
© Greta Maria Gross (Illustratorin)
gretamariasgallery

Aufsatz

Es waren zwei Königskinder: zum Problem des EU-US-Datentransfers

Fabio Stark

Fabio Stark wurde 1996 in Starnberg geboren und studiert seit 2017 Rechtswissenschaften an der LMU München mit Schwerpunkt im europäischen Wirtschaftsrecht, Wettbewerbsrecht und geistigem Eigentum.

Open Peer Review

Dieser Beitrag wurde lektoriert von: Ludovica Böltling und Jens Hansen

Der Wirtschaftsverkehr zwischen der Europäischen Union und den Vereinigten Staaten von Amerika machte im Jahr 2020 42 % des Welthandels aus.[1] Dabei betrug der Wert aller Waren, die zwischen den beiden Wirtschaftsräumen ausgetauscht wurden, rund 556,2 Mrd. €.[2] Gleichzeitig flossen ca. 18 % der jeweiligen Gesamtexporte an den jeweils anderen, was bis heute eine wechselseitige Stellung als wich-

1 Infografik des Europäischen Rates zum EU-US-Handel, hier abrufbar (Stand: 25.05.2022).
2 Europäische Kommission, EU trade relations with the United States. Facts, figures and latest developments, hier abrufbar (Stand: 25.05.2022).

tigster Exportpartner[3] begründet.[4] Dass hierbei insbesondere dem Datentransfer eine herausragende Rolle zukommt, ist selbsterklärend: Im Waren- und Dienstleistungshandel müssen, von den Vertragsverhandlungen über den Leistungsaustausch bis zum Geschäftsabschluss, zwangsläufig Informationen zwischen den Geschäftspartnern fließen.[5] Dies gilt umso mehr, als Telekommunikations- und Unternehmensdienstleistungen per se zu den drei wichtigsten ‚Exportschlagern' der USA zählen.[6] Dieser Umstand hält spürbaren Einzug in unseren Alltag: jeder Post auf Twitter und Instagram, jede E-Mail, jede Suchanfrage auf Google kann hier in Deutschland getätigt werden, wird aber stets auf Unternehmensservern in den USA verarbeitet. Der Großteil der digitalen Dienste, die in Deutschland in Anspruch genommen werden, werden von US-Unternehmen angeboten. Es überrascht also keineswegs, dass die Urteile Schrems I und II, welche der EuGH 2016 und 2020 erließ, wie ein Blitz einschlugen: Ein gewichtiger Teil der Rechtsgrundlage des EU-US-Datentransfers wurde für unwirksam erklärt. Doch wie ist das möglich? In einem voran--gegangenen Artikel dieser Reihe wurden die Geschichte, die Grundsätze und die Systematik des europäischen Datenschutzes beleuchtet.[7] Nun wollen wir uns mit dem US-Datenschutz, dem US Privacy Law,[8] vor allem aber mit dem kommerziellen Datenaustausch zwischen den USA und der EU befassen. Dabei wird sich an drei Fragen orientiert:

> „Jeder Post, jede E-Mail, jede Suchanfrage kann hier in Deutschland getätigt werden, wird aber stets auf Unternehmensservern in den USA verarbeitet."

1. Was zeichnet das US Privacy Law gerade in Abgrenzung zum EU-Datenschutz grundsätzlich aus?

2. Welche rechtlichen Probleme bereitet der EU-US-Datentransfer konkret?

3. Wie kann der Datenverkehr zwischen den beiden Weltmächten rechtssicher ausgestaltet werden?

A. Der US-Datenschutz

Das US-Rechtssystem unterscheidet sich bereits in seinen Grundsätzen erheblich vom kontinentaleuropäischen. So kommt, ganz allgemein, der Rechtsgestaltung durch Rechtsprechung oder durch behördliche Dekrete eine wesentlich bedeutendere Rolle zu als hierzulande. Doch gerade der Datenschutz lässt einige besonders eklatante Differenzen erkennen, welche die Transferproblematik überhaupt erst begründen. Ein Blick auf einige dieser Grundlagen hilft, die Verschiedenheit der dahinter stehenden Wertungen besser zu verstehen und den American Approach an den Themenkomplex nachvollziehbar zu machen.

I. ‚The Right to Privacy'- Die Ausgangslage

Es war das deutsche Bundesland Hessen, das 1970 mit dem HDSG das weltweit erste Datenschutzgesetz erließ.[9] Dennoch begann die Debatte um das Konzept des Datenschutzes auf US-amerikanischem Boden: mit dem 1890 von den Juristen S. Warren und L. Brandeis im Harvard Law Review veröffentlichten bahnbrechenden Artikel „The Right to Privacy". In diesem sprachen sich die Autoren, angesichts der expandierenden Presselandschaft sowie dem Aufkommen der Fotografie, für ein

3 Zum Zwecke der besseren Lesbarkeit wird bei personenbezogenen Hauptwörtern nur die männliche Form verwendet. Diese Begriffe sollen für alle Geschlechter gelten.
4 Statistisches Monatsheft Baden-Württemberg 5/2020, Die EU, USA und China – drei Kraftzentren der Weltwirtschaft im Vergleich, 8, hier abrufbar (Stand: 25.05.2022).
5 *ECIPE*, The Economic Importance of getting Data Protection Right, 2013, 1 (7).
6 Infografik des Europäischen Rates zum EU-US-Handel, hier abrufbar (Stand: 25.05.2022).
7 *Stark*, CTRL 1/2022, 87 ff.
8 Dies dient der sauberen Abgrenzung zum Begriff der Datensicherheit, welche im Englischen stellenweise auch als Data Protection bezeichnet wird. Letzteres betrifft weniger den Individual- und Persönlichkeitsschutz als die technische Sicherheit von Daten jedweder Art, vgl. *Forbes Technology Council*, Data Privacy Vs. Data Protection: Understanding The Distinction In Defending Your Data, hier abrufbar (Stand: 25.05.2022).
9 *Stark*, CTRL 1/2022, 87 (88).

„Recht alleine gelassen zu werden“ aus.[10] Der somit erstmals rechtlich abgebildete Konflikt, zwischen dem Privatheitsinteresse des Einzelnen und einer zunehmend technisierten und bürokratisierten Allgemeinheit, wurde im Laufe des 20. Jahrhunderts nur noch schärfer. An beiden Ufern des Atlantiks wuchsen die Gefahren für die informationelle Selbstbestimmung durch technologischen Fortschritt zusehends. Entsprechend wurde der Ruf nach konkreten Datenschutzgesetzen - bald vermehrt gegen staatliche Eingriffe - ab den 1970ern auf beiden Kontinenten lauter. Auch hierbei blieben die Vereinigten Staaten lange Zeit ‚Taktgeber der Diskussion‘.[11]

Dennoch trennten sich die Herangehensweisen der beiden Rechtsräume an das gemeinsame Problem alsbald grundlegend voneinander. In Europa setzte sich ein universelles Schutzsystem durch: gekennzeichnet von Einheitlichkeit, einem möglichst weit gefassten Schutzraum und geringer Differenzierung zwischen staatlichen und privaten Stellen.[12] In den Vereinigten Staaten hingegen begann sich ein bereichsspezifischer, sog. sektoraler Ansatz abzuzeichnen, der ein weder umfassendes noch landesweit harmonisiertes Privacy Law zur Folge hatte. Heute speist sich der lückenhafte und z.T. sogar widersprüchliche US-Datenschutz teils aus Rechtsprechung, teils aus verfassungs-, bundes- und gliedstaatlichen Quellen.

