität wie für den Daten-

[1618] Darüber hinaus soll nach lit. d auch der Wechsel zwischen Datenverarbeitungsdiensten erleichtert und es sollen nach lit. f Interoperabilitätsnormen entwickelt werden. Zu diesen Zwecken enthält die DV in den Kapiteln VII und VIII zahlreiche Vorgaben. Diese enthalten auch Vorgaben zur Datenübertragbarkeit (siehe Art. 35 Abs. 2 lit. b DV). Von den beiden Kapiteln sind aber im Wesentlichen Cloud-Dienste erfasst, die vorliegend nicht untersucht werden. Siehe grundlegend dazu und eine Abgrenzung auch zur Portabilität aufzeigend Siglmüller, MMR 2024, *passim*.

[1619] Siehe hierzu die Berichtigung in ABl. L 2025/90691 vom 9. September 2025, Ziff. 13.

inhaber kontinuierlich und in Echtzeit bereitstellen (Art. 4 Abs. 1 DV). Auf Verlangen eines Nutzers ist der Dateninhaber auch zur Weitergabe von ohne Weiteres verfügbaren Daten an einen Dritten verpflichtet (Art. 5 Abs. 1 DV). Das entspricht im Wesentlichen dem datenschutzrechtlichen Recht auf Datenübertragung nach Art. 20 Abs. 2 DSGVO resp. Art. 28 Abs. 2 DSG. Diese Daten sind ebenfalls einschliesslich der erforderlichen Metadaten bereitzustellen, und zwar unverzüglich, für den Nutzer unentgeltlich, in derselben Qualität, die dem Dateninhaber zur Verfügung steht, einfach, sicher, in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, kontinuierlich und in Echtzeit (Art. 5 Abs. 1 DV).

610 Die Portabilitätsrechte nach der DV verfolgen wettbewerbsrechtliche und innovationsfördernde Zielsetzungen. Dies geht aus den Erwägungsgründen hervor[1620] und wird auch in der Literatur vertreten[1621]. Die DV betritt damit in mehrerer Hinsicht Neuland und lässt das datenschutzrechtliche Portabilitätsrecht in einem neuen Licht erscheinen. Sie nimmt mehrere beim datenschutzrechtlichen Portabilitätsrecht ins Feld geführte Kritikpunkte auf und nimmt sich dieser an (dazu sogleich). Gleichzeitig macht die DV klar, dass «besondere Pflichten» zur Bereitstellung von Daten aufgrund von Rechtsvorschriften, die bis zum 11. Januar 2024 in Kraft getreten sind, von der Verordnung unberührt bleiben (Art. 44 Abs. 1 DV). Auch besondere Bedürfnisse eines Sektors in Bezug etwa auf technische Aspekte des Datenzugangs «berührt» die DV nicht (Art. 44 Abs. 2 DV), weshalb zukünftige sektorspezifische Regelungen möglich bleiben.[1622]

(2) Weiter Datenbegriff

611 Der Datenbegriff in der DV geht einerseits deutlich weiter als derjenige im Datenschutzrecht. Sie erfasst zwar nur Daten mit einem IoT-Bezug (sog. Produktdaten und verbundene Dienstdaten),[1623] doch werden in der DV erstmals

1620 Siehe Erw.G 1, 30, 32 f. und 40 DV.

1621 Arioli, iusNet DigR 2024, 1; BeckOK DSR-Brink/von Ungern-Sternberg, Einführung zum Data Act (DA) N 1; Hennemann/Steinrötter, NJW 2024, 1; Schweitzer/Metzger, GRUR Int. 2023, 339.

1622 Lippert/Schreyer-Bestmann, BB 2024, 333.

1623 Produktdaten sind gemäss Art. 2 Ziff. 15 DV «Daten, die durch die Nutzung eines vernetzten Produkts generiert werden und die der Hersteller so konzipiert hat, dass sie über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang von einem Nutzer, Dateninhaber oder Dritten – gegebenenfalls einschließlich des Herstellers – abgerufen werden können». Verbundene Dienstdaten sind demgegenüber ge-

sowohl personenbezogene als auch nicht personenbezogene Daten umfassend reguliert. Andererseits sind Inhaltsdaten generell nicht von den Portabilitätsrechten nach Kapitel II DV erfasst (Art. 1 Abs. 2 lit. a DV).

Nach Art. 4 DV herauszugeben sind die «ohne Weiteres verfügbare[n] Daten einschließlich der zur Auslegung und Nutzung der Daten erforderlichen Metadaten». Erstere sind nach Art. 2 Ziff. 17 DV Produktdaten und verbundene Dienstdaten, die ein Dateninhaber rechtmässig von dem vernetzten Produkt oder verbundenen Dienst erhält oder erhalten kann.[1624] Sie sind nur «ohne Weiteres verfügbar», wenn dies «ohne unverhältnismäßigen Aufwand, der über eine einfache Bearbeitung hinausgeht» geschieht.[1625] Unter Metadaten wird eine strukturierte Beschreibung der Inhalte oder der Nutzung von Daten verstanden, die das Auffinden dieser Daten bzw. deren Verwendung erleichtert (Art. 2 Ziff. 2 DV). Von Art. 5 DV erfasst sind die gleichen Daten, einschliesslich Metadaten.[1626] 612

Eine Einschränkung auf nur «bereitgestellte» bzw. «bekanntgegebene» Daten gibt es in der DV nicht, auch beobachtete Daten fallen darunter:[1627] Erfasst sind absichtlich aufgezeichnete Daten ebenso wie solche, die Nutzerhandlungen indirekt generieren, bspw. Umgebungsdaten (Erw.G 15 DV). Erfasst sind ferner Daten, die von einer Benutzerschnittstelle oder über einen verbundenen Dienst generiert werden, was sämtliche Daten umfasst, die ein vernetztes Produkt infolge einer solchen Nutzung generiert (Erw.G 15 DV). Dazu zählen gemäss Erw.G 15 DV etwa sensorgenerierte Daten und Daten, die eingebettete Anwendungen aufzeichnen, einschliesslich Anwendungen, die den Hardwarestatus und Funktionsstörungen angeben.[1628] Daten, die generiert werden, während der Nutzer inaktiv ist, sollen ebenfalls umfasst sein (Erw.G 15 DV). Ferner erfasst sind Daten in Rohform, die sich auf Datenpunkte beziehen, die ohne weitere Form der Verarbeitung automatisch generiert werden, sowie Daten, die aufbereitet wurden, um sie verständlich und nutzbar zu machen (Erw.G 15 DV). 613

mäss Art. 2 Ziff. 16 DV «Daten, die die Digitalisierung von Nutzerhandlungen oder Vorgängen im Zusammenhang mit dem vernetzten Produkt darstellen und vom Nutzer absichtlich aufgezeichnet oder als Nebenprodukt der Handlung des Nutzers während der Bereitstellung eines verbundenen Dienstes durch den Anbieter generiert werden». Nicht erfasst sind etwa Smartphones oder Tablets, siehe Lazarotto, EJLT 2024, 10.

1624 Siehe hierzu die Berichtigung in ABl. L 2025/90691 vom 9. September 2025, Ziff. 12.

1625 Siehe hierzu die Berichtigung in ABl. L 2025/90691 vom 9. September 2025, Ziff. 12.

1626 In der deutschen Fassung ist der Wortlaut von Art. 4 und 5 DV bezüglich der bereitzustellenden Daten leicht unterschiedlich. Dies dürfte aber keine inhaltliche Bedeutung haben, zumal der Wortlaut in anderen Sprachfassungen nicht abweicht.

1627 Dazu, noch basierend auf dem Vorschlag Tombal/Graef, 205 f.

1628 Dazu auch Hennemann/Steinrötter, NJW 2024, 2.

614 Wie im Datenschutzrecht sind hingegen abgeleitete Daten nicht erfasst, d.h. aus «Daten gefolgerte oder abgeleitete Informationen, die das Ergebnis zusätzlicher Investitionen in die Zuweisung von Werten oder Erkenntnissen aus den Daten sind» (Erw.G 15 DV).[1629]

615 Die DV soll die Entstehung «liquider, fairer und effizienter Märkte» auch für nicht personenbezogene Daten fördern (Erw.G 26 DV) und der Tatsache Rechnung tragen, dass nicht personenbezogene Daten ebenfalls einen wirtschaftlichen Wert aufweisen. Dies gilt besonders im Mobilitätssektor, wo Daten aus dem und über das Fahrzeug namentlich für *Aftermarket*-Dienstleistungen gebraucht werden und Anbieter von Dienstleistungen darauf angewiesen sind, dass man sie ihnen zur Verfügung stellt.[1630] Diese haben nicht immer einen Personenbezug oder ein solcher kann zumindest umstritten sein, weshalb das Recht auf Herausgabe und Übertragung nach der DV geeignet scheint, hier eine Lücke zu füllen. Obwohl die Daten keinen Personenbezug aufweisen müssen, bleibt die grundsätzliche Nutzerzentrierung bestehen.[1631] Diese Ausrichtung ergibt sich sonst nur aus dem Datenschutzrecht.[1632]

(3) Weiter sachlicher Anwendungsbereich

616 Die Portabilität nach der DV ist zwar beschränkt auf Produktdaten und verbundene Dienstdaten, gilt für diese aber weitgehend ohne weitere Einschränkungen. Nur ausnahmsweise lässt sich eine Portierung aus Sicherheits- und Gesundheitsgründen sowie zum Schutz der Geschäftsgeheimnisse einschränken (Art. 4 Abs. 2 und 6–8 DV). Anders als unter der DSGVO und dem DSG existiert keine Einschränkung auf nur freiwillig erfolgte Datenbearbeitungen. So ist ein Vertrag weder notwendig noch ausreichend.[1633] Dies ergibt sich auch daraus, dass die Art. 4 f. DV vom Dateninhaber und nicht vom Vertragspartner sprechen.[1634] Der Nutzer muss auch nicht einwilligen. Dies ist insb. für nicht

1629 Tombal/Graef, 206; für das DSG Rz. 179 und für die DSGVO Rz. 127.

1630 Dazu Rz. 639.

1631 Ähnlich Arioli, iusNet DigR 2024, 11; Hennemann/Steinrötter, NJW 2024, 7, die von einer bedeutsamen, aber auch umstrittenen Zuordnung des den Daten innewohnenden Werts an den Nutzer ausgehen.

1632 Eckardt/Kerber, EJLE 2024, 127, die eine Parallele zur datenschutzrechtlichen Einwilligung ziehen.

1633 Wunner, ZUM 2024, 430.

1634 Siehe indes Schmidt-Kessel, MMR 2024, 77 m.w.N., nach welchem die Portierungsverpflichtung jedenfalls in den Fällen, in welchem der Dateninhaber die Daten ausschliesslich für den Vertragspartner des Nutzers hält, wie das etwa bei Cloud-Anbietern häufig der Fall sein dürfte, allein beim Vertragspartner liegen.

personenbezogene Daten nur konsequent, hat aber Auswirkungen auf personenbezogene Daten, die damit ungeachtet ihrer konkreten Rechtmässigkeitsvoraussetzung nach Art. 6 DSGVO unter das Portabilitätsrecht nach der DV fallen. Sofern die Nutzerin auch die betroffene Person ist, können personenbezogene Daten ohne Weiteres an diese herausgegeben (Art. 4 DV) oder an einen Dritten weitergegeben werden (Art. 5 DV). In diesem Fall ist davon auszugehen, dass die Betroffene einwilligt, wenn sie die Portabilität initiiert.[1635] Ist das nicht der Fall, so muss in beiden Fällen eine datenschutzrechtliche Rechtsgrundlage vorliegen (siehe Art. 4 Abs. 12 und Art. 5 Abs. 7 DV). Allerdings kann, anders als die Betroffene unter der DSGVO und dem DSG, auch eine juristische Person «Nutzerin» und damit portabilitätsberechtigt sein (Art. 2 Ziff. 2 DV). Es sind damit in jedem Fall mehr Daten erfasst als unter dem Recht auf Datenportabilität nach der DSGVO, da die DV den sachlichen Anwendungsbereich nicht einschränkt.

(4) Enger persönlicher Anwendungsbereich

Die DV sieht vor, dass Torwächter im Sinne des DMA[1636] nicht als zugelassene Dritte i.S.v. Art. 5 DV gelten und somit nicht portabilitätsberechtigt sind (Art. 5 Abs. 3 DV). Dies wird damit begründet, dass es «zur Erreichung des Ziels der [DV] nicht erforderlich und somit in Bezug auf die den entsprechenden Pflichten unterliegenden Dateninhaber unverhältnismäßig [wäre], solchen Torwächtern ein Datenzugangsrecht einzuräumen» (Erw.G 40 DV). Die Portabilitätsrechte nach der DV – und mit ihnen die Einschränkungen für Torwächter – sollen zu einer grösseren Auswahl an Dienstleistungen für die Konsumenten beitragen (Erw.G 40 DV). Freiwillige Vereinbarungen zwischen Torwächtern und Dateninhabern bleiben aber möglich und auch sonst werden Torwächter nicht gehindert, dieselben Daten auf andere rechtmässige Weise zu erlangen und zu nutzen (Erw.G 40 DV). Es bleibt somit namentlich möglich, Daten auf dem Weg des datenschutzrechtlichen Portabilitätsrechts zu erlangen.[1637] 617

Demgegenüber sind Kleinst- und Kleinunternehmen von den Pflichten nach Kapitel II DV ausgenommen (Art. 7 Abs. 1 DV).[1638] Haben sie vernetzte Produkte hergestellt oder konzipiert und generieren diese Daten, oder erbringen sie 618

1635 Hennemann/Steinrötter, NJW 2024, 4.

1636 Dazu grundlegend Rz. 419 ff.

1637 Tombal/Graef, 209.

1638 Darunter fallen nach Art. 2 des Anhangs der Empfehlung 2003/361/EG Unternehmen mit weniger als 10 bzw. 50 Mitarbeitenden und einem Jahresumsatz von unter EUR 2 Mio. bzw. EUR 10 Mio. Siehe gerade auch in Abgrenzung zum Portabilitätsrecht nach der DSGVO Tombal/Graef, 205.

verbundene Dienste, deren Nutzung Daten erzeugt, so stehen sie trotzdem nicht in der Pflicht, Daten nach der DV bereitzustellen. Solche Unternehmen können entsprechende Daten aber zu fairen, angemessenen und nichtdiskriminierenden Bedingungen (FRAND) erhalten.[1639] Damit enthält die DV sowohl für portabilitätsverpflichtete Dateninhaber als auch für portabilitätsberechtigte Dritte relevante Differenzierungen und einen eingeschränkten persönlichen Anwendungsbereich, der einzig auf die mit der DV verfolgten wettbewerblichen Ziele zurückzuführen ist[1640] und überdies der zunehmenden Plattformisierung entgegentreten dürfte.

(5) Erkenntnisse

619 Bei der DV handelt es sich um einen grundlegend neuen Ansatz der Regulierung. Die DV beschränkt sich nicht darauf, ein Marktversagen zu beheben oder an besondere Schwellenwerte wie eine marktbeherrschende Stellung anzuknüpfen.[1641] Vielmehr verfolgt sie einen «marktgestaltenden» Ansatz, indem Zugangsrechte zu und Nutzungsrechte an Daten geschaffen werden, welche die Grundlage bilden, auf welcher sich Märkte zukünftig entwickeln sollen.[1642] Es geht damit darum, wie ein Datenmarkt ausgestaltet sein soll und nicht lediglich um dessen Sicherung.[1643] Gefördert werden sollen Innovationen auf den *Aftermarkets* und die Entwicklung völlig neuartiger Dienste (Erw.G 32 DV). Die DV geht also zumindest in wettbewerbsrechtlicher Hinsicht in eine ähnliche Richtung wie das Portabilitätsrecht nach dem DSG.[1644] In Bezug auf die Nutzung oder Weitergabe der portierten Daten ist die mobile Person indes eingeschränkt. Sie darf die erhaltenen Daten weder zur Entwicklung eines konkurrierenden Produktes nutzen oder weitergeben noch nutzen, um einen Einblick in die wirtschaftliche Lage, die Vermögenswerte und die Produktionsmethoden des Herstellers zu erhalten (Art. 4 Abs. 10 DV).

620 In der DV treten datenschutzrechtliche Zielsetzungen – trotz der Anwendbarkeit auf personenbezogene Daten – in den Hintergrund. Dies lässt sich da-

1639 Ausführlich hierzu METZGER, 75 ff.

1640 Dies mit einem die Innovation fördernden Datenfluss und der Vermeidung hoher Entwicklungs- oder Transaktionskosten begründend HARTMANN/MCGUIRE/SCHULTE-NÖLKE, RDi 2023, 58.

1641 METZGER/SCHWEITZER, ZEuP 2023, 48; SCHWEITZER/METZGER, GRUR Int. 2023, 339.

1642 SCHWEITZER/METZGER, GRUR Int. 2023, 338.

1643 HENNEMANN/STEINRÖTTER, NJW 2024, 6; BeckOK DSR-BRINK/VON UNGERN-STERNBERG, Einführung zum Data Act (DA) N 24, nach welchen die DV nicht Grenzen setzen, sondern vor allem Handeln ermöglichen soll.

1644 Dazu Rz. 294 ff., insb. 300 ff.

durch erklären, dass die DV der DSGVO umfassend Vorrang einräumt und nur letztere für die Verwirklichung datenschutzrechtlicher Ziele zu sorgen hat.[1645] Vor diesem Hintergrund ist beachtlich, dass eine eigentliche Nutzerzentrierung beibehalten wurde, gerade was nicht personenbezogene Daten angeht.[1646] Erw.G 18 DV begründet dies damit, dass der Nutzer die Risiken trage und die Vorteile der Nutzung des vernetzten Produkts geniesse und darum Zugang zu den von ihm generierten Daten haben sollte. Dabei handelt es sich jedoch nicht um eine Nutzerzentrierung, wie sie ein datenschutzrechtliches Verständnis nahelegen würde: Der Nutzer kann auch eine juristische Person sein und die Daten können sich auf Dritte beziehen. Die Literatur kritisiert denn auch diese Nutzerzentriertheit teils mit Blick auf die wettbewerbsrechtlichen Ziele.[1647]

621 Die DV setzt den nutzerzentrierten Ansatz teilweise konsequent um, etwa bei der mandatierten Echtzeitbereitstellung der Daten nach Art. 4 Abs. 1 DV, welche überdies den wettbewerbsrechtlichen Zielen förderlich ist, solange die Daten ausschliesslich dem Nutzer zukommen.[1648] Allerdings wird auch vertreten, dass die DV das Verhältnis zu einseitig zugunsten des Dateninhabers ausgestalte.[1649] Dies zeige sich dadurch, dass der Dateninhaber die technisch-faktische Kontrolle über die Daten behalte und sich vertraglich weitgehende Nutzungsrechte einräumen lassen könne; der Nutzer hingegen habe lediglich einen Anspruch auf Zugang.[1650] Kritisiert wird zudem, dass dem Nutzer häufig der Anreiz zur Datennutzung fehlen dürfte, wodurch befürchtet wird, dass die angestrebte datengestützte Innovation ausbleibt.[1651] Die DV gilt erst seit dem 12. September 2025 (Art. 50 DV), weshalb erste praktische Erfahrungen abzuwarten sind.

622 In der Schweiz gibt es bislang kein der DV entsprechendes Gesetz. Ein autonomer Nachvollzug des europäischen Rechts ist politisch noch offen.[1652] Aller-

1645 So stellt Art. 1 Abs. 5 DV klar, dass die DV «unbeschadet» der DSGVO gilt. Dies vermag allerdings das Spannungsverhältnis in Bezug auf personenbezogene Daten nicht aufzulösen, siehe ausführlich Bomhard, MMR 2024, 74; Sattler, Data Act, 103 ff.; BeckOK DSR-Veil, Art. 1 DA N 216 ff.

1646 Arioli, iusNet DigR 2024, 11; grundlegend dazu Eckardt/Kerber, EJLE 2024, 126 ff. , sowie 123 ff. zum Konzept der Zentrierung des Dateninhabers; siehe ferner Rohner, EuDIR 2025, 11.

1647 Drexl et al., Rz. 49; Funk, CR 2023, Rz. 14 ff., insb. Rz. 28; Wunner, ZUM 2024, 432.

1648 Wunner, ZUM 2024, 433.

1649 BeckOK DSR-Brink/von Ungern-Sternberg, Einführung zum Data Act (DA) N 25.

1650 BeckOK DSR-Brink/von Ungern-Sternberg, Einführung zum Data Act (DA) N 25 m.w.N.

1651 BeckOK DSR-Brink/von Ungern-Sternberg, Einführung zum Data Act (DA) N 26; Wiebe, 1578.

1652 IK-EUDP, 19.

dings könnte das Rahmengesetz zur Sekundärnutzung von Daten die Nutzung von nicht personenbezogenen Daten adressieren.[1653] Zudem wird das MODIG künftig den Datenfluss im Mobilitätsbereich sektoriell regeln.[1654]

b. Mobile Personen und Anbieter von Dienstleistungen

623 Mobile Personen in ihrer Rolle als betroffene Personen stehen mit Anbietern von Dienstleistungen zumeist in vertraglicher Beziehung.[1655] Aufgrund der zahlreichen Datenbearbeitungsszenarien liegt es zudem nahe, eine Einwilligung der mobilen Personen einzuholen.[1656] Handelt es sich um Daten, welche die mobile Person dem Anbieter von Dienstleistungen bekanntgegeben hat, ist das Recht auf Datenportabilität potenziell anwendbar. Die Art der portabilitätsrelevanten Daten ist dabei so vielfältig wie die möglichen Dienstleistungen, die im Mobilitätssektor erbracht werden können.

c. Mobile Personen und Staat

624 Soweit staatliche Akteure hoheitlich tätig sind, bleibt für das Recht auf Datenportabilität kein Raum.[1657] Da in bestimmten Fällen aber für staatliche Akteure die Vorgaben des Datenschutzrechts für Private gelten, kann das Portabilitätsrecht punktuell anwendbar sein. In diesen Fällen agiert der Staat jedoch wie ein Privater, weshalb auf weitere Ausführungen verzichtet wird.

d. Mobile Personen und Fahrzeughändler

625 Mobile Personen erwerben bei Fahrzeughändlern Fahrzeuge, Accessoires oder Ersatzteile. Diese Akteure stehen damit in einer vertraglichen Beziehung zueinander. Das Recht auf Datenportabilität kann daher in dieser Beziehung grundsätzlich anwendbar sein, wenn Daten an die Fahrzeughändler bekanntgegeben werden. Abzugrenzen sind dabei jedoch diejenigen Daten, die mobile Personen direkt (und nur) dem Fahrzeughersteller übermitteln. Dies dürfte der Hauptanwendungsfall sein, weshalb auf weitere Ausführungen verzichtet wird.

1653 Motion WBK-S 22.3890; ähnlich JOTTERAND, sic! 2025, 450; dazu bereits Rz. 329.
1654 Siehe Botschaft MODIG, 1 ff.
1655 METZGER, GRUR 2019, 132.
1656 METZGER, GRUR 2019, 131 f.
1657 Dazu Rz. 593.

e. Fahrzeughersteller und Anbieter von Dienstleistungen

aa. Allgemein

Anbieter von Dienstleistungen sind für das Anbieten ihrer Dienstleistung oft auf eine Beziehung zu den Fahrzeugherstellern angewiesen. Notwendig sind dafür zunehmend Daten. Datenschutzrechtlich stehen diese Akteure – wenn überhaupt – in einer Beziehung von Verantwortlichem und Auftragsbearbeiter.[1658] Zumeist besteht allerdings jenseits einiger bewusst eingegangener Kooperationen[1659] noch keine direkte datenschutzrechtliche Beziehung zwischen diesen Akteuren. 626

Durch die technologische Entwicklung generieren Hersteller immer mehr Fahrzeugdaten. Diese lagern sie zunehmend aus. Fahrzeuge sind daher nicht mehr in sich geschlossene Objekte, sondern ein Bestandteil des IoT.[1660] Entsprechend finden sich immer weniger physische Diagnosesysteme (sog. OBD-Konnektoren) in den Fahrzeugen und relevante Fahrzeugdaten werden über das Internet bereitgestellt.[1661] Dies führt dazu, dass Anbieter von Dienstleistungen nicht mehr physisch auf die für die Erbringung ihrer Dienstleistung notwendigen Fahrzeugdaten zugreifen können. Das gilt selbst dann, wenn ein Zugriff von mobilen Personen eigentlich gewünscht wäre, etwa für Reparaturen an ihrem Fahrzeug.[1662] 627

Da es Anbietern von Dienstleistungen oft an einem Zugriff auf die Fahrzeugdaten fehlt, sind sie auf die Zustimmung der Fahrzeughersteller angewiesen, welche die alleinige (technische) Kontrolle über den Zugang zu den Daten haben.[1663] Die Hersteller ihrerseits haben kaum Anreize, ihren Konkurrenten Zugriff auf die Daten zu gewähren, werden jedoch von ihren Kunden vermehrt unter Druck gesetzt.[1664] Fahrzeughersteller und Anbieter von Dienstleistungen 628

1658 Wenn eine Beziehung zwischen Verantwortlichem oder Auftragsverarbeiter und betroffener Person besteht, ist die Betroffene in ihrer Rolle als mobile Person zu qualifizieren.

1659 Siehe etwa «Mercedes-Benz und Google schließen Partnerschaft», Mercedes-Benz Medienmitteilung vom 22. Februar 2023, abrufbar unter: https://group.mercedes-benz.com/unternehmen/news/mercedes-benz-und-google.html sowie «Porsche erweitert Partnerschaft mit Google», Porsche Medienmitteilung vom 30. Oktober 2023, abrufbar unter: https://newsroom.porsche.com/de/2023/unternehmen/porsche-erweiterung-partnerschaft-google-34203.html.

1660 Reich/Krämer/Lenninger, ATZelektronik 2018, 42.

1661 C-ITS Platform, 74.

1662 Kerber/Gill, 86; siehe aus ökonomischer Perspektive Kerber/Gill, JIPITEC, 244 ff.

1663 Kerber/Gill, 86.

1664 Martens/Mueller-Langer, JCLE 2020, 133.

sind damit in Bezug auf das Portabilitätsrecht potenziell als alte und neue Verantwortliche zu qualifizieren. Dies macht die Beziehung portabilitätsrelevant.

