

Beiträge zum Informationsrecht

Band 42

**Grenzen der Datenübermittlungen
aus der EU in Drittstaaten –
anhand des Beispiels der USA**

Von

Sabrina Seak



Duncker & Humblot · Berlin

SABRINA SEAK

Grenzen der Datenübermittlungen
aus der EU in Drittstaaten –
anhand des Beispiels der USA

Beiträge zum Informationsrecht

Herausgegeben von Prof. Dr. Hansjürgen Garstka,
Prof. Dr. Michael Kloepfer,
Prof. Dr. Eva Inés Obergfell,
Prof. Dr. Friedrich Schoch

Band 42

Grenzen der Datenübermittlungen aus der EU in Drittstaaten – anhand des Beispiels der USA

Von

Sabrina Seak



Duncker & Humblot · Berlin

Die Rechtswissenschaftliche Fakultät
der Westfälischen Wilhelms-Universität Münster
hat diese Arbeit im Jahr 2021
als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in
der Deutschen Nationalbibliografie; detaillierte bibliografische Daten
sind im Internet über <http://dnb.d-nb.de> abrufbar.

D 6

Alle Rechte vorbehalten
© 2022 Duncker & Humblot GmbH, Berlin
Satz: 3w+p GmbH, Rimpfing
Druck: CPI buchbücher.de gmbh, Birkach
Printed in Germany

ISSN 1619-3547

ISBN 978-3-428-18505-4 (Print)
ISBN 978-3-428-58505-2 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☺

Internet: <http://www.duncker-humblot.de>

*Meiner Mutter, die stets an mich geglaubt hat, meine seelische
Stütze war und mich durchgehend motiviert hat.
Meinem Vater, der mit mir Ideen ausgetauscht und mir gezeigt
hat, dass man niemals aufhören sollte, zu lernen.
Meinem Opa, für seine kontinuierliche Unterstützung
und sein unentwegt offenes Ohr.
Meiner restlichen Familie für das Verständnis
und den Rückhalt.*

Vorwort

Die vorliegende Arbeit wurde von der Rechtswissenschaftlichen Fakultät der Westfälischen Wilhelms-Universität Münster im Sommersemester 2021 als Dissertation angenommen. An dieser Stelle möchte ich mich herzlich bei allen beteiligten Personen bedanken, die mich bei meinem Promotionsvorhaben unterstützt haben.

Mein erster persönlicher Dank gebührt Herrn Prof. Dr. Thomas Hoeren, der mir die Umsetzung meiner Dissertation ermöglicht und mich bekräftigt hat, Forschung in den USA zu betreiben. Hervorheben möchte ich zudem die ausgezeichnet organisierten Doktorandenseminare, bei denen ich wertvolle inhaltliche Anregungen und organisatorische Hilfestellungen erhalten habe sowie Freundschaften mit anderen Doktoranden knüpfen konnte.

Überdies möchte ich Herrn Prof. Dr. Lothar Determann für die rasche Erstellung des Zweitgutachtens und die Gelegenheit danken, einen direkten Einblick in die datenschutzrechtliche Perspektive aus US-amerikanischer Sicht zu werfen. Für die anregenden Gespräche und gesammelten Erfahrungen an der Universität von Kalifornien in Berkeley bin ich zutiefst dankbar.

Auch möchte ich Herrn Thomas Christiansen meinen Dank aussprechen, der mir die Möglichkeit erteilt hat, neben meiner beruflichen Weiterentwicklung als Legal Counsel in einem Software-Unternehmen in Dänemark mein Promotionsvorhaben zu realisieren, und mich in diesem Rahmen stets mit produktiven Gesprächen und motivierendem Zuspruch begleitet hat.

Des Weiteren möchte ich auch der NGO noyb und Maximilian Schrems meinen herzlichen Dank aussprechen. Durch die innovativen Ideen und stetigen Bemühungen der Datenschutzaktivisten wurde diese Arbeit maßgeblich geprägt. Zudem konnte ich durch meine Zeit als Teil des noyb-Teams hilfreiche Erkenntnisse zur Durchsetzung des Datenschutzes in der EU gewinnen und im Juli 2020 an der Verkündung des Schrems II-Urteils durch den EuGH teilnehmen.

Köln, im November 2021

Sabrina Seak

Inhaltsübersicht

Einleitung	27
A. Gegenstand der Arbeit	27
B. Gang der Untersuchung	28

Erstes Kapitel

Datenübermittlungen aus der EU in Drittstaaten nach der DSGVO	30
A. Grenzen der Datenübermittlungen in Drittstaaten	30
I. Gegenstand der Grenzen	30
II. Territorialer Anwendungsbereich der Grenzen	32
B. Zulässigkeit der Datenübermittlung	42
I. Allgemeine Anforderungen	42
II. Formale Bedingungen im fünften Kapitel	42

Zweites Kapitel

Angemessenes Datenschutzniveau als Schranke	49
A. Bedeutung und Ziele eines angemessenen Datenschutzniveaus	49
I. Anlehnung an die internationalen Vorbilder	49
II. Ermöglichung des freien Datenflusses	51
III. Wahrnehmung einer politischen Funktion	52
IV. Wahrung eines hohen Grundrechtsschutzes	53
V. Zwischenergebnis	58
B. Kriterien für ein angemessenes Datenschutzniveau	59
I. Datenschutzregime	59
II. Internationale Verpflichtungen	60
C. Endergebnis	61