II. Flickenteppich-Privacy – US-Datenschutzrechte im Überblick

1. Verfassungsrecht

Die wichtigste konstitutionelle Verankerung der Privacy Laws findet sich im vierten Amendment der US-Verfassung wieder. Dieses schützt die Privatsphäre von US-Bürgern vor unberechtigten hoheitlichen Durchsuchungen und Beschlagnahmungen.[13] Davon wird nach ständiger Rechtsprechung auch die elektronische Überwachung mittels Datenerhebungen erfasst.[14] Jede eingreifende Maßnahme verlangt demnach grundsätzlich eine gerichtliche Ermächtigung. Dies gilt jedoch nur, soweit (1) die Datenerhebung von staatlichen Stellen ausgeht, (2) der Betroffene ‚begründete Privatheitserwartungen‘ haben darf und (3) die Daten im unmittelbaren Zugriffsbereich des Betroffenen vorliegen, etwa auf seinem Server oder einem lokalen Datenträger.[15] Hat er sie bereits an einen Dritten weitergegeben, wie in Form einer E-Mail oder eines Posts bei Facebook, gelten sie als freiwillig veräußert und daher nicht länger schutzwürdig.[16]

Daneben spielen das Recht auf anonyme Meinungsfreiheit, auf Privatheit von Vereinigungen und der Schutz vor Selbstbelastung, aus dem ersten und fünften Amendment, eine untergeordnete Rolle.[17] Aus der Verfassung selbst erwächst indes keinerlei Schutz vor nicht-staatlicher Datenverarbeitung sowie vor Maßnahmen, die bei Dritten durchgeführt werden, etwa von Betreibern sozialer Netzwerke und sonstigen digitalen Dienstleistern. Und auch die Rechtfertigungsmöglichkeiten nach Eröffnung des Schutzbereichs sind bei weitem nicht so standfest wie für den europäischen Datenschutz üblich.[18]

2. Bundesrecht

Der US-Kongress erließ ab 1974 dutzende Regulierungen, welche Privacy zumindest als Bestandteil enthalten.[19] Allerdings wurden durch diese entweder nur bestimmte

10 *Warren/Brandeis*, The Right to Privacy, in Harvard Law Review, 1890, hier abrufbar (Stand: 25.05.2022).
11 Zit. *Lewinski*, Was Europa und die USA in Sachen Datenschutz unterscheidet, hier abrufbar (Stand: 25.05.2022); zur Entwicklung des Datenschutzes zudem Kühnl, Persönlichkeitsschutz 2.0: Profilbildung und -nutzung durch soziale Netzwerke am Beispiel von *Facebook* im Rechtsvergleich zwischen Deutschland und den USA, 2016, 215.
12 Zur Geschichte und Dogmatik des europäischen Datenschutzes *Stark*, CTRL 1/2022, 87 ff.
13 Wörtlich: *„The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.“*, hier abrufbar (Stand: 25.05.2022).
14 *Swire* in: Svantesson/Kloza, Transatlantic data privacy relations as a challenge for democracy, 2017, 89.
15 *Kühnl*, Persönlichkeitsschutz 2.0: Profilbildung und -nutzung durch soziale Netzwerke am Beispiel von Facebook im Rechtsvergleich zwischen Deutschland und den USA, 2016, 227 ff.
16 Zur sog. Third Party Doctrine: U.S. vs. Golden Valley Elec., Assn.689 F.3d 1108 1116 (9th Circ. 2012); *Wittmann*, Der Schutz der Privatsphäre vor staatlichen Überwachungsmaßnahmen durch die US-amerikanische Bundesverfassung, 2014, 181.
17 *Solove/Schwartz*, Privacy Law Fundamentals, 2019, 3.
18 Dies wird maßgeblich durch das Erfordernis der begründeten Privatheitserwartungen bedingt, vgl. *Kühnl*, Persönlichkeitsschutz 2.0: Profilbildung und -nutzung durch soziale Netzwerke am Beispiel von Facebook im Rechtsvergleich zwischen Deutschland und den USA, 2016, 229.
19 Übersicht zu sämtlichen Bundesgesetzen mit Datenschutzbezug: ebd., 4 f.

Informationstypen (Kredit[20]- oder Gesundheitsdaten[21] etc.) oder besondere Personengruppen wie beispielsweise Minderjährige[22] geschützt. Damit zeichnet sich das US Privacy Law durch einen im Schwerpunkt mehr verbraucherschützenden als abwehrrechtlichen Charakter aus.

Die Überwachung vieler dieser Vorschriften sowie insbesondere der Einhaltung von Selbstverpflichtungen obliegt der 1914 gegründeten Federal Trade Commission (FTC). Ihr kommt eine besondere Rolle im US Privacy Law zu, zumal vertragliche Abreden einen gewichtigen Anteil des geltenden Schutzstandards ausmachen.[23] Als Verbraucherschutz- und Wettbewerbsaufsicht gewährleistet sie die Durchsetzung entsprechender Rechte aufgrund Anträge von Betroffenen. Jedoch beschränkt sich dies zumeist auf Aufklärungspflichtverletzungen.[24] Mit einer europäischen Datenschutzbehörde ist die FTC daher nicht vergleichbar.

Wichtigstes abwehrrechtliches Datenschutzgesetz ist der Privacy Act von 1974. Als parlamentarische Antwort auf den Watergate-Skandal räumt er US-Bürgern gegenüber Bundesbehörden ein Recht auf Zugang und Kopie bereits erhobener persönlicher Daten sowie auf Korrektur von Falschinformationen ein. Auch der hierzulande bekannte Minimierungsgrundsatz sowie das Erforderlichkeitsgebot für Datenverarbeitungen hielten Einzug; wesentlich mehr Zugriffseinschränkungen gelten indes nicht.[25] Damit reichen die Betroffenenrechte des Privacy Acts nicht an den europäischen Standard heran.