629 Daten werden ferner nicht mehr einzig zu Werbezwecken verwertet, sondern können auch für andere Akteuren in ganz unterschiedlichen Branchen von hohem Nutzen sein.[1665] Diese zunehmende Bedeutung von Daten zeigt sich im Mobilitätssektor bei Anbietern von Dienstleistungen, die einen eigenen Dienst in einem Fahrzeug anbieten möchten. Gleichzeitig erweitern Fahrzeughersteller ihre Geschäftsmodelle und bieten eigenständig datenbasierte Zusatzdienste an, die über die Herstellung von Fahrzeugen hinausgeht (z.B. Betriebssysteme, Navigationsservices, Reiseplanung, Flottenmanagement für Unternehmen usw.).[1666] Daneben drängen u.a. die etablierten Technologieunternehmen in den Mobilitätssektor, um ihre bisherigen Geschäftsmodelle auch in Fahrzeugen anbieten zu können.[1667] Sie benötigen dafür Daten aus den Fahrzeugen. Diese müssen aktuell, richtig und qualitativ hochwertig sein.[1668] Die erhobenen Daten sind dabei nicht mehr bloss diagnostischer Natur und damit für eine Reparatur notwendig, sondern stellen in ihrer Fülle das Resultat der zahlreichen Sensoren dar, die in neuen Fahrzeugen verbaut sind.[1669] Auch in dieser Hinsicht ist die Beziehung somit portabilitätsrelevant.

630 Entstanden ist somit im Fahrzeugbereich ein neuartiger Markt, in welchem die mobile Person und deren kommerziell verwertbare Daten im Zentrum stehen. Dies gilt nicht nur im Kontext von klassischen Dienstleistungen, die im *Aftermarket* erbracht werden – etwa Reparatur- oder Serviceleistungen –, sondern immer mehr auch für neuartige Dienstleistungen. Die Verwertung der Daten ermöglicht neue (smarte) Produkte, die geeignet sind, herkömmliche Produkte zu ersetzen.[1670] Soweit es sich dabei um plattformbasierte Angebote handelt, sind sowohl Fahrzeughersteller als auch Anbieter von Dienstleistungen bereit, die Funktion der Plattform zu übernehmen. Diese Akteure sind zu Wettbewer-

1665 Drexl, Competitive Markets, 11.

1666 Kortus-Schultes, 98 und 104.

1667 Kortus-Schultes, 99. Dies ist ein gängiges Vorgehen der Techunternehmen, siehe Schallbruch et al., 17 f. Als Beispiele sind TomTom oder Car Play für Apple iOS und Android Auto für Google Android zu nennen. Siehe auch Weissenberg Peter, «So will die Autobranche Google und Apple die Stirn bieten», AutomotiveIT vom 7. August 2023, abrufbar unter: https://www.automotiveit.eu/technology/so-will-die-autobranche-google-und--apple-die-stirn-bieten-734.html.

1668 Rodríguez de las Heras Ballell, EBLR 2023, 12; siehe auch Früh, Jusletter IT Flash 2017, Rz. 11; Weber/Thouvenin, ZSR 2018, 65.

1669 Dazu Rz. 600 f.

1670 Drexl, Competitive Markets, 11.

bern geworden, die ihre Dienstleistungen mobilen Personen anbieten möchten.

In diesem Kontext stellen sich wettbewerbsrechtliche Fragen nach dem Datenzugang.[1671] Aus ökonomischer Perspektive könnte der Nichtzugang zu Daten nämlich dazu führen, dass Anbieter von Dienstleistungen aus diesen Märkten ausgeschlossen würden.[1672] Die Fahrzeughersteller könnten so grosse Teile des ihre Fahrzeuge betreffenden *Aftermarkets* exklusiv beanspruchen.[1673] Die beiden Akteure haben denn auch divergierende Interessen: Die Fahrzeughersteller als Dateninhaber im Primärmarkt haben wenig Interesse daran, Fahrzeugdaten zu liefern, wenn sie selbst, handelnd durch ihre gebundenen Händler und Garagen, auf dem *Aftermarket* tätig sind. Ein Ausschluss für Anbieter von Dienstleistungen hätte für den *Aftermarket* jedoch negative Folgen: Höhere Preise, tiefere Dienstleistungsqualität, weniger Innovation und eine schlechtere Auswahl für die Konsumenten wären mögliche Konsequenzen.[1674] Aus ökonomischer Perspektive kann daher eine regulatorische Lösung für den diskriminierungsfreien Zugang zu den notwendigen Daten angebracht sein. 631

Diese Konstellation ist in der Kartellrechtsliteratur ausführlich aufgearbeitet worden: Diskutiert wird etwa ein Zugang unter FRAND-Bedingungen als geeignete Lösung zum Schutz des Wettbewerbs.[1675] In der Folge könnte ein Anbieter von Dienstleistungen der mobilen Person bspw. eine andere Autogarage vorschlagen, um einen Schaden zu reparieren, als dies der Fahrzeughersteller tun würde.[1676] Diese Multidimensionalität greift das Portabilitätsrecht im Dreiecksverhältnis zwischen betroffener Person und alten und neuen Verantwortlichen auf, indem es neben der Datenherausgabe auch eine Datenübertragung ermöglicht. Die mobilen Personen können ihr Recht auf Datenportabilität aus- 632

1671 Grundlegend Hawker, The Antitrust Bulletin 2011, *passim*. Siehe auch Erw.G 30 DV.

1672 Kerber/Gill, JIPITEC, 246; siehe zur Frage, ob der Wettbewerb zwischen den Fahrzeugherstellern nicht auch den nachgelagerten *Aftermarket* umfassen sollte Kerber, JIPITEC 2018, Rz. 27 ff. Diese auch als *system competition* bezeichnete Situation geht davon aus, dass ein genügender Wettbewerb zwischen den Fahrzeugherstellern (einschliesslich *Aftermarket*) existiert, weshalb die Fahrzeughersteller (einschliesslich *Aftermarket*) wettbewerbsfähige Angebote machen und kein Eingriff in den Markt nötig ist. Zu Recht weist Kerber allerdings darauf hin, dass bei Bestehen einer solchen *system competition* die jahrzehntealten Diskussionen rund um den Ersatzteile- und Reparatur-*Aftermarket* kaum aufgekommen wären; grundlegend hierzu Katz/Shapiro, JEP 1994, *passim*.

1673 Kerber/Gill, JIPITEC, 246; Martens/Mueller-Langer, JCLE 2020, 118; Zäch/Heizmann, Rz. 757.

1674 Kerber/Gill, JIPITEC, 246.

1675 Kerber/Gill, JIPITEC, 246.

1676 McCarthy et al., 89.

üben und dabei mittelbar auch aus wettbewerbsrechtlicher Sicht profitieren, wenn der Verantwortliche die sie betreffenden Daten nicht nur herausgegeben, sondern auch übertragen muss.[1677] Unmittelbar von einer Übertragung profitieren zudem Anbieter auf dem Sekundärmarkt für Reparaturdienstleistungen und Ersatzteile, die darauf angewiesen sind, dass ihnen Daten bereitgestellt werden. Ferner profitieren diejenigen Anbieter, die mit datenbasierten Zusatzdiensten in den Mobilitätssektor drängen.

633 Es geht damit bei Fahrzeugdaten im Wesentlichen um einen Datenzugang für Anbieter von Dienstleistungen. Ein solcher Datenzugang soll sicherstellen, dass der Wettbewerb auf dem *Aftermarket* funktioniert und ein Marktversagen verhindern.[1678] Diese Problematik ist, wie erwähnt, nicht neu. In der EU und in der Schweiz gibt es mehrere sektorielle Initiativen und spezialgesetzliche Vorgaben, die sie adressieren.

bb. Europäische C-ITS-Initiative

634 Die Beziehung zwischen den beiden Akteuren und die damit einhergehenden wettbewerbsrechtlichen Fragen haben unabhängig vom Datenportabilitätsrecht in der EU zur Diskussion geführt, wer Zugriff auf welche Fahrzeugdaten erhalten und wie dieser Zugriff geregelt sein soll. Die EU-Kommission hat darüber im Rahmen der sog. C-ITS-Initiative seit Mitte der 2010er-Jahre mit Branchenvertretungen diskutiert und zu diesem Zweck mehrere Arbeitsgruppen eingesetzt. Eine Arbeitsgruppe untersuchte technische Fragen des Datenzugangs und vertrat dabei im Grundsatz die Haltung, dass die betroffene Person entscheiden können müsse, ob Daten weitergegeben werden sollen und an wen.[1679]

635 Die Arbeitsgruppe schlug unterschiedliche Konzepte vor, um den Datenzugang technisch zu regeln: Mit einer *on-board application platform* verblieben Daten etwa im Fahrzeug. Verschiedene zertifizierte Applikationen unterschiedlicher Anbieter erhielten bei diesem Modell Zugriff auf die Fahrzeugdaten.[1680] Die Systeme wären dabei notwendigerweise offen und interoperabel,

---

1677 Von «indirect beneficiaries» sprechend Graef/Husovec/Van den Boom, EuCML 2020, 9; ähnlich auch Duller, 317.

1678 Allgemein Collovà et al., 8 f.; in Bezug auf die Rechtfertigung einer gesetzlichen Regelung für den Datenzugang zu Fahrzeugdaten siehe Europäische Kommission, Free Flow, 25; Weber/Thouvenin, ZSR 2018, 65.

1679 C-ITS Platform, 75. Das Recht auf Datenportabilität existierte zum Zeitpunkt des Berichts 2016 noch nicht und wurde auch nicht erwähnt.

1680 C-ITS Platform, 76.

was sie anfällig für Angriffe machen und hohe Sicherheitsanforderungen bedingen würde.[1681] Über ein *in-vehicle interface* könnte das Fahrzeug demgegenüber mit externen Geräten verbunden werden.[1682] Die Fahrzeugdaten würden dabei über eine physische Schnittstelle im Fahrzeug bereitgestellt.[1683] An diese Schnittstelle liesse sich eine externe *connectivity control unit* anschliessen, die den Datenstrom erfassen, verarbeiten und sich mit externen Empfängern, wie einem Backend-Server, verbinden könnte.[1684] Diesen beiden Konzepten standen allerdings die Fahrzeughersteller kritisch gegenüber.[1685]

Sie präferierten eine *data server platform*-Lösung. Dabei wird ein Fahrzeug so konfiguriert, dass es generierte Daten nicht mehr lokal speichert, sondern diese direkt an einen Server überträgt.[1686] Die Datenübertragung erfolgt dabei über das Mobilfunknetz.[1687] Wer die Server betreiben soll, ist umstritten: Denkbar wäre eine *extended-vehicle*-Lösung, bei welcher die Fahrzeughersteller die Server betreiben.[1688] Es handelt sich dann beim Fahrzeug um ein Produkt, das einerseits das physische Fahrzeug und andererseits externe Software beinhaltet, um bestimmte Leistungen zu erbringen.[1689] Dieses Konzept hat zur Folge, dass eine Drittpartei, die bspw. Dienstleistungen in diesem Zusammenhang anbieten möchte, nur über diesen zentralen Server auf die Daten zugreifen kann.[1690] Eine solche Lösung ist bereits hinsichtlich ihrer wettbewerbsrechtlichen Zulässigkeit kritisch diskutiert worden[1691] und geht wenig überraschend auf die Fahrzeughersteller zurück. Auf europäischer Ebene sprach sich namentlich die ACEA, der Verband der 14 grössten europäischen Autohersteller, dafür aus.[1692] Sie wollte Anbietern von Dienstleistungen einen Zugang zu den

636

1681 Specht-Riemenschneider/Kerber, 58 f.; siehe auch Kerber, JIPITEC 2018, 319, der darauf hinweist, dass die Sicherheitsprobleme in der ohnehin zunehmend vernetzten und automatisierten Mobilität zu betrachten seien. Zudem sei es unzutreffend, wenn davon ausgegangen würde, dass es einen Kompromiss zwischen den Zielen der Sicherheit und des fairen und unverfälschten Wettbewerbs geben müsse. Ferner McCarthy et al., 77, die eine sichere Ausgestaltung für technisch machbar halten; sich darauf beziehend auch Kerber, 456.

1682 C-ITS Platform, 76.

1683 C-ITS Platform, 83.

1684 C-ITS Platform, 83.

1685 C-ITS Platform, 83.

1686 Metzger, GRUR 2019, 130; Pautke/Oest, Rz. 26.

1687 Kerber/Frank, 23.

1688 C-ITS Platform, 78; kritisch und m.w.N. Kerber/Gill, JIPITEC, 249.

1689 C-ITS Platform, 78.

1690 Kerber/Frank, 23.

1691 Kerber/Frank, 23 ff.; Kerber/Gill, JIPITEC, 253; Picht, IIC 2020, 946 m.w.N.

1692 ACEA, 2; siehe auch McCarthy et al., 13.

Daten ermöglichen, ihn aber von einer B2B-Einigung zwischen den Parteien abhängig machen.[1693] Ein Datenzugang soll m.a.W. Verhandlungssache sein und eine Regulierung ausbleiben.[1694] Einen direkten Zugang für Dritte zu den *in-vehicle*-Daten hielt die ACEA aus Datensicherheitsgründen nicht für angezeigt.[1695]

637 Der Automobilverband FIA Region I, der die europäischen Automobilclubs und etwa den TCS vertritt, stand dieser Ansicht kritisch gegenüber und befürchtete, dass Innovation gehemmt und das Geschäft von Konkurrenten überwacht werden könnte, wenn ausschliesslich die Hersteller die Daten kontrollierten.[1696] Er schlug vor, die Daten auf den Servern einer neutralen Drittpartei zu hosten (sog. *shared data server solution*).[1697] Weitere Stimmen bevorzugten ebenfalls eine Lösung, in welcher eine neutrale Drittpartei die Server verwaltet.[1698]

638 Die EU-Kommission hält es für am wahrscheinlichsten, dass sich der Vorschlag der ACEA etablieren wird, wenn eine Marktintervention ausbleibt.[1699] In diesem Fall wäre zu erwarten, dass die Fahrzeughersteller entsprechende technische Standards für die Schweiz übernehmen. Solche existieren denn auch mittlerweile für die *extended-vehicle*-Lösung.[1700] Diskussionen dazu sind in der Schweiz jedoch bislang nicht auszumachen.

cc. Europäische Datenverordnung (DV)

639 Trotz ihrer Nutzerzentriertheit[1701] kann die DV unmittelbar zwischen Fahrzeugherstellern und Anbietern von Dienstleistungen Wirkung entfalten. Stellt ein Dateninhaber nach Art. 5 DV Daten im Rahmen von Geschäftsbeziehungen zwischen Unternehmen einem Datenempfänger bereit, muss diese Bereitstellung zu FRAND-Bedingungen und in transparenter Weise im Einklang mit den Vorgaben nach Kapitel III und IV erfolgen (Art. 8 DV). Die Daten darf der Dateninhaber einem Datenempfänger (auch exklusiv) jedoch nur dann bereitstellen, wenn der Nutzer dies gemäss Kapitel II verlangt hat (Art. 8 Abs. 4 DV). Er-

1693 ACEA, 5.
1694 KERBER/FRANK, 23.
1695 ACEA, 5; hierzu auch KERBER/GILL, 86.
1696 FIA Region I, 5.
1697 FIA Region I, 5; diesen Vorschlag ebenfalls besprechend PICHT, IIC 2020, 946.
1698 C-ITS Platform, 78.
1699 MCCARTHY et al., 13.
1700 Siehe ISO 20077-1:2017.
1701 Dazu Rz. 620 f.

hält ein Dritter (der auch Datenempfänger sein kann[1702]) Daten auf Verlangen eines Nutzers, darf er diese nach Art. 6 Abs. 2 lit. e DV nicht nutzen, um ein konkurrierendes Produkt zu entwickeln oder die Daten zu diesem Zweck an einen anderen Dritten weitergeben. Dieselbe Bestimmung untersagt ihm zudem, bereitgestellte nicht-personenbezogene Produktdaten oder verbundene Dienstdaten zu nutzen, um Einblicke in die wirtschaftliche Lage, die Vermögenswerte und die Produktionsmethoden des Dateninhabers oder die Nutzung durch den Dateninhaber zu gewinnen. Mit Blick auf das gerade im *Aftermarket* zwischen den Akteuren bestehende Wettbewerbsverhältnis befürchtet die Literatur teilweise, dass Datenzugriffsmöglichkeiten in Echtzeit für Konkurrenten die Anreize zur Datensammlung minimieren könnten.[1703] Da die DV nicht zur Speicherung von Daten verpflichtet, würde dies dazu führen, dass Dateninhaber bestimmte IoT-Daten gar nicht mehr erfassen.[1704]

dd. Europäische TypgenehmigungsVO

Nach EU-Recht müssen Fahrzeughersteller bereits heute zwingend Diagnostikdaten bereitstellen. Rechtliche Grundlage dafür ist die TypgenehmigungsVO, die als sektorspezifischer Erlass im Mobilitätssektor anwendbar ist.[1705] Unabhängige Wirtschaftsakteure, also etwa Anbieter von Dienstleistungen, können gestützt auf die TypgenehmigungsVO Zugang zu Fahrzeug-OBD-Informationen, Diagnose- und anderen Geräten und Instrumenten sowie zu Fahrzeugreparatur- und -wartungsinformationen erhalten (Art. 61 Abs. 1 TypgenehmigungsVO).[1706] Dies soll den wirksamen Wettbewerb auf dem Markt für Dienstleistungen zur Bereitstellung solcher Informationen sicherstellen und ein festgestelltes Marktversagen beheben (Erw.G 50 TypgenehmigungsVO).[1707] Für ein besseres Funktionieren des Binnenmarkts, insb. für den freien Warenverkehr, die Niederlassungsfreiheit und die Dienstleistungsfreiheit, sei ein solches Vorgehen notwendig (Erw.G 50 TypgenehmigungsVO). Der unabhängige

640

1702 Siehe Art. 2 Ziff. 14 DV.

1703 Wunner, ZUM 2024, 433.

1704 Wunner, ZUM 2024, 433.

1705 Grundlegend Hübener/Lutz, ZWeR 2024, 143 ff.; Kerber/Gill, JIPITEC, 244 ff.

1706 Bei solchen Daten steht deren technischer Aussagegehalt im Vordergrund. Es ist jedoch nicht auszuschliessen, dass sie einen Personenbezug aufweisen, mithin die betroffenen Personen zumindest bestimmbar sind siehe Graef/Husovec/Van den Boom, EuCML 2020, 8, siehe aber auch a.a.O., 10, wonach die TypgenehmigungsVO «keine personenbezogenen Daten betrifft». Dies trifft insofern zu, als die Verarbeitung von Personendaten gemäss Erw.G 62 TypgenehmigungsVO weiterhin den Vorgaben der DSGVO untersteht.

1707 Noch mit Verweis auf die Vorgängerverordnungen Europäische Kommission, Datenstrategie, 4; siehe auch Duller, 299 f.

Markt der Fahrzeugreparatur und Fahrzeugwartung soll gemäss Erw.G 52 TypgenehmigungsVO mit Vertragshändlern konkurrieren können.

641 Die Angaben sind leicht zugänglich und in Form von maschinenlesbaren und elektronisch verarbeitbaren Datensätzen bereitzustellen.[1708] Sie müssen nach Art. 61 Abs. 2 UAbs. 2 TypgenehmigungsVO i.d.R. auf der Website der Hersteller veröffentlicht werden. Der Fahrzeughersteller darf keine über die TypgenehmigungsVO hinausgehenden Bedingungen für den Datenzugang vorsehen. So ist ihm namentlich untersagt, eine Verbindung des Diagnosegeräts mit einem vom Hersteller bestimmten Server oder eine vorherige Registrierung bzw. Anmeldung der unabhängigen Wirtschaftsakteure beim Hersteller zu verlangen.[1709] Dem unabhängigen Wirtschaftsakteur ist es erlaubt, die Informationen, zu welchen er Zugang erhält, zu verarbeiten und zu verwerten.[1710]

642 In Zukunft soll ein Normungsgremium die einschlägigen Normen vereinheitlichen (siehe Art. 61 Abs. 2 UAbs. 1 TypgenehmigungsVO). Dies ist jedoch ein mehrjähriger Prozess, dessen Abschluss noch nicht absehbar ist.[1711] Fest steht allerdings, dass bei der Ausarbeitung eines gemeinsamen strukturierten Verfahrens für den Datenaustausch sowohl die Interessen der Fahrzeughersteller als auch der unabhängigen Wirtschaftsakteure zu berücksichtigen und Lösungen wie durch eindeutige Metadaten definierte offene Datenformate zu prüfen sind (Erw.G 54 TypgenehmigungsVO). Bereits heute existieren indessen in einer ergänzenden Verordnung der EU-Kommission Interoperabilitätsvorgaben: Die Informationen müssen den technischen Spezifikationen mehrerer sog. OASIS-Dokumente sowie «möglichst weitgehend» der Norm ISO 15031-2 entsprechen (Art. 61 Abs. 11 TypgenehmigungsVO i.V.m. Anhang XIV Ziff. 2 TypgenehmigungsErgänzungsVO).[1712] Die Fahrzeughersteller dürfen dafür nach

1708 Das war noch unter der Vorgängerverordnung nicht der Fall. Die Fahrzeughersteller durften den unabhängigen Wirtschaftsakteuren auch nur einen Lesezugriff ermöglichen. Unter der TypgenehmigungsVO ist dies nicht mehr der Fall, siehe EuGH C-296/22 vom 5. Oktober 2023 Rz. 28 f.; EuGH C-527/18 vom 19. September 2019 Rz. 26 und 34.

1709 EuGH C-296/22 vom 5. Oktober 2023, Rz. 38.

1710 EuGH C-390/21 vom 27. Oktober 2022, Rz. 29; Hübener/Lutz, ZWeR 2024, 145.

1711 Siehe dazu Wagner/Karagkouni, EuZW 2019, 110.

1712 Nach der Vorgabe müssen die Informationen dem OASIS-Dokument SC2-D5, Format für Kraftfahrzeug-Reparaturinformationen, Fassung 1.0 vom 28. Mai 2003 und der Abschnitte 3.2, 3.5 (ausgenommen 3.5.2), 3.6, 3.7 und 3.8 des OASIS-Dokuments SC1-D2, Spezifikationsvorschriften Autoreparatur, Fassung 6.1 vom 10. Januar 2003 entsprechen, wobei ausschliesslich offene Text- und Grafikformate oder Formate verwendet werden dürfen, die nur mit Hilfe herkömmlicher Software-Plug-ins angezeigt und gedruckt werden können, welche frei erhältlich sind, sich einfach installieren lassen und mit allgemein gebräuchlichen Computer-Betriebssystemen funktionieren.

Art. 63 Abs. 1 TypgenehmigungsVO angemessene und verhältnismässige Gebühren erheben.[1713]

Die relevanten Bestimmungen der TypgenehmigungsVO gelten in ihrer Fassung vom 14. Juni 2018 unmittelbar für die Schweiz (siehe Anhang 2 Ziff. 111 VTS), weshalb in der Schweiz dieser Zugang ebenfalls zu ermöglichen ist. Gleiches gilt für die Interoperabilitätsvorgaben der TypgenehmigungsErgänzungsVO (siehe Anhang 2 Ziff. 112 VTS). Umfasst sind aber nur diejenigen Informationen, die von einem OBD-System generiert werden, das sich in einem Fahrzeug befindet oder an einen Motor angeschlossen ist (Art. 3 Ziff. 49 TypgenehmigungsVO). Damit fallen viele der heute relevanten Daten gar nicht mehr unter die entsprechenden Verordnungen, da sie, wie erläutert, nicht mehr lokal gespeichert werden (müssen).[1714] Ein Zugang zu Daten, die für innovative mobile Reparatur- und Wartungsdienstleistungen notwendig sind sowie zu Daten, die für die vielfältigen Dienstleistungen im Bereich des vernetzten Fahrens genutzt werden, wird dadurch nicht gewährt.[1715] 643

Dennoch wird in der TypgenehmigungsVO ein praktikables und hilfreiches Instrument zur Regulierung im Mobilitätssektor gesehen.[1716] So haben Evaluationen der Vorgängerregulierung der TypgenehmigungsVO gezeigt, dass die Verordnung die wettbewerbsfördernden Zwecke grundsätzlich erreicht.[1717] Auch die Tatsache, dass Anbieter von Dienstleistungen regelmässig den EuGH anrufen, um den Datenzugang gerichtlich durchzusetzen, spricht dafür, dass sie der TypgenehmigungsVO in der Praxis durchaus einen Wert beimessen.[1718] 644

ee. KFZ-Verordnung

In der Schweiz hat der Bundesrat aus kartellrechtlichen Überlegungen die KFZ-Verordnung (KFZV) erlassen. Sie gilt für vertikale Wettbewerbsabreden beim Vertrieb von neuen Kraftfahrzeugen und Ersatzteilen sowie bei der Erbringung von Instandsetzungs- und Wartungsdienstleistungen (Art. 2 Abs. 1 KFZV). Ziel ist, dass der Zugang zu technischen Informationen nicht be- 645

1713 Siehe dazu Martens/Mueller-Langer, JCLE 2020, 121, die einwenden, dass die Diskriminierung der unabhängigen Wirtschaftsakteure bei der Preisgestaltung für die Computerprogramme und die Zugangscodes zum Lesen und Interpretieren der OBD-Daten erfolge. Dies hindere sie daran, die gleichen Preise wie die Fahrzeughersteller anzubieten.

1714 Kerber/Gill, JIPITEC, 249; Picht, IIC 2020, 962 f.; dazu Rz. 635 ff.

1715 Kerber/Gill, 89.

1716 Picht, IIC 2020, 962 f. m.w.N.

1717 Europäische Kommission, Evaluation, 6; besonders bezugnehmend auf Lock-In-Effekte EY/FIA Region I, 21; Kerber/Gill, JIPITEC, 247.

1718 EuGH C 296/22 vom 5. Oktober 2023; EuGH C 390/21 vom 27. Oktober 2022.

schränkt ist. Deshalb gelten bestimmte Abreden zwischen Fahrzeugherstellern[1719] und Mitgliedern eines Vertriebssystems als qualitativ schwerwiegende Beeinträchtigungen des Wettbewerbs i.S.v. Art. 5 Abs. 1 KG, wenn diese den Zugang von unabhängigen Marktteilnehmenden zu den für die Instandsetzung und Wartung von Kraftfahrzeugen oder für Umweltschutzmassnahmen erforderlichen technischen Informationen, Diagnosegeräten sowie anderen Geräten und Werkzeugen nebst einschlägiger Software oder die fachlichen Unterweisungen verweigern (Art. 6 Abs. 1 KFZV). Erfasst ist somit die hier untersuchte Beziehung zwischen Fahrzeugherstellern und Anbietern von Dienstleistungen.