Drittes Kapitel

EU-Datenschutzrechtsniveau als Vergleichsmaßstab	63
A. Hohes Datenschutzniveau unter der DSGVO als Vergleichsmaßstab	63
I. Datenschutzgrundsätze	64
II. Rechtmäßigkeit der Datenverarbeitung	66
III. Rechte der betroffenen Personen	69

IV. Pflichten des Verantwortlichen	74
V. Gewährleistung der praktischen Wirksamkeit in der EU	77
B. Europäische Rahmenbedingungen für Behördenzugriffe	81
I. Kein Vergleichsmaßstab im EU-Recht	81
II. EuGH-Rechtsprechung als Vergleichsmaßstab	81
III. Rechtsprechung des EGMR als Vergleichsmaßstab	86
IV. Vier Garantien als Auslegungshilfen	87

Viertes Kapitel

Angemessenes Datenschutzniveau in den USA?	92
A. Verfassungsrecht auf Bundesebene	92
I. Vierter Verfassungszusatz	92
II. Erster Verfassungszusatz	97
B. Datenverarbeitungen durch Private	97
I. Ausgewähltes Bundesrecht	97
II. Föderales Recht am Beispiel von Kalifornien	114
C. Datenverarbeitungen durch öffentliche Stellen	136
I. Allgemeine Datenverarbeitungen	136
II. Endergebnis	157
D. Überwachungen durch US-Behörden	158
I. Recht zur Überwachung von aus der EU übermittelten Daten	159
II. Zugriff US-amerikanischer Geheimdienste auf Daten in der EU	188

Fünftes Kapitel

Legitimierungen von Datenübermittlungen in die USA	201
A. Mechanismen zur Legitimierung von Datenübermittlungen	202
I. Standardvertragsklauseln (SCC)	202
II. Andere Übermittlungsgarantien	218
III. Ausnahmen im fünften Kapitel	225
B. Zusätzliche Schutzmaßnahmen	235
I. Rechtsgrundlage	235
II. Lage in den USA	236
III. Zusätzliche Maßnahmen zu allen Übermittlungsgarantien	237
IV. Einzelabwägung	238
V. Konkrete zusätzliche Maßnahmen für Datenübermittlungen in die USA	248
C. Ausblick und Endbewertung	267
I. Zusätzliche Maßnahmen in einem dritten Datenschutzschild	267
II. Anpassung anderer Übermittlungsgarantien für die USA	268
III. Verlagerung von Datenverarbeitungen in die EU	269
IV. Auswirkungen auf den Handel	270
V. Erschwerung der Tätigkeit der US-Überwachungsbehörden	271

VI. Prüfung der Verhältnismäßigkeit für zusätzliche Maßnahmen	272
VII. Veränderung des „angemessenen Datenschutzniveaus“?	274
VIII. Herausforderung für Artikel 3 Abs. 2 DSGVO	275
IX. Durchsetzung und Bindung	277
Literaturverzeichnis	280
Sachwortverzeichnis	289

Inhaltsverzeichnis

Einleitung	27
A. Gegenstand der Arbeit	27
B. Gang der Untersuchung	28

Erstes Kapitel

Datenübermittlungen aus der EU in Drittstaaten nach der DSGVO	30
A. Grenzen der Datenübermittlungen in Drittstaaten	30
I. Gegenstand der Grenzen	30
II. Territorialer Anwendungsbereich der Grenzen	32
1. Niederlassungsprinzip	32
2. Marktortprinzip	33
a) Anbietet von Waren oder Dienstleistungen an Betroffene	33
b) Beobachtung des Verhaltens Betroffener	34
c) Zwischenergebnis	34
3. Verhältnis von Artikel 3 Absatz 2 zum fünften Kapitel der DSGVO	35
a) Status Quo: Keine öffentliche Klarstellung	35
b) Argumente zur Anwendbarkeit des fünften Kapitels	36
aa) Durchsetzungsprobleme	36
(1) Vertragliche Bindung	36
(2) Vertreter in der EU	37
bb) Schrems-Rechtsprechung	38
cc) Schutzabweichung	39
(1) Generelle Anforderungen	39
(2) Risikoanalyse	40
(3) Ergebnis	40
c) Konsequenzen des Ergebnisses	40
aa) Funktionsfähigkeit der digitalen Welt	40
bb) Anwendbarkeit auf die Direkterhebung	41
cc) Wahrung der Bedeutung eines angemessenen Datenschutzniveaus	41

B. Zulässigkeit der Datenübermittlung	42
I. Allgemeine Anforderungen	42
II. Formale Bedingungen im fünften Kapitel	42
1. Angemessenheitsentscheidungen der EU-Kommission	42
a) Allgemeine Beschlüsse	43
b) Beschlüsse für selbstzertifizierte Unternehmen in den USA	44
aa) Schrems I – Ungültigkeit von Safe Harbor	44
bb) Entstehung von Privacy Shield	45
cc) Schrems II – Ungültigkeit von Privacy Shield	46
2. Andere Übermittlungsgarantien	46
3. Ausnahmen	47
4. Zwischenergebnis	48