Insoweit erscheint der Electronic Communications Privacy Act (ECPA) von 1986, zur Einschränkung elektronischer Überwachung von US-Bürgern durch Bundesbehörden, schon wirkmächtiger.[26] Im Unterschied zum Privacy Act verbietet Letzterer den Zugriff von Bundesbehörden auf Bürgerdaten unter bestimmten Voraussetzungen gänzlich. Und zwar, im Gegensatz zum vierten Amendment, auch dann, wenn sie an Dritte weitergegeben wurden. Allerdings nur, soweit sie u.a. nicht länger als sechs Monate gespeichert wurden. Vor allem deshalb ist der ECPA wiederholt scharfer Kritik ausgesetzt.[27]

3. Gliedstaatliche Rechte

Während das Bundesrecht also weiterhin nur vereinzelte und unvollständige Regelungen zum Datenschutz enthält, zeichnet sich auf bundesstaatlicher Ebene seit 2018 eine Kehrtwende ab.[28] Zum Zeitpunkt der Veröffentlichung dieses Artikels haben bereits vier Bundesstaaten eigene allgemeine Verbraucherdatenschutzgesetze verabschiedet, in zwölf weiteren Staaten werden entsprechende Regelungen vorbereitet.[29] Allen gemein ist der Anspruch, sämtliche personenbezogenen Daten von Verbrauchern vor möglichst vielen privaten Organisationen zu schützen. In den einzelnen Bestimmungen sind jedoch erhebliche Unterschiede feststellbar. So weist der Vorreiter Kalifornien in seinem California Consumer Privacy Act (CCPA) ein der DSGVO noch ähnliches Schutzkonzept auf. Neben einem Anspruch auf Zugang und Löschung persönlicher Daten gegenüber den Verarbeitern sieht er auch eine Opt-Out-Lösung vor. Demnach hat der Betroffene, nachdem er über die Verarbeitungen seiner Daten (verpflichtend) informiert worden ist, das Recht, diese abzulehnen.[30] Auch der Schutzbereich ist über den verwendeten Datenbegriff nahezu

20 So im Gramm-Leach-Bliley Act (GLBA) von 1999 als Verbraucherschutzregelungen im Bank- und Finanzwesen, hier abrufbar (Stand: 25.05.2022); sowie im Fair Credit Reporting Act (FCRA) von 1970 zum Datenschutz bei Verbrauchermeldezentren, hier abrufbar (Stand: 25.05.2022).
21 Insb. im Health Insurance Portability and Accountability Act (HIPAA) von 1996 zum Schutz von Gesundheitsdaten bei medizinischen Dienstleistern, mehr Informationen hier abrufbar (Stand: 25.05.2022).
22 Geregelt im Children's Online Privacy Protection Act (COPPA) von 2000 zum Schutz persönlicher Daten von Minderjährigen unter dreizehn Jahren, hier abrufbar (Stand: 25.05.2022).
23 So verhängte die *FTC* 2012 gegen *Facebook* eine Geldbuße i.H.v. 5 Mrd. USD, nachdem unrichtige Angaben über die Datenlimitation sowie weitere Verarbeitungspraktiken gemacht wurden, vgl. hier abrufbar (Stand: 25.05.2022).
24 *Kühnl*, Persönlichkeitsschutz 2.0: Profilbildung und -nutzung durch soziale Netzwerke am Beispiel von Facebook im Rechtsvergleich zwischen Deutschland und den USA, 2016, 248 ff.
25 Dazu, aber auch als allgemeine Einführung ins US Privacy Law *Green*, Complete Guide to Privacy Laws in the US, hier abrufbar (Stand: 25.05.2022).
26 *Solove/Schwartz,* Privacy Law Fundamentals, 2019, 41 ff.
27 So *Kravets*, Aging ‚Privacy' Law Leaves Cloud E-Mail Open to Cops, hier abrufbar (Stand: 25.05.2022); oder *Kerr*, The Next Generation Communications Privacy Act, hier abrufbar (Stand: 25.05.2022).
28 So etwa die eBook-Regulierungen Missouris hier abrufbar (Stand: 25.05.2022); oder der Illinois Biometric Information Privacy Act (BIPA), hier abrufbar, (Stand: 25.05.2022).
29 Vgl. zur aktuellen Entwicklung den US State Privacy Legislation Tracker der *International Association of Privacy Professionals* (*IAPP*), hier abrufbar (Stand: 25.05.2022).
30 In Abgrenzung zum Erlaubnisvorbehalt der DSGVO (Opt-In-Lösung), vgl. *Klosowski*, The State of Consumer Data Privacy Laws in the US (And Why It Matters), hier abrufbar (Stand: 25.05.2022).

"europäisch" weit gefasst.[31] Andere Staaten wie Virginia wiederum bieten ein geringeres Schutzniveau, vor allem hinsichtlich der Massenverarbeitung von Daten.[32] Interessanterweise führte insbesondere die Frage nach der Klagebefugnis Privater in der jüngsten Vergangenheit regelmäßig zu Konflikten und sogar gescheiterten Gesetzesvorhaben.[33] All dies hat letztlich einen noch laufenden gesetzgeberischen Wettbewerb innerhalb der USA zur Folge, in welchem sich auf der einen Seite ein bürgerrechtlicher und auf der anderen ein freiheitlicher Ansatz gegenüberstehen. Der Ausgang dessen bleibt ungewiss.

4. Zwischenergebnis

Das sektorale US-Datenschutzrecht weist zumindest den potenziellen Vorteil einer einzelfallgerechteren Regelungsmöglichkeit auf. Während die DSGVO mitunter für die rigorose Gleichbehandlung von Ungleichem kritisiert wird, trifft das US-Recht spezifische Entscheidungen für unterschiedliche Adressaten, Daten- und Verarbeitungsformen. Dadurch räumt das Rechtssystem auch mehr Freiraum für den modernen Datenverkehr ein. Gleichzeitig entstehen durch den lückenhaften Datenschutz nicht nur erheblich mehr Risiken für die informationelle Selbstbestimmung der Betroffenen, sondern auch große Rechtsunsicherheit. Das unübersichtliche Dickicht bestehender bundesrechtlicher Vorschriften wird dabei zunehmend durch teils grundverschiedene einzelstaatliche Gesetze zusätzlich verkompliziert. Noch weniger eingeschränkt bleiben indes die staatlichen Eingriffsmöglichkeiten. Auch der aktuelle Gesetzgebungstrend auf Bundesstaatsebene bleibt dem Verbraucherschutzkonzept des US Privacy Laws unverändert treu.

	DSGVO	CCPA	VCPA
1. **Verarbeitung mit Einwilligungsvorbehalt (Opt-In)**	⊕	⊖	⊕
2. **Verarbeitung mit Widerrufsoption (Opt-Out)**	⊖	⊕	⊖
3. **Recht auf Auskunft über die Verarbeitung**	⊕	⊕	⊕
4. **Recht auf Zugang**	⊕	⊕	⊕
5. **Recht auf Löschung**	⊕	⊕	⊕
6. **Technische u. organisatorische Maßnahmen**	⊕	⊕	⊖
7. **Recht auf Berichtigung falscher Daten**	⊕	⊖	⊕
8. **Adressiert private Stellen**	⊕	⊕	⊕
9. **Adressiert staatliche Stellen**	⊕	⊖	⊖
10. **Klagebefugnis Privater**	⊕	⊕	⊖
11. **Finanzielle Höchststrafen**	**20 Mio €** oder **4 %** des weltweiten Jahresumsatzes	**2.500 $** bei fahrlässiger Verletzung **7.500 $** vorsätzlicher Verletzung	**7.500 $**