646 Zugänglich zu machen sind etwa Software, Fehlercodes und sonstige Parameter, Kfz-Identifizierungsnummern, Teilekataloge, Instandsetzungs- und Wartungsverfahren.[1720] Die Informationen dürften oft keinen Personenbezug aufweisen, obwohl ein solcher nicht ausgeschlossen ist, wenn die FIN oder das Kfz-Kennzeichen ebenfalls vorliegen und eine Verknüpfung dadurch möglich wird.[1721] Laut den Erläuterungen ist der Begriff der technischen Information weit zu fassen und jeweils anhand des technologischen Fortschritts auszulegen.[1722] Dabei ist die Art und Weise, in der die technischen Informationen bereitgestellt werden, zu berücksichtigen: Gemäss WEKO kann auch der Preis dadurch vom Zugang abschrecken, dass das Ausmass der Nutzung der Informationen durch den unabhängigen Marktteilnehmenden unberücksichtigt bleibt oder ungebührliche Verzögerungen die Angaben nicht verwendungsfähig machen.[1723] Die Jahresberichte der WEKO lassen jedenfalls darauf schliessen, dass Fahrzeughersteller den Zugang zu technischen Informationen nicht immer störungsfrei gewähren.[1724]

3. Erkenntnisse und Überleitung

647 Aus der Strukturierung des Mobilitätsdatenökosystems geht hervor, dass das Portabilitätsrecht in unterschiedlichen Beziehungen innerhalb des Mobilitäts-

1719 In der Terminologie der KFZV «Kraftfahrzeuganbieter».
1720 WEKO, Erläuterungen KFZV, Ziff. 13.
1721 Dazu Rz. 602 f.
1722 WEKO, Erläuterungen KFZV, Ziff. 13.
1723 WEKO, Erläuterungen KFZV, Ziff. 14.
1724 Die WEKO hält für den Automobilsektor fest, dass sie regelmässig Anfragen von Händlern, Werkstätten und Endkunden zu beantworten hat, die den Zugang zu technischen Informationen betreffen, siehe WEKO, Jahresbericht 2021, 18; WEKO, Jahresbericht 2019, 18; WEKO, Jahresbericht 2018, 15.

datenökosystems anwendbar sein kann und dass bereits mehrere sektorielle Vorgaben für einen Datenzugang im Mobilitätssektor existieren. Für die datenschutzrechtlichen Ziele ergibt sich dabei in diesem Sektor keine herausragende Relevanz, sodass diese nachfolgend nur kurz zu behandeln sind. In wettbewerbsrechtlicher Hinsicht ist hingegen die Beziehung zwischen Fahrzeughersteller und Anbieter von Dienstleistungen bedeutend. Sie kommen als alte und neue Verantwortliche in Frage. Nachdem in § 2 festgestellt wurde, dass das Recht auf Datenportabilität auch die Verhinderung von Lock-In-Effekten und Markeintrittsschranken für Konkurrenten, die Senkung von Wechselkosten sowie die Ermöglichung eines freien Datenflusses bezweckt, ist deren Beziehung vertieft zu untersuchen. Dabei ist die Rolle der Betroffenen und deren Möglichkeiten bei der Ausübung des Datenportabilitätsrechts zu beleuchten. Anschliessend sind mögliche Handlungsspielräume für den Mobilitätssektor im Lichte der Ziele aufzuzeigen und Anpassungsvorschläge zu diskutieren.

B. Kritische Würdigung der Datenportabilität

1. Datenschutzrechtliche Ziele

Das Recht auf Datenportabilität wird der datenschutzrechtlichen Zielsetzung im Mobilitätsdatenökosystem weitgehend gerecht. Die mobile Person als datenschutzrechtlich Betroffene kann selbstbestimmt gegenüber anderen Akteuren in die Datenwirtschaft eingreifen und im Rahmen des ihr eingeräumten Portabilitätsrechts über die Zuordnung der sie betreffenden Daten des Mobilitätssektors entscheiden.[1725] Selbst bei Annahme eines traditionellen Verständnisses des Rechts auf informationelle Selbstbestimmung wird der betroffenen Person die Herrschaft über «ihre» Daten mit dem Recht auf Datenportabilität mit gewissen Einschränkungen ermöglicht. 648

Ein Problembereich zeigt sich jedoch beim Personenbezug der Daten. Es dürfte im Einzelfall oft unklar sein, welche Daten personenbezogen und entsprechend vom Portabilitätsrecht erfasst sind.[1726] Verantwortliche neigen dann möglicherweise dazu, einen Personenbezug zu bestreiten, um bestimmte Daten nicht portieren zu müssen.[1727] Dies kann nicht nur bezüglich der wettbe- 649

[1725] Siehe dazu EY/FIA Region I, 78.

[1726] Gill/Kerber, CPI Antitrust Chronicle 2020, 56; dazu auch die Ausführungen im Kontext der Fahrzeugdaten, Rz. 602 f.

[1727] Ähnlich EY/FIA Region I, 88 f.

werbsrechtlichen, sondern insb. bezüglich der datenschutzrechtlichen Zielsetzung zu unbefriedigenden Ergebnissen führen, weil Betroffene sie betreffende Daten nicht erhalten. Damit geht eine Rechtsunsicherheit einher, welche die Position der Betroffenen schwächt.

2. Wettbewerbsrechtliche Ziele beim Zugang zu Fahrzeugdaten für Anbieter von Dienstleistungen

a. Verringerung von Lock-In-Effekten und Markteintrittsschranken

650 Wie festgestellt, existiert im Automobilbereich ein Netzwerk aus offiziellen Händlern, welche exklusiv Reparatur- und weitere Leistungen für einen Fahrzeughersteller übernehmen und damit den OEM-*Aftermarket* bilden. Da Fahrzeuge heute ohne Datenzugang kaum noch repariert oder gewartet werden können, sind mobile Personen an offizielle Händler gebunden, wenn Anbieter von Dienstleistungen keinen Zugriff auf die notwendigen Daten erhalten. Es bestehen damit Markteintrittsschranken für Anbieter von Dienstleistungen. Ihnen ist es kaum möglich, in den datengetriebenen *Aftermarket* einzutreten.[1728] Dies kann dazu führen, dass der Mobilitätsmarkt kippt und nur noch der Fahrzeughersteller auf dem Markt verbleibt.[1729]

651 Ist ein Eintritt in den Markt noch möglich, haben mobile Personen noch immer Wechselkosten zu tragen, wenn sie den Anbieter wechseln möchten. Folglich besteht im Grundsatz ein *Lock-in* der mobilen Personen und ihrer Daten, der aufgrund der langen Lebensdauer von Fahrzeugen (etwa im Vergleich zu einem Account bei einem sozialen Netzwerk) besonders ausgeprägt ist.[1730] An diesem Punkt soll das Recht auf Datenportabilität ansetzen und die Grundlagen schaffen, damit ein solcher *Lock-In* zumindest verringert werden kann.[1731] Zahlreiche Autoren kritisieren allerdings, dass das Institut nicht wirkungsvoll genug sei, um den notwendigen Datenaustausch im Mobilitätssektor zu ermöglichen

1728 Dies gilt auch dann, wenn der Anbieter von Dienstleistungen zunächst mit dem Fahrzeughersteller über einen Datenzugang verhandeln muss, siehe dazu McCarthy et al., 198 f.

1729 Picht, IIC 2020, 947.

1730 Siehe Picht, IIC 2020, 946.

1731 In diese Richtung Bundesministerium für Verkehr und digitale Infrastruktur, 62 und 128; EY/FIA Region I, 24 und 86, durchaus mit kritischem Fazit; Kerber/Gill, 95; ähnlich auch Schätzle, PinG 2016, 72 f.

und die wettbewerbsrechtlichen Ziele zu erreichen.[1732] Damit offenbaren sich in mehrerer Hinsicht Unzulänglichkeiten.

Erstens sind zahlreiche notwendige (technische) Fahrzeugdaten nicht vom Portabilitätsrecht erfasst, was dessen wettbewerbsrechtliche Wirkung schmälern kann.[1733] In der Literatur wird denn auch vertreten, dass das Institut «völlig ungeeignet» sei, um den Zugang zu bestimmten diagnostischen Daten und Fahrzeugreparaturinformationen zu ermöglichen.[1734] Denn bei diesen handelt es sich regelmässig um Sachdaten oder um Personendaten, welche aus anderen Gründen nicht der Portierung unterliegen, etwa, weil sie nicht bekanntgegeben wurden. Solche können für Akteure dennoch elementar sein. Das Portabilitätsrecht kann hier also sein Ziel verfehlen.[1735] 652

Zweitens wird der Zeitrahmen, in welchem eine Anfrage erfüllt werden muss, kritisiert. Dieser mache das Institut für Reparatur und Wartung unbrauchbar.[1736] Eine Herausgabe erfolge zu langsam und zu fragmentarisch.[1737] Auch für andere Dienstleistungen reicht eine einmalige Portierung oft nicht aus: Gerade neu in den Markt eintretende Anbieter (etwa von Navigationsdiensten oder Infotainmentsystemen) können auf Daten des Fahrzeugherstellers angewiesen sein.[1738] Ohne Datenzugang lassen sich viele Dienstleistungen gar nicht erbringen. In dieser Hinsicht bewirkt das Portabilitätsrecht keine Verbesserung. 653

1732 EY/FIA Region I, 84; Gill/Kerber, CPI Antitrust Chronicle 2020, 55 f.; kritisch bezüglich Dienstleistungen in *Aftermarkets* schlechthin Janal, 342; Kerber/Gill, 96; Kerber, JIPITEC 2018, 326 f.; Martens/Mueller-Langer, 24, die zwar im Portabilitätsrecht eine wirkungsvolle Option zu sehen scheinen, dafür aber eine «volle» Portabilität verlangen und einräumen, dass es massgeblich auf die tatsächliche Auslegung und Umsetzung der Portabilitätsregelung im Kontext von Fahrzeugdaten ankomme; Picht, IIC 2020, 950 ff., nach welchem im Kern wohl aufgrund der Nutzerzentrierung das Portabilitätsrecht nur ungenügend Wirkung entfalten dürfte; davon ausgehend, dass die wettbewerblichen Ziele «derzeit» nicht erfüllt werden können Sackmann, 160; a.M. Störing, 17, der das Portabilitätsrecht breit auslegt und entsprechend «erhebliche Auswirkungen» auf vernetzte Fahrzeuge erwartet. Bisweilen wird auch angezweifelt, ob die wettbewerbsrechtlichen Zielsetzungen angesichts des langen Zeitraums, auf welchen ein Autokauf ausgelegt ist und dem zu zahlenden (hohen) Preis überhaupt erreicht werden können, siehe Gill/Metzger, EDPL 2022, 223, insb. Fn. 15.

1733 Siehe etwa Hübener/Lutz, ZWeR 2024, 147, die davon ausgehen, dass ein «signifikanter Teil» der Anwendungsfälle nicht von der DSGVO erfasst sind.

1734 Wendehorst/Schwamberger, DAR 2022, 543.

1735 Ähnlich Landolt, 189.

1736 Wendehorst/Schwamberger, DAR 2022, 543.

1737 Picht, IIC 2020, 951; ähnlich bemängelnd, dass eine regelmässige Datenübermittlung nicht möglich sei Hübener/Lutz, ZWeR 2024, 147.

1738 So wohl auch Kerber/Gill, 96.

654 Drittens muss die Betroffene das Portabilitätsrecht tatsächlich ausüben. Anbieter von Dienstleistungen benötigen Daten, können jedoch nur auf indirektem Weg zu diesen gelangen. Zwar ist es in der Schweiz möglich, das Portabilitätsrecht stellvertretend auszuüben.[1739] Dennoch existieren für Anbieter von Dienstleistungen Hürden, da Betroffene Transaktionskosten zu tragen haben und Anreize gesetzt werden müssen, damit sie das Portabilitätsrecht ausüben (lassen).[1740]

b. Allgemeine Wettbewerbs- und Innovationsförderung sowie Förderung des freien Datenflusses

655 Fahrzeuge stellen heute keine von der Umwelt abgeschlossenen Systeme mehr dar. Mit dem IoT erschliessen auch Akteure anderer Ökosysteme das Mobilitätsdatenökosystem, so dass eine Unterscheidung kaum mehr trennscharf möglich ist, etwa wenn das Mobiltelefon als Fahrzeugschlüssel dient. Der smarte Mobilitätsbereich wird zu einem Teil des *interconnected information space* und damit des Internets, in welchem bestehende Datensilos innovationshemmend sein können. Dies gilt auch für Fahrzeughersteller, auf deren Produkten und Datensätzen ein umfassender *Aftermarket* aufbaut. Der bereits in allgemeiner Weise ausgeführten Zielsetzung der allgemeinen Wettbewerbs- und Innovationsförderung, die nach hier vertretener Ansicht als primäres wettbewerbsrechtliches Ziel des Portabilitätsrechts zu betrachten ist, kommt angesichts dieser Entwicklung im Mobilitätsdatenökosystem eine grosse Bedeutung zu.[1741] Somit ist davon auszugehen, dass mit dem Recht auf Datenportabilität die Grundlagen für eine Zielerreichung geschaffen wurden.[1742] Damit einher gehen die datenpolitischen Überlegungen zur Förderung des freien Datenflusses für Daten schlechthin.[1743] Allerdings kennzeichnen sich diese Ziele gerade dadurch, dass sie sich nicht auf einzelne Akteure oder Sektoren beschränken, sondern auf sektorübergreifenden Überlegungen gründen, und die einzelnen Ökosysteme verbinden sollen.

1739 Dazu Rz. 217 f.
1740 EY/FIA Region I, 87; GILL/KERBER, CPI Antitrust Chronicle 2020, 56 f.
1741 Dazu Rz. 320 ff.
1742 EY/FIA Region I, 75.
1743 EY/FIA Region I, 77 f., die darin insb. einen Nutzen für die Öffentlichkeit und Gesellschaft sehen.

3. Einordnung unter Berücksichtigung der spezialgesetzlichen Datenzugangsregelungen

Bevor die sich aus den eben genannten Unzulänglichkeiten ergebenden Handlungsspielräume des Portabilitätsrechts dargelegt werden, gilt es in Erinnerung zu rufen, dass es bereits sektorielle Vorgaben gibt, die einen Datenzugang ermöglichen. Sie sind teilweise auf die gleichen Ziele wie das Recht auf Datenportabilität ausgerichtet. Zu denken ist dabei namentlich an eine Verringerung des *Lock-In* und an einen Abbau der Markteintrittsschranken durch die TypgenehmigungsVO oder die KFZV. In der EU existiert zudem mit der DV ein weiterer Erlass, der zwar nicht auf den Mobilitätssektor begrenzt ist, aber u.a. in diesem solche Ziele verfolgt. 656

Bislang ist unklar, wie sich die sektorspezifischen Vorgaben zum datenschutzrechtlichen Portabilitätsrecht verhalten und was dies für das Portabilitätsrecht beim Zugang zu Fahrzeugdaten bedeutet. Fest steht, dass die unterschiedlichen Instrumente ohne Weiteres parallel angerufen werden können.[1744] Unbestritten ist zudem, dass sich die Regelungen in mehrerer Hinsicht unterscheiden: Sie decken einen eingeschränkten, aber jeweils unterschiedlichen Bereich an Daten ab, wobei das datenschutzrechtliche Institut in seiner sektorübergreifenden Anwendbarkeit einerseits potenziell deutlich weiter geht, dabei aber andererseits nur Personendaten umfasst. Die sektoriellen Erlasse erfassen hingegen konkrete Sachverhalte und zielen dabei primär auf nicht personenbezogene, technische Daten ab. Doch selbst bei diesen lässt sich ein Personenbezug nicht immer ausschliessen. Weiter unterscheiden sich die berechtigten Personen: Während die Portabilitätsregelung die mobile Person ins Zentrum stellt, adressieren die TypgenehmigungsVO und die KFZV als wettbewerbsrechtliche Institute vor allem Anbieter von Dienstleistungen und ggf. Fahrzeughändler. Unterschiedlich sind auch die technischen Modalitäten: Die sektoriellen Erlasse sehen ein Zugangsrecht vor und keine Herausgabe oder Übertragung der Daten. Eine Angleichung hat zwar dadurch stattgefunden, dass ein reiner Lesezugriff für die Zugangsgewährung nicht mehr ausreicht.[1745] Dennoch kann sich ein Datenzugang, wie gesehen, von einer Portierung erheblich unterscheiden.[1746] Bereits durch diese Unterschiede ergibt sich ein unterschiedlicher Anwendungsbereich der Regelungen, der das Verhältnis zumindest teilweise klärt. 657

1744 Graef/Husovec/Van den Boom, EuCML 2020, 3.
1745 Siehe dazu Fn. 1708.
1746 Dazu Rz. 358 ff.

658 Verlagert sich der Blick auf die Zielsetzungen, so wird deutlich, dass das Portabilitätsrecht gegenüber der TypgenehmigungsVO und der KFZV selbst dort seine Berechtigung hat, wo im Einzelfall eine präzisere sektorielle Lösung existiert. Die Spezialerlasse beziehen sich primär auf Wartung und Reparatur von Fahrzeugen und damit zwar ebenfalls vor allem auf andersartige Anbieter von Dienstleistungen auf dem *Aftermarket*.[1747] Nur weil der von der Spezialgesetzgebung erfasste *Aftermarket* aus komplementären Angeboten besteht, sind jedoch nicht alle komplementären Angebote von der Spezialgesetzgebung erfasst. Mit dem Portabilitätsrecht soll gerade auch abseits der bestehenden Zugangsrechte für Wartung und Reparatur datengetriebene Innovation im *Aftermarket* möglich werden, weshalb es eine Portierung von Daten für unbestimmte Verwendungszwecke zulässt.[1748] Betroffene sollen Daten an andersartige Anbieter von Dienstleistungen übertragen (lassen) können, sodass neue Angebote entstehen und sie von diesen profitieren können. Dies ist unter den spezialgesetzlichen Regelungen – mit Ausnahme der in der Schweiz nicht übernommenen DV – nicht in dieser Breite möglich. Dazu kommt, dass die spezialgesetzlichen Regelungen, anders als das Recht auf Datenportabilität, keine datenschutzrechtlichen Ziele verfolgen.

659 Dennoch wird in der Literatur im Kontext der Fahrzeugdaten für sektorielle Lösungen votiert, etwa mit der Begründung, dass das datenschutzrechtliche Portabilitätsrecht für sich genommen die Probleme rund um den Zugang zu Fahrzeugdaten kaum lösen könne.[1749] Gerade in der TypgenehmigungsVO wird ein Beleg dafür gesehen, dass eine sektorielle Regulierung ein praktikables und hilfreiches Instrument im Mobilitätssektor sein kann.[1750] Folglich wäre auf spezifische Unzulänglichkeiten, die das Portabilitätsrecht zu adressieren versucht, nicht mittels einer Anpassung ebendieses zu reagieren, sondern bei den sektoriellen Regelungen anzusetzen. Denkbar wäre, bereits bestehende Regelungen anzupassen oder neuartige zu schaffen. Sektorspezifisch – und damit zielgerichteter – liesse sich etwa eine bestimmte technische Architektur wie die *on-board application platform* vorschreiben, welche die Verarbeitung von Daten lokal im Fahrzeug sicherstellt.[1751]

1747 Graef/Husovec/Van den Boom, EuCML 2020, 12.

1748 So auch Graef/Husovec/Van den Boom, EuCML 2020, 12, die das Portabilitätsrecht sowohl auf komplementäre als auch auf substitutive Dienste abzielen sehen.

1749 Eckardt/Kerber, 21 f., die nicht nur das Portabilitätsrecht nach Art. 20 DSGVO, sondern auch die neuen Regelungen der DV als ungenügend betrachten und für eine Modernisierung der TypgenehmigungsVO plädieren; EY/FIA Region I, 100 und 104; Gill/Metzger, EDPL 2022, 236 f.; Wendehorst/Schwamberger, DAR 2022, 544.

1750 Picht, IIC 2020, 963 m.w.N.; Podszun, 96 m.w.N.

1751 EY/FIA Region I, 100.

In der EU sollte namentlich die DV viele der Schwächen des Datenportabilitätsrechts ausgleichen.[1752] Ungeachtet dessen ist in der EU eine Erweiterung der TypgenehmigungsVO in Planung. Denn die EU-Kommission ist der Ansicht, dass die Bestimmungen der DV nicht genügend detailliert seien, um den hohen Anforderungen für die Erbringung datenabhängiger Dienstleistungen im Automobilsektor gerecht zu werden.[1753] Eine solche Erweiterung der TypgenehmigungsVO würde voraussichtlich von der Schweiz erneut übernommen. Es wird zu beobachten sein, wie sich dieses Vorhaben weiterentwickelt.[1754] Eine der DV nachempfundene Regelung ist in der Schweiz bis anhin jedenfalls nicht geplant.[1755] 660

Schliesslich ist anzumerken, dass bei den sektoriellen Lösungen stets sog. Spill-Over-Effekte zum datenschutzrechtlichen Portabilitätsrecht möglich sind. Namentlich könnten sektorielle Vorgaben dazu führen, dass bestimmte Regelungen faktisch auch beim (breiteren) Portabilitätsrecht Anwendung finden.[1756] So ist denkbar, dass sich etablierte Abläufe und Standards in einem Sektor auf die Anwendung des Datenportabilitätsrechts in diesem Sektor auswirken, selbst wenn das DSG keine strengeren Vorgaben enthält. Dies könnte insgesamt zu einem funktionierenden Zusammenspiel zwischen sektorübergreifenden und sektoriellen Regelungen führen, wobei dem sektorübergreifenden Portabilitätsrecht mehr Gewicht zukäme, wenn die Modalitäten in einzelnen Sektoren tragfähiger wären. Damit würde in Zukunft ein funktionierender Datenaustausch in und zwischen den Sektoren entstehen, der der holistischen Denkweise eines Datenrechts gerecht wird. Folglich tragen selbst Anpassungen sektorieller Vorgaben dazu bei, dass das Portabilitätsrecht nach Art. 28 DSG seine Ziele im Mobilitätssektor besser erreichen kann. 661

1752 Dazu Wendehorst/Schwamberger, DAR 2022, 543.

1753 Europäische Kommission, Aufforderung zur Stellungnahme, 2 f.; dazu auch Wendehorst/Schwamberger, DAR 2022, 543.

1754 Siehe https://perma.cc/2TZR-RSGN.

1755 Dazu Rz. 622.

1756 Bspw. könnten APIs auch bei der Geltendmachung des Portabilitätsrechts Standard werden, wenn sektorielle Vorgaben diese verpflichtend vorsehen, siehe dazu Graef/Husovec/Van den Boom, EuCML 2020, 13.

4. Mögliche Handlungsspielräume

a. Extensive Auslegung des Begriffs «bekanntgegeben»

662 Nach dem Gesagten könnte es sich aufdrängen, das Recht auf Datenportabilität innerhalb des DSG extensiver zu verstehen. Möglich wäre, die Einschränkung auf «bekanntgegebene» Personendaten aufzugeben.[1757] Alternativ liesse sich die Bekanntgabe extensiver auslegen. Umfasst sein könnten zudem abgeleitete Daten, um so der wettbewerbs- und konsumentenschutzrechtlichen Zielsetzung, besonders der Verhinderung von Lock-In-Effekten,[1758] Rechnung zu tragen. Dies würde der Betroffenen in datenschutzrechtlicher Hinsicht zudem (noch) mehr Mitspracherecht geben, wofür allerdings aus der vorliegenden Untersuchung kein Bedarf hervorgeht. Dritte, etwa Anbieter von Dienstleistungen, wären in der Lage, einen umfassenden Zugriff auf die Personendaten der Betroffenen zu erhalten und könnten ihre Angebote verbessern. Dies könnte für die Erreichung der wettbewerbsrechtlichen Ziele förderlich sein.

663 Ein sämtliche Personendaten umfassendes Portabilitätsrecht wurde allerdings im Gesetzgebungsprozess durch die Räte verworfen.[1759] Auch die Konkretisierung in Art. 20 Abs. 1 DSV lässt für ein solches weitgehendes Verständnis keinen Raum. Diese Auslegung erschiene überdies in der Sache nicht angemessen: Unweigerlich würden sich Fragen zum Schutz der Geschäftsgeheimnisse und des geistigen Eigentums stellen, da gerade abgeleitete Daten das Ergebnis spezifischer Investitionen und ein zentraler Teil des Innovationswettbewerbs sind.[1760]

b. Engere Orientierung an Normen und Standards

664 Da bereits unter geltendem Recht oft unklar ist, welche Daten im hochtechnischen Mobilitätsbereich vom Portabilitätsrecht erfasst sind, sollten sich die Akteure vermehrt an Normen und Branchenstandards orientieren. Diese las-

1757 Landolt, 189; für das europäische Recht etwa Wendehorst/Schwamberger, DAR 2022, 543; siehe auch Sackmann, 155, nach welchem bei Fahrzeugdaten sämtliche an einen bestimmten Fahrzeugnutzer gebundenen Informationen vom Recht auf Datenportabilität umfasst sein sollen. Massstab soll hierbei sein, ob die Person ohne Zugriff auf die Daten möglicherweise am Umstieg auf ein anderes Fahrzeugmodell von einem anderen Hersteller gehindert werden könnte. Da bei diesem Vorschlag der Personenbezug konkreter Daten keine Rolle mehr spielen kann, ist er abzulehnen.

