Internationaler Datentransfer zwischen der EU und den USA

Rechtliche und technische Anforderungen auf europäischer und US-amerikanischer Ebene

Inauguraldissertation
zur Erlangung des Grades eines Doktors des Rechts
durch die
Rechts- und Staatswissenschaftliche Fakultät der Rheinischen
Friedrich-Wilhelms-Universität Bonn

vorgelegt von

Dr. Bagauri Tatia

aus Tiflis / Georgien

2024

Dekan: Gez. Professor Dr. Jürgen von Hagen
Erstreferent: Prof. Dr. Michael Loschelder
Zweitreferent: Prof. Dr. Louisa Specht-Riemenschneider
Tag der mündlichen Prüfung: 19.04.2024

Meinem Großvater
zur Erinnerung

Vorwort

Das Thema „Internationaler Datentransfer“, das auf das XVII. und XVIII. Jahrhundert zurückgeht, war noch nie so wichtig wie heute. Weltweite Anstrengungen tragen eine ausgezeichnete Arbeit bei und vereinfachen viele Prozesse. Trotzdem gibt es sehr viele Hindernisse, die berücksichtigt sowie analysiert werden sollten, damit der internationale Datentransfer rechtmäßig und reibungslos funktioniert. Aus diesem Grund wird diese Monographie angefertigt und als Dissertationsschrift an der Reinischen Friedrich-Willhems-Universität Bonn angenommen.

Die Erstellung dieser Arbeit zugrunde liegt die hervorragenden Betreuung durch meinen Doktorvater Prof. Dr. Michael Loschelder, der mir stets wertvolle Ratschläge gab und mich über zwei Jahre begleitete, was mir ermöglichte, diese Dissertation bestmöglich zu erstellen. Frau Prof. Dr. Specht-Riemenschneider betreute meine Dissertation als Zweitgutachterin, was ich ebenfalls sehr schätze.

Bedanken möchte ich mich auch bei meinen ehemaligen Kollegen Cornelia Sasse, Dr. Florian Wrobel, Jan-Henning Evers und Kyle Duncan, mit denen ich Interviews geführt habe, durch die ich wichtige Inhalte erhalten habe, um das Thema bestmöglich zu überarbeiten und sehr praxis-orientierte Lösungen herauszufinden. Ein besonderer Dank gilt für Frau Sasse, die mir immer zur Seite stand, um mich auch in der Praxis im Bereich des Datenschutzes anzuleiten. Dies hat es mir ermöglicht, mein theoretisches Wissen und meine juristischen Recherchen während des Promotionsstudiums in die Praxis umzusetzen.

Anschließend möchte ich meiner Familie von Herzen danken, die immer an meiner Seite steht und sich immer für meinen Erfolg begeistert. Ein besonderes Dankeschön an meinen Vater, Avtandil Bagauri, dessen Unterstützung und Rückhalt es mir überhaupt ermöglicht, diesen Weg zu gehen.

Mai 2024 Dr. Tatia Bagauri

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs. ……..	Absatz / Absätze
Abschn. …….	Abschnitt
AEMR ……..……....	Allgemeine Erklärung der Menschenrechte von 10.12.1948
AEUV……	Vertrag über die Arbeitsweise der Europäischen Union
AMRK…….……..	Amerikanische Menschenrechtskonvention von 22.11.1969
Art.……	Artikel/Article
Artt. ……..	Artikel / Articles
Aufl. …….	Auflage
AWS ……...	Amazon Web Services
BDSG ……...……	Bundesdatenschutzgesetz
Bd. ……	Band
BGB ...……..	Bürgerliches Gesetzbuch
BGH …….	Bundesgerichtshof
BKA……..	Bundeskartellamt
BRJ ……...	Bonner Rechtsjournal
BSI…….	Bundesamt für die Sicherheit in der Informationstechnik
bzw. ……	beziehungsweise
Cal. Civ. Code. ….……	California Civil Code
CCPA …….……..	California Consumer Privacy Act of 2018
CEO …….	Chief Executive Officer
Cir. ……	Circuit
CISA …….	Cybersecurity and Infrastructure Security Agency
CISO ……	Chief Information Security Officer
CLOUD Act …….	Clarifying Lawful Overseas Use of Data Act
CLPO ……...	Civil Liberties Protection Officer
CoC ……..	Code of Conduct
CPRA ……...	California Privacy Rights Act
CR ……...	Computer und Recht
CSIRT ……..	Computer Security Incident Response Team
CTO …….	Chief Technology Officer
DDOS ……..	Distributed-Denial-of-Service
DLP …….	Data Leakage Prevention / Data Loss Prevention
DORA……...	EU Digital Operational Resilience Act
DOS …….	Denial-of-Service
DPF ……..……	Data Privacy Framework
DPRC…….....	Data Protection Review Court
DSK ……..	Datenschutzkonferenz
DSGVO / GDPR ..……..….	Verordnung (EU) 2026/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogene Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG
d. h. ...……..	das heißt

ECPA……	Electronic Communications Privacy Act of 1986
EDPB……...	European Data Protection Board
EMRK……...	Europäische Menschenrechtskonvention von 03.09.1953
ENISA……...	European Union Agency for Cybersecurity
ErwGr. ……..……	Erwägungsgrund
EU / E.U. ……...…..	Europäische Union / European Union
EUGH ……...……	Europäische Gerichtshof
EWR ……	Europäischer Wirtschaftsraum
E. O. …….	Executive Order
FBI……	Federal Bureau of Investigation
ff. ……..	folgend
FISA……..	Foreign Intelligence Surveillance Act
FISMA……..	Federal Information Security Management Act of 2002
FTC ……..	Federal Trade Commission
gem. ……..……	gemäß
ggf. ……..	gegebenenfalls
GPP …….	OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980
GrCh ……...……..	Charta der Grundrechte der Europäische Union, 2000/C 364/1
GSM ……	Global System for Mobile Communication
HIPAA ……..……	Health Insurance Portability and Accountability Act
Hrsg. ……..……...	Herausgeber
Hs. ……...…….	Halbsatz
iapp ……..	The International Association of Privacy Professionals
IDPL……..	International Data Privacy Law
IEC……	International Electrotechnical Commission
IpbpR ……	Der Internationalen Pakt über bürgerliche und politische Rechte von 19.12.1966
ISB……	Informationssicherheitsbeauftragter
ISMS……..……..	Information Security Management System
ISO…….....	International Organization for Standardization
IT …….	Information Technology
lit. ……..……..	littera
MLAT……...	Mutual Legal Assistance Treaty
m. E. ……	meines Erachtens
NSA …….	U.S. National Security Agency
NIST……..	The National Institute of Standards and Technology

NIS-2-Richtlinie ……..…….	Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union
Nr. …….……..	Nummer
OECD ……..	The Organisation for Economic Co-operation and Development
OIA ……..	Office of International Affairs
PDCA……	Plan-Do-Check-Act
PPD-28 ……	Presidential Policy Directive 28
Rev. …….	Revision
RMF …….	Risk Management Framework
Rn. ……..…….	Randnummer(n)
SCA……...	US Stored Communications Act von 1986
sog. ……..	sogenannte(r)
SP …….	Special Publication
SWP …….	Stiftung Wissenschaft und Politik
S. ……..	Satz / Seite
s. ……..……	siehe
TOM ……	technische und organisatorische Maßnahmen
UN ……...	United Nation / Vereinigte Nationen
Urt. …….…….	Urteil
USA Freedom Act…….	Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015
USA PATRIOT Act ……...	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
u. a. …..……..…..	unter anderem
US / USA / U.S. ……..	United States
U.S. Const. ……..……	The Constitution of the United States of America of 17.09.1787
U.S.C. ……..	United States Code
Vers. ……	Version
VPN …….	Virtual private network
VV. ……..	Verse
v. ……..…….	von / vom
v. / vs. ……..	versus
vgl. ……..…….	vergleich(e)
V.S.A ……...	Vermont Statutes Annotated
WLAN…….	Wireless Local Area Network
WP ……..…….	Working Paper / Arbeitspapiere der Art. 29-Datenschutzgruppe
zit. ……...	zitiert
z. B. …..……..	zum Beispiel

1 Einleitung

„Einige frühe Käufer beschwerten sich über Defekte wie nicht richtig ausfahrende Türgriffe oder Scheibenwischer mit einem irren Tempo. Bei einem so teueren Auto war das unentschuldbar, doch Tesla kümmerte sich meist mit intelligenter Effizienz darum. Während der Besitzer schlief, griffen Tesla-Ingenieure über die Internetverbindung auf das Auto zu und spielten Software-Updates auf. Wenn der Kunde dann morgens eine Runde drehte und plötzlich alles funktionierte, hatte er das Gefühl, magische Elfen hätten sein Auto repariert."[a]

Das Hindernis, auf das Tesla stieß, sowie die daraus resultierende Lösung brachten den Besitzer, die Tesla-Ingenieure und Software-Updates zusammen. Wenn im Auto softwaremäßig alles in Ordnung war, war das Auto in Ordnung und der Besitzer glücklich. Was kann das aber bitte mit dem antiken Theater, mosaischen Gesetzen und Binärsystem zu tun haben? Wahrscheinlich gar nichts? – Die Antwort ist ja; sie haben viel gemeinsam.

Das Wort „Persönlichkeit" hatte im Lateinischen eine Bedeutung, die den Charakter eines Akteurs beschrieb. Der Charakter einer Person umfasste damals wie heute Aspekte wie ihre Rolle, ihren Status sowie Würde. All dies schuf bzw. schafft eine Gemeinsamkeit von Informationen, die eine Person beschrieben bzw. beschreiben und ihr die Möglichkeit gaben bzw. geben, sich zu entwickeln und ihr Leben nach ihren Wünschen und Vorstellungen zu führen: Damals in den antiken Theatern und heute im Besitz des Tesla.

Persönlichkeit ist das höchste Gut einer Person, das zur freien Entfaltung dieser ebenso gehört wie die Menschenwürde. Um dies zu ermöglichen, wurden erste Grundsätze niedergeschrieben, wie Menschen miteinander umgehen sollten: Die mosaischen Gesetze.