Rechtsvergleich zwischen der DSGVO, dem CCPA und dem VCPA im Überblick

III. Datenstrom mit Hindernissen - die Problematik des EU-US-Datentransfers

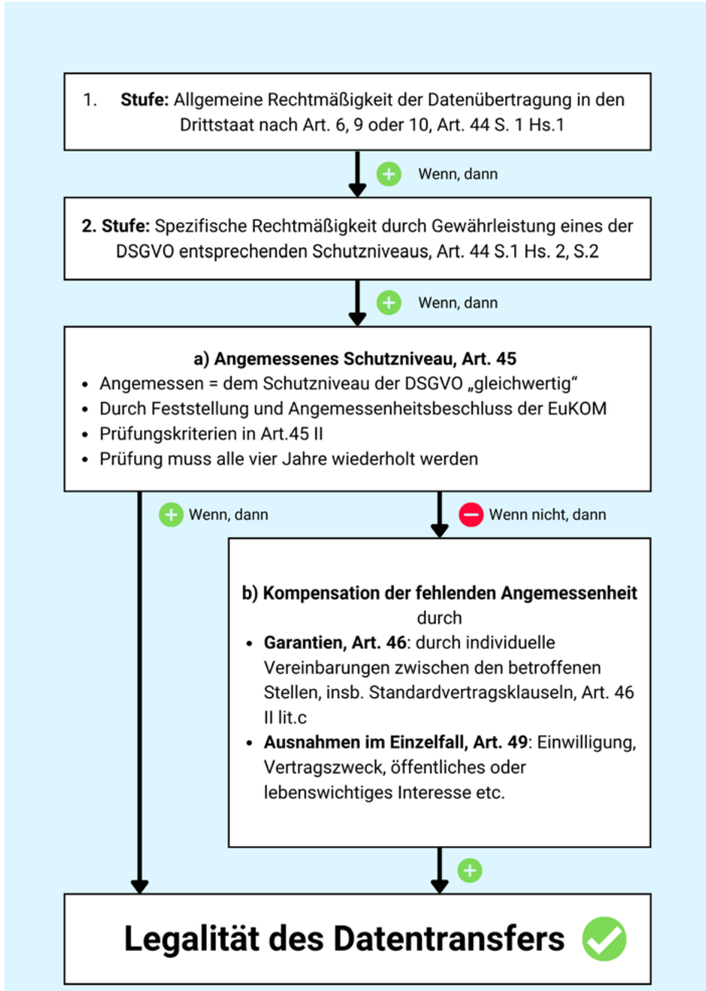
Es wird deutlich, dass bereits die generelle Systematik des US Privacy Laws in einem scharfen Kontrast zum hiesigen Datenschutz steht.[34] In der Literatur wird auch zwischen einem würde- und einem freiheitsbasierten Ansatz differenziert. Ersterer verweist auf den grundrechtlichen Charakter des europäischen Datenschutzes, der einen umfassenden und effektiven Schutz des Einzelnen in seinem Persönlichkeitsrecht verlange. Letzterer stelle wiederum nicht nur die Dispositionsfreiheit des US-Bürgers selbst, sondern auch die Freiheit der dortigen Gesellschaft und dritter Akteure in den Vordergrund, an persönlichen Daten schrankenlos teilhaben zu können.[35] Dass dieser Dissens in Zeiten des globalen Datenverkehrs zu Konflikten führen muss, ist bereits für sich genommen erwartbar. Zwei konkrete Besonderheiten verschärfen dies jedoch umso mehr.

31 Geschützt werden als personal informations „information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.", vgl. hier (Stand: 16.05.2022).
32 *Rippy*, Virginia passes the Consumer Data Protection Act, hier abrufbar, (Stand: 25.05.2022).
33 *Klosowski,* The State of Consumer Data Privacy Laws in the US (And Why It Matters), hier abrufbar (Stand: 25.05.2022).
34 Zur europäischen Dogmatik *Stark*, CTRL 1/2022, 87 ff.
35 Zur Unterscheidung *Lewinski,* Was Europa und die USA in Sachen Datenschutz unterscheidet, hier abrufbar (Stand: 25.05.2022).

1. General Protection vs. General Surveillance - die Ausgangslage

Wie bereits die Datenschutz-Richtlinie von 1995[36] (DS-RL) enthalten auch die geltenden Vorschriften Bestimmungen zum Transfer personenbezogener Daten in Nicht-EU-Länder, sog. Drittstaaten, Art. 44 ff.[37] Dabei gelten folgende Regeln: Mit dem Grundsatz der Gewährleistung eines angemessenen Schutzniveaus verlangt die DSGVO Geltung über die Grenzen der EU hinaus.[38] Statt der üblichen Lösung zwischenstaatlicher Rechtskollisionen über völkerrechtliche Vereinbarungen diktiert sie Drittstaaten ihren eigenen Datenschutzstandard als Maßstab. Dies entspricht zwar der generell protektiven Konzeption des EU-Datenschutzes, stellt aber den kommerziellen Datenverkehr vor erhebliche Herausforderungen.[39] Schließlich drohen bei Verstößen gegen die Art. 44 ff. Geldstrafen bis zu 20 Mio. € bzw. für Unternehmen bis zu 4 % des weltweit erzielten Jahresumsatzes, Art. 83 V lit. c.

Die andere Besonderheit liegt im US-Nachrichtendienstwesen. Im Gegensatz zur Inlandsüberwachung unterliegen auslandsnachrichtendienstliche Aktivitäten nicht den Anforderungen des vierten Amendments und auch nicht des ECPA. Rechtsgrundlage bezüglich der behördlichen Verarbeitung von Nicht-US-Bürgerdaten in den USA, und damit vor allem für die Überwachungsprogramme PRISM und UPSTREAM, ist der 1978 erlassene Foreign Intelligence Surveillance Act (FISA). Bereits seinerzeit mit großzügigen Eingriffsrechten der Behörden ausgestattet, erfuhr der FISA insbesondere nach 2001 noch weitere Anpassungen, welche die staatlichen Überwachungsbefugnisse erheblich ausgedehnt haben. Dass Dauer und Intensität der FIS-Eingriffe zumindest dem Zweck nach erforderlich und angemessen sein müssen, bleibt dabei die wichtigste materiellrechtliche Einschränkung.[40]



Zulässigkeitsprüfung der Drittstaatenübermittlung nach Art. 44-49 DSGVO

Nach Section 702 des FISA sind US-Telekommunikationsunternehmen gegenüber US-Sicherheitsdiensten ganz ohne richterliche Anordnung zur bedingungslosen Auskunft verpflichtet. Damit ist auch die Freigabe persönlicher Daten von Nicht-US-Bürgern aus Drittstaaten gemeint, soweit sie in die USA gelangen.[41] Zwar erfordern FIS-Maßnahmen die Zustimmung des FIS-Courts: einer Kammer aus unabhängigen Bundesrichtern, denen die US-Behörden gegenüber auskunftspflichtig sind. Allerdings genehmigt dieses Gericht nur die generelle Durchführung von Maßnahmen zu bestimmten Zwecken (zum Beispiel das Sammeln von Kontaktdaten deutscher Staatsbürger, die in Verbindung zu einem mutmaßlichen Terroristen stehen), nicht hingegen jede Datenerhebung oder -auswertung im Einzelfall.[42] Noch weitreichender zeigt sich die 1981 erlassene Executive Order 12333

36 Art. 25 der 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.
37 Alle Art. ohne weitere Bezeichnung sind solche der DSGVO.
38 Dieser heute in Art. 44 II kodifizierte Grundsatz ist dem EuGH-Urteil Schrems I geschuldet (s.u.). Art. 25 DS-RL zielte mit seiner *„Angemessenheit"* noch nicht auf die Gleichwertigkeit des Schutzniveaus ab, sondern ließ Qualitätsunterschiede der herrschenden Auslegung zufolge noch durchaus zu, vgl. *Rüpke/v. Lewinski /Eckhardt*, Datenschutzrecht. Grundlagen und europarechtliche Neugestaltung, 2018, 266 Rn. 13.
39 *Schweighofer*, Principles for US-EU Data Flow Arrangements, in: *Svantesson/Kloza*, Transatlantic data privacy relations as a challenge for democracy, 2017, 35.
40 *Solove/Schwartz*, Privacy Law Fundamentals, 2019, 57 ff.
41 *Karthäuser,* Und jetzt?, hier abrufbar (Stand: 25.05.2022).
42 CRS Report, EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield, 2021, 8 ff.