Zweites Kapitel

Angemessenes Datenschutzniveau als Schranke	49
A. Bedeutung und Ziele eines angemessenen Datenschutzniveaus	49
I. Anlehnung an die internationalen Vorbilder	49
II. Ermöglichung des freien Datenflusses	51
1. EU-Binnenmarkt	51
2. Mit Handelspartnern	51
III. Wahrnehmung einer politischen Funktion	52
IV. Wahrung eines hohen Grundrechtesschutzes	53
1. Datenschutz als europäisches Grundrecht	53
2. Anspruch auf Fortwahrung des Grundrechtesschutzes	53
3. Verhältnismäßigkeit zu tangierten Grundrechten	55
a) Recht auf informationelle Selbstbestimmung	55
b) Unternehmensfreiheit	55
c) Recht auf Sicherheit	56
d) Abwägung im Rahmen der Verhältnismäßigkeit	56
e) Hohes Schutzniveau als Leitlinie	57
f) Wesensgehalt des Grundrechts auf Datenschutz	57
V. Zwischenergebnis	58
B. Kriterien für ein angemessenes Datenschutzniveau	59
I. Datenschutzregime	59
1. Werte der EU	59
2. Einschlägiges Recht	59
3. Unabhängige Aufsichtsbehörde	60
II. Internationale Verpflichtungen	60

C. Endergebnis 61

Drittes Kapitel

EU-Datenschutzrechtsniveau als Vergleichsmaßstab 63

A. Hohes Datenschutzniveau unter der DSGVO als Vergleichsmaßstab 63

 I. Datenschutzgrundsätze 64

 1. Rechtmäßigkeit, Fairness und Transparenz 64

 2. Zweckbindung und zusammenhängende Grundsätze 65

 3. Integrität und Vertraulichkeit 66

 4. Rechenschaftspflicht 66

 II. Rechtmäßigkeit der Datenverarbeitung 66

 1. Einwilligung 67

 2. Weitere Legitimierungen 67

 a) Im Interesse des Betroffenen 67

 b) Verpflichtungen zur Verarbeitung 68

 c) Überwiegende Interessen bei Verarbeitung durch Private 68

 3. Besonders schutzbedürftige Datenverarbeitungen 68

 4. Zwischenergebnis 69

 III. Rechte der betroffenen Personen 69

 1. Informationspflichten in Bezug auf die Datenverarbeitung 69

 2. Auskunftsrecht und der Erhalt von Kopien 70

 3. Recht auf Datenübertragbarkeit 70

 4. Widerspruchsrecht 71

 5. Recht auf Löschung und Vergessenwerden 71

 a) Recht auf Löschung 71

 b) Recht auf Vergessenwerden 72

 c) Abwägung mit der Meinungsfreiheit 73

 6. Zwischenergebnis 73

 IV. Pflichten des Verantwortlichen 74

 1. Pseudonymisierung und Verschlüsselung 74

 2. Datenschutz-Folgenabschätzung und Datenschutzbeauftragter 75

 3. Privacy by Design and Default 76

 4. Wiederherstellungsmaßnahmen 76

 5. Meldepflichten bei Verletzungen 76

 6. Zwischenergebnis 76

 V. Gewährleistung der praktischen Wirksamkeit in der EU 77

 1. Überwachung durch unabhängige Aufsichtsbehörden 77

2. Verwaltungsrechtliche und gerichtliche Rechtsbehelfe	78
a) Bedingungsloses Beschwerderecht bei allen Aufsichtsbehörden	78
b) Klage gegen Aufsichtsbehörden	78
c) Klage gegen den Verantwortlichen	78
d) Verbandsklage	79
e) Bewertung	79
3. Sanktionen	79
a) Festgelegte Bedingungen	79
b) Hohe Geldbußen im Ermessen der Behörde	80
c) Ausnahme bei öffentlicher Datenverarbeitung	80
d) Zwischenergebnis	80
B. Europäische Rahmenbedingungen für Behördenzugriffe	81
I. Kein Vergleichsmaßstab im EU-Recht	81
II. EuGH-Rechtsprechung als Vergleichsmaßstab	81
1. Rechtsprechung zur Vorratsdatenspeicherung als Beispiel	82
a) Metadatenchutz unter der ePrivacy-Richtlinie	82
b) Anwendbarkeit von ePrivacy auf die Vorratsdatenspeicherung	83
c) Normierte Anforderungen an Eingriffe	83
d) Übertragungen auf Behördenzugriffe	84
e) Zulässigkeit der Bewertung durch den EuGH	85
III. Rechtsprechung des EGMR als Vergleichsmaßstab	86
IV. Vier Garantien als Auslegungshilfen	87
1. Transparente Eingriffsnorm	88
2. Verhältnismäßigkeit	88
3. Unabhängige Aufsicht	89
4. Effektive Beschwerdemöglichkeit	89
5. Bewertung	90

Viertes Kapitel

Angemessenes Datenschutzniveau in den USA?	92
A. Verfassungsrecht auf Bundesebene	92
I. Vierter Verfassungszusatz	92
1. Privatsphärenschutz	92
2. „Third-party doctrine“	93
a) FISC-Rechtsprechung zu Metadaten	93
b) Subjektive Erwartungshaltung	94
c) Schutzaufrechterhaltende Rechtsprechung	95
d) Bewertung durch die EU-Kommission	96