Hat sich das Leben durch technologische Entwicklungen und die daraus resultierenden wirtschaftlichen und sozialen Veränderungen weiterentwickelt, reichten diese handschriftlichen Gesetze nicht mehr aus, und es war die Rede von den verbindlichen Manifestationen der Normen, die sowohl von jedem Einzelnen als auch von der Stadt zu beachten waren. Heutzutage ist der Schutz personenbezogener Daten ein wesentlicher Bestandteil einer nachhaltigen Demokratie, die die Grundrechte und -freiheiten natürlicher Personen schützen sollte.

1 *Vance*, Tesla, PayPal, SpaceX: Wie Elon Musk die Welt verändert – Die Biografie, S. 242.

Das Binäresystem, das auf das XVII. / XVIII. Jahrhundert zurückgeht, hat die technologische Entwicklung beschleunigt. Im XX. Jahrhundert wurden Daten zum ersten Mal digital übertragen. Die digitale Datenübertragung hält derzeit in allen Bereichen Einzug, sei es im täglichen Leben, in der nationalen sowie internationalen Sicherheit, in der Wirtschaft oder darüber hinaus. Dies schafft eine Lage, die sowohl rechtlich als auch technisch geregelt und gesichert werden muss. In diesem Zusammenhang kommt IT-Unternehmen bzw. IT-Dienstleistern oder Cloud-Service-Anbietern eine besondere Bedeutung zu.

Im heutigen Alltag ist die Datenverarbeitung bzw. der Datentransfer sehr oft eine internationale Angelegenheit und hat zunehmend eine grenzüberschreitende, extraterritoriale Wirkung. Sie kennt keine internationalen Grenzen mehr und steht vor rechtlichen Herausforderungen, die in einem internationalen Kontext besonders ausgeprägt sind und in der globalen digitalen Wirtschaft eine zentrale Rolle spielen.[2] Der Datenfluss über bestehende nationale Grenzen hinweg, zwischen privaten und staatlichen Stellen oder zwischen verschiedenen nationalen, supranationalen sowie internationalen Behörden ist heute an der Tagesordnung.[3]

Laut dem europäischen Parlament werden derzeit ,,am meisten Daten zwischen der EU und den USA ausgetauscht".[4] Laut dem White House ist der transatlantische Datenverkehr für die 7,1 Billionen Dollar schweren Wirtschaftsbeziehungen zwischen der EU und den USA von entscheidender Bedeutung.[5] Die meisten Computer-Dienstleister sind Amerikaner und dadurch ein besonders wichtiger Partner für die EU.[6]

Der (internationale) Datentransfer spielt u. a. im Strafverfahren eine wichtige Rolle. Vor dem Aufkommen des Cloud Computing waren Beweise für Straftaten in der Regel nur innerhalb des Hoheitsgebiets des ersuchenden Landes verfügbar.[7] Heute werden beispielsweise die Inhalte von E-Mails oft in einem anderen Land gespeichert.[8] Eine Studie der EU-Kommission aus dem Jahr 2018 ergab, dass in etwa 85 % aller strafrechtlichen Ermittlungen elektronische Beweise benötigt werden, und in zwei Dritteln dieser Fälle müssen die Beweise von Online-Dienstleistern mit Sitz in einem anderen Land beschafft werden.[9]

2 *Voigt/von dem Bussche*, EU-Datenschutz-Grundverordnung (DSGVO), S. 1; *Bagauri*, BRJ 01/2022, 1, 43.
3 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 37.
4 Europäisches Parlament, 4. Arbeitsdokument (A), 11.03.2019, S. 2.
5 FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework, abrufbar: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/, zuletzt abgerufen am 02.08.2023.
6 *Christakis/Terpan*, IDPL, Vol. 11, Nr. 2, 81, 89.
7 *Christakis/Terpan*, IDPL, Vol. 11, Nr. 2, 81, 85.
8 *Christakis/Terpan*, IDPL, Vol. 11, Nr. 2, 81, 85.
9 *Christakis/Terpan*, IDPL, Vol. 11, Nr. 2, 81, 85.

Der digitale Datentransfer ist ein sehr hilfreiches Instrument, ist jedoch mit vielen Hindernissen verbunden. Rechtswidrige Datenverarbeitung, behördliche Aufforderungen zur Datenweitergabe bzw. -offenlegung und Hackerangriffe sind nur einige Beispiele davon. Die Globalisierung der strafrechtlichen Beweismittel sowie der einfache Zugang zu diesen Daten stellt die große Herausforderung dar. Den Zugang zu personenbezogenen Daten bekommen US-Behörden und Geheimdienste wie FBI manchmal „over a few beers".[10] Sie verlangen, dies auch z. B. durch den Einbau einer Hintertür / „Backdoor" in ein Betriebssystem zu erreichen, wie im Fall von Apple geschehen (United States vs. New York Telephone Co.)[11] Hinzu kommen die Sorge und der Verdacht, dass kommerziell lukrative Daten aus der EU auch auf amerikanischer Seite abgegriffen werden können.[12]

Darüber hinaus erlassen Länder Gesetze und Vorschriften für den digitalen Bereich, die die Datenverarbeitung sowohl innerhalb als auch außerhalb ihrer Landesgrenzen beeinflussen[13] (die extraterritoriale Wirkung). Die Ansichten über die Bedeutung des Schutzes der Privatsphäre unterscheiden sich von Land zu Land, was größtenteils auf die kulturellen Unterschiede zwischen den Regionen zurückzuführen ist.[14] Die Datenverarbeitung unterliegt verschiedenen Rechts- und Verwaltungsvorschriften, die miteinander in Konflikt stehen oder sich gegenseitig beeinträchtigen können.[15] Auf dem Weg zu einer globalen Wirtschaft wird es daher immer wichtiger, die Unterschiede in den Gesetzen zu verstehen und in Einklang zu bringen, die zwar nationalen Ursprungs sind, aber internationale Auswirkungen haben.[16] Neben der Wirtschaft wird dies auch die nationale Sicherheit sowie die Rechte und Freiheiten jedes Einzelnen gewährleisten.

10 How an app to decrypt criminal messages was born 'over a few beers' with the FBI, abrufbar: https://theconversation.com/how-an-app-to-decrypt-criminal-messages-was-born-over-a-few-beers-with-the-fbi-162343, zuletzt abgerufen am 05.08.2023.

11 *Farivar*, habeas data, S. 33.

12 Legal rift between the EU and USA: Data handling & data transfer and the implications for enterprises, abrufbar: https://blog.cryptshare.com/en/legal-rift-eu-usa-data-handling-data-transfer-implications-for-enterprises?hs_amp=true, zuletzt abgerufen am 02.08.2023.

13 How the CLOUD-Act works in data storage in Europe, abrufbar: https://english.ncsc.nl/latest/weblog/weblog/2022/how-the-cloud-act-works-in-data-storage-in-europe, zuletzt abgerufen am 05.08.2023.

14 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. XXVII.

15 How the CLOUD-Act works in data storage in Europe, abrufbar: https://english.ncsc.nl/latest/weblog/weblog/2022/how-the-cloud-act-works-in-data-storage-in-europe, zuletzt abgerufen am 05.08.2023.

16 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. XXVII.

1.1 Gegenstand der Untersuchung

Seit dem XX. Jahrhundert wurden auf der ganzen Welt Datenschutzgesetze zum Schutz von Online-Daten erlassen, von denen einige internationale Auswirkungen haben.[17] Die Ansätze der Länder, die diese Gesetze umsetzen, unterscheiden sich jedoch je nach der Kultur, der dieses Land angehört.[18] Die meisten Länder betrachten den Datenschutz als ein Grundrecht, das in einem umfassenden Gesetz, wie in der europäische Verfassung, verankert ist.[19]

Im Gegensatz dazu gibt es in den USA keine derartig umfassende, universelle Grundgesetzgebung.[20] Diese Unterschiede erschweren es den Organisationen, sich an die Gesetze zu halten, während sie grenzüberschreitend arbeiten, was in der heutigen globalen Gesellschaft gang und gäbe geworden ist.[21] Wie bei vielen Themen in der globalen Wirtschaft besteht ein Kompromiss zwischen der Vereinheitlichung, um die Dinge zu vereinfachen und gleichzeitig in der internationalen Gemeinschaft voranzukommen, und der Wahrung der kulturellen Perspektiven, die eine Nation einzigartig machen.[22] Im Bereich der (inter-) nationalen Sicherheit ist die Vereinfachung und Beschleunigung der Datenverarbeitung ebenfalls wichtig, um die Sicherheit jedes Einzelnen zeitgerecht garantieren zu können.

Zwischen der EU und den USA gibt es eine Reihe von Konflikten im Bereich des Datenschutzes.[23] Diese Konflikte können u. a. im Rahmen sozialer Netzwerke, beim Abschluss von Verträgen[24] oder bei der Strafverfolgung auftreten (z. B. die Datenübermittlung über Verstöße im Straßenverkehr zwischen den Ländern oder Terroristenlisten nach einer Resolution der Vereinten Nationen[25]). Vorschriften im internationalen Kontext legen die Anforderungen fest, die erfüllt werden müssen, um Daten rechtskonform in ein anderes Land zu übermitteln.[26]

Die Rechtssysteme der Europäischen Union und der Vereinigten Staaten von Amerika verfolgen in dieser Hinsicht unterschiedliche Ansätze: In der EU gibt es eine große Zahl von Vorschriften, während in den USA kaum Regelungen für den grenzüberschreitenden Datenverkehr bestehen.[27] In der EU decken die Datenschutzgesetze alle denkbaren Fälle der Datenverarbeitung im „Voraus“ ab; die USA reagieren sektoral auf Datenschutzkonflikte, die im Zuge der Datenverarbeitung entstehen, und erlassen entsprechende Vorschriften.[28]

17 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. XXVII.
18 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. XXVII.
19 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. XXVII.
20 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. XXVII.
21 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. XXVII.
22 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. XXVII.
23 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 37.
24 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 37.
25 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 37.
26 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 37.
27 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 37.
28 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 73.