(EO 12333).[43] Präsident Reagan regelte darin die umfassenden Zugriffsrechte der US-Geheimdienste auf Nicht-US-Bürgerdaten außerhalb der USA. Denn dort entfaltet der FISA keine Wirkung und somit auch nicht seine Rechtsschutz- und Beschränkungsbestimmungen. Folglich ist der Zugriff auf persönliche Daten von Nicht-US-Bürgern, die auf dem Weg in die USA‘ sind, legal. Zudem ist er weniger Rechtsstaatsprinzipien unterworfen: Die EO 12333 kennt weder einen richterlichen Vorbehalt noch Einschränkungen über den Minimierungsgrundsatz hinaus.[44]

2. Transferabkommen, die Erste – Safe Harbor

Ihren ersten Angemessenheitsbeschluss i.S.d. heutigen Art. 45 I, III hinsichtlich den USA traf die Europäische Kommission im Jahr 2000, mit ihrer sog. Safe-Harbor-Entscheidung.[45] Dieser gingen jahrelange Verhandlungen mit der US-Administration voraus, weshalb auch von einem Abkommen die Rede ist. Einen völkerrechtlich verbindlichen Vertrag hat es indes nie gegeben.[46]

Nach Safe Harbor verpflichteten sich US-Unternehmen freiwillig, sieben bestimmte, an die Standards der DS-RL angelehnte Kriterien (‘Grundsätze’), sowie fünfzehn FAQs zu erfüllen und sich dabei der Kontrolle der FTC bzw. des US-Handelsministeriums zu unterstellen.[47] Dogmatisch erscheint es vertretbar, diese Bedingungen der Entscheidung als Garantie i.S.d. Art. 46 II[48] zu deuten.[49] Jedenfalls stellte die EuKOM die Angemessenheit des US-Datenschutzes bereits seinerzeit nicht bedenkenlos fest, ohne besondere Bedingungen an den Datentransfer zu stellen.

Bereits vor Schrems I wurde scharfe Kritik an der Entscheidung laut. Konkrete Anknüpfungspunkte waren maßgeblich die mangelhafte Überprüfung der Pflichtentreue[50], sowie die Tatsache, dass die Bestimmungen jedenfalls in der Praxis keine sonderliche Beachtung fanden.[51] Ganz erhebliche Kopfschmerzen bereitete, spätestens ab dem PRISM-Skandal 2015, zudem Abschnitt B des 4. Anhangs der Safe-Harbor-Abkommen. Dieser sah vor, dass “Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen (in den USA)“ stets Vorrang vor den Grundsätzen des Abkommens gehabt hätten. Dies bedeutet, dass US-Organisationen zur Datenweitergabe an US-Behörden verpflichtet blieben, auch wenn dies den Safe-Harbor-Anforderungen widersprach.[52] Oder ‚in a nutshell’: FISA brach Safe Harbor. Der EuGH traf in seinem Schrems I Urteil, angelehnt an Art. 25 DS-RL, nur wenige Aussagen zu den allgemeinen Anforderungen an ein Transferabkommen. Zunächst beschied er, dass ein “angemessenes Schutzniveau” zwar kein dem Unionsrecht identisches, wohl aber ein “der Sache nach Gleichwertig(es)” verlange, wobei die DS-RL sowie die GRCh als Maßstab gelten.[53] Diesem strengen Grundsatz folgend stellte er weiter fest, dass in Safe Harbor weder der Angemessenheit noch der Gewährleistung des Schutzniveaus Genüge getan wurde. Unangemessen

> „In a nutshell’:
> FISA brach Safe Harbor.“

erschienen die unbegrenzten US-dienstlichen Eingriffsrechte, welche das Abkommen sogar gänzlich verdrängen konnte.[54] Für eine ausreichende Gewährleistung fehle es wiederum sowohl an wirksamen Überwachungs- und Kontrollmechanismen bzgl. der praktischen Einhaltung der Selbstverpflichtungen,[55] als auch an hinrei-

43 Executive Order 12333, United States Intelligence Activities, hier abrufbar (Stand: 25.05.2022).
44 Übersicht zu den Ermächtigungen und Einschränkungen der EO 12333 hier abrufbar (Stand: 25.05.2022); zum verringerten Schutzniveau ggü. FIS-Maßnahmen vgl. EuGH, C-311/18, „Schrems II“, (Rn. 63, 183), hier abrufbar (Stand: 25.05.2022).
45 Dieser bezog sich, wie Privacy Shield, auf den Datentransfer privater Stellen. Der Datenaustausch zwischen Ermittlungsbehörden wurde in weiteren Abkommen wie dem Umbrella-Agreement v. 2015, dem PNR-Agreement v. 2016 sowie dem SWIFT-Agreement v. 2010 geregelt. Ersteres setzt zwar hohe Anforderungen, findet jedoch keine Anwendung auf privaten, insb. kommerziellen Datenverkehr, vgl. *Schweighofer,* Principles for US-EU Data Flow Arrangements, in *Svantesson/Kloza,* Transatlantic data privacy relations as a challenge for democracy, 2017, 38-40.
46 Ebd., 36.
47 *Paal/Pauly*, DSGVO u. BDSG, 3. Aufl. 2021, Rn. 9.
48 Zum Zeitpunkt des Safe-Harbor-Beschlusses geregelt in Art. 26 II DS-RL 95/46/EG.
49 So *Lewinski,* EuR 2016, 405 (408).
50 Mitteilung der Europäischen Kommission vom 27.11.2013, KOM (2013) 847 final(5).
51 BeckOK DatenschutzR BDSG aF/*Schantz,* § 4b, Rn. 32; *Schweighofer*, Principles for US-EU Data Flow Arrangements, in *Svantesson/Kloza*, Transatlantic data privacy relations as a challenge for democracy, 2017, 41.
52 EuGH, C-362/14, „Schrems I“, (Rn.86), hier abrufbar (Stand: 25.05.2022).
53 EuGH, C-362/14, „Schrems I“, (Rn.73), hier abrufbar (Stand: 25.05.2022).
54 EuGH, C-362/14, „Schrems I“, (Rn.86), hier abrufbar (Stand: 25.05.2022).
55 EuGH, C-362/14, „Schrems I“, (Rn.81), hier abrufbar (Stand: 25.05.2022).