e) Ergebnis	96
II. Erster Verfassungszusatz	97
B. Datenverarbeitungen durch Private	97
I. Ausgewähltes Bundesrecht	97
1. Children's Online Privacy Protection Act	98
a) Konkrete Anforderungen an die Einwilligung	98
b) Datenminimierung	99
2. Schutz von Finanzdaten	100
a) Vergleichbare Rechte zur DSGVO	100
b) Keine Transparenz für behördliche Datenzugriffe	101
c) Grundsätzliche Erlaubnis zur Verarbeitung	102
d) Einwilligung durch Opt-Out	102
e) Aufsicht durch die Federal Trade Commission	102
aa) Handlungspotenzial	103
bb) Unabhängigkeit der FTC	104
3. Health Insurance Portability and Accountability Act	105
a) Umfangsreiche Zugangsrechte	105
b) Datensicherheit	105
c) „De-Identifizierung“	106
d) Schutz für innovative Herausforderungen?	107
aa) Adressatenkreis	107
bb) Selbstzertifizierung am Beispiel biometrischer Daten	107
cc) Zwischenergebnis	108
4. Bewertung der Angemessenheit des Bundesrechts	109
a) Vergleichbarkeit der Betroffenenrechte	109
b) Berücksichtigung von Analogien	110
c) Schwerpunkt bei der Auswahl der Schutzmaßnahmen	110
d) Angemessenheit ohne Datenminimierung?	111
e) Ergebnis	111
f) Ausblick: Einheitliches US-Datenschutzrecht	112
aa) Aktuelle Debatten	112
bb) Bedeutung für die EU	113
II. Föderales Recht am Beispiel von Kalifornien	114
1. Entstehungsgeschichte	114
2. Anwendungsbereich für persönliche Informationen	115
a) Verbraucher	115
b) Erfassung des Haushalts	115
c) Referenz zu Gerätedaten	116
3. Adressatenkreis	117

4. Verantwortlichkeit	118
5. Schutzausschluss	118
a) Verbraucherstandort außerhalb Kaliforniens	118
b) De-Identifizierung und Aggregation	118
c) Vorrang vom Bundesrecht	119
6. Schutzmaßnahmen	119
a) Erhebung und Verkauf von Daten	119
b) Datenschutzgrundsätze	120
c) Recht auf Löschung	121
aa) Umfang des Anspruchs	121
bb) Meinungsfreiheit und andere Ausnahmen	121
d) Datenübertragbarkeit	122
7. Rechtsdurchsetzung	123
a) Generalstaatsanwalt	123
b) Haftung und Anspruch auf Schadenersatz	123
c) Sanktionen und Bußgelder	124
8. Bewertung des Datenschutzniveaus in Kalifornien	125
a) Angemessener Anwendungsbereich des CCPA	125
b) Teilweise gleichwertige Rechte und Pflichten in CPPA	125
aa) Fortschritt durch Widerspruchsrecht	125
bb) Schutz bei einer Weiterübermittlung	125
cc) Steigerungspotenzial	126
dd) Untergeordnete Rolle der Datenschutzgrundsätze	126
ee) Auswirkung der fehlenden Datenminimierung	127
c) Verbesserungsmöglichkeiten bei der Durchsetzung	128
d) Zwischenergebnis	129
e) Ausblick: Angemessenheitsentscheidung durch den neuen CPRA?	129
aa) Änderungen des CCPA durch den CPRA	129
(1) Risikobasierter Anwendungsbereich	129
(2) Erweiterung des Opt-Out-Rechts	130
(3) Angemessener Schutz durch Opt-Out?	131
(4) Neue Rechte nach dem Vorbild der DSGVO	132
(5) Erstmalige Definierung sensibler Daten	133
(6) Einführung der Datenminimierung	133
(7) Eigene Datenschutzbehörde	134
bb) Praktische Herausforderungen	135

C. Datenverarbeitungen durch öffentliche Stellen	136
I. Allgemeine Datenverarbeitungen	136
1. Privacy Act 1974 und Freedom of Information Act	136
a) Verarbeitungsgrundsätze	137
aa) Übereinstimmungen mit der DSGVO	137
bb) Offenlegungen und Weiterübermittlungen	138
b) Rechte betroffener Personen	138
aa) Recht auf Zugang, Korrekturen und Kopien	138
bb) Kein Widerspruchsrecht	139
c) Vielseitige Maßnahmen zur Effektivität	140
d) Anforderungen an Ausnahmen	141
e) Bewertung der Angemessenheit des Privacy Acts	142
aa) Unionsgleicher Anwendungsbereich und vergleichbare Grundsätze	142
bb) Besonderheiten behördlicher Datenverarbeitungen	143
cc) Missachtung unionsrelevanter Anforderungen	143
dd) Effektivität des Rechtsschutzes	144
ee) Folgen von Ausnahmen	144
ff) Ergebnis	145
2. Korrekturen durch ausgehandelte Rechtsakte?	145
a) Judicial Redress Act für EU-Strafverfolgungsbehörden	145
aa) Vorstellung des Schutzes	145
bb) Geltung des Schutzes	146
b) Umbrella Agreement	147
aa) Unionsgleiche Verarbeitungsgrundsätze	148
bb) Löschung und Ausnahmen	148
cc) Speicherungslimit im US-Recht	149
dd) Sensible Daten	149
ee) Einwilligungsbedingte Weiterübermittlung	149
ff) Pflichten bei Verletzungen	150
gg) Benennung geeigneter Aufsichtsstellen	151
hh) Rechtsbehelfe	152
ii) Todesstrafe als Folge einer Übermittlung	153
jj) Aufhebung des Schutzes durch Trump-Dekret?	153
c) Bewertung des JRA und des Umbrella Agreements	154
aa) Ergänzungen des Privacy Acts	154
bb) Korrekturen des Privacy Acts	155
cc) Aufsichtsstellen	155
dd) Gleichstellung zu US-Staatsangehörigen	156
ee) Einfluss auf die US-Nachrichtendienste	156
II. Endergebnis	157