1758 Sackmann, 155.

1759 Siehe den Vorschlag von Glättli, Votum NR Glättli, AB 2019 N 1814 f.; dazu Rz. 102 ff.

1760 Schweitzer, GRUR 2019, 571.

sen sich bei der Auslegung bereits heute heranziehen. Dabei wirken sich die existierenden sektoriellen Regelungen auf das Datenschutzrecht aus: Sie sind präziser ausgestaltet und können als Leitlinie etwa bei der Bestimmung des Personenbezugs von Mobilitätsdaten dienen.[1761] Zudem ist zu erwarten, dass die spezifischen Zugangsregelungen des Mobilitätssektors mit der Zeit das Verständnis des datenschutzrechtlichen Portabilitätsrechts im Mobilitätssektor prägen werden (*Spill-Over*).[1762] Dies gilt auch für europäische Normen, welche in diesem Zusammenhang ausgearbeitet werden sollen. Aufgeführt wurden etwa die unter der TypgenehmigungsVO vorgesehenen gemeinsamen strukturierten Verfahren und offenen Datenformate. Wenngleich es sich dabei um europäische, für die Schweiz nicht rechtlich bindende Normen handelt, dürften sie sich auf die Schweiz auswirken[1763] und in der Lage sein, die Anwendung des Portabilitätsrechts im Mobilitätssektor zu beeinflussen.

c. Erweiterung des Portabilitätsrechts auf Sachdaten

Die Bedeutung von Sachdaten nimmt zu. Gleichzeitig wird die Abgrenzung zu Personendaten schwieriger. Vor diesem Hintergrund wäre es denkbar, das Portabilitätsrecht auf Sachdaten zu erweitern. Die wettbewerbsrechtliche Ausrichtung des Instituts könnte diese Erweiterung des Portabilitätsrechts an sich rechtfertigen.[1764] Wird die Datenportabilität nicht ausschliesslich persönlichkeitsrechtlich aufgefasst, muss sie auch nicht notwendigerweise auf diejenigen Daten beschränkt sein, die personen- und damit persönlichkeitsbezogen sind. 665

Bislang existiert hierzulande keine Regulierung für Sachdaten, die sich nicht aus anderen Gebieten wie dem Kartell- oder dem Strafrecht herleiten lässt.[1765] Die Einführung eines «Datenrechts» wird in der Schweiz jedoch seit längerem gefordert.[1766] Eine der DV nachgebildete Regelung wäre damit in der Schweiz ebenfalls denkbar, da sich die festgestellten wettbewerbsrechtlichen Zielset- 666

1761 Siehe auch Graef/Husovec/Van den Boom, EuCML 2020, 14.

1762 Graef/Husovec/Van den Boom, EuCML 2020, 14; siehe auch Hübener/Lutz, ZWeR 2024, 133, welche einen Grund dafür, dass Ansprüche in der Praxis auf die TypgenehmigungsVO gestützt werden, darin sehen, dass für diesen Erlass weitgehend Klarheit zu den erfassten Daten, zum Format und zur Art und Weise wie die Daten zur Verfügung gestellt werden müsste, herrsche; dazu bereits Rz. 661.

1763 Dazu bereits die Ausführungen in Fn. 1330.

1764 So für das europäische Recht Wendehorst/Schwamberger, DAR 2022, 543.

1765 Jotterand, sic! 2025, 443; weitergehend IGE, 20.

1766 Baeriswyl, Big Data, 57 f.; Cichocki, Jusletter IT 2015, Rz. 20 ff.; Epiney, Jusletter IT 2015, Rz. 31; insb. für das Gesundheitsrecht Sprecher, ZBJV 2018, Teil 2, 543 f.

zungen für Sachdaten übernehmen lassen. Eine solche Regelung wäre aber nicht innerhalb des DSG möglich, weshalb auf weitere Ausführungen verzichtet wird.[1767]

d. Erweiterung des Portabilitätsrechts auf eine Echtzeitübertragung

667 Ein weiterer Handlungsspielraum ist eine Verpflichtung zur Echtzeitübertragung von Daten. Eine solche sieht das Portabilitätsrecht bislang nicht vor.[1768] Befürworter argumentieren, dass es bereits ein funktionierendes Beispiel für eine solche Echtzeitübertragung im Finanzsektor gebe.[1769] Dabei handelt es sich aber nicht um ein generelles Recht auf Datenportabilität, sondern um ein sektorspezifisches Recht, das auf einen Anwendungsfall massgeschneidert wurde. Entsprechend erfasst es nicht Personendaten, sondern Daten, die für eine Zahlung relevant sind – ungeachtet eines allfälligen Personenbezugs. Weitere Beispiele für solche Verpflichtungen sind die in Art. 7 DMA vorgesehene Interoperabilität für Gatekeeper[1770] oder die Portierung nach der DV, die nur unter bestimmten Umständen erfolgen muss[1771].

668 Würde das Portabilitätsrecht Fahrzeughersteller verpflichten, eine Echtzeitübertragung bereitzustellen, so könnte das deren Wettbewerbsvorteil verringern. Fahrzeughersteller verfügen als Dateninhaber und alte Verantwortliche i.d.R. selbst über einen Echtzeitzugang zu den Daten, während neue Verantwortliche nur periodisch Zugang erlangen können.[1772] Dieses Problem besteht, wie ausgeführt wurde, namentlich im Mobilitätsdatenökosystem, in welchem eine schnelle, periodische Übertragung vielfach elementar ist. Gerade mit der Zunahme von Mobilgeräten könnte eine Echtzeitportabilität weiter an Dringlichkeit gewinnen. Denn mit einer solchen Zunahme geht einher, dass die Geräte zunehmend vernetzt sind[1773] und ein Datenaustausch notwendig wird.

1767 Siehe allerdings noch Rz. 720 ff.

1768 Dazu Rz. 156 und Rz. 212.

1769 Martens/Mueller-Langer, 19. Die PSD2 sieht offene Standards vor, die eine Interoperabilität zwischen verschiedenen Kommunikationslösungen bei der Zahlungsauslösung gewährleisten sollen (Art. 66 f. PSD2; siehe auch Erw.G 93 PSD2). Nur so könnten Zahlungen online in Echtzeit abgewickelt werden, siehe dazu Graef/Husovec/Van den Boom, EuCML 2020, 12.

1770 Dazu Rz. 425.

1771 Dazu Rz. 604 ff.

1772 So auch Graef/Husovec/Purtova, GLJ 2018, 1387.

1773 Drexl, Challenges, 28.

Ein erweitertes Recht auf Datenportabilität könnte bspw. die Verpflichtung vorsehen, die Portierung über eine API anzubieten. Auch die Artikel 29-Datenschutzgruppe hat ein solches Vorgehen vorgeschlagen[1774] und einige Mobilitätsakteure verfügen über Schnittstellen, welche sie bereits im Zuge von Open Data Projekten (für Sachdaten) geöffnet haben.[1775] Mit den im Rahmen der C-ITS-Initiative vorgeschlagenen Lösungen wäre eine solche Zugangsgewährung zumindest technisch wohl nicht ausgeschlossen. Tatsächlich in Echtzeit erfolgte eine solche Übertragung jedoch nicht, da die Daten zuerst hoch- und dann wieder runtergeladen werden müssten, zumindest wenn sich die *data server platform*-Lösung durchsetzen sollte.[1776] Werden Daten in Clouds aufbewahrt, muss zudem eine entsprechende technische Infrastruktur sichergestellt werden.[1777] Dabei sind Dritte einzubeziehen, namentlich Telekommunikationsanbieter, welche die Datenübertragung abwickeln.[1778] Dies wäre etwa über das drahtlose Netzwerk WWAN möglich, das eine Datenübertragung über grössere Reichweiten ermöglicht als WLAN.[1779] 669

Verschiedene Autoren befürworten eine vom Recht auf Datenportabilität ausgehende Echtzeitübertragung. Vereinzelt wurde gar die Möglichkeit vorgebracht, Art. 20 DSGVO so auszulegen, dass die Betroffene ein Recht auf Echtzeitübertragung der Daten hat.[1780] Andere Autoren äussern sich eher einer zusätzlichen Regulierung – gerade im Kontext des vernetzten Autos – gegenüber offen, wobei sie festhalten, dass die konkrete Ausgestaltung weitergehender Forschung bedürfe.[1781] Ein weiterer Autor sieht eine Notwendigkeit für einen Echtzeitzugang bei Maschinendaten, um sicherzustellen, dass zeitliche Verzögerungen das missbräuchliche Verhalten nicht verschärfen.[1782] Angesetzt werden solle dabei aber an der datenschutzrechtlichen Regelung.[1783] 670

Andere Stimmen postulieren hingegen, dass eine Echtzeitübertragung dazu führen könnte, dass Branchen entstünden, die sich nicht mehr mit der Erhe- 671

1774 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 22.

1775 So etwa https://developer.lufthansa.com/; https://data.sncf.com/api; https://developer.jcdecaux.com; https://developer.sbb.ch/; https://opentransportdata.swiss/de/; siehe auch Europäische Kommission, Free Flow, 13.

1776 Kerber/Gill, JIPITEC, 248; McCarthy et al., 48.

1777 Siehe dazu https://perma.cc/7W7P-DZM9.

1778 Bundesministerium für Verkehr und digitale Infrastruktur, 19.

1779 Siehe dazu etwa https://perma.cc/HF5Y-7J5T.

1780 Drexl, Data Access, 12 und 110; Tombal/Graef, 208, dabei gleichwohl auch andere Ansichten betonend.

1781 EY/FIA Region I, 104; Kerber/Gill, 96.

1782 Deuring, 324.

1783 Deuring, 324.

bung von Daten beschäftigten, sondern nur noch Daten von Dritten abgriffen.[1784] Dadurch würden Anbieter, die sich mit der Erhebung von Daten befassten, einen deutlich stärkeren Eingriff in ihre Innovationen und Investitionen erfahren, als dies ohne Echtzeitübertragung der Fall wäre.[1785] Weiter wird vorgebracht, dass eine neue Verantwortliche auch bei einem erweiterten Portabilitätsrecht keine Rohdaten erhielte, sondern gefilterte und aggregierte Daten, wobei der alte Verantwortliche stets im Bild darüber ist, welche Daten er an die konkurrierende neue Verantwortliche überträgt.[1786]

672 Ebenfalls kritisch äusserte sich die Kommission Wettbewerbsrecht 4.0, die sich in ihrem Bericht allerdings vorwiegend mit Plattformen beschäftigte. Ihr zufolge könnte eine entsprechende Verpflichtung kontraproduktiv sein und die Markteintrittskosten für kleinere Anbieter deutlich erhöhen.[1787] Grössere Anbieter könnten hingegen profitieren, wenn Kunden ihre Daten aus selten genutzten Accounts bei kleineren Unternehmen einem grossen Anbieter (bspw. dem Fahrzeughersteller) übertragen.[1788] Sie schlagen daher sowohl sektorielle als auch auf marktbeherrschende Unternehmen beschränkte Anpassungen des Rechts auf Datenportabilität vor, namentlich durch eine Pflicht zur Verwendung «interoperabler» Datenformate und zur Gewährleistung einer Echtzeitübertragung von Daten.[1789] Ein auf diese Weise erweitertes Portabilitätsrecht solle jedoch, ebenso wie die Interoperabilitätsvorgabe, über Art. 20 DSGVO hinausgehen, und liesse sich entsprechend kaum als datenschutzrechtliches Institut ausgestalten.[1790] Freilich wäre je nach konkreter Ausgestaltung einer Echtzeitlösung der Übergang von Portabilität zu einer Interoperabilität fliessend.[1791]

673 Eine weitere Autorin spricht sich demgegenüber für ein neues Portabilitätsrecht aus, das nur den B2B-Bereich abdeckt, da Unternehmen regelmässig auf eine Echtzeitübertragung angewiesen seien.[1792] Während das Recht auf Datenportabilität *de lege lata* wichtige Datenschutzfunktionen erfülle, würden Unternehmen ein Plattformmodell bevorzugen, das den Datenaustausch in Echt-

1784 Fix, 164.
1785 Fix, 164.
1786 Kerber/Gill, JIPITEC, 248. Letzteres ist indes bereits heute bei einer direkten Übertragung an die neue Verantwortliche so.
1787 Schallbruch et al., 41.
1788 Schallbruch et al., 41.
1789 Schallbruch et al., 41.
1790 Schallbruch et al., 55.
1791 Steffen/Wieworra/Kroon, 75.
1792 Janal, 340.

zeit über APIs ermöglicht.[1793] Sie sieht in Art. 20 DSGVO aber keine Vorlage für ein solches Portabilitätsrecht, sondern ist vielmehr der Ansicht, dass die Bestimmung dazu dienen könne, Fehler bei einem B2B-Portabilitätsrecht zu vermeiden.[1794] Sie schliesst daher nicht aus, dass ein sektorspezifischer statt eines *one-size-fits-all*-Ansatzes besser geeignet sein könnte.[1795] Denkbar wäre damit etwa, die Zugriffsrechte der Anbieter von Dienstleistungen unter der TypgenehmigungsVO zu erweitern, um so den mobilen Personen eine Auswahl zu ermöglichen.[1796] Ein darauf gestützter Fernzugriff könnte auch einen Datenzugang in Echtzeit ermöglichen.[1797]

Sowohl die Lehrmeinungen als auch die europäischen Vorgaben lassen darauf schliessen, dass in der Schweiz für den Mobilitätssektor eine Erweiterung des Rechts auf Datenportabilität auf eine Echtzeitübertragung grundsätzlich begrüssenswert wäre. Dies könnte festgestellte Unzulänglichkeiten beheben und wäre mit den oben aufgeführten Zielsetzungen vereinbar. Ein so ausgestaltetes Portabilitätsrecht würde zudem neuartige Angebote begünstigen. Wechselkosten dürften sinken und Lock-In-Effekte sich verringern, wobei zu bedenken ist, dass im Fall einer umfassenden Interoperabilität zwischen Anbietern u.U. gar keine Notwendigkeit mehr für einen Wechsel besteht. Die datenschutzrechtlichen Ziele stehen einer solchen Erweiterung jedenfalls kaum im Weg. Die einschränkenden Voraussetzungen in Art. 28 DSG sind, wie erwähnt, eine Folge der konfligierenden Ziele und aus datenschutzrechtlicher Warte nicht erforderlich und für die Zielerreichung nicht wesentlich.[1798] 674

Ob ein solches Recht jedoch sektorübergreifend einzuführen wäre oder ob sektorspezifische Lösungen für gewisse Bereiche des Mobilitätssektors besser geeignet sind, ist in § 5 zu besprechen. Es lässt sich allerdings bereits festhalten, dass eine sektorübergreifende Verpflichtung zu einer Echtzeitübertragung technisch anspruchsvoll wäre. Bei der Umsetzung wäre zudem zu berücksichtigen, dass der Mobilitätssektor bereits zahlreiche Spezialgesetzgebungen kennt. 675

1793 Janal, 340.
1794 Janal, 341.
1795 Janal, 341 f.; ebenso Kerber, JCLE 2019, 422, der hierbei von einem «broad consensus» ausgeht.
1796 Kerber/Gill, JIPITEC, 253; ähnlich Gill/Metzger, EDPL 2022, 237.
1797 Kerber/Gill, JIPITEC, 253.
1798 Dazu Rz. 267 ff.

5. Erkenntnisse

676 Das Recht auf Datenportabilität schafft im Mobilitätsdatenökosystem die Grundlagen, um die verfolgten datenschutzrechtlichen Ziele erreichen zu können. Allerdings ist sein Anwendungsbereich in diesem Sektor häufig zu eng, was dazu führt, dass die Erreichung der Ziele erschwert wird, weil Betroffene für sie wichtige Daten nicht erhalten können. Eine Erweiterung der erfassten Daten wäre in dieser Hinsicht wünschenswert, aber wohl kaum praktikabel. Stattdessen sollte man – dem Vorbild der sektorspezifischen Regelungen folgend – vermehrt auf einheitliche Standards und Normen zwischen den Akteuren setzen.

677 Vielschichtiger erscheint die Lage in wettbewerbsrechtlicher Hinsicht. Es ist in Frage zu stellen, ob das Recht auf Datenportabilität für die Beziehung zwischen Fahrzeugherstellern und anderen Akteuren in seiner aktuellen Ausgestaltung tatsächlich die Grundlagen für mehr Wettbewerb zu schaffen vermag. Dies liegt daran, dass besonders technische und damit oft nicht personenbezogene Daten relevant sind und für viele Angebote ein Echtzeitzugang benötigt wird. Dem wird das Portabilitätsrecht in unterschiedlicher Hinsicht nicht gerecht, etwa bei den auf eine analoge Welt zugeschnittenen Modalitäten der Portierung, die nur langsam, fragmentarisch und einmalig zu erfolgen hat.

678 Diese Unzulänglichkeiten fangen sektorspezifische Regelungen teilweise auf. Sie sind im Vergleich zur Regelung im DSG detailliert ausgestaltet und damit eher in der Lage, zielgerichtet den Wettbewerb zu fördern. So könnte etwa die TypgenehmigungsVO Lock-In-Effekte und Markteintrittsschranken verringern. Dies gilt jedoch nur eingeschränkt, da sie kaum noch die heute in der Datenwirtschaft relevanten Datenbearbeitungen abdeckt. Die KFZV, die den Zugang zu technischen Informationen ermöglicht, ist diesbezüglich zwar ebenfalls ein erster Schritt in die richtige Richtung. Dennoch bestehen in Abgrenzung zum datenschutzrechtlichen Portabilitätsrecht mehrere Unterschiede im Anwendungsbereich, weshalb einige Handlungsspielräume aufgezeigt wurden.

679 Auf der einen Seite lassen sich mehrere dieser diskutierten Handlungsspielräume nicht oder nicht praktikabel mit dem datenschutzrechtlichen Portabilitätsrecht vereinbaren. Namentlich ist das Portabilitätsrecht innerhalb des Datenschutzrechts nicht auf Sachdaten erweiterbar. Möglicherweise wäre eine solche Erweiterung aber ausserhalb des Datenschutzrechts notwendig. Auf der anderen Seite sind jedoch verschiedene Handlungsspielräume ersichtlich, die im Mobilitätssektor dienlich sein könnten. Im Vordergrund steht eine Erweiterung des Portabilitätsrechts weg von einer Einzelübertragung hin zu re-

gelmässigen, periodischen Übertragungen. Wünschenswert wäre teilweise gar eine Echtzeitübertragung, die aber angesichts der technischen Komplexität sektorspezifisch zu regeln wäre. Auffallend ist schliesslich, dass die DV sämtliche aufgeführten Handlungsspielräume auf die eine oder andere Weise adressiert. Sie geht deutlich weiter als das Portabilitätsrecht unter dem DSG und ist im (europäischen) Mobilitätssektor weitgehend anwendbar, da regelmässig Produktdaten und verbundene Dienstdaten vorliegen. Eine DV für die Schweiz könnte also auf diese Zielsetzungen eingehen, wobei erst vertieft zu untersuchen wäre, welche (wettbewerblichen) Konsequenzen eine solche Regulierung in der Schweiz hätte.

§ 5 Erkenntnisse

I. Einleitung

680 Das Portabilitätsrecht ist in allen untersuchten Datenökosystemen grundsätzlich anwendbar und geeignet, gewisse der festgestellten Ziele herbeizuführen oder zumindest dazu beizutragen, dass die Ziele erreicht werden können. Allerdings sind nicht *alle* Ziele in *sämtlichen* untersuchten Sektoren einschlägig. Zudem sind einzelne Ziele – der sektorübergreifenden Anwendbarkeit zum Trotz – besonders auf das Anwendungsbeispiel soziale Netzwerke zugeschnitten.

681 Nach der Untersuchung in § 4 ist aber anzuzweifeln, ob das Portabilitätsrecht bei sozialen Netzwerken überhaupt zum Erreichen der Ziele beitragen kann. Denn für spezifische Ziele schafft es kaum die Grundlagen. So ist das Portabilitätsrecht nicht geeignet, einen (userinduzierten) Lock-In-Effekt zu verringern. Vielmehr zeigt die sektorielle Untersuchung, dass der Gesetzgeber userinduzierte Lock-In-Effekte bei sozialen Netzwerken verringern wollte, das Institut aber gerade in anderen Sektoren seine volle Wirkung entfalten könnte. Dies, weil dort andere Faktoren als die starken Netzwerkeffekte für einen *Lock-In* verantwortlich sein können. Zudem haben Datensätze in sozialen Netzwerken häufig einen Doppelbezug. Dies kann die Anwendbarkeit des Portabilitätsrechts schmälern, stellt in anderen Sektoren jedoch nicht den Regelfall dar.[1799] Dort, wo das Portabilitätsrecht wirken *sollte*, schafft es somit kaum die Grundlagen, um die Ziele zu erreichen. In anderen Fällen, die der Gesetzgeber weniger bedacht hat, schafft es die Grundlagen hingegen eher.

682 Gleichzeitig weisen die untersuchten Sektoren viele Eigenheiten auf. Sie verfügen über besondere gesetzliche Vorgaben und teils spezifische Portabilitätsrechte. Diese verfolgen oft gleiche, manchmal aber auch andere Ziele als das Recht auf Datenportabilität im DSG, besonders in wettbewerbsrechtlicher Hinsicht. Rechtsvergleichend zeigte sich zudem in der EU ein deutlich weiter fortgeschrittenes Regulierungsnetz. Die EU hat zahlreiche neuartige Portabilitätsrechte oder andere Zugangsregelungen geschaffen, welche teilweise auf eine ähnliche Wirkung wie das datenschutzrechtliche Portabilitätsrecht abzielen. Dies verdeutlicht, dass sektoriell durchaus spezifischer Handlungsbedarf bestand und nach Erlass des datenschutzrechtlichen Portabilitätsrechts weiterhin bestehen kann.

1799 JANAL, 322 f.; zum Doppelbezug Rz. 191 und spezifisch bei sozialen Netzwerken Rz. 435.

Somit ist in einem ersten Schritt zu diskutieren, wann eine sektorübergreifende Lösung angebracht ist. Wie das letzte Kapitel zeigte, wäre ebenfalls denkbar, die sektoriell festgestellten Probleme und Unzulänglichkeiten sektoriell zu lösen und mehrere parallel existierende, sektorielle Lösungen zu schaffen. Nur wenn eine Anpassung sektorübergreifend einen Mehrwert verspricht, lässt sich eine Anpassung von Art. 28 DSG diskutieren.[1800] 683

In einem zweiten Schritt sind die möglichen Handlungsspielräume festzustellen. Sie müssen für das Institut als Ganzes belastbar sein, da die Forschungsfrage darauf abzielt, das (sektorübergreifende) Portabilitätsrecht anzupassen. Aus dem letzten Kapitel ging jedoch nicht hervor, ob sich die jeweils festgestellten Handlungsspielräume auf das Portabilitätsrecht als Ganzes verallgemeinern lassen oder ob diese nur sektoriell tragfähig sind. Da sich sektorielle Lösungen nicht *tel quel* auf andere Sektoren übertragen lassen,[1801] sind sie auch nicht ohne Weiteres auf das Portabilitätsrecht als Ganzes übertragbar.[1802] Folglich müssen aus der vorangehenden Untersuchung Muster und Regelmässigkeiten erkannt werden: Nur was sich in allen untersuchten Sektoren als stichhaltig gezeigt hat, kann möglicherweise auch in anderen Sektoren und damit generell für das Recht auf Datenportabilität gelten.[1803] 684

1800 Siehe dazu auch THOUVENIN/WEBER/FRÜH, 97 f.; Ferner bereits Rz. 26.

1801 Vorwiegend mit den wettbewerbsrechtlichen Zielen vor Augen JANAL, 341 f.; KERBER, 462; mit Blick auf die technische Umsetzung einer Portierung LI, 150.

1802 SCHALLBRUCH et al., 41.

1803 Dazu Rz. 26.

II. Verhältnis zwischen sektorübergreifenden und sektorspezifischen Portabilitätsrechten

A. Vorteile sektorspezifischer Regelungen

685 Da sich nicht sämtliche Ziele in allen untersuchten Sektoren wiederfinden, könnten statt einer sektorübergreifenden Regulierung mehrere sektorielle Regulierungen angezeigt sein. Sie wären weniger dem Vorwurf ausgesetzt, dass es sich bei ihnen nicht um das mildeste Mittel, sondern um «überschiessendes Wettbewerbsrecht»[1804] handle und sie die beabsichtigten Ziele gar nicht erreichen könnten. Dadurch liessen sich sektorielle Besonderheiten besser berücksichtigen. Damit geht die implizite Annahme einher, dass sektorielle Regelungen dem Verhältnismässigkeitsgrundsatz besser Rechnung tragen. In der (vorwiegend wettbewerbsrechtlich geprägten) Literatur zu Datenzugangsrechten werden solche Regelungen denn auch oft als effektiver betrachtet, weil sie spezifischer und zielgerichteter ausgestaltet werden können als sektorübergreifende Portabilitätsrechte.[1805] Mit sektoriellen Datenzugangsregeln lassen sich zudem die unterschiedlichen Interessen der Beteiligten besser auf die wirtschaftlichen und technologischen Umstände eines Sektors zuschneiden, was einen höheren Grad an Akzeptanz innerhalb des Sektors ermöglicht.[1806]

686 Sektorspezifische Regelungen bezwecken allerdings nur einzelne und teils gänzlich andere als die vorliegend untersuchten Zielsetzungen.[1807] Die bisweilen fundamentalen Unterschiede erschweren es, die Regelungen miteinander zu vergleichen. In allgemeiner Weise lässt sich jedoch festhalten, dass eine sektorielle Regelung in gewissen Situationen als zielführender und in anderen Situationen als gar nicht notwendig betrachtet werden kann. In § 4 wurden

---

1804 Zu diesem Begriff siehe bereits die Diskussion in Rz. 314 ff.

1805 Drexl et al., European Data Economy, Rz. 23; Drexl, Data Access, 159; Früh, digma 2019, 175, der sie jedoch nur gegenüber einer Regulierung im Kartellrecht vorzieht; Kerber, 455 ff.; Schweitzer/Welker, 127.

1806 Landolt, 362 m.w.N.; Kerber, 457; ähnlich Kerber/Specht-Riemenschneider, 44 f.

1807 Darauf hinweisend, dass unterschiedliche Datenflüsse, Datenzuordnungen und Akteure die sektorielle Ausgestaltung mitbestimmen Früh/Schibli/Braun Binder, SZW 2023, 79.

denn auch bereits sektorielle Regelungen aufgezeigt und Handlungsspielräume diskutiert, die sich einzig auf sektorielle Regelungen beziehen können – etwa, weil sie sachlich an den betreffenden Sektor anknüpfen.