chenden Rechtsschutzmechanismen bei bereits erfolgten, insbesondere staatlichen Eingriffen.[56] Generell habe die Kommission keine ausreichende Prüfung des US-Rechts vorgenommen. Diese Annahme genügte dem Gericht, um die Entscheidung der EuKOM, und damit die Rechtsgrundlage für einen beträchtlichen Teil des EU-US-Datentransfers, für insgesamt unwirksam zu erklären.[57]

3. Transferabkommen, die Zweite - Privacy Shield

Unter entsprechendem Druck trat, nur wenige Monate nach Schrems I und wiederholten Verhandlungen mit US-Vertretern, am 12.07.2016 das Privacy-Shield-Abkommen in Kraft. In sechs Artikeln, sieben Annexen und 155 Erwägungsgründen bemühte man sich, die wenigen Vorgaben aus Schrems I zufriedenstellend umzusetzen. Dabei hielten auch zahlreiche Erklärungen von US-Regierungsvertretern Einzug, die als mehr oder weniger verbindliche Versprechen gedeutet werden konnten. Während die materiellen Anforderungen Safe Harbors nunmehr als „Principles" in Privacy Shield weitestgehend übernommen wurden,[58] erfuhren Kontrolle und Rechtsschutz einige Erweiterungen. Dies entsprach der Gewichtung des Urteils. Hierfür war zum einen eine dem US-Außenministerium unterstellte Ombudsperson[59] vorgesehen, die auf Antrag europäischer Stellen hin tätig werden und mögliche Rechtsverletzungen prüfen sollte.[60] Zum anderen wurde ein verschärftes Kontrollrecht des US-Handelsministeriums und der FTC zugesichert, sowie eine beschränkte Klagebefugnis für Nicht-US-Bürger eingeführt.[61] Darüber hinaus wurden schriftliche Zusicherungen von US-Sicherheitsbehörden beigefügt, die Überwachungsaktivitäten gegenüber EU-Bürgern einzuschränken. Dabei spielte insbesondere ein Verweis auf die Presidential Policy Directive 28 (PPD-28) eine gewichtige Rolle. In letzterer wies der damalige Präsident Obama die US-Sicherheitsdienste unter anderem an, Ausländerüberwachungen nur auf einer rechtlichen Grundlage gestützt, auf das erforderliche und notwendige Maß beschränkt und nicht zu Zwecken der Diskriminierung von Meinungen und Personengruppen durchzuführen.[62]

Doch auch damit zeigte sich der bereits vor dem Erlass angerufene EuGH nicht zufrieden. Dabei wurde er in seiner Begründung zwar ausführlicher, in der Sache blieben die Kritikpunkte jedoch identisch. Erwartbar war die Bemängelung jener Klauseln, die den Sicherheitsinteressen der USA wiederholt Vorrang vor Privacy Shield einräumten. Diese fanden sich, trotz Schrems I, nahezu unverändert im neuen Abkommen wieder.[63] Auch gewährleiste der FISA zu wenig Einschränkungen der Datenzugriffs- und -verarbeitungsrechte und lege weder den Umfang noch die Tragweite der Überwachung fest. Damit fehlte es wiederholt an der Angemessenheit des Schutzniveaus.[64] Dies könne auch nicht durch die PPD-28 kompensiert werden: Zum einen räume diese betroffenen EU-Bürgern keine eigenen Rechte ein, wie es die Angemessenheit nach Art. 45 II lit. a verlange. Zum anderen gestatte sie Massendatenerhebungen, die einen hinreichenden Individualschutz erst gar nicht ermöglichen würden.[65] Auch der Ombudsmechanismus wurde bemängelt: Der Ombudsmann könne schon aufgrund seiner Abhängigkeit vom US-Außenministerium und der fehlenden Weisungsbefugnis gegenüber den Sicherheitsdiensten keinem gerichtlichen Kontrollorgan gleichkommen, wie es die DSGVO vorsehe.[66] Die altbekannte Folge: Unwirksamkeit des gesamten Beschlusses.[67]

4. Letzte Bastion - Standardvertragsklauseln

Ist nun jeder Datentransfer von hier nach Übersee rechtswidrig? Nein. Wie aus Abbildung 2 hervorgeht, verbleiben zwei Rechtfertigungsmöglichkeiten trotz Fehlen eines wirksamen Angemessenheitsbeschlusses. Art. 46 I erlaubt die genehmigungsfreie Übermittlung, soweit die EU-ansässigen Verantwortlichen in Kooperation mit ihren Partnern im Drittland geeignete Garantien schaffen, die

56 EuGH, C-362/14, „Schrems I", (Rn.89), hier abrufbar (Stand: 25.05.2022).
57 EuGH, C-362/14, „Schrems I", (Rn.98, 105), hier abrufbar (Stand: 25.05.2022).
58 Hier abrufbar (Stand: 16.05.2022).
59 Ombudsman ist eine unparteiische Schiedsperson; vgl. auch *Heinzke*, GRUR-Prax 2022, 436, 437.
60 *Brauneck*, EuZW 2020, 933, 935, hier abrufbar (Stand 25.05.2022).
61 Durch den 2016 erlassenen „Judicial Redress Act" (JRA), der jedoch nur gilt, soweit es um Strafverfolgungen geht, vgl. *Lewinski,* EuR 2016, 405 (414).
62 Auswahl von Maßnahmen des US-Gesetzgebers und der US-Regierung in Bezug auf die Überwachungstätigkeit der US-Geheimdienste seit Sommer 2013, BT-WD 3 - 3000- 150/15, S.6, hier abrufbar (Stand 25.05.2022).
63 EuGH, C-311/18, „Schrems II", (Rn.163 f.), hier abrufbar (Stand: 25.05.2022).
64 EuGH, C-311/18, „Schrems II", (Rn.176, 180), hier abrufbar (Stand: 25.05.2022).
65 EuGH, C-311/18, „Schrems II", (Rn.181, 183 f.), hier abrufbar (Stand: 25.05.2022).
66 EuGH, C-311/18, „Schrems II", (Rn.190 ff.), hier abrufbar (Stand: 25.05.2022).
67 EuGH, C-311/18, „Schrems II", (Rn.199), hier abrufbar (Stand: 25.05.2022).

das mangelhafte gesetzliche Schutzniveau vertraglich kompensieren. Um nun nicht jedwede Verantwortung auf die Verarbeiter abzuwälzen, hat die EuKOM bereits vor langem Musterverträge, sog. Standardvertragsklauseln (SVK) i.S.d. Art. 6 II lit c, vorgegeben.[68] Durch sie verpflichten sich die Verarbeiter dies- und jenseits des Atlantiks, freiwillig Datenschutzmaßnahmen einzuhalten, die den strengen Anforderungen der DSGVO genügen. Andernfalls drohen Unterlassungs- und Schadensersatzansprüche. So gilt nach Klausel 8 der SVK bspw. das Zweckbindungs-, Transparenz- und Richtigkeitsgebot.[69]