D. Überwachungen durch US-Behörden	158
I. Recht zur Überwachung von aus der EU übermittelten Daten	159
1. Section 702 FISA	159
a) Ausländische Geheimdienstinformationen	159
b) Anbieter elektronischer Kommunikationsdienste	160
c) Foreign Intelligence Surveillance Court	160
d) Minimierungsmaßnahmen	161
e) Genehmigte Überwachungsprogramme	162
aa) Prism	162
bb) Upstream – Glasfaserkabelanzapfung	163
cc) About-collection	163
f) Betroffenenrechte	164
aa) Schweigeanordnung	164
bb) Freedom Act	164
cc) Klageberechtigung	165
2. NSL	165
3. EO12333	166
a) Befugnisse	166
b) Unklarer territorialer Anwendungsbereich	167
c) Ausländerdiskriminierung und Verhältnismäßigkeit	167
4. Bewertung	168
a) Anwendungsbereich des FISA	168
b) Gefährdungszusammenhang von FISA und NSL	168
c) Korrekturen durch den Freedom Act?	168
d) Anwendungsbereich von der EO12333	169
e) Begrenzungen und Rechtsschutz	169
5. Erweiterte Schutzmaßnahmen unter PPD-28	170
a) Gleichstellung von Ausländern	171
b) Zweckbeschränkungen	171
c) Ombudsmechanismus	172
aa) Kontaktstelle für EU-Staatsangehörige	172
bb) Einfache Antragsstellung	172
cc) Auf Prüfung beschränkte Kompetenz	173
dd) Derzeitige Besetzung	173
6. Zusicherungen von Sicherheitsbehörden im Privacy Shield	174
a) Prozesse im Hintergrund der Überwachung	174
b) Gesteigerte Transparenz	175
c) Überwachung der nachrichtendienstlichen Tätigkeit	175

7. Bewertung unter Gegenüberstellung offizieller Einschätzungen	176
a) Hinreichender Schutz nach Einschätzung der EU-Kommission	176
aa) Einbeziehung behördlicher Zusagen	176
bb) Notwendigkeit und Verhältnismäßigkeit durch die PPD-28	176
cc) Ombudsstelle als effektiver Rechtsbehelf	177
b) Kein angemessenes Datenschutzniveau für den EuGH	178
aa) Keine Verhältnismäßigkeit der Ausnahmen	178
bb) Kein effektiver Rechtsschutz in den USA	179
cc) Keine Korrektur durch Ombudsperson	180
c) Eigene Bewertung	180
aa) Transparente Eingriffsbefugnisse?	180
(1) Die EU übersteigende Transparenz	180
(2) Festgelegte Strategien zur Abwägung	181
(3) Stabilität und Verbindlichkeit	181
bb) Gewährleistung der Verhältnismäßigkeit durch die PPD-28?	182
(1) Gleichstellung zu US-Staatsangehörigen	182
(2) Präzisierungen der Anwendungsbereiche	182
(3) Zulässigkeit von Massenerhebungen	183
(4) Ausnahmen	183
(5) Rechte aus der PPD-28	184
cc) Überwachung auf verschiedenen Ebenen	184
dd) Effektiver Rechtsbehelf durch die Ombudsperson?	185
(1) Neue einfache Abhilfestelle	185
(2) Keine Information über konkrete Betroffenheit	185
(3) Keine Weisungsbefugnis	186
(4) Bedenken an der Unabhängigkeit und die Kompetenz	186
(5) Künftige Verbesserungsmöglichkeit	187
ee) Zusammenfassung	187
II. Zugriff US-amerikanischer Geheimdienste auf Daten in der EU	188
1. Befugnis zur Datenanfrage außerhalb der USA	188
a) Section 702 FISA und EO12333	188
b) Vierter Verfassungszusatz als territoriale Beschränkung?	189
c) Supreme Court-Entscheidung und Erlass des CLOUD-Acts	190
d) Voraussetzung des CLOUD-Acts	190
2. Eigener Rechtsbehelf im CLOUD-Act	190
a) Schutz für ausländische Staatsangehörige	191
b) Wesentliches Risiko der Rechtsverletzung	191
c) Abkommen im Sinne des CLOUD-Acts	191

3. Auswirkungen von Abkommen unter dem CLOUD-Act	192
a) Anwendung von Artikel 48 DSGVO	192
aa) CLOUD-Act als internationale Übereinkunft	192
bb) Rechtfertigung von Datenübermittlungen nach Artikel 48 DSGVO	193
(1) Wörtliche und systematische Auslegung	193
(2) Historische und sinngemäße Auslegung	193
b) Einfluss auf Ausnahmen nach Artikel 49 DSGVO	195
c) Einfluss auf der ersten Stufe der Rechtfertigung	195
aa) Öffentliches Interesse der USA	196
bb) Rechtliche Verpflichtung	196
cc) Berechtigtes Interesse des Telekommunikationsanbieters	196
dd) Zwischenergebnis	197
d) Einfluss durch Abkommen mit anderen Drittstaaten	197
e) Bewertung	198
aa) Fokus auf effektiven Rechtsbehelf	198
bb) Internationales Übereinkommen unter dem CLOUD-Act	198
cc) Globale Lösungen	199
dd) Ergebnis	200