Vorschriften über den Datenverkehr im internationalen Kontext führen häufig dazu, dass ein Land den Anspruch erhebt, bei der Ausfuhr von Daten weiterhin seine bestehenden Datenschutzregelungen anzuwenden.[29] Dies führt zwangsläufig zu den Konflikten, insbesondere bei unterschiedlichen Datenschutzkonzepten, bei denen eine Vielzahl von Interessen datenschutzrechtlicher, wirtschaftlicher oder sicherheitspolitischer Natur eine Rolle spielt.[30]

Außerdem haben die EU-Staaten rechtlich verbindliche Regelungen zum Datenschutz, während die USA mehr auf Selbstregulierung setzen und nur über Empfehlungen verfügen, deren Umsetzung auf freiwilliger Basis erfolgt.[31] Aufgrund dieser unterschiedlichen Arten von Datenschutzbestimmungen ergeben sich Herausforderungen, die im internationalen Kontext trotz bestehender Regelungen zum Datenverkehr nicht immer zufriedenstellend gelöst werden können.[32]

Eines der meistdiskutierten Beispiele für sich widersprechende Rechtsvorschriften sind die DSGVO und der CLOUD Act. Europäische Daten, die in den USA oder in der EU verarbeitet werden, unterliegen dem Recht der Europäischen Union und damit der DSGVO. Gleichzeitig fallen diese Daten auch unter das amerikanische Rechtssystem, das den Zugriff auf diese Daten überwacht. Der CLOUD Act erlaubt es den Bundesbehörden in den USA, Technologieunternehmen vorzuladen oder zu verpflichten, angeforderte Daten von Nutzern herauszugeben, selbst wenn diese Daten im Ausland gespeichert sind (z. B. in der EU).[33] Dadurch sind die US-Anbieter gezwungen, die personenbezogener Daten offenzulegen, die den Bestimmungen der DSGVO unterliegen.[34]

Dazu kommt, dass es kein Rechtshilfeabkommen zwischen der EU und den USA bezüglich des CLOUD Acts gibt. Folglich, sobald Unternehmen mit US-Cloud-Computing in Berührung kommen, sind ihre Dienste nicht mehr datenschutzkonform. Es wird automatisch gegen die DSGVO verstoßen, wenn Unternehmen in der EU gespeicherte Daten weitergeben. Für Dienstleister aus den USA, die europaweit Daten verarbeiten, ist dies ein Dilemma. Sie müssen sich entscheiden, ob sie Daten unter Verletzung der DSGVO oder des CLOUD Acts verarbeiten wollen.[35]

29 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 37 ff.
30 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 37 ff.
31 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 74.
32 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 74.
33 Die in diesem Abschnitt dargestellte Auffassung wird in dem folgenden Artikel beschrieben. S.: How the CLOUD-Act works in data storage in Europe, abrufbar: https://english.ncsc.nl/latest/weblog/weblog/2022/how-the-cloud-act-works-in-data-storage-in-europe, zuletzt abgerufen am 05.08.2023.
34 Edpb, ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence, S. 1.
35 Die in diesem Abschnitt dargestellte Auffassung, findet sich in dem folgenden Artikel. S.: The Cloud Act – Attention to US Cloud Services, abrufbar: https://teamdrive.com/en/blog-en/the-cloud-act-attention-to-us-cloud-services, zuletzt abgerufen am 29.07.2023.

EU-Dienstleister bzw. deren Daten, die ihre Dienste über US-Server in Auftrag geben oder ihre Server von US-Dienstleistern betreiben lassen (z. B. Google Drive), können ebenfalls betroffen sein.[36] Problematisch wird es auch im Hinblick auf die Verantwortung gegenüber den eigenen Kunden.[37] Denn Unternehmen, die Cloud-Anbieter von US-Unternehmen nutzen, sind nicht mehr sicher, was das Vertrauen der eigenen Kunden schwächt.[38]

Aufgrund dieser Hindernisse und des gegensätzlichen Charakters der Gesetze wird viel über alternative Mechanismen diskutiert. Zu nennen sind hier die folgenden: Das MLAT (Rechtshilfe-abkommen) gilt nach wie vor, das die rechtskonforme Datenübermittlung bei strafrechtlichen Ermittlungen oder Verfahren in einem anderen Land regelt. Eine neue Regelung, die vor allem die Wirtschaftsbeziehungen bei der Datenübermittlung zwischen der EU- und den US-Unternehmen vereinfachen wird, ist der neue EU-US-Datenschutzrahmen. Da sich die Technologie schneller entwickelt bzw. beschleunigt hat als das Recht,[39] sind die derzeitig vorgeschriebenen Gesetze oder Vorschriften trotzdem nicht ausreichend oder enthalten Unstimmigkeiten und Schwachstellen.

Die Lösung zur Gewährleistung des internationalen Datentransfers und des gefilterten Eingriffs der Behörden in die Privatsphäre einer Person ist in den verschiedenen Bereichen zu suchen. Die Implementierung und nachhaltige Umsetzung des Rechts auf Privatsphäre und Persönlichkeits-rechte ist nicht nur Aufgabe der Rechtswissenschaft. Der Schutz der Persönlichkeitsmerkmale im digitalen Alltag umfasst neben dem Recht auch den technischen und organisatorischen Bereich. Deren Schutz ist gekennzeichnet durch den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Daten. Im Rahmen einer Organisation ist die Umsetzung im besten Fall nach der ISO/IEC 27000-Reihe möglich.

Wenn diese präventive Maßnahmen den Cybervorfall nicht verhindern konnten, treten andere Hindernisse auf. Die Daten werden nicht mehr im Einklang mit dem Gesetz transferiert bzw. verarbeitet, und die Persönlichkeitsrechte sind nicht mehr gewährleistet. Da viele Bedrohungen der Privatsphäre keine nationalen Grenzen kennen, müssen hilfreiche Ideen zum Schutz der Privatsphäre gesucht und angewandt werden.[40]

36 IONOS, aktueller Rechtslage S. 7.

37 The Cloud Act – Attention to US Cloud Services, abrufbar: https://teamdrive.com/en/blog-en/the-cloud-act-attention-to-us-cloud-services, zuletzt abgerufen am 29.07.2023.

38 The Cloud Act – Attention to US Cloud Services, abrufbar: https://teamdrive.com/en/blog-en/the-cloud-act-attention-to-us-cloud-services, zuletzt abgerufen am 29.07.2023.

39 Diese Meinung wurde auf der Global GRC, Data Privacy & Cyber Security ConfEx am 31.05.2023 in NY/USA geäußert.

40 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. XXVII.

Die Cybersicherheit gewinnt für Juristen an Bedeutung und ist ebenso ein rechtliches wie ein technisches Thema.[41] In einer Studie aus dem Jahr 2015 für die Mauser School of Law der Indiana University identifizierte das Forschungsunternehmen Hanover Research das Cyber Law als Wachstumsfeld in Bezug auf die Rechtspraxis.[42] Daher ist es von entscheidender Bedeutung, eine entsprechende Reaktion auf Cyberangriffe in jeder Organisation zu implementieren, die sowohl rechtlich als auch technisch gesichert ist.

1.2 Gang der Untersuchung

In dieser Monographie wird das Thema „Internationaler Datentransfer" auf europäischer und amerikanischer Ebene behandelt. Zunächst werden die Persönlichkeitsrechte sowie ihre Rolle im Hinblick auf den internationalen Datentransfer dargestellt (Teil 1 – Persönlichkeitsrechte). Dann wird das Thema „Internationaler Datentransfer" detailliert analysiert, um die entsprechenden Lösungen als Ergebnisse zum sicheren und datenschutzkonformen Datentransfer zusammenzufassen (Teil 2 – (Internationaler) Datentransfer). Nachher werden präventive Maßnahmen zur Gewährleistung der Persönlichkeitsrechte beschrieben (Teil 3 – Präventive Maßnahmen). Anschließend werden die genauen Schritte für den Fall, wenn die Daten und damit der Schutz der Persönlichkeitsrechte gefährdet sind (Teil 4 – Nachgelagerte Maßnahmen), untersucht.

Der Schwerpunkt des Untersuchungsgegenstandes liegt auf dem internationalen Datentransfer bei strafrechtlichen Ermittlungen oder Verfahren (d. h. zwischen einer Behörden und einem Unternehmen) sowie bei wirtschaftlichen Tätigkeiten (d. h. zwischen den Unternehmen) zwischen der EU und den USA. Diese Untersuchung in diesen vier Teilen wird ermöglichen, ein solches Rechtsinstrument zu schaffen, das auch technisch durchführbar ist und die (Persönlichkeits-) Rechte jedes Einzelnen (inklusive der besonderen Ausprägung der Persönlichkeitsrechte) gewährleistet.

Die vorliegende Arbeit hat den Stand **Mai 2024** und berücksichtigt alle relevanten gesetzlichen Änderungen, Rechtsprechung sowie Literatur, die bis zu diesem Zeitpunkt von der EU und / oder den USA vorgenommen werden.

Bei der Darstellung verschiedener Themen auf internationaler Ebene werden manchmal Ansichten verwendet, deren Autoren diese nur in Bezug auf die EU- oder US-Normierung lenken. Dies ist lediglich dann der Fall, wenn sie auch auf internationaler Ebene der Wahrheit entsprechen.

Zur besseren Lesbarkeit wird in dieser Dissertation das generische Maskulinum verwendet. Die angewendten Personenbezeichnungen beziehen sich auf alle Geschlechter.

41 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 14.
42 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 14.