B. Rechtfertigung der sektorübergreifenden Regelung

Für die Rechtfertigung des sektorübergreifenden Portabilitätsrechts sind die einzelnen Zielsetzungen zu unterscheiden. Es wurde bereits grundlegend festgestellt, dass die Portabilitätsregelung *an sich* aus mehreren Gründen – sowohl hinsichtlich der datenschutzrechtlichen als auch der wettbewerbsrechtlichen Ziele – gerechtfertigt ist.[1808] Auch die Gründe für eine übergreifende Regelung wurden dabei gestreift. Eng damit verbunden ist die Rechtfertigung der sektorübergreifenden Regelung spezifisch in Abgrenzung zu mehreren parallel bestehenden, sektoriellen Portabilitätsrechten. 687

1. Datenschutzrechtliche Rechtfertigung

Das Datenportabilitätsrecht bezweckt zunächst ein datenschutzrechtliches *Empowerment* der Betroffenen. Es ist sogar primär ein datenschutzrechtliches Institut, das *auch* wettbewerbsrechtliche Ziele verfolgt. Dies lässt den weiten, sektorübergreifenden Anwendungsbereich nicht nur zu, sondern erfordert diesen geradezu.[1809] Im Zentrum steht die von einer Datenbearbeitung betroffene Person und deren Möglichkeit zur Datendisposition in der Datenwirtschaft. Angeknüpft wird dabei an Personendaten, wodurch – dem Datenschutzrechts als Querschnittsmaterie entsprechend – nicht nach Sektoren unterschieden wird. Dadurch grenzt sich das Portabilitätsrecht im DSG von sektorspezifischen Portabilitätsrechten ab, die zumeist wettbewerbsrechtlich ausgerichtet sind. 688

2. Wettbewerbsrechtliche Rechtfertigung

Einzelne wettbewerbsrechtliche Ziele sind darauf angelegt, sektorübergreifend zu wirken. So soll das Portabilitätsrecht in allgemeiner Weise den Wettbewerb fördern. Zudem verfolgt es datenpolitische Ziele, indem es einen freien 689

1808 Dazu Rz. 376 ff.

1809 Ähnlich auch WEBER/THOUVENIN, 74, die dabei jedoch eine Unterscheidung der Normadressaten, etwa nach wirtschaftlicher Grösse eines Unternehmens, ablehnen.

Datenfluss bewirkt. Dadurch lässt sich den zunehmend grösser werdenden Datensilos entgegentreten. Es war das Ziel, Daten auch zwischen andersartigen Anbietern und über Sektoren hinweg auszutauschen und so neue, innovative Angebote zu ermöglichen. Diese Ziele waren in allen Sektoren in jeweils unterschiedlicher Ausprägung zu erkennen. Die dafür notwendige Interkonnektivität zwischen den Sektoren lässt sich aber nur sektorübergreifend schaffen, ansonsten sie ihren Zweck nicht erfüllen kann.

690 Für eine sektorübergreifende Regulierung spricht zudem, dass Marktentwicklungen in der Datenwirtschaft kurzlebig und kaum sektorspezifisch antizipierbar sind.[1810] Befürchtet wurde zudem, dass gerade grosse Internetplattformen sektorielle Regelungen einseitig zu ihren Gunsten nützen könnten. Sie könnten so Daten aus einem Sektor erhalten, müssten ihre Datensätze aber umgekehrt nicht herausgeben, weil die sektoriellen Regelungen sie nicht erfassen.[1811] Mit einer sektorübergreifenden Regulierung lässt sich verhindern, dass durch eine einseitige Ausübung eines sektorspezifischen Portabilitätsrechts Asymmetrien entstehen oder verstärkt werden.[1812] Die Datenwirtschaft sollte damit umfassend erfasst werden.[1813] Es ist dem Portabilitätsrecht also inhärent, nicht bloss sektoriell zu wirken. Denkbar wäre zwar, nur an bestimmten Eigenschaften des Verantwortlichen anzuknüpfen, etwa an Schwellenwerten oder Marktanteilen. Dies ist jedoch nicht angezeigt, da entsprechende Verfahren langwierig sind.[1814]

691 Schliesslich kann eine sektorübergreifende Lösung in der sich rasant wandelnden Datenwirtschaft als Vorlage für sektorielle Vorgaben dienen.[1815] Das Portabilitätsrecht setzt den Anstoss und den Rahmen, um (Personen-)Daten in der Datenwirtschaft weiterverwenden zu können. Es legt dabei fest, dass die Betroffenen an der Weiterverwendung beteiligt sein sollen. Das Institut ist ein

1810 Brenner, EuR 2014, 690; Fix, 92, der damit jedoch das Fehlen von Schwellenwerten begründet.

1811 Illustriert am Beispiel der PSD2 etwa OECD, Mapping Initiatives, 13; siehe auch Votum NR Glättli, AB 2019 N 1814; weitergehend hierzu Rz. 102.

1812 Kerber, 453, insb. Fn. 25; weitergehend für den Bankensektor Di Porto/Ghidini, IIC 2020; OECD, Mapping Initiatives, 13; Reimsbach-Kounatze/Molnar, 10.

1813 Siehe auch Weber, Sector-specific Regulation, 260 ff., der in allgemeiner Weise anregt, den relevanten Markt breiter zu fassen entweder als Markt für Onlinewerbung, der dann sämtliche (so erscheinenden) Onlineplattformen abdecken würde oder als Markt für die Aufmerksamkeit der User. Er bezieht sich dabei aber nur auf den Internetmarkt, während das Portabilitätsrecht breiter ist.

1814 Fix, 92; in diese Richtung auch Weber, Sector-specific Regulation, 264. Zudem würde dies die datenschutzrechtliche Perspektive aussen vor lassen. Dazu bereits Rz. 314 ff. und 320 f.

1815 Drexl, Data Access, 159 f.; siehe auch Tombal/Graef, 221.

erster Baustein der sich im Aufbau befindenden Datenstrategie und sollte versuchsweise und zunächst nur für Personendaten auf die genannten Entwicklungen reagieren. In dieser Makrozielsetzung steckt ein Grundsatzentscheid zugunsten eines Mitspracherechts der Betroffenen, der sich nicht auf einzelne Sektoren beschränken lässt.

C. Folgerung

Aus den genannten Gründen rechtfertigt sich ein sektorübergreifendes Portabilitätsrecht nicht nur generell, sondern auch in Abgrenzung zu mehreren sektoriellen Portabilitätsrechten: Das (sektorübergreifende) Portabilitätsrecht ist mehr als die Summe seiner (sektoriellen) Teile, besonders da es die unterschiedlichen Sektoren verbinden und damit eine Interkonnektivität über Sektoren hinweg herstellen kann (siehe Anhang 2). Zugleich schliesst ein sektorübergreifendes Portabilitätsrecht punktuelle sektorielle Regulierungen keineswegs aus.[1816] Vielmehr sollte der Gesetzgeber bei sektoriellen Problemen spezifisch in den Sektoren ansetzen, wenn Handlungsbedarf besteht.[1817] 692

Für die weitere Untersuchung bedeutet dies, dass eine Anpassung des sektorübergreifenden Portabilitätsrechts nur in Frage kommt, wenn der in den einzelnen Sektoren festgestellte Regelungs- bzw. Anpassungsbedarf sektorübergreifend besteht. Ein solcher Bedarf besteht hinsichtlich der datenschutzrechtlichen Ziele und der wettbewerbsrechtlichen Makroziele. Auf sie ist der Fokus möglicher Anpassungen zu legen. 693

Erschwerend kommt hinzu, dass sich gerade die wettbewerbsrechtlichen Ziele und die allfälligen positiven Auswirkungen auf den Wettbewerb in einem Sektor nur sektorspezifisch feststellen und nur schwer sektorübergreifend bestimmen lassen.[1818] Da eine Datenportierung in allen Wirtschafts- und Lebensbereichen möglich ist, ist generell schwer nachzuweisen, ob sie wirkt. Eine Besonderheit dieser *ex ante*-Regulierung ist zudem, dass sich deren Wirkung nicht vorab in der Realität beobachten lässt, sondern im Voraus abgeschätzt werden muss.[1819] Die genaue Wirkung einer Datenportabilitätsregelung ist daher eine empirische Frage, die nicht abstrakt beurteilt werden kann.[1820] 694

1816 So im Kontext möglicher neuartiger, sektorübergreifender Portabilitätsrechte Drexl, Data Access, 164.

1817 Kerber, 462; dazu auch Landolt, 361 ff.; Reimsbach-Kounatze/Molnar, 26.

1818 Von «kontextspezifisch» sprechend Lynskey, European Law Review 2017, 806; Kerber, 464 f.

1819 Haucap/Kruse, 3.

1820 Lynskey, European Law Review 2017, 809; Weber/Thouvenin, 65.

695 Somit lassen sich mögliche Anpassungen des datenschutzrechtlichen Portabilitätsrechts vorliegend nur aus rechtswissenschaftlicher Perspektive beurteilen. Dies beschränkt die Untersuchung auf eine Prüfung der Verhältnismässigkeit der möglichen Handlungsspielräume. Diese stellen – wie bereits das Portabilitätsrecht an sich[1821] – Eingriffe in die Wirtschaftsfreiheit der Verantwortlichen dar, die eine Rechtfertigung benötigen.[1822] Hierbei ist insb. zu berücksichtigen, dass die Geeignetheit bereits dann angenommen werden kann, wenn eine Anpassung in Bezug auf das verfolgte Ziel nicht wirkungslos oder gar kontraproduktiv ist.[1823] Dies dürfte im Fall des «überschiessenden Wettbewerbsrechts» jeweils zutreffen.[1824] Bei der Erforderlichkeit fällt ins Gewicht, dass in datenschutzrechtlicher Hinsicht eine Kontrolle über die eigenen Personendaten angestrebt und nicht einzig eine wettbewerbsrechtliche Zielsetzung verfolgt wird. Eine gewisse Eingriffsintensität ist durch das Mitspracherecht der Betroffenen in datenschutzrechtlicher Hinsicht also gesetzgeberisch gewollt. Doch auch in wettbewerbsrechtlicher Hinsicht zielen die Makroziele aus den oben genannten Gründen bewusst auf einen weiten Anwendungsbereich des Instituts ab. Damit kann es erforderlich sein, das Portabilitätsrecht anzupassen und zu erweitern, wenn sich damit die Grundlagen schaffen lassen, die Ziele (besser) zu erreichen. Erscheint eine bestimmte Anpassung auch zumutbar, ist es verhältnismässig, das Institut anzupassen. Ausgehend davon ist der sektorübergreifende Anpassungsbedarf des Datenportabilitätsrechts zu prüfen.

1821 Dazu Rz. 379 f.
1822 Siehe LANDOLT, 365 f.; WEBER/THOUVENIN, 64.
1823 WEBER/THOUVENIN, 65; ausführlich HOFSTETTER, 143 f.; dazu bereits Rz. 381.
1824 Dazu Rz. 314 ff.

III. Mögliche Handlungsspielräume und deren Grenzen

A. Keine generelle Erweiterung des Anwendungsbereichs erforderlich

Aus datenschutzrechtlicher Perspektive wurde in den einzelnen Sektoren ein Bedarf für eine extensive Auslegung oder eine Erweiterung des Anwendungsbereichs des Portabilitätsrechts sichtbar. So ist im Mobilitätssektor oft umstritten, ob Daten personenbezogen sind. Dadurch sind u.U. für die Betroffene relevante Daten nicht vom Portabilitätsrecht erfasst.[1825] Im Sektor der sozialen Netzwerke sind die portierten Daten für Betroffene vielfach unvollständig und kaum zu mehr als Archivierungszwecken nutzbar, weil die relevanten Daten regelmässig einen Doppelbezug aufweisen.[1826] Auch im Gesundheitswesen zeigten sich unterschiedliche Handlungsspielräume. Die dort bearbeiteten Daten und deren enger Bezug zur Betroffenen erfordern es, auch abgeleitete Daten vom Portabilitätsrecht zu erfassen. Eine weitere Unzulänglichkeit im Gesundheitswesen liegt darin, dass die Daten kantonaler Spitäler regelmässig nicht portabel sind, weil sie nicht dem DSG unterstehen.[1827] 696

Damit gibt es zwar in allen Sektoren Unzulänglichkeiten, welche sich durch ein weitergehendes Verständnis oder eine Erweiterung des Anwendungsbereichs des Portabilitätsrechts beseitigen liessen. Diese jeweils bloss sektoriellen Unzulänglichkeiten gründen jedoch auf keinem gemeinsamen Nenner und wären je nach Sektor auf unterschiedliche Weise zu adressieren. Sie sind damit nicht auf das Portabilitätsrecht als Ganzes verallgemeinerbar. Es lässt sich aus der sektoriellen Betrachtung kein sektorübergreifender Handlungsbedarf in Form einer Erweiterung des Rechtsinstituts ableiten.[1828] Eine generelle Erweiterung des Anwendungsbereichs des Rechts auf Datenportabilität ist somit nicht erforderlich und wäre unverhältnismässig. 697

1825 Dazu Rz. 602 f.

1826 Dazu Rz. 433 ff.

1827 Dazu Rz. 568 ff.

1828 Namentlich ist keine Erfassung von beobachteten Daten zu fordern, weil diese unter dem DSG bereits ausdrücklich erfasst sind. Anders jedoch unter der DSGVO, für welche vielerorts verlangt wird, dass diese ausdrücklich umfasst werden sollen, siehe statt vieler Krämer, JCLE 2021, 293.

B. Präzisierung der technischen Vorgaben

1. Keine umfassende Interoperabilität erforderlich

698 Bei sozialen Netzwerken und im Gesundheitswesen zeigte sich, dass es notwendig sein könnte, das Portabilitätsrecht in Richtung einer Interoperabilität zu entwickeln. Auch im Mobilitätssektor ist eine Modernisierung und dabei besonders die Möglichkeit einer Echtzeitportierung angezeigt. Anpassungsbedarf ergab sich dabei jeweils vorrangig für Portierungen innerhalb des Sektors, was die zahlreichen Diskussionen rund um unterschiedliche sektorielle Datenzugangsregelungen untermauern. Um den Zielen des Portabilitätsrechts, und dabei besonders den wettbewerbsrechtlichen Makrozielen, besser gerecht zu werden, wäre allerdings die Forderung nach einer umfassenden Interoperabilität *zwischen* den Sektoren ebenfalls denkbar.[1829] Dies ist aus den nachfolgenden Gründen aber nicht erforderlich.

699 Die technische Umsetzung einer solchen weitreichenden Lösung über sämtliche datenbasierten Sektoren hinweg wäre in jedem Fall äusserst komplex und die dafür anfallenden Kosten wären mit Blick auf den versprochenen Nutzen wohl unverhältnismässig hoch.[1830] Dies gilt besonders, wenn bereits bestehende Systeme nachträglich interoperabel werden sollen.[1831] Zudem könnten entsprechende Vorgaben Innovation eher verhindern als fördern, da die Entwicklung neuer Angebote ausbliebe, wenn die Interoperabilität gewahrt werden muss, und sich daher ein Standard verfestigt.[1832] Eine solche Erweiterung des Portabilitätsrechts könnte hinsichtlich der anvisierten Ziele also sogar kontraproduktiv sein, da gerade etablierte Unternehmen die Vorgaben

1829 Siehe dazu etwa die Argumente bei Landolt, 398 ff.; für die DSGVO Geminn/Rossnagel, 127 f., die eine deutliche Erweiterung des Portabilitätsrechts fordern und namentlich das Erfordernis eines «interoperablen Formats» in Art. 20 DSGVO aufnehmen möchten; Krämer/Schnurr, JCLE 2022, 307 ff., die eine kontinuierliche Datenportabilität und damit eine Spielart der Interoperabilität fordern; siehe auch Palfrey/Gasser, 89 ff., die grundsätzlich von positiven Effekten auf Wettbewerb und Innovation ausgehen; zum unklaren Begriff der Interoperabilität in diesem Kontext Rz. 113 f.

1830 Kerber/Schweitzer, JIPITEC 2017, 42; OECD, Mapping Initiatives, 21; Van Der Auwermeulen, CLSR 2017, 69.

1831 Kühling/Hildebrandt/Bulowski, K&R 2022, 677.

1832 Kerber/Schweitzer, JIPITEC 2017, 42; Krämer, JCLE 2021, 275; OECD, Mapping Initiatives, 21; Palfrey/Gasser, 106; siehe auch das BKartA, Sektoruntersuchung, 45, das in seiner Sektoruntersuchung zwar grundsätzliche positive Effekte in Bezug auf Innovationsanreize sieht, gerade in digitalen Märkten jedoch keine Innovationsentwicklung sieht, welche feste Regeln folgt und daher auch negative Effekte sieht.

besser umsetzen könnten und der Eintritt in einen neuen Markt dadurch erschwert statt vereinfacht würde.[1833] Kleinere Akteurinnen hätten im Vergleich deutlich höhere Hürden zu überwinden, was Innovation zusätzlich hemmen könnte.[1834] Zudem stellten sich Fragen der Datensicherheit, etwa, ob sich Ende-zu-Ende-Verschlüsselungen (E2EE) beibehalten liessen[1835] oder ob nicht vielmehr das Datenschutzniveau gesamthaft sänke. Auch in Bezug auf Immaterialgüterrechte würden sich neue Fragen stellen.[1836]

2. Minimalvorgaben und Förderung von offenen Standards

Dies bedeutet jedoch nicht, dass keine Anstrengungen in Richtung einer vermehrten Interoperabilität unternommen werden sollten. Eine gewisse Interoperabilität ist durch die Förderung gemeinsamer Standards erreichbar.[1837] In vielen Sektoren existieren bereits heute Industriestandards, die sich durchgesetzt haben und berücksichtigt werden sollten.[1838] Daher muss der Dialog über bestehende Interoperabilitäts- und Portabilitätsstandards weiter gefördert und eine semantische Klärung von Begriffen, stets unter Einbezug der relevanten Akteurinnen, vorgenommen werden.[1839] Auch über das Format der herauszugebenden Daten sollten sich die Akteurinnen verständigen, da ein möglichst standardisiertes Vorgehen wünschenswert ist.[1840] 700

Dabei kommt den Akteurinnen auf dem Markt eine grosse Bedeutung zu, denn letztlich müssen deren Angebote durch ihre Benutzerfreundlichkeit überzeugen: Das Beispiel der Nummernportabilität zeigt, dass sich ein Konzept dann durchsetzt, wenn Betroffene lediglich noch einwilligen müssen und die Ver- 701

1833 OECD, Mapping Initiatives, 21; SCHALLBRUCH et al., 41; SCHWEITZER/WELKER, 127.
1834 SCHWEITZER/WELKER, 127.
1835 BKartA, Sektoruntersuchung, 64.
1836 OECD, Mapping Initiatives, 21.
1837 SCHWEITZER et al., 89.
1838 DULLER, 149; siehe auch HEMPEL/SCHMID, 241 f.
1839 FURMAN et al., 58 f. und 74; GRAEF/HUSOVEC/PURTOVA, GLJ 2018, 1387; in diese Richtung auch International Working Group on Data Protection in Technology, 10; JENTZSCH, 34; Swiss Data Alliance, Whitepaper Datenraum, 25; ein solches Vorgehen dürfte auch auf Zustimmung in den einzelnen Sektoren stossen, siehe Europäische Kommission, Aufbau Datenraum, 11; siehe ferner die Interoperabilitätsplattform des BFS, abrufbar unter: https://perma.cc/LE2N-ZLFR.
1840 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 21; OECD, Data Portability, 45; in Bezug auf soziale Netzwerke NICHOLAS/WEINBERG, 18 f.

antwortlichen sämtliche technischen Einzelheiten übernehmen.[1841] Solche Standards sind damit zunächst in den einzelnen Sektoren zu entwickeln[1842] und daraufhin sektorübergreifend zu erweitern, wenn ein tatsächlicher Bedarf besteht.[1843] Dies trägt dazu bei, Datensilos abzubauen. Die Literatur fordert denn auch jenseits der isolierten Betrachtung des datenschutzrechtlichen Portabilitätsrechts weniger ein proaktives staatliches Eingreifen, sondern eher die Schaffung einer generellen rechtlichen Infrastruktur, die den Akteurinnen ein Experimentieren in geordnetem Rahmen ermöglicht.[1844]

702 Ein solches Experimentieren sollte das Portabilitätsrecht ebenfalls ermöglichen. Im Idealfall könnte sich der Gesetzgeber darauf beschränken, Minimalvorgaben zu machen, etwa in Bezug auf die Offenheit der zu verwendenden Standards und Formate (Open Source) oder eine Orientierung an den FAIR-Prinzipien.[1845] Denkbar wäre zudem, lediglich Basisfunktionen interoperabel machen zu müssen, nicht aber Zusatzfunktionen.[1846] Ferner könnte eine Koordinationsstelle, wie sie im Gesundheitswesen mit der NDKS und dem SwissHDS vorgesehen ist, sektorübergreifend die Entwicklung von Standards erleichtern und damit die Interoperabilität fördern.[1847] In diese Richtung soll die im Januar 2025 in Betrieb genommene «Anlaufstelle Datenökosystem Schweiz» tätig sein. Sie soll u.a. sicherstellen, dass Datenräume interoperabel

1841 Krämer/Senellart/De Streel, 76; ebenfalls «nachdrücklich» eine Zusammenarbeit der unterschiedlichen Akteurinnen empfehlend Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 21.

1842 Cichocki, Jusletter IT 2015, Rz. 51, der der Dynamik von Big Data im Allgemeinen durch Soft-Law-Regelwerke durch Branchenverbänden begegnen will, da diese zwar nicht bindende, aber dafür umso flexiblere Rahmenbedingungen schaffen könnten.

1843 Ähnlich Stiftung Datenschutz, Praktische Umsetzung, 48; kritisch bezüglich der Implementierung von sektorübergreifenden Standards Hempel/Schmid, 240.

1844 Zur Rolle des Staats und privater Akteurinnen Palfrey/Gasser, 161 ff.; siehe auch Schweitzer et al., 116; ausdrücklich auch im Kontext der Datenportabilität Ansätze einer «regulierten Selbstregulierung» fordernd Stiftung Datenschutz, Praktische Umsetzung, 47; siehe auch zur Möglichkeit einer positivrechtlichen «experimentellen Gesetzgebung» für eine beschränkte Zeit Weber/Thouvenin, 67.

1845 Landolt, 401. Nach den FAIR-Prinzipien müssen Daten einfach auffindbar (*Findable*), zugänglich (*Accessible*), interoperabel (*Interoperable*) und wiederverwendbar (*Reusable*) sein, siehe dazu https://perma.cc/NQ2A-UUBP; siehe auch Krämer/Schnurr, JCLE 2022, 309, die sich eine stärkere staatliche Intervention vorstellen können, wenn nach einer bestimmten Zeit noch keine Branchenstandards implementiert werden konnten.

1846 Kühling/Hildebrandt/Bulowski, K&R 2022, 673.

1847 Hempel/Schmid, 242; siehe etwa am Beispiel von *Open Banking* im Vereinigten Königreich Reimsbach-Kounatze/Molnar, 23 f. m.w.N. Dies ist allerdings, wie ebenda eingeräumt wird, sektorübergreifend deutlich schwieriger zu erreichen als im Bankenbereich, in welchem die vorhandenen Daten bereits relativ strukturiert sind.

sind und diese sich in das Schweizer Datenökosystem integrieren.[1848] Verbindliche Vorgaben macht die Anlaufstelle aber nicht. Daneben erscheint es lediglich punktuell erforderlich, dass der Gesetzgeber anknüpfend an wettbewerbliche Parameter konkretere Vorgaben zur Schaffung einer Interoperabilität in bestimmten Bereichen macht. Als Beispiel hierfür sind die besonderen Regelungen in der EU unter dem DMA zu nennen, die die Schweiz aber bislang nicht übernommen hat. Auch die Rechtsprechung kann entsprechende Vorgaben entwickeln.[1849]

Das Ziel ist demnach nicht unbedingt eine maximale sektorübergreifende Interoperabilität, sondern ein optimaler Grad an Interoperabilität, der an konkreten Bedürfnissen ansetzt und Kosten und Nutzen ausgewogen berücksichtigt.[1850] Insgesamt wäre eine solche Entwicklung zu begrüssen, da eine zunehmende Interoperabilität auf der Grundlage von offenen Standards und Formaten besonders ein offenes Web fördern und dazu beitragen würde, Datensilos abzubauen.[1851] Bereits für sich allein genommen werden gemeinsamen Standards innovationsfördernde Effekte zugeschrieben.[1852] Den Netzwerkeffekten und dem Kippen eines Marktes liesse sich – etwa im Bereich der Internetplattformen – mit solchen Entwicklungen ebenfalls entgegentreten.[1853] Allerdings erscheint das Datenschutzrecht ungeeignet, um etwaige Minimalvorgaben zu machen oder zwingende Standards vorzugeben. Die Anpassungen sind datenschutzrechtlich nicht zu rechtfertigen, weshalb es nicht erforderlich erscheint, Art. 28 DSG entsprechend anzupassen. 703

3. Periodizität der Portierung

Betroffene sollten Daten wiederkehrend erhalten und übertragen lassen können.[1854] Aus diesem Grund könnte Art. 28 DSG ein explizites Recht auf eine periodische Datenportierung vorsehen. Bereits aufgezeigt wurde, dass das Por- 704

1848 Bundesrat, Medienmitteilung vom 15. Januar 2025; weitergehend https://perma.cc/PD23-Q3JE.

1849 Eine kartellrechtliche Fortentwicklung in Bezug auf die Herstellung von Interoperabilität und Fragen des Datenzugangs sieht HEINEMANN, ZWeR 2022, 317.

1850 KERBER/SCHWEITZER, JIPITEC 2017, 42; grundlegend auch PALFREY/GASSER, 76.

1851 FURMAN et al., 71; KERBER/SCHWEITZER, JIPITEC 2017, 58.

1852 GAL/RUBINFELD, New York University Law Review 2019, 740; OECD, Mapping Initiatives, 36; LANDOLT, 397 ff., der Argumente für und gegen den Erlass von Vorgaben aufzeigt.