Fünftes Kapitel

Legitimierungen von Datenübermittlungen in die USA	201
A. Mechanismen zur Legitimierung von Datenübermittlungen	202
I. Standardvertragsklauseln (SCC)	202
1. Wirksamkeit für die USA	202
2. Bislang genutzte SCC	203
a) Zwei vorgesehene Konstellationen	203
b) Anwendung der SCC auf weitere Konstellationen	203
c) Allgemeine vorformulierte Pflichten	204
d) Pflichten in Bezug auf Zugriffe von Sicherheitsbehörden	204
aa) Informationspflichten auch bei Schweigepflicht	204
bb) Prüfungspflicht	205
3. Entwurf der neuen SCC	206
a) Verfahren	206
b) Übergangsfrist	206
c) Änderungen	207
aa) Weitere Verarbeitungskonstellationen durch neue Module	207
bb) Klare und detaillierte Pflichten	208
cc) Praxisorientierte Anpassungen an die DSGVO	208

dd)	Ausdrückliche weitreichende Pflichten bei behördlichen Zugriffsanfragen	210
(1)	Keine Unsicherheiten mehr bezüglich der Meldepflicht	210
(2)	Bemühung um Aufhebung von Schweigeanordnungen	211
(3)	Veröffentlichung über ergangene Anordnungen	211
(4)	Aufbewahrungspflicht	211
(5)	Ausdrückliche Pflicht zur Aussetzung oder Kündigung	212
(6)	Überprüfung der Legalität und Rechtsmittelausschöpfung	212
(7)	Datenminimierung	212
ee)	Widerrufsmöglichkeit	213
ff)	Anwendbarkeit der SCC auf Artikel 3 Absatz 2 DSGVO	213
d)	Bewertung	214
aa)	Komplexerer Aufbau	214
bb)	Ersetzung der alten SCC	215
cc)	DSGVO-übertreffende Pflichten	215
dd)	Keine vollständige Anpassung an die DSGVO	215
ee)	Verbesserungsmöglichkeiten für Behördenanfragen	216
(1)	Genehmigungsfreiheit	216
(2)	Unterstützung	217
(3)	Verhältnismäßigkeit	218
ff)	Klarstellungen zum Ausschluss der SCC auf das Marktortprinzip	218
II.	Andere Übermittlungsgarantien	218
1.	Angemessenheitsentscheidungen	219
a)	Drittes Datenschutzschild	219
b)	Selbstzertifizierung und Durchsetzung durch die FTC	220
2.	SCC von Aufsichtsbehörden	221
3.	Binding Corporate Rules	222
4.	Weitere Übermittlungsgarantien	223
5.	Durchsetzbare Rechte und wirksame Rechtsbehelfe	224
III.	Ausnahmen im fünften Kapitel	225
1.	Ausnahmetatbestände zugunsten öffentlicher Interessen	225
a)	Schutz lebenswichtiger Interessen	225
b)	Öffentliches Interesse in der EU	226
aa)	Keine Pflichten im Umbrella-Agreement	227
bb)	Kein öffentliches Interesse durch PNR-Abkommen	227
cc)	Kein öffentliches Interesse durch SWIFT-Abkommen	228
dd)	Zwischenergebnis	229
c)	Erforderlichkeit von Rechtsansprüchen	229
d)	Wahrung zwingender berechtigter Interessen	230

2. Ausnahmetatbestände zugunsten der Privatautonomie	231
a) Einwilligung	231
b) Verträge	233
c) Zwingende berechnigte Interessen	234
3. Ergebnis	234
B. Zusätzliche Schutzmaßnahmen	235
I. Rechtsgrundlage	235
II. Lage in den USA	236
1. Unverhältnismäßige Zugriffsrechte der Nachrichtendienste	236
2. Beschränkung auf die nationale Sicherheit?	237
III. Zusätzliche Maßnahmen zu allen Übermittlungsgarantien	237
1. Notwendigkeit für die neuen SCC	237
2. Notwendigkeit für die anderen Übermittlungsgarantien	238
IV. Einzelabwägung	238
1. Primäre Verantwortung des Datenexporteurs	238
a) Prüfung des Datenschutzniveaus im Drittstaat durch alle Beteiligten ...	238
b) In der DSGVO begründete Rechenschaftspflicht	239
aa) Direkte Anwendbarkeit auf den Datenexporteur	239
bb) Ausweitung auf den Datenimporteur durch die neuen SCC	240
2. In die Abwägung einzubeziehende Umstände in den USA	241
a) Datenempfänger	242
aa) Kommunikationsanbieter	242
bb) Empfänger vergangener Behördenanfragen	242
cc) PRISM-Kooperationspartner	243
dd) Verantwortliche und Auftragsverarbeiter	243
ee) US-amerikanische Behörden	243
b) Art der Daten und Zweck	244
aa) Unternehmensbezogene Daten	244
bb) Allgemein zugängliche Daten	244
cc) Vom US-Überwachungsrecht erfasste Daten	244
dd) Sensible Daten	245
c) Art der Verarbeitung	245
d) Umfang der Datenübermittlung	246
e) Besonderheiten von Übermittlungen in die USA	246
aa) Mögliche Unterwasserkabelanzapfung	246
bb) CLOUD-Act	247
cc) Vertraulichkeitserwartung	247
f) Zwischenergebnis	248