2 Persönlichkeitsrechte

2.1 Persönlichkeit – ihre Bedeutung und ihr Bezug auf das Rechtswesen

2.1.1 Bedeutung der Persönlichkeit

Das Wort „Persönlichkeit" findet seine Wurzeln im lateinischen Wort „**Persona**".[43] Dort hatte es eine Bedeutung im sozialen Leben als eine Rolle, einen Status oder eine Würde einer Person und im antiken Theater als die Maske, die eine bestimmte Rolle eines Schauspielers charakterisierte.[44] In beiden Fällen ging es darum, eine Person unter Bezugnahme auf einen Stereotyp oder eine soziale Rolle zu beschreiben.[45]

Heutzutage bezieht sich der Begriff „**Persönlichkeit**" zum einen auf eine konkrete Person hinter der Maske und über die bloße Rolle hinaus.[46] Die in der Persönlichkeitspsychologie verwendete Definition lautet wie folgt: *„[…] die Gesamtheit aller nichtpathologischen Persönlichkeitseigenschaften, nämlich individueller Besonderheiten in der körperlichen Erscheinung und in Regelmäßigkeiten des Verhaltens und Erlebens, in denen sich jemand von Gleichaltrigen derselben Kultur unterscheidet."*[47]

Persönlichkeitsmerkmale lassen sich sowohl aus Verhaltensbeobachtungen als auch aus den Spuren, die Menschen in ihrem Umfeld hinterlassen, ableiten.[48] Sie sind sowohl in Form von schriftlichen Dokumenten als auch im Internet in großer Zahl zu finden und lassen sich so gut auswerten, wie es zumindest enge Freunde oder Familienmitglieder getan hätten.[49] Daraus ergibt sich die Notwendigkeit, diese persönlichen Merkmale als Daten bzw. Informationen über natürliche Personen zu betrachten und deren Persönlichkeitsrechte[50] gesetzlich zu verankern.

Und was bedeutet heute überhaupt das Wort „**Person**" bzw. „**natürliche Person**"? Unter natürlichen Personen wird in der Regel 1. menschliches Wesen, 2. geborene, 3. derzeit lebende und 4. empfindungsfähige Personen verstanden.[51] Um eine aktive Rechtspersönlichkeit an den Tag zu legen, muss eine Person außerdem über ausreichende Vernunft und ein ausreichendes Alter verfügen.[52]

---

43 *Asendorpf*, Persönlichkeit: was uns ausmacht und warum, S. 4.
44 *Asendorpf*, Persönlichkeit: was uns ausmacht und warum, S. 4.
45 *Asendorpf*, Persönlichkeit: was uns ausmacht und warum, S. 4.
46 *Asendorpf*, Persönlichkeit: was uns ausmacht und warum, S. 2.
47 *Asendorpf*, Persönlichkeit: was uns ausmacht und warum, S. 8.
48 *Asendorpf*, Persönlichkeit: was uns ausmacht und warum, S. 97.
49 *Asendorpf*, Persönlichkeit: was uns ausmacht und warum, S. 97.
50 Wenn über „Persöonlichkeitsrechte" auf der deutsprachigen und englischsprachigen Ebene gesprochen wird, sind einige Feinheiten zu beachten: Der Begriff „Persönlichkeitsrechte" entspricht dem Begriff „Individual Rights". Es ist zwar nicht wörtlich übersetzt, aber der Begriff „Individual Rights" passt am besten inhaltlich zum Begriff „Persönlichkeitsrechte". Der wörtlich übersetzte Begriff „Persönlichkeitsrechte" als „personality rights" passt am besten zu „Recht auf Privatsphäre" / „Right of Privacy" und „Recht auf Öffentlichkeit" / „Right of Publicity". Es gibt zwar die entsprechende Rechte auf der europäische Ebene, aber es existiert kein Oberbegriff dafür.
51 *Gellers*, RIGHTS FOR ROBOTS, S. 31.
52 *Gellers*, RIGHTS FOR ROBOTS, S. 31.

2.1.2 Grundlegende Regelungen der Persönlichkeitsrechte

Als ein integraler Bestandteil der Würde einer Person ist in Zeiten des digitalen Wandels der Schutz personenbezogener Daten aufgenommen worden.[53] Folglich hat die Verletzung dieser Daten einen solchen rechtlichen Status wie die Verletzung des engsten Besitzes eines Menschen, da beides gleichermaßen entscheidend für Selbstbestimmung und letztlich Freiheit einer Person sind.[54]

Aus diesem Grund sind die Persönlichkeitsmerkmale sowie die daraus resultierten Rechte, zu denen insbesondere der Schutz der personenbezogenen Daten, der Privatsphäre, der freien Entfaltung der Persönlichkeit oder der Menschenwürde gehören, von großer Bedeutung. Sie gehören jedem Menschen, sind völkerrechtlich abgesichert und in der Gesetzgebung jedes Landes verankert.

Obwohl der Begriff „Persönlichkeitsrecht" in den Gesetzen nicht ausdrücklich erwähnt wird, stützen sich die Vorschriften auf diese Rechte und garantieren das, was zu ihrem Schutz vorgesehen ist. Auf internationaler Ebene garantieren **Art. 12 S. 1 AEMR** sowie **Art. 17 IPbpR** den Schutz des Privatlebens, der das Recht auf Privatsphäre stärkt und ergänzt. Nach diesen Artikeln ist es nicht erlaubt, willkürlich in das Privatleben, die Familie, die Wohnung und die Korrespondenz einer Person einzugreifen oder ihre Ehre und ihren Ruf zu schädigen. Auf diesem internationalen und absoluten Recht basieren die Grundrechte und Grundfreiheiten, die in der Europäische Union als auch in den Vereinigten Staaten gelten.[55]

Auf europäischer Ebene sind die Persönlichkeitsrechte durch **Art. 8 EMRK** sowie **Artt. 7 und 8 GrCh** geschützt. Artikel 8 EMRK schützt u. a. die Privatsphäre, der Teil des Rechts auf informationelle Selbstbestimmung ist, beschreibt einen Teil des Schutzes der Persönlichkeitsrechte[56] und schafft den Raum für die freie Entfaltung der Persönlichkeit.[57] Die Rechte nach Art. 7 GrCh korrespondieren mit den Schutzbereichen des Art. 8 EMRK[58] und geben jeder Person die Möglichkeit, auf ihre Privatsphäre zu achten. Artikel 8 GrCh gewährleistet das Recht auf den Schutz personenbezogener Daten, das auch die Privatsphäre einer Person schützt und ihr die Möglichkeit gibt, ihre Persönlichkeit frei zu entfalten.

53 *Pell/Grace,* United States of America v. Microsoft Corporation: On Writ of Certiorari to the United States Court of Appeals for the Second Circuit, S. 2.

54 *Pell/Grace,* United States of America v. Microsoft Corporation: On Writ of Certiorari to the United States Court of Appeals for the Second Circuit, S. 2.

55 *Bagauri*, BRJ 01/2022, 1, 43.

56 Privatsphäre und Familienleben, abrufbar: https://www.menschenrechtskonvention.eu/privatsphaere-und-familienleben-9292/, zuletzt abgerufen am 30.07.2023.

57 *Franzen u. a. -Schubert*, Kommentar zum Europäischen Arbeitsrecht, Art. 8 EMRK, Rn. 1.

58 Artikel 7 - Achtung des Privat- und Familienlebens, abrufbar: https://fra.europa.eu/de/eu-charter/article/7-achtung-des-privat-und-familienlebens#explanations, zuletzt abgerufen am 30.07.2023.

Auf amerikanischer Ebene sind nach **Art. 11 AMRK** Ehre und Würde jedes Menschen anerkannt, und es ist die Gewährleistung der Privatsphäre für jeden Menschen festgelegt. Hiernach hat jeder das Recht auf den Schutz gegen willkürliche oder mißbräuchliche Eingriffe in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrige Angriffe auf seine Ehre bzw. seinen Ruf.

2.1.2.1 Ausgangspunkt der Persönlichkeitsrechte – Menschenrechte

> *„Du sollst deinen Vater und deine Mutter ehren, […] du sollst nicht ehebrechen […] [und] nicht das Haus deines Nächsten begehren" (Die Bibel: Neue-Welt-Überserzung, 2. Mose, Kapitel 20, VV. 12, 14 und 17) – Die Gebote, die als moralische Prinzipien seit den mosaischen Gesetzen die Menschengeschichte prägten, formten globale Prinzipien der allgemeinen Menschenrechte und sind in jedem Land anerkannt.*

Die derzeitige Ausprägung moralischer Prinzipien von mosaischen Gesetzen sind in der modernen Welt im Völkerrecht als Menschenrechte gekennzeichnet. Laut der Definition der Vereinten Nationen / „United Nations" (UN) sind Menschenrechte die Rechte, die allen Menschen zustehen, unabhängig von Rasse, Geschlecht, Nationalität, ethnischer Zugehörigkeit, Sprache, Religion oder einem anderen Status.[59] Sie bezeichnen die Rechte, die alle Menschen allein aufgrund ihres Menschseins beanspruchen können, und gelten als **absolute subjektive Rechte**.[60] Sie sind universell, unveräußerlich sowie unteilbar und stellen moralisch begründete Ansprüche dar.[61] Zu den Menschenrechten gehören u. a. das Recht auf Leben, persönliche Freiheit, Freizügigkeit und Schutz des Privatlebens sowie die Presse- und Meinungsfreiheit.[62]

Die Menschenrechte verfügen über ein wechselseitiges Verhältnis.[63] Eine der Pflichten der Menschenrechte besteht darin, die Menschenwürde sowie die Rechte anderer zu achten und das eigene Recht nicht auf Kosten der Rechte anderer Menschen wahrzunehmen.[64]

Zu den zulässigen Zwecken von Menschenrechtseingriffen gehören beispielsweise die Aufrechterhaltung der nationalen Sicherheit oder die Verhütung von Straftaten.[65]

59 Peace, dignity and equality on a healthy planet, abrufbar: https://www.un.org/en/global-issues/human-rights, zuletzt abgerufen am 30.07.2023.
60 *Koenig u.a.*, Menschenrechte, S. 8 ff.
61 *Gandenberger/Krennerich*, Politik & Unterricht, Heft 3/4 – 2014, S. 2.
62 *Gandenberger/Krennerich*, Politik & Unterricht, Heft 3/4 – 2014, S. 4.
63 *Gandenberger/Krennerich*, Politik & Unterricht, Heft 3/4 – 2014, S. 6.
64 *Gandenberger/Krennerich*, Politik & Unterricht, Heft 3/4 – 2014, S. 7.
65 *Gandenberger/Krennerich*, Politik & Unterricht, Heft 3/4 – 2014, S. 7.