Die gute Nachricht: der EuGH hat die SVK in ihrer bestehenden Form grundsätzlich für zulässig erklärt.[70] Allerdings sei der Verantwortliche verpflichtet, vorab das Schutzniveau des Drittlands nach den Umständen des Einzelfalls zu überprüfen. Sollte er zu dem Ergebnis kommen, dass es nicht angemessen sei, habe der Datenexporteur den Transfer auszusetzen, der Importeur die bereits übermittelten Daten sogar zu vernichten.[71] Ende 2021 erneuerte daraufhin die EuKOM die SVK und führte Klausel 14 und 15 ein. Letztere sieht vor, dass der Datenimporteur im Falle eines Auskunftsersuchens von US-Behörden diese auf ihre Rechtmäßigkeit hin zu prüfen, den Exporteur und den Betroffenen zu informieren und gegen das Ersuchen vorzugehen hat. In Klausel 14 ist wiederum die oben genannten Prüfungspflicht statuiert, das sog. Transfer Impact Assessment (TIA). In dieser sind die geltenden Rechtsvorschriften und Gepflogenheiten des Drittstaates zu berücksichtigen. Dabei legen Wortlaut und Begründung[72] nahe, dass auch eine evidenzbasierte Risikoberechnung erfolgen darf. Es könnte also genügen, dass nur die Wahrscheinlichkeit eines behördlichen Datenzugriffs nachweislich gering ist, auch wenn er rechtlich möglich ist.[73] Hierfür wurden bereits eigene mathematische Verfahren entwickelt, um eben diese Risikobestimmung zu ermöglichen.[74] Neben erheblichen praktischen Problemen der Quantifizierung stellt sich dabei aber die drängende Frage, ob dies als "der Sache nach gleichwertig" zum europäischen Schutzniveau gelten darf. Denn auch das geringe Risiko eines nach der DSGVO unrechtmäßigen Zugriffs wird, so er nach US-Recht legal wäre, dem Unionsrechtsstandard nicht gerecht. Eben diese Streitfrage bietet echtes Potenzial für ein Schrems-III-Urteil.[75] Zudem können EU-Aufsichtsbehörden SVKs jederzeit kippen, sollten ihnen Zweifel am angemessenen Schutzniveau aufkommen.[76]

Ohne SVK verbleibt nur noch die ausnahmsweise Rechtfertigungen nach Art. 49, der jedoch für spezifische Einzelfälle konzipiert wurde und daher für den relevanten Massendatenverkehr keine geeignete Rechtsgrundlage darstellt.

B. Über den Nutzen globaler Regeln auf globalen Märkten - Conclusion

Es ist unumstößlich: Der EU-US-Datentransfer benötigt einen wirksamen Angemessenheitsbeschluss der EuKOM. Eine Abwälzung von Prüfungspflicht und Haftung auf Verantwortliche i.S.d. DSGVO mittels Standardvertragsklauseln geht nicht nur mit einer erheblichen Belastung für zahlreiche Private, insb. kleine u. mittelständische Unternehmen, einher: Sie steht auch, wie gezeigt, auf tönernen Füßen. Dies gilt vor allem dann, wenn es um die hochrelevanten Massendatenübermittlungen an Dienstleister wie Meta Platforms (früher: Facebook) oder Alphabet geht. Denn gerade diese Unternehmen unterliegen nach FISA Section 702 und der EO 12333 jenen staatlichen Zugriffsrechten, die nicht nur nach US-Recht durchaus möglich, sondern nur schwerlich vertraglich abdingbar sind. Von der prinzipiellen Kontrollproblematik unüberschaubarer Datenströme mal ganz zu schweigen. Eine Unterbrechung der Datentransfers hätte wiederum ungeahnte wirtschaftliche Schäden zur Folge.[77] Was also ist die Lösung des Problems? Hält man die aufgezeigten Widersprüche zwischen dem EU-Datenschutz und dem US-Privacy-Kon-

68 *Scholl*, Die neuen Standardvertragsklauseln: Eine Bestandsaufnahme, hier abrufbar (Stand: 25.05.2022).
69 Aktuelle Fassung hier abrufbar (Stand: 25.05.2022).
70 EuGH, C-311/18, „Schrems II", (Rn. 148), hier abrufbar (Stand: 25.05.2022).
71 EuGH, C-311/18, „Schrems II", (Rn. 142 ff.), hier abrufbar (Stand: 25.05.2022).
72 *„Zur Ermittlung der Auswirkungen derartiger Rechtsvorschriften und Gepflogenheiten auf die Einhaltung dieser Klauseln können in die Gesamtbeurteilung verschiedene Elemente einfließen. Diese Elemente können einschlägige und dokumentierte praktische Erfahrungen im Hinblick darauf umfassen, ob es bereits früher Ersuchen um Offenlegung seitens Behörden gab, die einen hinreichend repräsentativen Zeitrahmen abdecken, oder ob es solche Ersuchen nicht gab. […] Sofern anhand dieser praktischen Erfahrungen der Schluss gezogen wird, dass dem Datenimporteur die Einhaltung dieser Klauseln nicht unmöglich ist, muss dies durch weitere relevante objektive Elemente untermauert werden."*, vgl. hier (Stand: 25.05.2022).
73 Zur Deutung der Begründung *Diercks/Roth*, Data Transfer to unsafe Third Countries, hier abrufbar (Stand: 16.05.2022).
74 *Kötter*, Drittland Übermittlung: Leitfaden zu Transfer Impact Assessments, hier abrufbar (Stand: 25.05.2022).
75 So in: EU-Kommission verabschiedet DSGVO-Standardvertragsklauseln, hier abrufbar (Stand: 25.05.2022).
76 *Karthäuser*, Und jetzt?, hier einsehbar (Stand: 25.05.2022).
77 Nach einer Studie des *ECIPE* aus 2013 hätte das BIP der EU seinerzeit durch eine Unterbrechung des kommerziellen Datentransfers in die USA um bis zu 1,3 % zusammenbrechen können, vgl. *ECIPE*, The Economic Importance of getting Data Protection Right, 2013, 3.

zept für unüberwindbar, verbleibt nur noch eine Option: eine ausschließlich auf europäischem Boden stattfindende Verarbeitung von EU-Bürgerdaten, gänzlich umschlossen vom Schutzbereich der DSGVO. So fordern es auch Schrems und seine Organisation NOYB.[78] Ob dieser radikale Einschnitt indes erforderlich ist, erscheint zweifelhaft. Zunächst einmal ist festzustellen, dass sowohl die USA als auch die EU demokratische Rechtsstaaten sind.[79] Wenn schon die Kollision zwischen diesen beiden Rechtsräumen nicht gelöst werden kann, wie soll es dann erst mit anderen Handelspartnern, insbesondere aus Südostasien gelingen, denen der westliche Persönlichkeitsschutz oftmals gänzlich fremd ist?[80] Solche Begegnungen sind jedoch in Zeiten des notwendigerweise globalen Datenverkehrs unvermeidbar. Dies wirft die Frage auf, ob die strenge Angemessenheitskontrolle des EuGH bezüglich Drittstaaten überhaupt weiter Bestand haben kann oder sollte.[81] Auch empirische Erhebungen zur wirtschaftlichen Wirkung des Datenschutzes zeigen, dass strengere Regeln den Freihandel sowie die Produktivität insbesondere mittelständischer Unternehmen erheblich beeinträchtigen.[82]