V.	Konkrete zusätzliche Maßnahmen für Datenübermittlungen in die USA	248
1.	Vertragliche Garantien	248
a)	Relevanz trotz der neuen SCC	249
b)	Empfehlung des Landesbeauftragten BW	249
aa)	Information an den Betroffenen über die Datenübermittlung	250
bb)	Abstimmung mit der Aufsichtsbehörde	250
cc)	Rechtswegbeschreitung bis zur letzten Instanz	250
c)	Handlungsempfehlungen des europäischen Datenschutzausschusses	251
aa)	Fragenkatalog als Vertragsbestandteil	251
bb)	Verpflichtung zur Vornahme zusätzlicher TOM	251
cc)	Keine Backdoors	252
(1)	Privacy by Design and Default	252
(2)	Internationale Bewegungen mit ermittlungsbegünstigendem Ansatz	252
dd)	Kurzfristige Reaktionsmöglichkeiten	253
(1)	Effektivere Audits durch den Datenexporteur	253
(2)	Eigenständiges Handeln durch den Datenimporteur	253
(3)	Schnelles Aussetzen der Datenübermittlungen	253
ee)	Erweiterte Transparenz	254
(1)	Tägliche Mitteilung an den Datenexporteur	254
(2)	Informierung der US-Behörde über den Konflikt	254
ff)	Keine freiwillige Schutzverringeringung	254
gg)	Unterstützung der betroffenen Person	255
hh)	Vermeidung von Weiterübermittlungen	255
d)	Ankündigungen von Microsoft	255
aa)	Angriff jeder Behördenanfrage	255
bb)	Finanzieller Schadensausgleich	256
e)	Zwischenergebnis	256
2.	Organisatorische Maßnahmen	256
a)	Erschwerung unzulässiger Behördenanfragen	256
aa)	Begrenzung der zugriffsberechtigten Personen	257
bb)	Reduzierung der Datenmenge	257
cc)	Datentreuhand-Modell	258
dd)	Vermeidung des Anwendungsbereichs von FISA und EO12333	258
b)	Aufdeckung erfolgter Zugriffe	259
aa)	Protokollierung	259
bb)	Vollständigkeitsprüfung	259
c)	Vorfalmanagement	259
aa)	Mitarbeitersensibilisierung	260
(1)	Sensibilisierung für die Rechtmäßigkeit nach dem US-Recht	260

(2) Keine Sensibilisierung für die EU-Grundrechtecharta	260
bb) Reaktionsplan	261
cc) Bestellung eines Expertenteams	261
d) Zwischenergebnis	262
3. Technische Vorkehrungen	262
a) Ende-zu-Ende-Verschlüsselung	262
b) Pseudonymisierung	263
c) Datenverschleierung	264
d) Versand von Datenträgern	264
e) Trennungsprinzip	264
f) Mehrparteienverarbeitung	264
g) Überwachung der Leitung	265
aa) Eigene Leitungen	265
bb) Auswahl der Netzbetreiber	266
h) Schutz nach Erhalt der Daten	266
i) Zwischenergebnis	266
C. Ausblick und Endbewertung	267
I. Zusätzliche Maßnahmen in einem dritten Datenschutzschild	267
II. Anpassung anderer Übermittlungsgarantien für die USA	268
1. Verpflichtungen der neuen SCC als vertraglicher Mindeststandard	268
2. Zusätzliche technische und organisatorische Maßnahmen	268
3. Im Einzelfall: Kein angemessenes Datenschutzniveau	269
III. Verlagerung von Datenverarbeitungen in die EU	269
IV. Auswirkungen auf den Handel	270
V. Erschwerung der Tätigkeit der US-Überwachungsbehörden	271
VI. Prüfung der Verhältnismäßigkeit für zusätzliche Maßnahmen	272
1. Grundrechtsabwägung im Rahmen der Risikoabwägung	272
2. Vernachlässigung anderer Grundrechte	273
VII. Veränderung des „angemessenen Datenschutzniveaus“?	274
VIII. Herausforderung für Artikel 3 Abs. 2 DSGVO	275
IX. Durchsetzung und Bindung	277
1. Internationaler Pakt über bürgerliche und politische Rechte	277
2. Übereinkommen Nr. 108 des Europarats	278
3. Gewohnheitsrecht	279
Literaturverzeichnis	280
Sachwortverzeichnis	289

Einleitung

A. Gegenstand der Arbeit

In dieser Arbeit werden die Grenzen der Übermittlungen personenbezogener Daten von der EU in Drittstaaten anhand des Beispiels der USA untersucht.

Der europäische Gerichtshof hat am 16. Juli 2020 wie bereits fünf Jahre zuvor¹ die von der europäischen Kommission ausgehandelten Rahmenbedingungen für Datenübermittlungen in die USA für ungültig erklärt.² Der Grund hierfür sind die möglichen Zugriffe auf die personenbezogenen Daten durch die US-Behörden. Diese Rechtsprechung gilt aufgrund der Herkunft der führenden Technologiekonzerne der Welt und der einhergehenden Anzahl grenzüberschreitender Datenübermittlungen dringlichst zu beleuchten. Eine Lösungsfindung zum Recht der nationalen Sicherheit in den USA, die den Anforderungen des europäischen Gerichtshofs gerecht wird, ist ein wesentliches Ziel dieser Arbeit.

Der Hauptteil dieser Arbeit widmet sich dem bestehenden Datenschutzniveau in den USA unter Berücksichtigung aktueller rechtlicher Entwicklungen. In den USA findet derzeit ein datenschutzrechtlicher Wandel statt, der durch die vermehrte Einreichung von Gesetzesentwürfen manifestiert wird. Diese Arbeit erhebt den Anspruch, das US-Datenschutzrecht umfassend zu beleuchten, um zukunftsorientierte Lösungen für Datenübermittlungen an private und öffentliche Datenempfänger zu skizzieren.