Diese Rechte können jedoch zu einer Reihe von Kontroversen und Konflikten führen.[66] Dazu gehören u. a. das Spannungsverhältnis zwischen internationalem Menschenrechtsschutz und staatlicher Souveränität sowie das Verhältnis zwischen dem universalistischen Anspruch der Menschenrechte und der Vielfalt der Kulturen.[67]

2.1.2.2 Inhalt der Persönlichkeitsrechte

> *„Wer, wes Volkes bist du und wo ist deine Geburtsstadt? Und wo liegt das Schiff, das dich und die tapferen Genossen brachte? fragen Penelopeia und Laertes den noch nicht erkannten Fremden[,] und der listenreiche Odysseus verzögert zu seinem Schutze die Antwort, die getreuen und besorgten Fragesteller damit verletzend“.*[68]

Unter Menschenrechte fallen Persönlichkeitsrechte. Sie sind in jeder von den Menschenrechten geprägten Rechtsordnung gegeben.[69] Es ist allerdings zu erwähnen, dass der Begriff „Persönlichkeitsrecht“ schwer zu fassen ist.[70] Es lassen sich sein Inhalt sowie seine Grenzen sehr allgemein und abstrakt definieren, da die mit ihm in Verbindung stehenden technologischen Entwicklungen sowie daraus resultierende wirtschaftliche und soziale Veränderungen immer neue Herausforderungen mit sich bringen.[71]

Die Persönlichkeitsrechte sind von idealistischen Maßstäben gewirkt.[72] Sie ermöglichen es jedem Einzelnen, sein Leben ohne Einmischung anderer Menschen, von Institutionen oder Organisationen, vom Staat bzw. von Behörden zu gestalten. Diese Rechte beantworten die Frage: ***„Wie weit darfst du dein Ich betreiben?“***[73]

Die Persönlichkeitsrechte setzen der Presse- und Medienfreiheit Grenzen und gewähren den Schutz vor der Verletzung der Intim- und Privatsphäre, vor unwahrer Berichterstattung sowie vor unerwünschter kommerzieller Ausbeutung.[74]

66 *Koenig u.a.*, Menschenrechte, S. 8.
67 *Koenig u.a.*, Menschenrechte, S. 8.
68 *Ehmann*, Der Begriff des Allgemeinen Persönlichkeitsrechts, S. 1.
69 *Ehmann*, Der Begriff des Allgemeinen Persönlichkeitsrechts, S. 2.
70 *Ehmann*, Der Begriff des Allgemeinen Persönlichkeitsrechts, S. 1.
71 *Götting u.a. -Götting*, Handbuch Persönlichkeitsrecht, S. 3.
72 *Götting*, Persönlichkeitsrechte als Vermögensrechte, S. 4.
73 *Ehmann*, Der Begriff des Allgemeinen Persönlichkeitsrechts, S. 1.
74 *Wandtke/Ohst -Boksanyi/Koehler*, Medienrecht Praxishandbuch, S. 116.

Die Persönlichkeitsrechte können in folgenden Fällen verletzt werden: 1. wenn eines seiner Rechte die Rechte anderer überwiegt, 2. wenn die Behörden im überwiegenden öffentlichen Interesse handeln oder ihre Macht missbrauchen, 3. wenn die Verletzung dieser Rechte bei der Ausübung und Durchsetzung von Interessen erfolgt, die durch (Verfassungs-) Recht geschützt sind (z. B. Strafverfolgungszwecke), und 4. wenn die Verletzung bei der Ausübung legitimer Interessen erfolgt (z. B. mit Durchsuchungsbefehl).[75]

2.1.2.3 Zweck und Gegenstand der Persönlichkeitsrechte

Die Persönlichkeitsrechte dienen dazu, die höchsten, unveräußerlichen und unverletzlichen Rechtsgüter des Einzelnen zu gewährleisten.[76] Dies ermöglicht es jedem, sein Leben nach seinem Willen zu gestalten und seine Persönlichkeit frei zu entfalten, ohne Einmischung von Seiten der Regierung, Organisationen und anderen Menschen. Dies gewährleistet in hohem Maße den Schutz der persönlichen Merkmale einschließlich der Daten bzw. Informationen zu einer Person. Diese Rechte sorgen dafür, dass niemand ohne Einwilligung in den persönlichen Bereich anderer eindringt und ungefragt persönliche Angelegenheiten veröffentlicht.[77] Damit wird das Individuum vor Bedrohungen seiner Integrität sowie seiner Selbstbestimmung geschützt und sein autonomer Lebensbereich gewährleistet, ,,indem er seine Identität unter Ausschluss anderer entwickeln und wahrnehmen kann“.[78]

Schutzobjekt bzw. Gegenstand der Persönlichkeitsrechte ist das ,,Innere“ des Menschen als ,,Intimperson“ (innere Ehre, Intim- sowie Privatsphäre) sowie ,,Sozialperson“ (äußere Ehre, Sozialsphäre) und nicht äußeres Haben (Besitz, Vermögen oder Eigentum).[79] Diese Rechte gelten für den unmittelbaren Freiheitsbereich des Menschen, die ihm vor staatlichen sowie privaten Eingriffen schützt.[80]

75 *Ehmann*, Der Begriff des Allgemeinen Persönlichkeitsrechts, S. 1.
76 *Götting*, Persönlichkeitsrechte als Vermögensechte, S. 4.
77 Persönlichkeitsrechte, abrufbar: https://webhelm.de/persoenlichkeitsrechte/, zuletzt abgerufen am 30.07.2023.
78 *Götting u.a. -Götting*, Handbuch Persönlichkeitsrecht, 2019, S. 5; *Beater*, Medienrecht, S. 156 ff.
79 *Ehmann*, Der Begriff des Allgemeinen Persönlichkeitsrechts, S. 1.
80 Wissenschaftliche Dienste des Deutschen Bundestages, WD 10 - 3000 – 110/08, S. 18.

2.1.2.4 Träger der Persönlichkeitsrechte

Schutzsubjekt bzw. Träger der Persönlichkeitsrechte ist zuerst jede **natürliche Person**.[81] Unabhängig von ihrer Geschäftsfähigkeit und ihrem Alter, stehen ihr diese Rechte von Geburt an zu.[82] [83]

Gruppen, die zu einem konkreten Kollektiv gehören, sind mangels eines Zuordnungssubjekts nicht Träger der Persönlichkeitsrechte (z. B. eine Familie).[84]

Juristische Personen sowie nichtrechtfähige Personenvereinigungen sind grundsätzlich Träger eines (Unternehmens-) Persönlichkeitsrechts.[85] Allerdings gewähren diese keinen gleichwertigen Schutz wie der Schutz für natürliche Personen, da der Bezug zur Menschenwürde fehlt.[86] So haben beispielsweise Personenvereinigungen im Gegensatz zu natürlichen Personen keinen Anspruch auf eine immaterielle Entschädigung in Geld.[87]

Verstorbene haben kein Persönlichkeitsrecht. Dieses endet mit dem Tod der natürlichen Person,[88] weil der Verstorbene die freie Entfaltung seiner Persönlichkeit nicht vollziehen kann. Um die Würde und Persönlichkeit eines Menschen nach seinem Tod zu schützen, wurde ein postmortales Persönlichkeitsrecht entwickelt, das die über das allgemeine Persönlichkeitsrecht hinausgehende Menschenwürde des Betroffenen schützt. [89]

2.1.2.5 Rechtsnatur der Persönlichkeitsrechte

Technologie und zunehmende Digitalisierung schaffen eine rechtliche Lage, in der auf der einen Seite das sich entwickelnde positive Recht und auf der anderen Seite die Überlegungen zu den Belangen der betroffenen Person stehen.[90] Die Persönlichkeitsrechte prägen diese Überlegungen „als Institut der Rechtsfortbildung und offenen Tatbestand in der judikativen Anwendung“.[91]

---

81 *Wandtke/Ohst -Boksanyi/Koehler*, Medienrecht Praxishandbuch, S. 118.

82 So können kleine Kinder sowie Menschen, die z.B. aufgrund einer Behinderung oder Krankheit nicht in der Lage sind, ihre eigene Verletzung der Ehre oder Intimsphäre zu empfinden, entsprechende Ansprüche im Falle einer Verletzung geltend machen. S.: *Wandtke/Ohst -Boksanyi/Koehler*, Medienrecht Praxishandbuch, S. 118.

83 *Wandtke/Ohst -Boksanyi/Koehler*, Medienrecht Praxishandbuch, S. 118.

84 *Wandtke/Ohst -Boksanyi/Koehler*, Medienrecht Praxishandbuch, S. 119.

85 *Wandtke/Ohst -Boksanyi/Koehler*, Medienrecht Praxishandbuch, S. 120.

86 *Wandtke/Ohst -Boksanyi/Koehler*, Medienrecht Praxishandbuch, S. 120.

87 *Wandtke/Ohst -Boksanyi/Koehler*, Medienrecht Praxishandbuch, S. 120.

88 *Wandtke/Ohst -Boksanyi/Koehler*, Medienrecht Praxishandbuch, S. 122.

89 *Wandtke/Ohst -Boksanyi/Koehler*, Medienrecht Praxishandbuch, S. 122.

90 *Ruppel*, PERSÖNLICHKEITSRECHTE AND DATEN? DELIKTSRECHTLICHER DATENSCHUTZ NACH § 823 ABS. 1 BGB ZWISCHEN INFORMATIONELLER SELBSTBESTIMMUNG, RECHTSGÜTERSCHUTZ UND EINGRIFFS-TYPISIERUNG, S. 2.