1853 FURMAN et al., 57.

1854 Für ein ähnliches, aber wohl weitergehendes Recht auf «kontinuierliche Datenportabilität» plädierend, welches auch eine Datenübertragung in Echtzeit ermöglichen würde KRÄMER, JCLE 2021, 295 f.; KRÄMER/SENELLART/DE STREEL, 79 ff.

tabilitätsrecht gerade auch auf andersartige Anbieterinnen abzielt und damit komplementären Diensten den Eintritt in den Markt vereinfachen soll. Während ein (substitutiver) Wechsel zwischen zwei gleichartigen Anbieterinnen mit einer einmaligen Geltendmachung des Portabilitätsrechts verwirklicht werden kann, reicht für die komplementäre Nutzung zweier Dienste – ggf. über Sektoren hinweg – eine Einmalübertragung nicht aus.[1855] Nachdem verbindliche Vorgaben für eine umfassende Interoperabilität, wie soeben ausgeführt, abzulehnen sind, könnte eine periodische Datenübertragung als milderes Mittel die parallele Nutzung mehrerer Angebote oder sogar ein *Multi-Homing* ermöglichen.[1856] Denn Angebote eines jeweiligen *Aftermarkets* hängen in vielen Sektoren wesentlich davon ab, ob eine solche Datenübertragung möglich ist.[1857] Dies gilt grundsätzlich unabhängig vom Sektor und gerade auch zwischen den einzelnen Sektoren, weshalb sich eine (generelle) Regelung im DSG aufdrängt. Dazu kommt, dass die Dringlichkeit für eine periodische Übertragung in Zukunft aufgrund der ansteigenden Vernetzung zunehmen dürfte. Dies lässt sich momentan bei den (meist nicht personenbezogenen) Daten des IoT beobachten, wird aber für Personendaten unter dem DSG ebenfalls vermehrt zu diskutieren sein. Dies gilt umso mehr, als mit Big Data in einem Datensatz enthaltene Sachdaten durch die Verknüpfung mit Personendaten zunehmend als personenbezogen gelten können.[1858]

705 Um dies technisch umzusetzen, müssen die Akteure – analog zur Interoperabilität – auf offene Standards und Protokolle und fachkundige private Initiativen in den jeweiligen Sektoren setzen.[1859] Gerade APIs, die eine standardisierte Kommunikation von Softwarekomponenten festlegen, könnten den periodischen Datenfluss erleichtern, indem sie beschreiben, welche Arten von Daten abrufbar sind, wie sie abrufbar sind und in welchem Format sie weitergegeben werden sollen.[1860] Durch solche Standards können marktgerechte und anpassungsfähige Angebote dort entstehen, wo sie sich in der Realität bewähren. Ein

1855 Crémer/De Montjoye/Schweitzer, 81 f.; Duller, 322; Podszun, 99; Schweitzer/Welker, 119; BJ, Erläuternder Bericht DSV, 48, wonach «denkbar» ist, dass der Verantwortliche eine sichere API zur Verfügung stellt. Das BJ will zudem eine unzulässige Behinderung durch den alten Verantwortlichen bereits darin erkennen, dass dieser keine API anbiete.

1856 Krämer/Schnurr, JCLE 2022, 307.

1857 Janal, 340; Schweitzer, GRUR 2019, 574, die indes den «reibungslosen Echtzeitzugang» und eine «volle Interoperabilität» gleichsetzt.

1858 Graef/Husovec/Van den Boom, EuCML 2020, 14; Landolt, 340 f. m.w.N.

1859 Krämer/Schnurr, JCLE 2022, 308; in diese Richtung auch Kranz et al., BISE 2023, 605. Bereits oben wurde für die vorliegend untersuchten Sektoren etwa FHIR, die *Data Transfer Initiative* oder die C-ITS-Initiative vorgestellt.

1860 Schweitzer et al., 89; Gal/Rubinfeld, New York University Law Review 2019, 750.

Beispiel sind sog. *Webhooks*, welche eine sektorübergreifende Portierung ermöglichen.[1861] Dabei wird zumeist eine API so ausgestaltet, dass ein Datentransfer nicht von der Empfängerin initiiert wird («pull-basiert»), sondern von der Senderin («push-basiert»), was eine kontinuierliche Übertragung in Echtzeit ermöglicht.[1862] Des Weiteren könnten Koordinationsstellen besonders zwischen den Sektoren eine vermittelnde Position einnehmen und die Schaffung von entsprechenden Standards fördern. Auf diese Weise könnte die Datensicherheit gebührend berücksichtigt werden.[1863] Zudem wäre dem Grundgedanken des *interconnected information space* weiterhin Rechnung getragen.

Wie bereits zur Interoperabilität aufgeführt, erscheinen unter dem Portabilitätsrecht keine sektorübergreifenden Verpflichtungen zu Echtzeitübertragungen oder Schnittstellenzugriffen (d.h. Datenzugängen) angezeigt.[1864] Nur wenn vertiefte Untersuchungen ergeben, dass weitergehende staatliche Interventionen notwendig sind, sollte der Gesetzgeber bestimmte Standards verpflichtend machen.[1865] Diese müsste er aber in erster Linie dort spezialgesetzlich verankern, wo eine Notwendigkeit spezifisch festgestellt wurde, etwa aufgrund eines Marktversagens.[1866] Denn für Verantwortliche stellen die notwendigen technischen Anpassungen einen schwereren Eingriff in die Wirtschaftsfreiheit dar, welcher sich kaum alleine mit den datenschutzrechtlichen Zielen oder der in dieser Hinsicht zu pauschalen Makrozielsetzung der Innovations- und Wettbewerbsförderung rechtfertigen lässt.[1867] Als milderes Mittel sollte 706

1861 Rajendra-Nicolucci, 53 und *passim*.

1862 Rajendra-Nicolucci, 54; siehe auch die Empfehlung für einen Standard «WebSub», https://perma.cc/CR2F-ZFUA.

1863 OECD, Mapping Initiatives, 30.

1864 Dies u.a. damit begründend, dass eine solche Regelung auch nicht personenbezogene Daten erfassen sollte Duller, 148; a.A. jedoch Deuring, 324; Krämer, JCLE 2021, 296, der ebenfalls auf die zahlreichen Risiken einer Echtzeitportierung aufmerksam macht; Krämer/Schnurr, JCLE 2022, 307 f.; ebenso Krämer/Schnurr/Broughton Micova, 106 ff., die sich dabei auch für nicht personenbezogene Daten eine Echtzeitportierung wünschen.

1865 Mögliche Marktversagen aufzeigend etwa Gal/Rubinfeld, New York University Law Review 2019, 762 ff., die dabei darauf hinweisen, dass gerade die zunehmende Vernetzung des IoT auch vermehrt zu gegenläufigen Interessen der Akteurinnen führen könnte.

1866 Duller, 148; OECD, Data Portability, 24 f.; Schweitzer/Welker, 151. Dadurch könnten auch sektorielle Eigenheiten gebührlich berücksichtigt werden. Wie erwähnt, wäre eine Übertragung in Echtzeit nicht in jedem Sektor gleich zu verstehen, dazu Rz. 360 ff.

1867 Siehe auch Krämer, JCLE 2021, 297, der zwar eine entsprechende Pflicht befürwortet, dann aber einräumt, dass der Grundsatz der Verhältnismässigkeit beachtet werden müsse und durch eine solche Verpflichtung ein höherer Nutzen als die anfallenden Kosten resultieren müsse; ähnlich für eine Interoperabilitätsregelung Kühling/Hildebrandt/Bulowski, K&R 2022, 673.

der Gesetzgeber indes bereits heute ausdrücklich festhalten, dass eine periodische Portierung zulässig ist. Der Bundesrat kann die DSV in diesem Sinn konkretisieren. Dabei sollte er klarstellen, dass wiederholte Portierungsgesuche nicht per se querulatorischer Natur sind.[1868]

C. Auf den modernen Datenverkehr angepasste Modalitäten

707 Mit Blick auf die Umsetzung des Portabilitätsrechts gibt es in allen untersuchten Sektoren vergleichbare Unzulänglichkeiten. Die aktuell festgelegten Modalitäten in der DSV sind unabhängig vom Sektor für die moderne Datenbearbeitungskadenz unbefriedigend und werden den Zielen des Instituts nicht gerecht. Entsprechend wurden in den Sektoren jeweils unterschiedliche Möglichkeiten diskutiert, wie das Portabilitätsrecht angepasst werden könnte.

708 Die einzelnen Handlungsspielräume und möglichen Anpassungen können zwar im Kontext eines Sektors angebracht sein. Sektorübergreifend und generell sind sie indes nicht notwendig, wie das Beispiel der Interoperabilität zeigt. In einer Hinsicht erscheint es jedoch auch sektorübergreifend nötig, das Portabilitätsrecht anzupassen. Dabei ist nicht erforderlich, das Portabilitätsrecht an sich zu erweitern. Vielmehr sollten die Modalitäten der Portierung deutlicher auf die gängigen Praktiken des modernen Datenverkehrs zugeschnitten sein.[1869] Denn nicht nur ein geeignetes (d.h. ein «gängiges, elektronisches») Format, sondern auch die Modalitäten sind bedeutsam, wenn das Portabilitätsrecht tatsächlich ermöglichen soll, dass Daten weiterverwendbar sind. Dies spiegelt das Institut bis anhin nur unzureichend wider. Dass gegenwärtig Daten per Post oder E-Mail herausgegeben oder übertragen werden können, erscheint jedenfalls aus der Zeit gefallen. Die Ziele des Portabilitätsrechts lassen sich durch eine solche Portierung kaum verwirklichen. Der pauschale Verweis auf die Modalitäten des in verschiedener Hinsicht anders gelagerten Auskunftsrechts[1870] in Art. 22 DSV überzeugt nicht.

709 Das Institut sollte daher so ausgestaltet sein, dass es der besonderen Natur des Portabilitätsrechts besser Rechnung trägt. Verantwortliche, die Daten automatisiert bearbeiten, sollten in der Lage sein, Daten medienbruchfrei in elektronischer Form herauszugeben, d.h. zeitnah zumindest einen Download

1868 Dazu grundlegend Rz. 223.
1869 So auch KRÄMER/SCHNURR, JCLE 2022, 308.
1870 Dazu Rz. 346 ff.

anzubieten oder eine anderweitige medienbruchfreie Portierung der Daten zu ermöglichen.[1871] In dieser Hinsicht sind die für das Mobilitätsdatenökosystem gemachten Ausführungen durchaus auf andere Sektoren übertragbar.[1872]

Hinzu kommt, dass Normadressatinnen anderer Portabilitätsregelungen bereits heute oft strengere sektorielle Vorgaben erfüllen müssen, weshalb eine solche Herausgabe unter dem Rechtstitel von Art. 28 DSG ebenfalls kein Problem darstellen sollte.[1873] Ohnehin ist zu erwarten, dass sich die sektoriellen Portabilitätsrechte auf das Verständnis des Datenportabilitätsrechts im DSG auswirken werden (*Spill-Over*).[1874] Gleiches gilt für die unterschiedlichen Portabilitätsrechte in der EU, welche vielfach für Unternehmen in der Schweiz ebenfalls massgeblich und faktisch der Standard sind. 710

Damit erscheint die heute geltende Frist von 30 Tagen zur Portierung ebenfalls nicht sachgerecht und muss überdacht werden.[1875] Mit Blick auf die hohe Kadenz des Datenverkehrs sollte grundsätzlich eine unverzügliche Datenherausgabe oder -übertragung erfolgen müssen, wobei die konkrete Frist von den Umständen beim Verantwortlichen abhängen sollte.[1876] Dies sieht die europäische Regelung heute schon vor.[1877] Auch in diesem Fall ist zu berücksichtigen, dass in einigen Sektoren bereits heute eine Datenherausgabe zwingend innert kürzerer Frist erfolgen muss. Unter den EU-Regelungen sind sogar Echtzeitzugänge, wie gesehen, teils verpflichtend. Damit einher gehen weitere Spill-Over-Effekte, die dazu führen können, dass sich das Verständnis und die Auslegung des datenschutzrechtlichen Portabilitätsrechts verändern und ein Verantwortlicher dem Portierungsgesuch innert deutlich kürzerer Frist als 711

1871 Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 17.

1872 Dazu Rz. 653.

1873 Graef/Husovec/Van den Boom, EuCML 2020, 16.

1874 Graef/Husovec/Van den Boom, EuCML 2020, 16; dazu bereits Rz. 661.

1875 Krämer, JCLE 2021, 295; Krämer/Senellart/De Streel, 79 ff.; zumindest darauf hinweisend, dass die Fristenregelung unter der DSGVO der praktischen Wirksamkeit des Instituts Grenzen ziehen würde Schweitzer, GRUR 2019, 574; a.A. noch Weber/Thouvenin, 81.

1876 Gerade Anbieter in der Datenwirtschaft dürften zumeist in der Lage sein, Anfragen in kürzester Zeit zu bearbeiten, siehe Artikel 29-Datenschutzgruppe, Leitlinien Datenübertragbarkeit, 17. Für das BJ besteht hingegen eine Pflicht, die Daten «binnen vernünftiger Zeit» zur Verfügung zu stellen, siehe BJ, Erläuternder Bericht DSV, 44.

1877 Die englische Sprachfassung spricht indes von «without undue delay», was bereits weniger Dringlichkeit impliziert. Gerade wenn in einem Sektor ein Recht auf Echtzeitübertragung besteht, kann mit einer «unverzüglichen» Herausgabe aber kaum mehr ein Monat gemeint sein, diesbezüglich dürfte sich das Verständnis grundlegend verändern, siehe Graef/Husovec/Van den Boom, EuCML 2020, 14; dazu Rz. 156.

den heute geltenden 30 Tagen entspricht.[1878] Diese Entwicklung kann sich zudem darauf auswirken, was als «unverhältnismässiger Aufwand» i.S.v. Art. 28 Abs. 2 DSG gilt.

712 Die erforderlichen Anpassungen sind allesamt auf Stufe der Verordnung möglich. Diese konkretisiert einerseits den unverhältnismässigen Aufwand (Art. 21 Abs. 3 DSV) und andererseits die Frist und die Modalitäten der Portierung (Art. 22 DSV). Denkbar wären gleichwohl Ausnahmen für Verantwortliche, für welche eine solche Verpflichtung nach wie vor unverhältnismässig wäre und die nicht ohnehin unter die Haushaltsausnahme fallen, etwa Kleinunternehmen.

D. Keine Beschränkung auf spezifische Normadressatinnen

713 Die aktuelle Regelung erfasst mit wenigen Ausnahmen sämtliche Verantwortlichen und ist damit sehr weitgehend anwendbar. Mit Blick auf die datenschutzrechtlichen Ziele und die oben gemachten Ausführungen zur sektorübergreifenden Rechtfertigung, wäre eine Einschränkung des Kreises der Normadressatinnen denn auch kaum geboten.[1879] Denkbar wäre indes, eine asymmetrische Regelung innerhalb des datenschutzrechtlichen Gefüges zu schaffen, die für bestimmte Verantwortliche besondere – weitergehende – Vorgaben vorsähe.[1880] Dies wäre mit den Zielsetzungen des Portabilitätsrechts vereinbar und entspräche dem gesetzgeberischen Ansinnen, besonders die grossen Internetplattformen in die Pflicht zu nehmen. Gleichzeitig würden der Grundsatz der Verhältnismässigkeit und der risikobasierte Ansatz im Datenschutzrecht beachtet, weil nicht jeder Verantwortliche weitergehende Vorkehrungen für eine Portierung treffen müsste.

1878 So geht etwa Duller, 173, davon aus, dass bereits heute eine nicht weiter konkretisierte Anfrage an einen Gatekeeper i.S.d. DMA in jedem Fall als Gesuch nach Art. 6 Abs. 9 DMA und nicht nach Art. 20 DSGVO behandelt werden müsste, da die Voraussetzungen des DMA in unterschiedlicher Hinsicht (Sachdaten, Echtzeitübertragung) weiter gehen.

1879 So auch Weber/Thouvenin, 74, nach welchen eine Differenzierung zumindest einen erheblichen Begründungsaufwand zur Folge hätte; ähnlich Graef, CPI Antitrust Chronicle 2020, 38.

1880 Dies auch ausdrücklich im Gefüge des Datenschutzrechts vorschlagend Kerber/Specht-Riemenschneider, 48 f.; ebenso Graef, CPI Antitrust Chronicle 2020, 38, die aufgrund des risikobasierten Ansatzes entsprechenden Spielraum in der DSGVO sieht.

Anpassungen in diese Richtung wurden bereits bei den sozialen Netzwerken diskutiert.[1881] Eine solche Regelung wäre wohl zu grossen Teilen der im DMA verankerten Portabilitätspflicht nachempfunden und somit zwar sektorübergreifend, aber nur «gatekeeper-spezifisch» anwendbar. Bei einer bloss isolierten Betrachtung wäre der Lösungsansatz mit Blick auf die Forschungsfrage wohl zielführend und damit begrüssenswert. Unter der europäischen Rechtslage wird bisweilen sogar diskutiert, dass Art. 20 DSGVO nunmehr im Einklang mit der neuen DV so auszulegen sei, dass Torwächter nicht als neue Verantwortliche Daten erhalten oder Betroffene zu einer Übertragung auffordern dürften.[1882] Tatsächlich sollte aber für die Schweiz erst ganzheitlich geprüft werden, ob nicht eine umfassendere Übernahme des DMA unter Einbezug der zahlreichen weiteren, hier nicht interessierenden Verpflichtungen für Torwächter (siehe nur schon etwa Art. 6 Abs. 1–13 DMA) in Frage kommt. Auch die Tatsache, dass der DMA Sachdaten ebenfalls erfasst, spricht gegen eine Anpassung im DSG. Eine asymmetrischen Regulierung für Torwächter oder andere bestimmte Personenkreise ist im DSG aktuell nicht angezeigt. Es ist auf die vorherigen Ausführungen zu verweisen.[1883] 714

E. Vermehrter Einsatz von PIMS

PIMS sind als Idee nicht neu und werden seit jeher als möglicher Handlungsspielraum beschrieben. Im Gesundheitswesen und im Mobilitätssektor wurden sie als mögliches Bindeglied zwischen den Akteurinnen diskutiert,[1884] und im Gesundheitsdatenraum ist mit der NDKS eine Datentreuhänderin geplant, welche mit einem PIMS vergleichbar ist. In anderen Datenökosystemen sind ähnliche Entwicklungen möglich. Ferner existieren Initiativen, die auf eine sektorübergreifende Anwendung von PIMS abzielen.[1885] 715

1881 Dazu Rz. 465 ff.

1882 Dies aufbringend, letztlich aber mit Verweis auf den einschlägigen Erw.G 40 DV ablehnend SATTLER, Data Act, 109 f.

1883 Dazu Rz. 419 ff.; in der EU ist eine solche Ausgestaltung nicht ausgeschlossen, siehe Rz. 733.

1884 Siehe für das Gesundheitswesen Rz. 566; zum Mobilitätsbereich und dabei besonders zur *shared data server solution* Rz. 638.

1885 Zu nennen ist etwa das von BERNERS-LEE (siehe Rz. 87 f.) mitgegründete Unternehmen *Inrupt*, das betroffenen Personen ein Datenwallet (sog. *Pods*) basierend auf einem Solid-Protokoll zur Verfügung stellen möchte. Dabei handelt es sich um ein Datenspeicher, in welchem Betroffene individuell über ihre Daten verfügen können. Eine (Dritt-)Anwendung erhält somit nur nach Massgabe der Betroffenen Zugriff auf bestimmte Daten und kann diese nicht mehr eigenständig und getrennt von den Betroffenen in einem Silo verwalten. Dies soll auch eine Interoperabilität ermöglichen, siehe weitergehend https://perma.cc/

716 Nutzen Betroffene vermehrt PIMS, fördert dies die Ziele des Portabilitätsrechts, zumal damit nicht nur datenschutzrechtliche Kernanliegen wie das *consent management*, sondern auch wettbewerbsrechtliche Ziele gebührend Berücksichtigung finden können.[1886] Für komplementäre Dienste gilt dies allerdings nur eingeschränkt, da PIMS bislang, soweit ersichtlich, kein *Multi-Homing* ermöglichen. Falls diese aber auch eine sektorübergreifende Interoperabilität herzustellen vermögen, dürfte sich dies ändern.[1887]

717 Möchten Betroffene hingegen (substitutiv) zwischen Anbieterinnen wechseln, können PIMS nützlich sein. Gerade bei sektorübergreifenden Datenübertragungen tragen PIMS dazu bei, dass Betroffene über die weitere Verwendung von Daten besser informiert sind und die Daten selbstbestimmt kontrollieren können.[1888] Mit der vermehrten Nutzung von PIMS würden auch die Machtasymmetrien zugunsten der Betroffenen ausgeglichen. Ferner sind PIMS in der Lage, sektorübergreifend für die Forschung eine tragende Rolle einzunehmen, da sie als Intermediärinnen Daten in standardisierter Form bereitstellen können.[1889] Dies macht die Daten vieler Betroffener gleichzeitig nutzbar. Die grössten Vorteile von PIMS liegen denn auch darin, Daten aggregieren und selbst bei grossen Datenmengen eine durchwegs hohe Datenqualität – und damit Vergleichbarkeit – garantieren zu können. Dadurch lassen sich namentlich die wettbewerbsrechtlichen Ziele, deren Erreichung oft von mehr als nur einer einzelnen Person abhängt, fördern.[1890]

718 Bislang konnten sich PIMS nicht durchsetzen. Notwendig wäre, dass sie eine kritische Grösse erreichen, bevor eine relevante Wirkung zu erwarten ist («Henne-Ei-Problem»).[1891] Es bestehen allerdings technische Hürden und profitable Geschäftsmodelle sind noch nicht ersichtlich.[1892] Daher wird in der Li-

J469-6EKY sowie Ottenheimer Davi/Schneier Bruce, «The Return to Identity-First Architecture: How the Solid Protocol Restores Digital Agency», Inrupt Blog vom 22. Juli 2025, abrufbar unter: https://perma.cc/E2K6-8FUN.

1886 Krämer, JCLE 2021, 265; Landolt, 404; Schallbruch et al., 43 f.

1887 Am Beispiel des DGA Gatti, EJPLT 2024, 164 f.

1888 Specht-Riemenschneider/Kerber, 27.

1889 Ähnlich Chao et al., CLSR 2025, 9, die hierbei von «collective agents» sprechen und am Vorgehen beim EHDS anknüpfen möchten; zur Problematik von nach unterschiedlichen Standards erhobenen Daten Weber/Thouvenin, 76.

1890 Siehe dazu Chao et al., CLSR 2025, 8 f., die zwischen einer individuellen und einer kollektiven Ebene des Portabilitätsrechts unterscheiden. Letzterer werde in der aktuellen Umsetzung zu wenig Rechnung getragen.

1891 Weber/Thouvenin, 39.

1892 Krämer/Senellart/De Streel, 76; Weber/Thouvenin, 39 ff.

teratur teils eine regulatorische Lösung gefordert.[1893] Es wird ferner vorgeschlagen, dass Verantwortliche dazu verpflichtet sein sollten, mit PIMS zu kooperieren.[1894] Zudem wird in diesem Kontext betont, dass eine zunehmende Standardisierung essenziell ist.[1895] Schliesslich hat die EU mit dem DGA nunmehr einen Rahmen für die Weiterverwendung von Daten öffentlicher Stellen aufgestellt, welcher «Datenvermittlungsdienste» sowie «datenaltruistische Organisationen» und damit PIMS-ähnliche Konstrukte adressiert (siehe Art. 1 DGA). Sie sollen u.a. mithilfe von allgemein verwendeten offenen Standards eine Interoperabilität untereinander gewährleisten (Art. 12 lit. d und i DGA).[1896] Da der Erlass erst seit dem 24. September 2023 wirksam ist, muss sich dessen Effektivität in der Praxis noch zeigen.

719 Die Schweiz schlägt demgegenüber einen anderen Weg ein, denn hierzulande existieren bislang keine verbindlichen, sektorübergreifenden Vorgaben für PIMS. Stattdessen will der Bund mit einem freiwilligen Verhaltenskodex die Datenportabilität fördern.[1897] Dieser enthält verschiedene Empfehlungen für den Betrieb von Datenräumen und richtet sich sowohl an private als auch an staatliche Akteurinnen.[1898] In diesem Zusammenhang soll die neue «Anlaufstelle Datenökosystem Schweiz» als Vermittlerin zwischen beteiligten Akteurinnen auftreten und so eine Funktion übernehmen, die einem PIMS nahekommt.[1899] Dies ermöglicht es, Daten weiterhin sektoriell zu bündeln, aufzubereiten und an eine neue Verantwortliche zu übertragen. So lässt sich das spezifische Fachwissen innerhalb eines Sektors, etwa zur Bereitstellungsform der Daten, optimal nutzen. Damit anerkennt auch der Verhaltenskodex, dass gewisse seiner Empfehlungen nur für einzelne Akteurinnen oder bestimmte Datenräume bzw. Sektoren sinnvoll sein können.[1900] Eine sektorübergreifende, verbindliche Regelung zu PIMS erschiene damit verfrüht, zumal mit dem Recht auf Datenportabilität sektorübergreifend die rechtliche Möglichkeit besteht, an Daten zu gelangen. Die eben geschilderte Initiative, die die Ausübung des Rechts in tatsächlicher Hinsicht begünstigt, erscheint aktuell ausreichend.

1893 So etwa KERBER, 469 f.
1894 SPECHT-RIEMENSCHNEIDER/KERBER, 30.
1895 SPECHT-RIEMENSCHNEIDER/KERBER, 30 f.; ferner CHAO et al., CLSR 2025, 10.
1896 Siehe hierzu GATTI, EJPLT 2024, 164 f.
1897 Siehe Verhaltenskodex Datenräume, 20 und *passim*, der sich auf freiwilliger Basis an private und staatliche Akteurinnen richtet.
1898 Verhaltenskodex Datenräume, 3 f.
1899 Siehe https://perma.cc/PD23-Q3JE; dazu bereits Rz. 702.
1900 Verhaltenskodex Datenräume, 3.