In der EU wurde durch den Eintritt der Datenschutzgrundverordnung ein hoher europäischer Datenschutzstandard etabliert. Staatsangehörige der EU haben einen Anspruch auf Beibehaltung dieses Schutzes bei einer Datenübermittlung.³ Die Datenschutzgrundverordnung begrenzt daher notwendigerweise globale Datenverarbeitungen, auch wenn personenbezogene Daten und ihr Transfer einen enormen Wert sowohl für globale Unternehmen als auch für Ermittlungsbehörden darstellen.⁴ Dabei besteht besonders in der Aufrechthaltung des europäischen Datenschutzstandards über das Gebiet der EU hinaus eine Herausforderung. Diese resultiert daraus, dass das US-Recht nicht „europäisiert“ und die digitale Welt nicht „regionalisiert“ werden kann.⁵

¹ EuGH, U. v. 6. 10. 2015 – C-362/14.

² EuGH, U. v. 16. 7. 2020 – C-311/18.

³ EuGH, U. v. 6. 10. 2015 – C-362/14 = ZD 2015, 549, 553 Rn. 72.

⁴ Vgl. *Skouris*, NVwZ 2016, 1359, 1363.

⁵ *Heckmann/Starnecker*, jM 2016, 58, 61.

Ein weiterer Schwerpunkt dieser Arbeit ist die Auseinandersetzung mit dem europäischen Datenschutzniveau und die daraus resultierenden Anforderungen an Datenübermittlungen in Drittstaaten. Die leitgebende Frage dieser Untersuchung ist, welche Grenzen das Unionsrecht und das Völkerrecht Datenübermittlungen von der EU in die USA setzen.

B. Gang der Untersuchung

Das erste Kapitel dient dem Einstieg in die Thematik der Grenzen, die in der DSGVO für Datenübermittlungen von der EU in Drittstaaten gesetzt werden. Dafür wird vor dem Hintergrund der Erweiterung des Anwendungsbereichs der DSGVO untersucht, auf welche Datenverarbeitungen diese Grenzen überhaupt Anwendung finden.

Im zweiten Kapitel wird die Bedeutung eines „angemessenen Datenschutzniveaus“ untersucht, das die normierte Grenze für Datenübermittlungen in Drittstaaten darstellt. Das Kriterium des angemessenen Datenschutzniveaus verfolgt als Schranke für die Übermittlung personenbezogener Daten verschiedene Ziele, die bei der Auslegung der resultierenden Anforderungen und der Bewertung des US-amerikanischen Rechts zugrunde gelegt werden müssen.

Für die Bewertung der Angemessenheit des Datenschutzniveaus steht – unabhängig von weiteren Anforderungen – fest, dass diese einen Vergleich der Rechtsordnung und Praxis des Drittstaates mit der EU erfordert.⁶ Das dritte Kapitel widmet sich den konkreten Anforderungen, die in der EU als Vergleichsmaßstab vorgegeben werden.

In dem vierten Kapitel findet die Prüfung statt, ob das US-Recht ein angemessenes Datenschutzniveau unter Berücksichtigung der zuvor festgestellten Anforderungen bietet. Das US-Recht zeichnet sich durch strukturelle Unterschiede zum europäischen Recht aus. Um diese zu veranschaulichen, beginnt die Prüfung mit der US-Verfassung und ausgewählten Datenschutzgesetzen, die das bestehende Datenschutzniveau in der gesamten USA prägen.

Mit dem Ziel, die aktuelle datenschutzsteigernde Entwicklung in den USA und ihre Folgen für Datenübermittlungen von der EU in die USA zu untersuchen, wird die Angemessenheit des Datenschutzrechts des US-Bundesstaates Kalifornien geprüft und Lösungen für die Legitimierung der Datenübermittlungen erarbeitet.

Anschließend werden Datenverarbeitungen durch Behörden in den USA diskutiert, um eine umfassende Bewertung der möglichen Aufrechterhaltung des unter der DSGVO gewährten Schutzes bei Datenübermittlungen zu ermöglichen. Dabei werden Behördenzugriffe auf personenbezogene Daten einer gesonderten Prüfung

⁶ *Dammann/Simitis*, DSRL, Art. 25 Rn. 8; *Grabitz/Hilf/Nettesheim/Brühmann*, DSRL, Art. 26 Rn. 15; *Simitis/Hornung/Spiecker/Schantz*, DSGVO, Art. 45 Rn. 6.

unterzogen, um passgenaue Lösungen für die vom Europäischen Gerichtshof festgestellten Defizite herauszuarbeiten. In diesem Rahmen werden auch extraterritoriale Zugriffsrechte der US-Behörden und ihre Folgen für das Datenschutzniveau in den USA untersucht.

Basierend auf den vorangegangenen Ergebnissen werden im fünften und gleichzeitig letzten Kapitel dieser Arbeit die bestehenden Möglichkeiten, rechtmäßige Datenübermittlungen in die USA vorzunehmen, untersucht. Der Schwerpunkt stellt die Auseinandersetzung mit dem neuen EU-Kommissionsentwurf⁷ zu den Standardvertragsklauseln⁸ dar. Zudem werden andere Mittel zur Legitimierung von Datenübermittlungen und ihre Vorzüge beleuchtet. Anschließend werden im Einklang mit der Rechtsprechung des europäischen Gerichtshofs zu Datenübermittlungen in die USA verschiedene Schutzmaßnahmen untersucht, die das Risiko eines unberechtigten Zugriffs von US-Nachrichtendiensten senken.⁹ Die Arbeit endet mit einem Ausblick auf eine globale Lösungsfindung.

⁷ *EU-Kommission*, Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries, 12. November 2020. Abrufbar unter: <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries>.

⁸ Art. 46 Abs. 1 lit. c DSGVO: „Standarddatenschutzklauseln“.

⁹ EuGH, U. v. 16.7.2020 – C-311/18 =MMR 2020, 597, 602 Rn. 133: „zusätzliche Maßnahmen“.