91 *Ruppel*, PERSÖNLICHKEITSRECHTE AND DATEN? DELIKTSRECHTLICHER DATENSCHUTZ NACH § 823 ABS. 1 BGB ZWISCHEN INFORMATIONELLER SELBSTBESTIMMUNG, RECHTSGÜTERSCHUTZ UND EINGRIFFS-TYPISIERUNG, S. 2.

Der Persönlichkeitsschutz wirkt bezüglich des Persönlichkeitsrechts in doppelter Hinsicht: 1. In statischer Hinsicht „in Ruhe gelassen zu werden“ und 2. in dynamischer Hinsicht „auf freie Entfaltungsmöglichkeiten und aktive Entschließungs- und Handlungsfreiheit“.[92]

2.1.3 Zivilrechtlicher Persönlichkeitsschutz

Zu den Persönlichkeitsrechten gehören nichtkörperliche Aspekte der Person, worunter insbesondere das Recht auf Würde, Autonomie und Privatsphäre fallen.[93] Sie sind die Persönlichkeitsrechte oder ein übergreifendes allgemeines Persönlichkeitsrecht, unter denen sich die Persönlichkeitsinteressen entwickelt haben.[94] Hierbei sind ideelle und materielle Interessen zu betrachten.

Bei Persönlichkeitsrechten geht es um den Schutz von primär **ideellen / nichtwirtschaftlichen** Interessen an emotionaler Ruhe, Privatsphäre oder Freiheit von seelischem Leid.[95] Ideelle Interessen lassen sich oft nicht vollständig durch eine bestimmte Geldzahlung ausgleichen.[96] Sie können nicht objektiv bewertet werden, sondern sind von Natur aus subjektiv bewertete Interessen.[97]

Neben den ideellen Interessen sind die **materiellen / wirtschaftlichen** Interessen des Einzelnen zu berücksichtigen, wenn es um die kommerzielle Nutzung der Persönlichkeitsmerkmale geht. Wird eine Person durch die unbefugte Verwendung der Persönlichkeitsmerkmale finanziell benachteiligt, drückt sich dies meist nur in Geld aus.[98]

In typischen Fällen, in denen es um den Schutz der Privatsphäre oder ideeller Interessen geht, verteidigt sich eine Person, um in Ruhe gelassen zu werden, während im Falle materieller Interessen der Kläger den materiellen Wert seiner Bekanntheit gegen Trittbrettfahrer verteidigt.[99]

92 *Götting u.a. -Götting*, Handbuch Persönlichkeitsrecht, S. 5.
93 *Brüggemeier u.a.*, Personality Rights in European Tort Law, S. 6.
94 *Brüggemeier u.a.*, Personality Rights in European Tort Law, S. 6.
95 *Beverley-Smith u.a.*, Privacy, Property and Personality, S. 2.
96 *Beverley-Smith u.a.*, Privacy, Property and Personality, S. 2.
97 *Beverley-Smith u.a.*, Privacy, Property and Personality, S. 2.
98 *Beverley-Smith u.a.*, Privacy, Property and Personality, S. 2.
99 *Beverley-Smith u.a.*, Privacy, Property and Personality, S. 3.

Die Trennung zwischen ideellen und materiellen Persönlichkeitsinteressen erfolgt in Europa durch einen **dualistischen Ansatz** und ist dadurch gekennzeichnet, dass in diversen begrifflichen Ausprägungen und thematischen Variationen für eine Entbindung sowie Verselbständigung der vermögensrechtlichen Komponenten der Persönlichkeitsrechte von ideellen Interessen der Persönlichkeitsschutz entwickelt wird, ähnlich wie im Immaterialgüterrecht.[100] Diese dualistische Trennung ist in den USA ausgeprägt im Recht auf Privacy, das auf den Schutz immaterieller Interessen abzielt, und dem Recht auf Publicity, das auf den Schutz wirtschaftlicher Interessen zugeschnitten ist.[101]

2.1.3.1 Zivilrechtlicher Persönlichkeitsschutz in der EU

Das europäische Privatrecht geht von subjektiven Rechten aus: 1. (Absolute) Eigentumsrechte an körperlichen Gegenständen oder geistigen Leistungen (z. B. das Eigentum am Grundstück) und 2. (relationale) Forderungen (z. B. das Recht eines Gläubigers, von einem Schuldner Geld zu fordern).[102] Sie sind veräußerbar, vererbbar sowie von Geldwert und stellen das Vermögen einer Person dar.[103] Die Persönlichkeitsrechte passen nicht in diese Dichotomie, da sie für die nicht-körperlichen Aspekte der Person fungieren.[104] Diese Bezeichnung hat dazu beigetragen, dass sie im Privatrecht anerkannt werden, allerdings als hybride, als eine Art privater Menschenrechte.[105]

Der Schutz der **immateriellen Interessen** dient vor allem dem Schutz des Rechts auf Wertschätzung und Achtung der Persönlichkeit.[106] Handelt es sich bei der Verletzung des Persönlichkeitsrechts um einen schwerwiegenden Eingriff, bei dem „die Beeinträchtigung nicht in anderer Weise befriedigend ausgeglichen werden kann“, kommen sowohl Abwehr- als auch Schadensersatzansprüche in Betracht, die sowohl auf Ersatz des immateriellen als auch auf Ersatz des materiellen Schadens gerichtet sein können.[107]

100 *Götting u.a. -Götting*, Handbuch Persönlichkeitsrecht, S. 206.
101 *Götting u.a. -Götting*, Handbuch Persönlichkeitsrecht, S. 206.
102 *Brüggemeier u.a.*, Personality Rights in Europian Tort Law, S. 5 ff.
103 *Brüggemeier u.a.*, Personality Rights in Europian Tort Law, S. 6.
104 *Brüggemeier u.a.*, Personality Rights in Europian Tort Law, S. 6.
105 *Brüggemeier u.a.*, Personality Rights in Europian Tort Law, S. 6.
106 BGH, Urt. v. 01. 12. 1999 - I ZR 49/97 (KG) - LM H. 10/2000, II.1 – Marlene Dietrich.
107 BGH, Urt. v. 01. 12. 1999 - I ZR 49/97 (KG) - LM H. 10/2000, II.1 – Marlene Dietrich.

Kommerziellen Interessen an Persönlichkeitsrechten sollen die Entscheidung des Einzelnen schützen, ob und unter welchen Bedingungen die Persönlichkeitsmerkmale (z. B. das Bild) für die geschäftlichen Interessen Dritter nutzbar gemacht werden.[108] Dies kommt meistens bei bekannten Persönlichkeiten im Betracht.[109] Da das Persönlichkeitsrecht im Hinblick auf die wirtschaftlichen Interessen auch eine vermögensrechtliche Komponente enthält, sind im Falle einer Verletzung des Persönlichkeitsrechts auch Ersatzansprüche zu prüfen.[110]

2.1.3.2 Zivilrechtlicher Persönlichkeitsschutz in den USA

Bei den Persönlichkeitsrechten werden in den USA im Allgemeinen das Recht auf Privatsphäre / „Right of Privacy“ und das Recht auf Öffentlichkeit / „Right of Publicity“ unterschieden. Sie sind Gegenstand staatlicher Gesetze, die von Staat zu Staat unterschiedlich sind.[111] In vielen Staaten gibt es Gesetze zum Schutz der Privatsphäre und / oder der Öffentlichkeit.[112] In manchen Staaten werden diese Rechte nicht anerkannt oder werden im Rahmen anderer staatlicher Gesetze oder gewohnheitsrechtlicher Rechtssätze (z. B. widerrechtliche Aneignung und falsche Darstellung) anerkannt.[113]

In den Rechtsordnungen des Common Law wird der ideelle Schutz der Persönlichkeit nur begrenzt anerkannt[114] und wird durch das **Recht auf Privatsphäre** (s. → S. 22-23) gewährleistet. Dieses Recht gibt jedem Menschen die Möglichkeit, sich frei bzw. unkontrollierbar zu agieren und in Ruhe gelassen zu werden.

108 BGH, Urt. v. 01. 12. 1999 - I ZR 49/97 (KG) - LM H. 10/2000, II.1 – Marlene Dietrich.
109 BGH, Urt. v. 01. 12. 1999 - I ZR 49/97 (KG) - LM H. 10/2000, II.1 – Marlene Dietrich.
110 BGH, Urt. v. 01. 12. 1999 - I ZR 49/97 (KG) - LM H. 10/2000, II.1 – Marlene Dietrich.
111 The rights of publicity and privacy, abrufbar: abrufbar: http://www.publicdomainsherpa.com/rights-of-publicity-and-privacy.html, zuletzt abgerufen am 30.07.2023.
112 The rights of publicity and privacy, abrufbar: abrufbar: http://www.publicdomainsherpa.com/rights-of-publicity-and-privacy.html, zuletzt abgerufen am 30.07.2023.
113 The rights of publicity and privacy, abrufbar: abrufbar: http://www.publicdomainsherpa.com/rights-of-publicity-and-privacy.html, zuletzt abgerufen am 30.07.2023.
114 *Beverley-Smith u.a.*, Privacy, Property and Personality, S. 8 ff.