F. Exkurs: Portierung von Sachdaten – eine Datenverordnung für die Schweiz?

720 Daten ohne Personenbezug können nicht vom DSG erfasst sein und unterstehen nicht dem datenschutzrechtlichen Portabilitätsrecht. Solche Sachdaten sind daher mangels Nähe zu einer betroffenen Person nicht von der Untersuchung erfasst. In den stark personenbezogenen Sektoren der sozialen Netzwerke und des Gesundheitswesens war kein Bedarf nach einem Portabilitätsrecht für Sachdaten feststellbar. Ein möglicher Bedarf ist aber aus dem Mobilitätssektor hervorgegangen. Zudem hat das Beispiel der im ganzen IoT anwendbaren DV gezeigt, dass die Möglichkeit zur Portierung von Sachdaten womöglich nicht bloss im Mobilitätssektor diskussionswürdig ist, sondern in zahlreichen anderen datengetriebenen Sektoren ebenfalls notwendig sein könnte. Dies gilt besonders hinsichtlich der wettbewerbsrechtlichen Makroziele, welche nicht notwendigerweise an einen Personenbezug der Daten gekoppelt sein müssen, sondern auch für Sachdaten vorgebracht werden können. Dabei ist mittlerweile wohl unbestritten, dass an der Wertschöpfung von Daten mehrere Personen beteiligt sind – auch bei Daten, die keinen Personenbezug aufweisen.[1901] In der EU hat sich daher die Ansicht durchgesetzt, dass auch bei nicht personenbezogenen Daten, «alle von der digitalen Dividende profitieren» sollten.[1902] Zudem existiert dort mit Art. 16 Abs. 4 DIRL bereits seit längerem eine Handhabe für Konsumentinnen, um bei der Beendigung eines Vertrags nicht personenbezogene Daten wiederzuerlangen. In der Schweiz steht die Diskussion hierzu noch am Anfang.

721 Nicht neu ist allerdings auch hierzulande die Forderung nach einem Portabilitätsrecht für Sachdaten.[1903] Sie dürfte durch den Erlass der DV neuen Schub erhalten. Es gibt gleichwohl Stimmen, welche ein Portabilitätsrecht für Sachdaten ablehnen, weil im Bereich des Austausches von Sachdaten kein Marktversagen vorliege.[1904] Da bei einem Portabilitätsrecht für Sachdaten jeder Bezug zur Persönlichkeit wegfällt, kommen einzig wettbewerbsrechtliche Argumente in Betracht, welche die Schaffung eines solchen Rechts sektorübergreifend rechtfertigen könnten. Ob ein solches Portabilitätsrecht verhältnismässig wäre, müsste ferner unter Berücksichtigung der existierenden Vor-

1901 Europäische Kommission, Aufbau Datenraum, 12; siehe auch JANAL, 324.
1902 Europäische Kommission, Datenstrategie, 1.
1903 Expertengruppe Zukunft, 2 und 107; JOTTERAND, sic! 2025, 454, der sich dabei auf digitale Dienste beschränkt; in diese Richtung auch WEBER/THOUVENIN, ZSR 2018, 58.
1904 IGE, 19.

gaben des Kartellrechts, etwa Art. 7 KG, vertieft untersucht werden.[1905] Damit wäre ein solches sektorübergreifendes Portabilitätsrecht ausserhalb des DSG denkbar.[1906] Diskutiert werden etwa Portabilitätsrechte, die an die Konsumenteneigenschaft anknüpfen, wobei der Personenbezug keine Rolle spielt.[1907]

Teilweise wird schliesslich grundlegend bezweifelt, ob die Unterscheidung zwischen Personen- und Sachdaten im Zeitalter von Big Data und einer drohenden De-Anonymisierung von Daten überhaupt noch sinnvoll sei,[1908] und ob nicht künftig bestimmte allgemeine Handlungspflichten für Daten an sich aufgestellt werden sollten.[1909] Auch diese Diskussion muss die Schweiz noch führen. Der Gesetzgeber wird – ähnlich wie bereits beim Portabilitätsrecht im DSG – eine Grundsatzentscheidung für Sachdaten zu treffen haben. Namentlich muss er die Frage beantworten, wer am Wert von (Sach-)Daten teilhaben soll. Ein Anlass hierfür könnte das bereits erwähnte Rahmengesetz für die Sekundärnutzung von Daten sein.[1910] Ein sektorübergreifendes Portabilitätsrecht als Rahmenregelung könnte jedenfalls nicht nur sektorielle Mikroziele, sondern auch die sektorübergreifenden Makroziele für Sachdaten berücksichtigen. Im Zuge der steigenden Relevanz von Sachdaten könnte für sie ebenfalls ein freier Datenfluss und ein Abbau von Datensilos anvisiert werden.[1911] Dies wäre m.E. mit Blick auf die bislang verfolgte Datenstrategie der Schweiz und ein einheitliches Datenrecht konsequent. Ob eine solche Regelung allerdings in die Vorlage zum Rahmengesetz für die Sekundärnutzung von Daten aufgenommen wird, ist noch offen.[1912] 722

1905 Eine Weiterentwicklung der Fallgruppen von Art. 7 KG durch die Gerichte nicht für ausgeschlossen haltend Weber/Thouvenin, 70.

1906 Ähnlich auch Weber/Thouvenin, 66.

1907 Gill/Kerber, CPI Antitrust Chronicle 2020, 57 f.; Kerber, 467 f.; in diese Richtung auch die Ausgestaltung in der DIRL, dazu bereits Fn. 412.

1908 Landolt, 385 f., der keine Gründe für eine «künstliche Aufspaltung von Datenzugangsfragen» aus Sicht des Wettbewerbs sieht und einen «holistischen Ansatz» vorziehen würde; Weber, Jusletter IT 2013, Rz. 22 ff.

1909 Weber, Rechtliche Perspektive, 26; ebenso Sprecher, ZBJV 2018, Teil 1, 518; für ein allgemeines Datenrecht plädierend Sprecher, ZBJV 2018, Teil 2, 544, welches zwar nicht das Datenschutzrecht ersetzen, jedoch Mindeststandards für jegliche Formen der Datennutzung setzen solle; siehe auch Bitter/Straker, 745 f., die strukturelle Elemente auf einer Zugangsebene (etwa Schnittstellen oder Formate) als Bezugspunkte einer Regulierung sehen; grundlegend auch Graef/Gellert/Husovec, European Law Review 2019, *passim*.

1910 Dazu Rz. 329.

1911 In diese Richtung Jotterand, sic! 2025, 451.

1912 IK-EUDP, 19; von einer im Vergleich zur EU zurückhaltenden Umsetzung ausgehend Jotterand, sic! 2025, 450.

IV. Fazit: Kaum sektorübergreifender Anpassungsbedarf

A. Mit Blick auf die datenschutzrechtlichen Ziele

723 Das Portabilitätsrecht ist bereits heute extensiv ausgestaltet. Es ist in allen untersuchten Sektoren anwendbar, allerdings in unterschiedlichem Ausmass. Entsprechend gibt es nur wenige Einschränkungen des Normadressatenkreises. Solche sind aus datenschutzrechtlicher Perspektive grundsätzlich nicht angezeigt und folglich *de lege ferenda* ebenfalls nicht notwendig.

724 Das Portabilitätsrecht ist auch nicht grundlegend zu erweitern; ein entsprechender Bedarf ist nicht erkennbar. Zwar ergeben sich beim gewählten *one-size-fits-all*-Ansatz in den einzelnen Sektoren stets gewisse Handlungsspielräume. Diese lassen sich jedoch nicht immer auf andere Sektoren übertragen. Das gilt hinsichtlich der datenschutzrechtlichen Ziele allein, aber besonders auch zusammen mit den wettbewerbsrechtlichen Zielen, welche sich noch deutlicher sektoriell unterscheiden und von den Begebenheiten im jeweiligen Sektor abhängen.

B. Mit Blick auf die wettbewerbsrechtlichen Ziele

725 In Bezug auf die wettbewerbsrechtlichen Ziele ist ebenfalls wenig sektorübergreifender Anpassungsbedarf erkennbar. Einige Ziele sind von vornherein einzig auf eine sektorielle Wirkung und dabei konkret auf Internetplattformen zugeschnitten. Das allgemeine Portabilitätsrecht darf aber nicht aufgrund sektorieller Unzulänglichkeiten angepasst werden, da es nicht auf diese Anwendungsfälle begrenzt ist. Allfällige Anpassungen müssten sektorspezifisch erfolgen.

726 Makroziele wie die allgemeine Wettbewerbs- und Innovationsförderung und die datenpolitische Förderung eines freien Datenflusses halten einer sektorübergreifenden Anwendung hingegen stand. Aus der sektoriellen Untersuchung erhellt, dass die in Bezug auf diese Ziele jeweils festgestellten Unzulänglichkeiten unterschiedlich adressiert werden könnten. Zu nennen sind Interoperabilitätsvorgaben, eine Portabilität für Sachdaten, eine Pflicht zur Schnittstellenimplementierung resp. Echtzeitübertragung, der Einbezug von abgeleiteten Daten oder passgenauere Vorgaben für die Durchführung der

Portierung. Diese Anpassungen erforderten aber einen hohen Grad an legislatorischer Präzision, wodurch sie den wettbewerbsrechtlichen Zielen wiederum kaum mehr sektorübergreifend dienlich wären. Zudem wäre deren Erforderlichkeit in vielen Fällen anzuzweifeln. Darüber hinaus würde eine notwendigerweise zielgerichtete Ausgestaltung damit kollidieren, dass das allgemeine Datenschutzrecht technologieneutral und generell anwendbar ist. Die sektoriell festgestellten Unzulänglichkeiten resp. die sich daraus ergebenden Handlungsspielräume sind aber vielfach solche, die sich vollends vom Datenschutzrecht – auch unter der hier vorgeschlagenen modernen Konzeption – entfernen würden. Deshalb würden sich mögliche Lösungen kaum herbeiführen lassen, indem das datenschutzrechtliche Portabilitätsrecht angepasst wird. Beispielhaft zu nennen ist die Portierung von Sachdaten. Sie könnte zwar erforderlich sein, wäre dann allerdings nicht im DSG, sondern getrennt von der datenschutzrechtlichen Zielsetzung in einem anderen Erlass zu verankern.

Mit Blick auf die Makroziele bleiben damit einzig punktuelle Anpassungen des Portabilitätsrechts. Dessen Modalitäten müssen modernisiert werden. Das Institut sollte es ermöglichen, dass Daten auf eine Weise portiert werden, die der heutigen Datenkadenz entspricht. Dazu müssen die Modalitäten in Art. 22 DSV von denjenigen des Auskunftsrechts getrennt und auf das Portabilitätsrecht zugeschnitten werden. Neu sind also präzise Vorgaben für das Portabilitätsrecht zu machen. So sollte der Verantwortliche die Daten elektronisch und medienbruchfrei herausgeben müssen. Dies sollte möglichst zeitnah, jedenfalls aber innert einer kürzeren Frist als den heute vorgesehenen 30 Tagen geschehen. Zudem ist ausdrücklich festzuhalten, dass Daten periodisch portiert werden dürfen. Ein solches *Update* der Modalitäten würde sektorübergreifend wirken und den schnelllebigen Entwicklungen der Datenwirtschaft zumindest ansatzweise gerecht. Dadurch könnte das Portabilitätsrecht den Betroffenen einen wirklichen Nutzen bieten. Gemeinsam mit allfälligen spezifischen, sektoriellen Vorgaben könnte es so künftig als Teil und Rahmen eines neuen holistischen Datenrechts dazu beitragen, dass die unterschiedlichen Ziele erreicht werden können. 727

C. One size (rarely) fits all

Die verschiedenen vom Recht auf Datenportabilität verfolgten Zielsetzungen lassen sich in den unterschiedlichen Anwendungsfällen nicht immer vereinen. Das Institut erscheint je nach konkretem Anwendungsbeispiel und Sektor in einem anderen Blickwinkel und kann nur teilweise die Grundlagen schaffen, um die Ziele zu erreichen. Damit geht einher, dass in den einzelnen Sektoren 728

verschiedene Unzulänglichkeiten und folglich unterschiedliche Handlungsspielräume feststellbar sind. Diese werden mitunter bereits durch sektorielle Regelungen adressiert.

729 Wenngleich sektorielle Regelungen – gerade in wettbewerbsrechtlicher Hinsicht – gewisse Vorteile aufweisen, so lässt sich das Recht auf Datenportabilität in seiner sektorübergreifenden Anwendbarkeit sowohl aus datenschutz- als auch aus wettbewerbsrechtlicher Perspektive rechtfertigen. Es charakterisiert sich *gerade* dadurch, dass es sektorübergreifend anwendbar ist und es ermöglicht, generell Daten über Sektoren hinweg portieren zu können, ohne dass dafür in wettbewerbsrechtlicher (oder datenschutzrechtlicher) Hinsicht ein Anlass bestehen muss. Das Recht auf Datenportabilität erlaubt eine Datenübertragung zwischen unterschiedlichen Akteuren, auch über Sektoren hinweg.[1913]

730 Vor dem Hintergrund potenzieller sektorspezifischer Regelungen wurden die Grenzen möglicher Anpassungen sichtbar: Es lassen sich aus der sektoriellen Betrachtung kaum generelle Anpassungsvorschläge für das Rechtsinstitut ableiten, die für alle angedachten Anwendungsfälle tragfähig sind. Damit ist das charakterisierende Merkmal des Rechts auf Datenportabilität zugleich seine grösste Schwäche, denn meist ist ein sektoriell erkannter Anpassungsbedarf über alle Sektoren hinweg gesehen nicht erforderlich und folglich unverhältnismässig.

731 Diese Erkenntnis ist nicht neu: Es handelt sich um ein «Grunddilemma der Netzregulierung»,[1914] welches sich wohl nicht vollends auflösen lässt. Denn: Sollen Anpassungen die Grundlage dafür schaffen, dass die Ziele besser erreicht werden, müssen sie präzise genug formuliert und in ihrer Ausgestaltung auf ein konkretes Umfeld abgestimmt sein. Erforderlich ist mithin eine hohe Regelungsdichte, die sektorielle Besonderheiten berücksichtigt. Umgekehrt sind generelle Anpassungen und Regelungen mit tiefer Regelungsdichte oft zu unspezifisch, um die Grundlage für eine bessere Zielerreichung zu schaffen.[1915] Das *one-size-fits-all*-Portabilitätsrecht passt daher nur beschränkt auf die

1913 Dazu Rz. 382 ff.

1914 Stiftung Datenschutz, Praktische Umsetzung, 46; ähnlich LANDOLT, 361, insb. Fn. 1644, nach welchem das Recht auf Datenportabilität «stellvertretend für die legislatorische Gratwanderung zwischen zu abstrakten und zu spezifischen Einheitslösungen» steht.

1915 Siehe LANDOLT, 361, der sektorübergreifende Lösungen als «grundkonzeptionell untauglich» sieht, weil diese «aufgrund der heterogenen technischen Rahmenbedingungen auf den verschiedenen Märkten von vornherein nicht in der Lage wären, die technisch-wirtschaftlichen Bedürfnisse der einzelnen Märkte zu bedienen».

durch viele Eigenheiten geprägten Sektoren, in welchen es anwendbar ist. Dies führt dazu, dass sich dessen wettbewerbsrechtliche Ziele nur schwer auf sämtliche Sektoren übertragen lassen. Möglich sind folglich stets nur Anpassungen, die dem kleinsten gemeinsamen Nenner entsprechen, etwa die vorgeschlagene Neuregelung der Modalitäten.[1916] Entsprechend gilt für mögliche Anpassungen, was bereits für das Institut an sich gilt: *one size rarely fits all.*

Insgesamt besteht somit wenig Anpassungsbedarf. Stattdessen sind gezielt sektorspezifische Regelungen zu schaffen, wo solche erforderlich sind. Sie erscheinen vielfach aussichtsreicher, um die Ziele zu erreichen. Einzig hinsichtlich der wettbewerbsrechtlichen Makroziele sind punktuelle Anpassungen nötig, damit das Portabilitätsrecht in der Datenwirtschaft wirksam sein kann. Diese Anpassungen sind über alle Sektoren hinweg umsetzbar. Damit ist der zweite Teil der Forschungsfrage beantwortet. 732

D. Ausblick

In der Schweiz wurde es seit dem Inkrafttreten des DSG still um das Recht auf Datenportabilität. In der EU haben die Diskussionen demgegenüber wieder an Fahrt aufgenommen. Damit sind nicht nur die zahlreichen neu geschaffenen Portabilitätsrechte in den europäischen Digitalerlassen gemeint, die auch in dieser Untersuchung Erwähnung fanden. Vielmehr prüft die EU derzeit, ob grundlegende Änderungen an der DSGVO notwendig sind.[1917] Parallel dazu hat ein Mitglied des EU-Parlaments die Diskussion lanciert, ob zukünftig ein dreistufiger risikobasierter Ansatz für die DSGVO gelten soll.[1918] Dieser würde Verantwortliche basierend auf ihrer Unternehmensgrösse, der Art der Datenverarbeitung und den Auswirkungen ihrer Tätigkeit auf die Privatsphäre 733

1916 Dazu gerade Rz. 727.

1917 Dazu der Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates vom 21. Mai 2025 zur Änderung der Verordnungen (EU) 2016/679, (EU) 2016/1036, (EU) 2016/1037, (EU) 2017/1129, (EU) 2023/1542 und (EU) 2024/573 hinsichtlich der Ausweitung bestimmter für kleine und mittlere Unternehmen verfügbarer Abhilfemaßnahmen auf kleine Midcap-Unternehmen sowie hinsichtlich weiterer Vereinfachungsmaßnahmen, COM(2025) 501 final.

1918 So Voss Axel, LinkedIn-Beitrag vom 5. März 2025, abrufbar unter: https://perma.cc/J22D-UP26. Dieser war als Mitglied des EU-Parlaments und Schattenberichterstatter bei der Ausarbeitung der DSGVO massgeblich involviert. Dazu auch Henning Maximilian, «Wenn Axel Voss und Max Schrems einer Meinung sind», Netzpolitik.org vom 7. März 2025, abrufbar unter: https://perma.cc/9DA7-ZHND.

erfassen.[1919] In diesem Zusammenhang wurde ferner angeregt, «veraltete» Bestimmungen aufzuheben oder zu überarbeiten, wobei das Recht auf Datenportabilität ausdrücklich genannt wurde.[1920]

734 Das Recht auf Datenportabilität kann sein Potenzial heute noch nicht vollends ausschöpfen.[1921] Diese Untersuchung zeigte, dass eine isolierte Betrachtung des Instituts nicht ausreicht, um belastbare Erkenntnisse abzuleiten, zumindest wenn das Recht nicht nur theoretisch existieren, sondern in konkreten Anwendungsfällen einen praktischen Nutzen haben soll. Das Portabilitätsrecht muss sich – in rechtlicher Hinsicht und in seiner technischen Umsetzung – an den real existierenden Bedürfnissen der unterschiedlichen Akteure orientieren und entsprechend ausgestaltet sein. Damit besteht weitergehender Forschungsbedarf nicht nur hinsichtlich spezifischer Datenzugangsrechte in einzelnen Sektoren, sondern auch hinsichtlich der sektorübergreifenden Wirkung der Portabilitätsregelung im DSG. Angesichts der Komplexität, die optimale Regelungsdichte zu treffen, wird sich der Gesetzgeber – in der Schweiz und der EU – mit der Frage auseinandersetzen müssen, in welchem Umfang eine Interkonnektivität über Sektoren hinweg gewünscht ist, wo sektoriell auf die Erreichung der unterschiedlichen Ziele hingewirkt werden soll, und wo es nicht notwendig ist, tätig zu werden. Daneben sind in Bezug auf das Zusammenspiel zwischen dem sektorübergreifenden Portabilitätsrecht und den unterschiedlichen sektorspezifischen Vorgaben zahlreiche Fragen offen. Um sie zu beantworten, ist weitere Forschung notwendig, auch solche, die interdisziplinäre Ansätze berücksichtigt. Mit dem Recht auf Datenportabilität in Art. 28 DSG ist aber der Anfang für eine zukunftsweisende Datenpolitik in der Schweiz gemacht. Weitere Schritte müssen folgen.

1919 Voss Axel, LinkedIn-Beitrag vom 5. März 2025, abrufbar unter: https://perma.cc/J22D-UP26.

1920 So wörtlich: «Key Changes: While keeping most of the existing GDPR rules applicable, the reform removes or revises outdated provisions (i.e. data portability requirements).», Voss Axel, LinkedIn-Beitrag vom 5. März 2025, abrufbar unter: https://perma.cc/J22D-UP26.

1921 So für die DSGVO-Regelung anlässlich einer ersten Evaluation Europäische Kommission, Zwei Jahre DSGVO, 10; ebenso Jotterand, sic! 2025, 443.

Zusammenfassung der Erkenntnisse

Die Erkenntnisse dieser Untersuchung sind jeweils am Ende eines (Unter-)Kapitels festgehalten. Zur besseren Übersichtlichkeit werden sie nachfolgend erneut zusammengefasst, wobei weiterführend auf die vorangehenden Teile sowie das Zwischenfazit und das Fazit verwiesen wird. 735

Der erste Teil der Untersuchung (§§ 1–3) befasst sich mit der Zielsetzung des Rechts auf Datenportabilität. Die Schweiz übernahm das Institut aus der DSGVO und verankerte es in Art. 28 des revidierten DSG. Nach Ansicht der Räte sollte es neue Wirtschaftsräume eröffnen und die Machtbalance zwischen kleinen und grossen Plattformen ausgleichen. Zudem sahen sie einen Mehrwert für Bürgerinnen, wenn diese Zugriff auf ihre Daten haben und diese für weitere Anwendungen nutzbar sind. Ein weiteres, womöglich entscheidendes Argument für die Räte war die Notwendigkeit eines Angemessenheitsbeschlusses durch die EU-Kommission. Sie setzten sich damit gegenüber dem Bundesrat durch, der zwar die Einführung sektorspezifischer Portabilitätsrechte prüfen, im DSG aber kein übergreifendes Portabilitätsrecht verankern wollte. Er vertrat, dass ein solches Institut wettbewerbsrechtliche Ziele verfolge, hohe Implementierungskosten verursache und ohnehin nur schwierig umzusetzen sei.[1922] 736

Die nunmehr gewählte Regelung in Art. 28 DSG entspricht vom Wortlaut her weitgehend derjenigen der DSGVO, wobei punktuelle Unterschiede in der Ausgestaltung existieren.[1923] Auch in systematischer Hinsicht sind die Institute grundsätzlich deckungsgleich: Sie sind beide im Datenschutzrecht verankert und als datenschutzrechtliche Betroffenenrechte ausgestaltet. Dabei handelt es sich zwar um eine gesetzgeberische Entscheidung, die auch anders hätte erfolgen können. Sie führt jedoch dazu, dass das Institut – zumindest bei rein systematischer Betrachtung – datenschutzrechtlich auszulegen ist, zumal das Portabilitätsrecht einzig Personendaten erfasst. Dies legt einen Konnex zur Persönlichkeit der Betroffenen und ihrer «informationellen Selbstbestimmung» zumindest nahe.[1924] 737

Aus der teleologischen Auslegung gehen demgegenüber sowohl datenschutz- als auch wettbewerbsrechtliche Ziele hervor. Die datenschutzrechtlichen Ziele er- 738

[1922] Dazu Rz. 226 ff. und ausführlich Rz. 97 ff.
[1923] Dazu Rz. 231 ff. und ausführlich Rz. 173 ff.
[1924] Dazu Rz. 382 und ausführlich Rz. 241 ff.

geben sich aus den durch die technologischen Entwicklungen und damit einhergehenden enormen Umwälzungen entstandenen neuen Schutzbedürfnissen der von Datenbearbeitungen betroffenen Personen. Solche Schutzbedürfnisse entstanden als Folge von Ungleichgewichten zwischen den Akteurinnen in der Datenwirtschaft, etwa durch Wissens- und Informationsungleichgewichte. Diese schränken Betroffene in ihrer Autonomie ein und hindern sie daran, selbstbestimmt am gesellschaftlichen Diskurs teilzuhaben. Dieser Entwicklung soll das Datenportabilitätsrecht entgegentreten. Daher zielt das Institut auf den Schutz der Persönlichkeit der von einer Datenbearbeitung betroffenen Person, indem es ihr die Möglichkeit zur selbstbestimmten Datendisposition vermittelt. Die Betroffene soll autonom entscheiden, ob sie ihre Daten selbst verwalten oder weitergeben möchte. Dafür benötigt sie angesichts der Ungleichgewichte ein rechtliches Mittel. Dies erklärt einerseits, weshalb das Portabilitätsrecht für Personendaten generell anwendbar ist. Andererseits verdeutlicht es, weshalb gewisse Einschränkungen auf automatisierte Datenbearbeitungen und freiwillig bekanntgegebene Daten vorgesehen sind: Das Portabilitätsrecht ist darauf angelegt, für Personendaten in der *ganzen* Datenwirtschaft anwendbar zu sein.[1925]

739 Diese datenschutzrechtliche Zielsetzung lässt sich zwar auf die bisherige, «klassische» Konzeption des verfassungsrechtlichen Datenschutzes und namentlich das sog. Recht auf informationelle Selbstbestimmung stützen. Dieses vom BVerfG entwickelte Grundrecht wurde in der Schweiz durch das BGer umfassend übernommen. Nicht übernommen hat das BGer bislang allerdings eine durch das BVerfG in seiner Entscheidung *Recht auf Vergessen I* vorgenommene Relativierung des Grundrechts. Demnach enthält das Grundrecht kein «allgemeines oder gar umfassendes Selbstbestimmungsrecht über die Nutzung der eigenen Daten».[1926] Der bereits ohne diese Relativierung weitgehend unklare Gehalt des informationellen Selbstbestimmungsrechts in der Schweiz hat sich durch diese Entscheidung noch weiter akzentuiert. Folglich finden sich in der Literatur zunehmend kritische Stimmen, die eine fundamentale Neuausrichtung des Konzepts fordern.[1927]

740 Es ist daher angezeigt, die Etablierung einer Datenwirtschaft nicht nur in das Verständnis des Portabilitätsrechts einfliessen zu lassen, sondern diese Entwicklung auch als Anlass zu nehmen, das Verständnis des verfassungsrechtlichen Datenschutzes an die jüngsten Umwälzungen anzupassen. Die veränderten Schutzbedürfnisse führen dazu, dass der verfassungsrechtliche Datenschutz nicht

1925 Dazu Rz. 382 und ausführlich Rz. 258 ff.
1926 BVerfGE 152, 152, 87. Dazu ausführlich Rz. 60 ff.
1927 Dazu Rz. 73 ff.