Reformbedarf besteht also hier wie da. Einige Probleme sind, wie aufgezeigt, systemspezifisch. In den USA sind dies vor allem die Unvollständigkeit des Datenschutzes, die damit eröffnete Möglichkeit der anlasslosen staatlichen Massenüberwachung und Rechtsunsicherheiten aufgrund des sektoralen Ansatzes, sowie die in den einzelnen Bundesstaaten divergierenden Rechtslagen. In der EU bereiten wiederum mangelnde Flexibilität, teils enorme bürokratische Anforderungen sowie die Wachstums- und Wettbewerbsbeeinträchtigung durch die DSGVO Kopfschmerzen.[83] Ob nun nach europäischer Opt-In- oder kalifornischer Opt-Out-Lösung: in beiden Fällen handeln Betroffene, Studien zufolge, alles andere als rational. Meistens sind sie von Datenschutzaufklärungen überfordert und widersprechen in ihren Handlungen den zuvor angegebenen Intentionen.[84] Man denke nur an die eigenen Erfahrungen mit sog. ‘Cookie-Bannern’ auf diversen Webseiten.

Die wirksamste Lösung für alle genannten Herausforderungen wäre also die Einführung eines gemeinsamen, optimierten Datenschutzstandards. Durch diesen würden nicht nur endlich Rechtssicherheit und wettbewerbsfreundliche Bedingungen zwischen den USA und der EU geschaffen werden.[85] Man könnte dies zum Anlass nehmen, die in beiden Rechtsregimen bekannten rechtlichen und tatsächlichen Mängel anzugehen. Hierbei könnten die USA von der EU lernen, wie Einheitlichkeit, effektive Kontrolle und auch Abwehrrechte im Datenschutz gewährleistet werden können. Umgekehrt kann die US-amerikanische Ausdifferenzierung des Datenbegriffs mehr Flexibilität in die starre DSGVO bringen. Gemeinsam könnten Konzepte entwickelt werden, die die gemeinsamen Probleme der Effektivität und der ungewollten Folgen lösen. Traumtänzerei muss dies langfristig nicht bleiben: der zunehmende Druck des EuGH, die weiterhin enorme wirtschaftliche Bedeutung des transatlantischen Handels und nicht zuletzt die Internationalität des Datenverkehrs per se lassen einen multilateralen Standard naheliegend erscheinen. Die Hürden bleiben indes hoch: hier wie da müssten mittels umfangreicher Reformen gesetzgeberische Kompromisse gemacht werden. Der Wille dazu ist auf beiden Seiten noch nicht erkennbar. Naheliegender erscheint ein bilateraler Vertrag, der die DSGVO-Anforderungen bindend erfüllt, ohne die Substanz des US-Rechts zu tangieren. Auf diesem Weg könnten gezielt für persönliche Daten von EU-Bürgern verbindliche völkerrechtliche Vertragsrechtsstandards eingeführt werden, die (auch) die USA zu berücksichtigen haben. Diese könnten überdies, im Gegensatz zum Administrativrecht der US-Regierung (wie im Privacy Shield vorgesehen) nicht ohne weiteres aufgehoben werden und wären daher erheblich standfester als die bisherigen Regelungen.[86]

78 So Schrems gegenüber *WELT* am 16.07.2020, hier abrufbar (Stand 25.05.2022).
79 So auch *Swire,* US Surveillance Law, Safe Harbour and Reforms since 2013, in *Svantesson/Kloza,* Transatlantic data privacy relations as a challenge for democracy, 2017, 86 ff.; sowie: Why U.S. Surveillance Law Protections Are Better Than Europe Thinks, 2015, hier abrufbar (Stand: 25.05.2022).
80 So auch *Lewinski*, Was Europa und die USA in Sachen Datenschutz unterscheidet, hier abrufbar (Stand: 25.05.2022).
81 Derzeit gewährleisteten nach Feststellung der Europäischen Kommission nur Andorra, Argentinien, die Schweiz, die Färöer-Inseln, Guernsey, Isle of Man, Jersey, Neuseeland und Uruguay sowie eingeschränkt Kanada und Israel das nach Art. 45 I erforderliche Schutzniveau, vgl. *Kühling/Klar/Sackmann:* Datenschutzrecht. 5. Aufl. 2021, 251 Rn. 59; andererseits geht die Theorie des sog. Brussels Effect davon aus, dass sich internationale Rechtsordnungen zunehmend dem Standard des EU-Rechts anpassen werden, *vgl. Bradford,* The Brussels Effect, 107 Nw. U. L. Rev.1-67, 2012.
82 *ECIPE,* The Cost of Data Protection, 2018, hier abrufbar (Stand 25.05.2022).
83 Dazu *Stark,* CTRL 1/2022, 95 ff.
84 *Acquisti/Grossklags,* Privacy and Rationality, in: Strandburg/Raicu, Privacy and Technologies of Identity, 2008, 15, 17 f, 27; *Nissenbaum*, Privacy in Context, 2010, 129 ff.
85 So auch, wenngleich auf die Regulierung von Profilbildung- und nutzung durch soziale Netzwerke beschränkt, *Kühnl,* Persönlichkeitsschutz 2.0: Profilbildung und -nutzung durch soziale Netzwerke am Beispiel von Facebook im Rechtsvergleich zwischen Deutschland und den USA, 2016, 314 f., 316.
86 So *Schweighofer,* Principles for US-EU Data Flow Arrangements, in Svantesson/Kloza, Transatlantic data privacy relations as a challenge for democracy, 2017, 44 f.

Am 25. März 2022 erklärten US-Präsident Biden und EU-Kommissionspräsidentin von der Leyen in einer gemeinsamen Pressekonferenz in Brüssel, dass ein neues Datentransferabkommen abgeschlossen worden sei.[87] Die Ausgestaltung ist derzeit noch unbekannt. Zwei Erfahrungssätze aber haben die Parteien aus dem bisher Geschehenen in jedem Fall zu berücksichtigen: beschränkt verbindliche Transferabkommen mit Hintertüren für US-Nachrichtendienste und beeinträchtigtem Rechtsschutz werden nach Unionsrecht auch künftig unwirksam bleiben. Zum anderen: sollte eine – durchaus wünschenswerte – Reform des Datenschutzrechts dies- oder jenseits des Atlantiks doch einmal zur Debatte stehen, führen wir sie am besten gemeinsam.

Talking Legal Tech – Folge 28

„Regulierung & Innovation - wie lässt sich beides vereinbaren, Martin Ebers?“

Zurück zum Inhaltsverzeichnis

87 Vgl. die Erklärung der Präsidentin *von der Leyen* mit US-Präsident Biden vom 25.03.2022, hier abrufbar (Stand: 25.05.2022).

CTRL

2/22
2. Jahrgang, 1. Ausgabe
www.legaltechcologne.de/ctrl

Cologne Technology
Review & Law

Hier geht es zur ganzen Ausgabe!

Reise in 15 Beiträgen durch die Legal-Tech-Welt:

Von Kolumbien bis nach Finnland
und von Compliance bis eSport.

LEGAL TECH LAB
COLOGNE