Aus dem Recht auf Privatsphäre hat sich das **Right of Publicity** entwickelt,[115] weil bei der Abgrenzung des Rechtes auf Privatsphäre im Mittelpunkt der Schutz von Interessen mit vermögensrechtlichem Charakter stand.[116] Viele Staaten erkennen das Recht auf Öffentlichkeit nicht unter diesem Namen an, sondern schützen es als Teil des Rechts auf Privatsphäre.[117] Die geschützten Eigenschaften des Rechtes auf Öffentlichkeit sind übertragbar, lizenzierbar und in vielen Staaten auch vererbbar.[118] Das Right of Publicity ist das ausschließliche Recht, die Verwertung des kommerziellen Werts der eigenen persönlichen Eigenschaften zu kontrollieren.[119] Es ist gewissermaßen das antithetische Gegenstück zum Recht auf Privatsphäre, da es auf wirtschaftliche Interessen ausgerichtet ist.[120]

Das Right of Publicity zielt auf den Schutz der Publizität und des damit verbundenen Vermögenswertes.[121] Demgemäß sind seine Grundgedanken auf Prominente / „celebrities" zugeschnitten, also auf Personen, die zumindest bei einem erheblichen Teil der Öffentlichkeit einen gewissen Bekanntheitsgrad erreicht haben.[122]

In der Rechtsprechung und in der Literatur wird teilweise die Auffassung vertreten, dass das Right of Publicity ausschließlich die Eigentumsinteressen von Prominenten schützt, weil lediglich diese in ihren Identitätsmerkmalen einen Publizitätswert erreicht haben, der Objekt einer „Enteignung" sein kann.[123] In einigen Fällen wird der „abstrakte" potenzielle Vermögenswert, der sich aus der Berühmtheit einer Person ergibt, nicht als ausreichend angesehen, um ihr dieses Recht zu gewähren.[124] Stattdessen ist ein zusätzlicher Nachweis erforderlich, dass die Person diesen Vermögenswert auch konkret verwertet, indem sie ihre Bekanntheit außerhalb ihres beruflichen Tätigkeitsbereichs kommerziell nutzt.[125]

115 US Court of Appeals for the 2nd Cir. 16.02.1953 - 202 F.2d 866 – Haelan Laboratories Inc v. Topps Chewing Gum Inc; Götting, Persönlichkeitsrechte als Vermögensrechte, S. 168; *Beverley-Smith u.a.*, Privacy, Property and Personality, S. 9.

116 US Court of Appeals for the 2nd Cir. 16.02.1953 - 202 F.2d 866 – Haelan Laboratories Inc v. Topps Chewing Gum Inc; vgl.: *Beverley-Smith u.a.*, Privacy, Property and Personality, S. 9.

117 Publicity, abrufbar: https://www.law.cornell.edu/wex/publicity, zuletzt abgerufen am 30.07.2023.

118 *Beverley-Smith u.a.*, Privacy, Property and Personality, S. 9.

119 *Götting*, Persönlichkeitsrechte als Vermögensrechte, S. 191.

120 *Götting*, Persönlichkeitsrechte als Vermögensrechte, S. 191.

121 *Götting*, Persönlichkeitsrechte als Vermögensrechte, S. 211.

122 *Götting*, Persönlichkeitsrechte als Vermögensrechte, S. 211.

123 *Götting*, Persönlichkeitsrechte als Vermögensrechte, S. 212.

124 *Götting*, Persönlichkeitsrechte als Vermögensrechte, S. 212.

125 *Götting*, Persönlichkeitsrechte als Vermögensrechte, S. 212.

2.1.3.3 Vergleich der zivilrechtlichen Persönlichkeitsschutz in der EU und in den USA

Werden die Persönlichkeitsrechte im Kontext des zivilrechtlichen Schutzes betrachtet, so lässt sich feststellen, dass sowohl auf europäischer als auch auf amerikanischer Ebene ideelle und materielle Interessen des Persönlichkeitsschutzes zu finden sind, allerdings mit unterschiedlichen Ansätzen. In der EU wird der zivilrechtliche Schutz der Persönlichkeitsrechte als ideelles und materielles Interesse dargestellt, in den USA als Right of Privacy und Right of Publicity.

Das **ideelle Interesse** wahrt die nichtwirtschaftlichen Interessen sowie die persönlichen Eigenschaften jedes Einzelnen vor unerwünschten Eingriffen in das Privatleben und schafft die Möglichkeit, die Persönlichkeit frei zu entfalten.

Das **materielle Interesse** wahrt die wirtschaftlichen Interessen sowie die persönlichen Eigenschaften eines Einzelnen vor unerwünschter kommerzieller Nutzung. Wird dies verletzt, kann der Einzelne Ansprüche geltend machen und sowohl materiellen als auch immateriellen Schadenersatz verlangen. Dies wird meistens auf bekannte Persönlichkeiten angewandt.

All dies deutet darauf hin, dass die Persönlichkeitsrechte sowohl in der EU und als auch in den USA geschützt sind. Daraus lässt sich ableiten, dass in der EU die nichtkörperlichen Aspekte einer Person grundsätzlich geschützt sind. Auf den ersten Blick ist dies in den USA nicht der Fall, weil das Right of Privacy und das Right of Publicity nur einen Teil der Persönlichkeitsrechte schützen. Da diese Rechte in den USA jedoch Gegenstand von einzelstaatlichen Gesetzen sind, die sich von Staat zu Staat unterscheiden, und da die USA alle Grundrechte und -freiheiten anerkannt haben, kann festgestellt werden, dass diese Rechte durch andere Gesetze vollständig garantiert werden können.

Wenn festgestellt wird, dass die Persönlichkeitsrechte sowohl in der EU als auch in den USA garantiert sind, muss klargestellt werden, ob sie tatsächlich gleichermaßen gewährleistet werden. Dies erfordert eine weitere Untersuchung der Überlegung, um sie zu begründen oder zu falsifizieren. Einerseits ist es wichtig, dass diese Rechte verankert sind, andererseits ist es auch wichtig festzustellen, wie sie sich in den verschiedenen Rechtsbereichen ausgeprägt und wie sie umgesetzt werden.

Im Folgenden erfolgt diese durch die Beschreibung und Analyse der einzelnen Ausprägungen der Persönlichkeitsrechte. Anschließend werden sie bewertet und miteinander verglichen. All dies schafft ein besonders tiefes Fundament für den internationalen Datentransfer und schützt die Menschen und ihre Rechte bei der digitalen Datenübermittlung.

2.2 Besondere Ausprägung der Persönlichkeitsrechte

Die Persönlichkeitsrechte in Bezug auf personenbezogene Daten finden im Grunde genommen ihre besondere Ausprägung im Recht auf Privatsphäre, dem Recht auf Datenschutz und dem Recht auf informationelle Selbstbestimmung.

2.2.1 Das Recht auf Privatsphäre

> *„There was some anxiety about the extent to which a general deterioration in privacy might affect the individual in future, and most people thought „privacy" to be important, even though there was no clear understanding of what it covered. The only conclusion to be drawn was that privacy is a basic need of both a free society and a mature personality [...] The trouble with privacy is that it is difficult to circumscribe and it is difficult to define."*[126]

Die Privatsphäre ist ausnahmslos für jeden Menschen wichtig. Sie ermöglicht die freie Entfaltung der Persönlichkeit und gibt jedem Einzelnen die Möglichkeit, in Ruhe gelassen zu werden. Die Gewährleistung der Privatsphäre garantiert wiederum die Persönlichkeitsrechte. In der digitalen Welt ist der Schutz der Privatsphäre und damit der Schutz der Persönlichkeitsrechte besonders wichtig, aber auch besonders schwierig. Die Verfügbarkeit von technischen Geräten, die Geschwindigkeit der Vervielfältigung und die Übermittlung von Daten mit persönlichem Inhalt machen es oft unmöglich, die digitale Welt bzw. den Datentransfer zu kontrollieren. Dies wiederum erschwert es, die Betroffenen vor einer unrechtmäßigen Verarbeitung ihrer Daten zu schützen und ihnen die Ausübung ihrer Rechte zu ermöglichen.

Das Recht auf Privatsphäre ist als ein Grundrecht auf der ganzen Welt anerkannt.[127] Im Grunde genommen garantiert es die private Sphäre ohne Einmischung eines anderen – sei es einer anderen Person, eines Unternehmens, einer Behörde oder einer Regierung. In unserem digitalen Zeitalter umfasst die Privatsphäre auch die private digitale Sphäre, wobei digitale Nutzerdaten eine entscheidende Rolle spielen. Privatsphäre ist gegeben, wenn sowohl eine subjektive Erwartung an die Privatsphäre besteht als auch die Gesellschaft als Ganzes diese Erwartung an die Privatsphäre anerkennt.[128]

126 *Dworkin*, The Younger Committee Report on Privacy, 399, 399 ff.
127 Datenschutz, abrufbar: https://edps.europa.eu/data-protection/data-protection_de, zuletzt abgerufen am 04.08.2023.
128 U.S. Supreme Court - 442 U.S. 735 (1979) – Smith v. Maryland; *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 248.

Die Verletzung der Privatsphäre bedeutet in der EU und in den USA dasselbe. Das Recht auf Privatsphäre wird verletzt, wenn in unangemessener Weise in die Privatsphäre eines anderen eingedrungen wird (z. B. wenn jemand durch das Fenster seines Hauses heimlich abfotografiert wird), wenn der Name oder das Bild eines anderen verwendet wird, wenn das Privatleben eines anderen in unangemessener Weise bekannt gemacht wird oder wenn eine andere Person in der Öffentlichkeit in ein falsches Licht gerückt wird.[129] Hierbei geht es nicht unbedingt um das Eindringen in einen physischen Raum oder Ort. Hier sind auch die Situationen einzubeziehen, in denen eine Person ohne ihren Willen gebracht wird, wie z. B. Rufschädigung oder ähnliches.

Obwohl die Privatsphäre international anerkannt ist, gibt es unterschiedliche Auffassungen darüber, was sie bedeutet und wie sie geschützt werden sollte bzw. wann sie verletzt wird. Es wurden mehrere Theorien aufgestellt und Umfragen durchgeführt, warum sich die Rechte, Gesetze und Anliegen zum Schutz der Privatsphäre in verschiedenen Kulturen unterscheiden: Die Unterschiede beziehen sich auf Unterschiede in den kulturellen Werten[130] – und dies insbesondere im Hinblick auf die digitale Welt. Sie spiegeln unterschiedliche Internet-Erfahrungen sowie unterschiedliche Ziele der zugrunde liegenden politischen Institutionen wider (ohne die Unterschiede in der Privatsphäre der tatsächlichen Nutzer des Internets widerzuspiegeln).[131] Der Online-Anteil eines Nutzers hängt davon ab, wie lange das Heimatland des Nutzers bereits Zugang zum Internet hat.[132] Darüber hinaus kommen bei der Betrachtung der kulturellen Unterschiede in Bezug auf die Rechte und den Schutz der Privatsphäre weitere Überlegungen ins Spiel, einschließlich der Auffassung der Nationen von Eigentumsrechten und der Redefreiheit.[133]

Es existiert eine Meinung, dass die EU-Datenschutzbehörden unangemessen anspruchsvoll sind, während ihre amerikanischen Pendants lächerlich lasch sind.[134] Ob diese der Wahrheit entspricht bzw. worin die Unterschiede sowie die Feinheiten der besonderen Ausprägung der Persönlichkeitsrechte nach EU- und US-Recht bestehen, wird im Folgenden erläutert und festgestellt.