mehr einzig abwehrrechtlich verstanden werden kann. Angeregt wird daher, den grundrechtlichen Schutz nicht mehr als blossen Schutz der Betroffenen *vor* Datenbearbeitungen zu verstehen. Vielmehr ist der Schutz auch auf eine positive Seite der Persönlichkeit der Betroffenen auszurichten, denn Daten stellen längst eine Ware und auch eine Währung dar. Die Betroffene soll aktiv über die Verwendung ihrer Daten mitbestimmen und von ihnen profitieren können. Entsprechend wird vertreten, dass der Gesetzgeber mit dem Recht auf Datenportabilität einen Aspekt des verfassungsrechtlichen Datenschutzes in einem neuen Verständnis auch unter Privaten verwirklicht hat, wenn er der Betroffenen in gewissen Konstellationen ein an die Datenwirtschaft angepasstes Mitspracherecht gibt. Das Verständnis des verfassungsmässigen Datenschutzes wurde mithin modernisiert – eine Entwicklung, die in der Literatur als «dogmatische Neuausrichtung» oder «Paradigmenwechsel» bezeichnet wird.[1928]

741 Das Recht auf Datenportabilität verfolgt auch wettbewerbsrechtliche Ziele. Betroffene Personen, zumeist Konsumentinnen, sollen mit dem Institut zu einer anderen Anbieterin wechseln können. Dies soll Wechselkosten senken, Lock-In-Effekte verhindern und Konkurrentinnen den Markteintritt ermöglichen. Diese «Mikroziele» sind offenkundig auf Internetplattformen und besonders die sozialen Netzwerke zugeschnitten. Auch der Gesetzgeber hatte besonders diese Ziele vor Augen. Allerdings dürften in diesen Fällen eher Netzwerkeffekte dafür verantwortlich sein, dass eine Person nicht die Anbieterin wechselt. Die Möglichkeit, Daten portieren zu können, beeinflusst einen *Lock-In* nur in geringem Umfang, da das Institut solchen Netzwerkeffekten kaum entgegentreten kann.[1929]

742 Da das Recht auf Datenportabilität jedoch nicht auf Internetplattformen beschränkt ist und sektorübergreifend gilt, ist es in seiner wettbewerbsrechtlichen Dimension breiter zu verstehen. Es stellt keine blosse *lex social media* dar, sondern dient über die Internetplattformen hinaus weiteren «Makrozielen», namentlich soll es allgemein den Wettbewerb sowie Innovation und freie Datenflüsse im Besonderen fördern. Das Institut ermöglicht damit nicht nur einen Wechsel zwischen Konkurrentinnen. Als Ausfluss der allgemeinen Wettbewerbsförderung soll es ausserdem ermöglichen, zu komplementären Angeboten anderer Anbieterinnen zu wechseln. Diese Ansicht stützt die historische Betrachtungsweise, wonach die Ursprünge des Portabilitätsgedankens in der Förderung von Offenheit und Interkonnektivität im Internet, besonders im *Open Web*, liegen. Dem Recht auf Datenportabilität liegt die Idee zugrunde,

[1928] Dazu Rz. 383 und ausführlich Rz. 270 ff.
[1929] Dazu Rz. 386 und ausführlich Rz. 294 ff.

dass der freie Austausch von Daten wesentlich dazu beigetragen hat, dass überhaupt neuartige innovative Angebote wie die sozialen Netzwerke entstehen konnten. Das Internet als *interconnected information space* soll damit bewahrt und der Freiraum, in dem solche innovative Angebote geschaffen werden, erhalten bleiben. Dabei wird im Ergebnis auf die sozialen Netzwerke und heute dominanten Internetplattformen abgezielt, aber nur, weil sie diejenigen Akteurinnen sind, die diese Makroziele gegenwärtig am deutlichsten gefährden.[1930]

743 Beim Recht auf Datenportabilität handelt es sich damit um eine grundlegende Neuausrichtung hinsichtlich der Partizipation an der Datenwirtschaft. Das Institut setzt den Rahmen und die Leitplanken für die Datenverwendung in der Datenwirtschaft. Darin ist für die Schweiz das vorläufige Fazit der Diskussion um die Rechte an und den Umgang mit Daten, namentlich ein mögliches «Dateneigentum», zu sehen. Das Recht auf Datenportabilität ist in seiner Zielsetzung somit nicht nur datenschutzrechtlich, sondern in einem grösseren Kontext als ein Teil der Schweizer Digitalstrategie zu würdigen: Datensilos sollen *generell* ab- und Datenzugänge vermehrt aufgebaut werden. Damit legt das Portabilitätsrecht im Sinn eines Grundsatzentscheids fest, dass der von einer Datenbearbeitung betroffenen Person ein Mitspracherecht verbleiben und sie zukünftig im Zentrum stehen soll. Zu diesem Zweck muss ein übergeordnetes und übergreifendes Institut existieren, das sich nicht auf einzelne Sektoren beschränkt. Gleichzeitig existieren punktuelle Einschränkungen, die den Anwendungsbereich auf zumindest potenziell wettbewerbsrechtlich relevante Anwendungsfälle in der Datenwirtschaft begrenzen, da nur dort entsprechende Vorgaben angezeigt sind.[1931]

744 Folglich ist das Recht auf Datenportabilität ein datenschutzrechtliches Instrument, das *auch* wettbewerbsfördernd wirken soll. Die beiden unterschiedlichen Ziele widersprechen sich nicht, sondern sind zwei Facetten eines sich neu in der Schweiz bildenden Datenrechts. Das Recht auf Datenportabilität ist mehr als die Summe seiner Teile, wenn diese aus zahlreichen sektoriellen Regelungen bestünden. Dies bedeutet im Übrigen, dass weitere Entwicklungen und andere Portabilitätsrechte absehbar sind, gerade in einzelnen Sektoren und mit Blick auf Entwicklungen in der EU.[1932]

745 Der zweite Teil der Untersuchung (§§ 4 und 5) befasst sich mit der Frage, welche Eigenschaften das Datenportabilitätsrecht umfassen sollte, um die er-

1930 Dazu Rz. 387 ff. und ausführlich Rz. 86 ff. und 314 ff.
1931 Dazu Rz. 314 ff.
1932 Dazu Rz. 388 ff.

kannten Ziele (besser) erreichen und allfällige bestehende Probleme und Unzulänglichkeiten lösen zu können. Aufgrund des breiten Anwendungsbereichs des Portabilitätsrechts wurde ein induktiver Ansatz verfolgt. Auf diese Weise wurden die Problembereiche dreier Sektoren dargestellt – der sozialen Netzwerke, des Gesundheitswesens und der Mobilität.[1933] Daraus liess sich erkennen, ob in den Anwendungsfällen die Grundlagen, um die Ziele zu erreichen, aktuell vorliegen und welche Anpassungen ggf. notwendig sind.

Das Recht auf Datenportabilität schafft die Grundlagen, um den datenschutzrechtlichen Zielen im Bereich der sozialen Netzwerke gerecht zu werden. Dabei muss man allerdings die vom Institut beabsichtigte Autonomie und Möglichkeit zur Datendisposition so verstehen, dass die Betroffene ihre Daten (lediglich) archivieren kann. Sobald der Doppelbezug von Daten und die «soziale» Komponente sozialer Netzwerke berücksichtigt werden, zeigen sich erhebliche Unzulänglichkeiten. Denn portierte Daten verlieren für Betroffene oft an Wert, da sie sich in den sozialen Netzwerken kaum sinnvoll aus ihrem Kontext herauslösen lassen.[1934] Dies wirkt sich auf die wettbewerbsrechtlichen Ziele aus. Diesbezüglich ist davon auszugehen, dass die Grundlagen nicht geschaffen werden, um einen *Lock-In* bei einem Wechsel zwischen sozialen Netzwerken zu verhindern. Dies liegt an den Netzwerkeffekten, die in diesem Sektor besonders wirken, aber vom Institut nicht spezifisch adressiert werden. Anders ist dies bei Akteurinnen, die nicht konkurrieren. Möchten Betroffene komplementäre Angebote nutzen, sind es kaum Netzwerkeffekte, die sie daran hindern zu wechseln. Zudem könnten in diesen Fällen kleinere Anbieterinnen von den Datensätzen profitieren, und dadurch in einen Markt eintreten. Damit tritt das Ziel der allgemeinen Wettbewerbs- und Innovationsförderung in den Vordergrund: Das Portabilitätsrecht baut Hürden für neue und innovative Angebote ab.[1935] 746

Im Sektor der sozialen Netzwerke könnte ein Echtzeitzugang zu Daten und in einem nächsten Schritt eine umfassende Interoperabilität notwendig sein, um die Ziele erreichen zu können. Hierfür wären allerdings spezifische Portabilitätsrechte gegenüber bestimmten Betreiberinnen zu bevorzugen. Ein solches Vorgehen hat der Unionsgesetzgeber denn auch mit dem DMA gewählt. In der Schweiz ist bislang jedoch nicht geplant, diese Regelung zu übernehmen.[1936] 747

1933 Dazu ausführlich Rz. 392 ff.
1934 Dazu Rz. 476 f. und ausführlich Rz. 433 ff.
1935 Dazu Rz. 478 f. und ausführlich Rz. 438 ff.
1936 Dazu Rz. 482 ff. und ausführlich Rz. 456 ff.

748 Auch im Gesundheitswesen ist das Recht auf Datenportabilität anwendbar und kann die Grundlage dafür schaffen, dass einige der anvisierten Ziele erreicht werden. Allerdings ist die Ausgangslage im Gesundheitswesen grundlegend anders: Die Gesundheit der Betroffenen steht im Vordergrund und eine weitgehende Übertragung der oft intimen Daten ist nur selten gewünscht. Dennoch lässt sich in datenschutzrechtlicher Hinsicht ein *Empowerment* der Betroffenen bewirken, weil diese über ihre Gesundheitsdaten verfügen kann. Dies gilt besonders, da sich Patientinnen heute mehr für ihren eigenen Gesundheitszustand interessieren und darum an aussagekräftigen Daten interessiert sind, die sie privat nutzen und verwerten können. Für den Gesundheitsbereich gilt jedoch einschränkend, dass das DSG nicht immer anwendbar ist: Öffentliche Spitäler fallen nicht unter das DSG, sondern unter die kantonale Datenschutzgesetzgebung, weshalb ihnen gegenüber kein Recht auf Datenportabilität besteht. Gleiches gilt etwa bei kantonalen Universitäten oder Fachhochschulen für die (medizinische) Forschung.[1937]

749 In wettbewerbsrechtlicher Hinsicht besteht im Gesundheitswesen ein «regulierter Wettbewerb». Da ein weitgehend freier Datenfluss nicht zwingend gewünscht ist, werden *walled gardens* in diesem Sektor oftmals begrüsst. Gleichzeitig lässt sich beobachten, wie Technologieunternehmen mit neuartigen Gesundheitsanwendungen in den nicht regulierten Bereich des Gesundheitswesens eintreten.[1938]

750 Im Gesundheitswesen gibt es vielfältige Handlungsspielräume. Mögliche Anpassungen sind spezifisch auf die dort vorherrschenden, besonderen Interessen ausgerichtet. So wäre mit Blick auf die Ziele wünschenswert, dass das Portabilitätsrecht auch kantonale Organe wie Spitäler oder Universitäten erfasst. Weiter sollte das Portabilitätsrecht auf abgeleitete Daten erweitert werden. Dies erscheint angesichts der besonderen Interessenlage im Gesundheitswesen notwendig, da Patientinnen nur so umfassend an die für sie relevanten Daten (wie bspw. Diagnosedaten) gelangen können.[1939] Schliesslich könnte auch das Gesundheitswesen in Richtung einer umfassenden Interoperabilität angepasst werden.[1940] Da allerdings viele dieser Handlungsspielräume bereits von spezialgesetzlichen Vorgaben wie dem EPD bzw. dem EGDG oder dem zukünf-

1937 Dazu Rz. 576 f. und ausführlich Rz. 552 ff.
1938 Dazu Rz. 578 und ausführlich Rz. 560 ff.
1939 Dazu Rz. 579 und ausführlich Rz. 570 f.
1940 Dazu Rz. 579 und ausführlich Rz. 572 ff.

tigen Gesundheitsdatenraum abgedeckt sein dürften, ist fraglich, inwiefern solche Anpassungen tatsächlich notwendig sind.[1941]

751 Im dritten untersuchten Bereich, dem Mobilitätssektor, kommt das Portabilitätsrecht ebenfalls zwischen unterschiedlichen Akteurinnen zur Anwendung. Zudem existieren dort bereits mehrere sektorielle Vorgaben für einen Datenzugang. Die datenschutzrechtlichen Ziele haben in diesem Sektor nur eine untergeordnete Bedeutung. Wichtiger erscheinen die wettbewerbsrechtlichen Ziele. So können etwa Fahrzeuge heute ohne Datenzugang kaum noch repariert oder gewartet werden. Mobile Personen sind deshalb an offizielle Händlerinnen gebunden, wenn die Anbieterin ihrer Wahl nicht auf die notwendigen Daten zugreifen kann. Dadurch entstehen mehrere Unzulänglichkeiten, welche sich aber teilweise mit den sektorspezifischen Regelungen auffangen lassen.[1942] Diese sind im Vergleich zur Regelung im DSG detailliert ausgestaltet und damit eher fähig, zielgerichtet den Wettbewerb zu fördern. Die in das Schweizer Recht übernommene TypgenehmigungsVO verpflichtet etwa Fahrzeugherstellerinnen, verschiedene Informationen bereitzustellen, was Lock-In-Effekte und Markteintrittsschranken verringern kann. Dies gilt heute jedoch nur noch eingeschränkt, da der genannte Erlass die relevanten Datenbearbeitungen kaum mehr abdeckt. In der Schweiz ermöglicht ausserdem die KFZV den Zugang zu technischen Informationen.

752 Gleichwohl bestehen mehrere Unterschiede zum datenschutzrechtlichen Portabilitätsrecht, weshalb einige Handlungsspielräume aufgezeigt wurden.[1943] Aus diesen ergibt sich, dass verschiedene Anpassungen datenschutzrechtlich nicht umsetzbar sind, etwa das Portabilitätsrecht auf Sachdaten zu erweitern. Dennoch könnte es notwendig sein, ein Portabilitätsrecht ausserhalb des Datenschutzrechts vorzusehen. Weitere Handlungsspielräume sind die Erweiterung des Portabilitätsrechts weg von einer Einzelübertragung hin zu regelmässigen, periodischen Übertragungen oder sogar eine Pflicht zur Echtzeitübertragung. Letztere wäre aber angesichts der technischen Komplexität eher sektorspezifisch zu regeln. Auffallend ist schliesslich, dass die europäische DV sämtliche Handlungsspielräume im Mobilitätssektor auf die eine oder andere Weise zu adressieren scheint. Sie sieht ebenfalls Portabilitätsverpflichtungen vor und geht dabei deutlich weiter als das Portabilitätsrecht unter dem DSG. Da ein solcher

1941 Dazu Rz. 563 f.
1942 Dazu Rz. 678 und ausführlich Rz. 626 ff. und 648 ff.
1943 Dazu Rz. 678 und ausführlich Rz. 640 ff.

Erlass dazu beitragen kann, die diskutierten Ziele zu erreichen, könnte sich eine entsprechende Regelung auch in der Schweiz aufdrängen.[1944]

753 Wie die Untersuchung der Sektoren zeigt, ist das Portabilitätsrecht zwar in allen Sektoren grundsätzlich anwendbar und kann dort dazu beitragen, dass die Ziele erreicht werden. Allerdings sind nicht *alle* Ziele in *sämtlichen* Sektoren einschlägig. Vielmehr sind mehrere Ziele besonders auf das Anwendungsbeispiel der sozialen Netzwerke zugeschnitten. Auch darum lassen sich die sektoriellen Erkenntnisse nicht *tel quel* auf das Portabilitätsrecht als Ganzes übertragen. Es müssen daher Muster und Regelmässigkeiten erkannt werden, die nicht nur sektorspezifisch, sondern sektorübergreifend vorliegen, und damit generell für das Recht auf Datenportabilität gelten.[1945]

754 Ferner zeigt sich, dass ein sektorübergreifendes Portabilitätsrecht auch in Abgrenzung zu mehreren, parallel bestehenden, sektoriellen Portabilitätsrechten gerechtfertigt ist. Es zielt auf ein datenschutzrechtliches *Empowerment*, was den weiten Anwendungsbereich nicht nur zulässt, sondern ihn vielmehr erfordert. In wettbewerbsrechtlicher Hinsicht sind die Makroziele zudem darauf angelegt, neue innovative Angebote zu ermöglichen und Daten über Sektoren hinweg auszutauschen. Das Portabilitätsrecht ist damit mehr als die Summe seiner (sektoriellen) Teile, da es in der Lage ist, unterschiedliche Sektoren zu verbinden und damit eine sektorübergreifende Interkonnektivität herzustellen.[1946]

755 Sektorübergreifend ist kaum Anpassungsbedarf erkennbar. Das Portabilitätsrecht ist bereits *de lege lata* extensiv ausgestaltet und es existieren aufgrund der datenschutzrechtlichen Natur des Instituts nur wenige Einschränkungen. Zwar sind angesichts des gewählten *one-size-fits-all*-Ansatzes in den einzelnen Sektoren stets gewisse Handlungsspielräume erkennbar. Diese lassen sich aber nicht per se auf andere Sektoren übertragen.[1947] Gleiches gilt für die wettbewerbsrechtlichen Ziele. Sie sind teilweise von vornherein nur auf Internetplattformen zugeschnitten und damit darauf angelegt, bloss sektoriell zu wirken. Aus den auf sektorielle Unzulänglichkeiten zugeschnittenen Handlungsspielräumen lassen sich indes keine Anpassungen des Portabilitätsrechts generalisieren, da das Institut nicht auf diese Anwendungsfälle begrenzt ist. Andere Ziele lassen sich hingegen sektorübergreifend begreifen. Mit Blick auf die sich daraus ergebenden Unzulänglichkeiten zeigt sich in den einzelnen Sektoren denn auch durchaus

1944 Dazu Rz. 679 und ausführlich Rz. 604 ff., 639 ff. und 662 ff.
1945 Dazu ausführlich Rz. 680 ff.
1946 Dazu ausführlich Rz. 685 ff.
1947 Dazu Rz. 723 f. und ausführlich Rz. 696 f.

Anpassungsbedarf, etwa Interoperabilitätsvorgaben, eine Portabilität für Sachdaten, eine Pflicht zur Schnittstellenimplementierung resp. Echtzeitübertragung, den Einbezug von abgeleiteten Daten oder passgenauere Vorgaben für die Durchführung der Portierung.

Allerdings würden solche Anpassungen einen hohen Grad an legislatorischer Präzision erfordern. Dadurch wären sie den wettbewerbsrechtlichen Zielen kaum sektorübergreifend förderlich. Damit bleibt – mit Blick auf die allgemeine Wettbewerbs- und Innovationsförderung und die Förderung eines freien Datenflusses, die als Makroziele auf eine sektorübergreifende Anwendung ausgerichtet sind – einzig eine punktuelle Modernisierung des Portabilitätsrechts als angezeigter Anpassungsbedarf. Ein *Update* der Modalitäten ist erforderlich, um den schnelllebigen Entwicklungen der Datenwirtschaft zumindest ansatzweise gerecht zu werden. Dieses sollte eine Verpflichtung zur zeitnahen, medienbruchfreien und periodischen Portierung umfassen, damit das Datenportabilitätsrecht in allen Sektoren einen praktischen Mehrwert bieten kann.[1948] 756

Somit besteht sowohl hinsichtlich der datenschutz- als auch der wettbewerbsrechtlichen Ziele insgesamt nur wenig Handlungsbedarf. Vielmehr erscheinen sektorspezifische Regelungen vielfach aussichtsreicher zur Erreichung konkreter Ziele. Einzig hinsichtlich der wettbewerbsrechtlichen Makroziele sind punktuelle Anpassungen, die über alle Sektoren hinweg implementierbar sind, nötig. Gemeinsam mit allfälligen spezifischeren, sektoriellen Vorgaben könnte das Portabilitätsrecht dadurch – als Teil und Rahmen eines neuen holistischen Datenrechts – in der Lage sein, zur Erreichung der vielfältigen Ziele beizutragen. 757

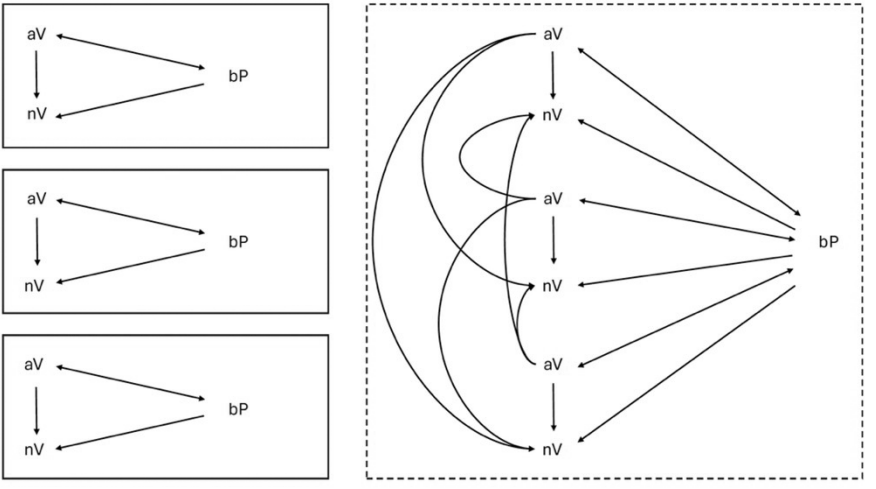
[1948] Dazu Rz. 725 ff. und ausführlich Rz. 698 ff.

Anhang

Anhang 1: Übersicht über die Metadaten einer .eml-Datei aus einer Beispielmail (rechts zugeschnitten).

FileType	Metadata	
FileTypePackage		
FileFormat	Integer	33
MimeType	String	message/rfc822
Extension	String	.eml
Email	Metadata	
EmlPackage		
Headers	Metadata	
EmailHeaderPackage		
Received	String	from ZR0P278MB0041.CHEP278.PROD.OUTLOOK.COM (2603:10a6:910:17::13) by GVAP278
From	String	=?utf-8?B?U2FtdWVsIE3DpHR6bGVy?= <samuel.maetzler@rwi.uzh.ch>
To	String	=?utf-8?B?U2FtdWVsIE3DpHR6bGVy?= <samuel.maetzler@rwi.uzh.ch>
Subject	String	=?utf-8?B?RGF0ZW5wb3J0YWJpbGl0w6R0IHVuZCBNZXRhZGF0ZW4=?=
Thread-Topic	String	=?utf-8?B?RGF0ZW5wb3J0YWJpbGl0w6R0IHVuZCBNZXRhZGF0ZW4=?=
Thread-Index	String	AQHYzoQhd21tCDdMek61tzq4pCUt9Q==
Date	String	Thu, 22 Sep 2022 13:06:30 +0000
Message-ID	String	<25E31357-4E4A-4342-995D-F03CBB3DE6C4@rwi.uzh.ch>
Accept-Language	String	de-DE, en-US
Content-Language	String	en-US
X-MS-Exchange-Organization-AuthAs	String	Internal
X-MS-Exchange-Organization-AuthMechanism	String	04
X-MS-Exchange-Organization-AuthSource	String	GVAP278MB0071.CHEP278.PROD.OUTLOOK.COM
X-MS-Has-Attach	String	
X-MS-Exchange-Organization-Network-Message-Id	String	db121130-250f-4b09-ea21-08da9c9b443f
X-MS-Exchange-Organization-SCL	String	-1
X-MS-TNEF-Correlator	String	
X-MS-Exchange-Organization-RecordReviewCfmType	String	0
x-ms-publictraffictype	String	Email
X-Microsoft-Antispam-Mailbox-Delivery	String	ucf:0;jmr:0;auth:0;dest:I;ENG:(910001)(944506478)(944626604)(920097)(425001)(930097);
X-Microsoft-Antispam-Message-Info	String	srNeM6i9y8NNngwU0k+y/XAxpLSARg/tFzDCNBLkq7YodeJywK8Gwfk7pnbX+mHFwy5T9OjCPqA
Content-Type	String	multipart/alternative; boundary="_000_25E313574E4A4342995DF03CBB3DE6C4rwiuzhch_"
MIME-Version	String	1.0
Sender	String	samuel.maetzler@rwi.uzh.ch
Subject	String	Datenportabilität und Metadaten
AttachedFileNames	StringArray	
Recipients	StringArray	[samuel.maetzler@rwi.uzh.ch]
CC	StringArray	
BCC	StringArray	

Anhang 2: Gegenüberstellung der Datenflüsse bei sektorspezifischen Portabilitätsrechten (links) zwischen altem Verantwortlichen (aV), neuer Verantwortlichen (nV) und betroffener Person (bP) und dem sektorübergreifenden Portabilitätsrecht nach dem DSG (rechts).



Curriculum Vitae

Samuel Mätzler studierte von 2012 bis 2018 Rechtswissenschaft an der Universität Basel und an der Université Paris II Panthéon-Assas. Nach Praktika in Advokatur und Verwaltung erlangte er 2021 das Anwaltspatent des Kantons Basel-Landschaft. Anschliessend war er als wissenschaftlicher Mitarbeiter am Center for Information Technology, Society, and Law (ITSL) der Universität Zürich tätig und doktorierte im Bereich des Datenschutzrechts. Seit 2026 arbeitet er als Rechtsanwalt in Zürich.

Das Recht auf Datenportabilität zählt zu den markantesten Neuerungen des totalrevidierten Datenschutzgesetzes. Es verleiht betroffenen Personen den Anspruch, ihre Personendaten von Verantwortlichen herauszuverlangen oder diese Daten direkt an Dritte übertragen zu lassen. Die vorliegende Dissertation untersucht das neuartige Rechtsinstitut in seiner ganzen Breite.

Der erste Teil beleuchtet die historischen, technisch-organisatorischen und rechtlichen Grundlagen sowie die Zielsetzungen des Rechts auf Datenportabilität an der Schnittstelle von Datenschutz- und Wettbewerbsrecht. Dabei wird rechtsvergleichend auch die Regelung der Europäischen Union herangezogen.

Der zweite Teil widmet sich dem Anpassungsbedarf der geltenden Rechtsgrundlagen. Drei Datenökosysteme – die sozialen Netzwerke, das Gesundheitswesen und die Mobilität – dienen als Fallbeispiele, um sektorspezifische Anpassungsvorschläge herzuleiten. Abschliessend geht die Arbeit der Frage nach, ob sich der sektorspezifische Anpassungsbedarf auf das Rechtsinstitut als Ganzes generalisieren lässt, und zeigt, wie eine praktikable Datenportabilität in der Schweiz ausgestaltet sein sollte.