129 The rights of publicity and privacy, abrufbar: abrufbar: http://www.publicdomainsherpa.com/rights-of-publicity-and-privacy.html, zuletzt abgerufen am 30.07.2023.
130 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. XXVII ff.
131 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. XXVII ff.
132 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. XXVII ff.
133 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. XXVII ff.
134 *McGeveran*, Arizona Law Review, 959, 959.

2.2.1.1 Recht auf Privatsphäre in der EU

Die Menschenwürde ist in der EU als absolutes Grundrecht aufgenommen und wird als gesellschaftlicher Wert betrachtet.[135] In diesem Verständnis von Menschenwürde spielen u. a. die Privatsphäre und die Kontrolle über eigenen Informationen eine entscheidende Rolle,[136] auf die ausnahmelos jede Person ein Recht hat.[137]

Die Privatsphäre umfasst nach der Rechtsprechung des EGMR (Europäische Gerichtshof für Menschenrechte) im Wesentlichen die Anerkennung eines privaten Raums oder einer privaten Sphäre, in die andere nicht eindringen dürfen.[138] Darüber hinaus beinhaltet die Privatsphäre das Recht einer Person, sich vor Belästigungen zu schützen, oder das Recht, die eigenen Informationen zu kontrollieren, eine Möglichkeit, Aspekte des Privatlebens einer Person aus der Öffentlichkeit herauszuhalten, sowie die Frage, wie und wann Informationen weitergegeben werden dürfen.[139] In hohem Maße wird Privatsphäre als ein Element der Freiheit betrachtet, d. h. als Recht, frei von staatlichen Eingriffen zu sein.[140]

Das Recht auf Privatsphäre und auf Privatleben ist in Art. 8 EMRK und Art. 7 GrCh verankert.[141] Der Begriff „Privatsphäre“ („Privat- und Famillienleben“ nach Art. 8 EMRK) wurde im Laufe der Zeit weiterentwickelt und umfasst nun auch die Verarbeitung von Informationen, die sich auf eine bestimmte oder bestimmbare Person beziehen, einschließlich Informationen über ihr Arbeitsumfeld.[142] Ein spezifisches Element des Rechts auf Privatsphäre ist die Vertraulichkeit der Kommunikation,[143] die stark die freie Entfaltung der Persönlichkeit ermöglicht und unterstützt.

135 Datenschutz, abrufbar: https://edps.europa.eu/data-protection/data-protection_de, zuletzt abgerufen am 04.08.2023.
136 Datenschutz, abrufbar: https://edps.europa.eu/data-protection/data-protection_de, zuletzt abgerufen am 04.08.2023.
137 Das Recht auf Privatsphäre im digitalen Zeitalter, abrufbar: https://www.welivesecurity.com/deutsch/2017/04/06/recht-privatsphaere-digitales-zeitalter/, zuletzt abgerufen am 30.07.2023.
138 *Fuster/Hijmans*, Discussion paper: The EU rights to privacy and personal data protection: 20 years in 10 questions: Discussion paper, S. 7.
139 Das Recht auf Privatsphäre im digitalen Zeitalter, abrufbar: https://www.welivesecurity.com/deutsch/2017/04/06/recht-privatsphaere-digitales-zeitalter/, zuletzt abgerufen am 30.07.2023.
140 Datenschutz, abrufbar: https://edps.europa.eu/data-protection/data-protection_de, zuletzt abgerufen am 04.08.2023.
141 Datenschutz, abrufbar: https://edps.europa.eu/data-protection/data-protection_de, zuletzt abgerufen am 04.08.2023.
142 *Fuster/Hijmans*, Discussion paper: The EU rights to privacy and personal data protection: 20 years in 10 questions: Discussion paper, S. 7.
143 *Fuster/Hijmans*, Discussion paper: The EU rights to privacy and personal data protection: 20 years in 10 questions: Discussion paper, S. 7.

2.2.1.2 Das Recht auf Privatsphäre / „the right to be left alone“ in den USA[144]

„It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage.“
Willes, J., in Millar v. Taylor, 4 Burr. 2303, 2312

Im US-Bundesverfassungsrecht gibt es keine ausdrückliche Normierung der Privatheit / „Privacy“; die Garantien ergeben sich jedoch aus einzelnen Verfassungsbestimmungen.[145] Amendement 1, 3, 4, 5 und 9 U.S. Const. regelt den persönlichen Schutz und damit das Recht auf Privatsphäre.[146] Der Privacy Act von 1974 erklärt, dass das Recht auf Privatsphäre ein persönliches und grundlegendes Recht ist, das durch die Verfassung der Vereinigten Staaten / „Constitution of the United States“ (U.S. Const.) geschützt wird.[147] Jedoch gibt es in den USA keine allumfassende Bundesgesetzgebung, die die Privatsphäre und den Schutz persönlicher Informationen gewährleistet; stattdessen wird auf Bundesebene ein sektorspezifischer Ansatz verfolgt.[148]

Der Privacy Act ist ein Bundesgesetz, das jedoch nicht das Recht auf Privatsphäre als Ganzes regelt, sondern nur einen Teilbereich davon. Der Zweck des Gesetzes besteht darin, ein Gleichgewicht zwischen der Notwendigkeit der Regierung, Informationen über Einzelpersonen zu erhalten und dem Recht der Menschen zu schaffen, von ungerechtfertigten Eingriffen in ihre Privatsphäre geschützt zu werden, die sich aus der Sammlung, Verwaltung, Verwendung und Offenlegung von personenbezogenen Daten durch Bundesbehörden ergeben.[149] Dieser Act wurde 1988 durch den **Computer Matching and Privacy Act** geändert. Später erließ der Kongress die **Computer Matching and Privacy Protection Amendments of 1990**.[150]

144 Benennung vom Louis Brandeis, Richter am Obersten Gerichtshof der USA. S.: What Are Individual Rights? Definition and Examples, abrufbar: https://www.thoughtco.com/individual-rights-definition-and-examples-5115456, zuletzt abgerufen am 30.07.2023.
145 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 207.
146 Privacy, abrufbar: https://www.law.cornell.edu/wex/Privacy, zuletzt abgerufen am 30.07.2023.
147 *Boyne*, Data Protection in the United States, S. 300.
148 *Boyne*, Data Protection in the United States, S. 299.
149 Privacy Act of 1974, 5 U.S.C. § 552a, abrufbar: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1279, zuletzt abgerufen am 30.07.2023.
150 Privacy Act of 1974, 5 U.S.C. § 552a, abrufbar: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1279, zuletzt abgerufen am 30.07.2023.

Das Recht auf Schutz der Privatsphäre umfasst zwei wichtige Arten der Einstufung der Privatsphäre.[151] Die erste ist die **Informationsprivatsphäre**, d. h. das Recht einer Person, die Weitergabe von persönlichen Informationen über sich selbst an andere zu kontrollieren.[152] Die zweite ist **persönliche Autonomie**, d. h. das Recht, wichtige Entscheidungen über die eigenen intimsten Beziehungen, das Familienleben und die Körperfunktionen zu treffen.[153] Das Recht auf Privatsphäre schützt das Recht, von anderen Menschen in Ruhe gelassen zu werden.[154]

2.2.1.3 Vergleich des Rechts auf Privatsphäre in der EU und in den USA

Das Recht auf Privatsphäre ist sowohl in der EU als auch in den USA als Grundrecht anerkannt. Es umfasst sowohl den privaten Raum / das Privatleben einer Person als auch ihren Einfluss auf die sie betreffenden Informationen. Außerdem schützt dieses Recht eine Person bzw. sein Wohlbefinden vor der Öffentlichkeit bzw. staatlichen Eingriffen, um jedem Einzelnen die Möglichkeit zu geben, seine Persönlichkeit frei und ungestört von äußeren Einflüssen zu entwickeln. Indem die EU- und US- Rechtssysteme die Privatsphäre als ein Grundrecht betrachten, versuchen sie, dem Einzelnen mehr Kontrolle über seine Daten zu geben.[155]

Der Unterschied zwischen der EU und den USA in Bezug auf dieses Recht besteht darin, dass das Recht auf Privatsphäre in der EU grundlegend garantiert ist und im ganzen Europa gesetzlich verankert wird, während die USA dieses Recht sektorspezifisch regeln. Dieses Recht ist nicht in einem länderübergreifenden Gesetz verankert. Daher ist eine Person in den USA nur in weniger Fällen und in geringerem Maße als in der EU geschützt.

Bei Betrachtung des Rechts auf Privatsphäre, einschließlich des Privacy Act, sowie anderer Gesetze und des gesamten Rechtssystems der USA lässt sich feststellen, dass der Schutz der Privatsphäre in der EU besser und umfassender gewährleistet ist als in den Vereinigten Staaten. Diese Feststellung wird die zwei folgenden Aussagen bestätigen: 1. Die Festlegung von Marie Boyne in The American Journal of comparative law: *„In many parts of Europe, privacy intrusions that Americans have come to take for granted, are prohibited.“*[156] *2.* Bemerkung von Bob Sullivan: *„Europeans reserve their deepest distrust for corporations, while Americans are far more concerned about their government invading their privacy.“*[157]

151 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 356.
152 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 356.
153 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 356.
154 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 248.
155 *Stucke*, Breaking Away: How to Regain Control Over Our Data, Privacy, and Autonomy, S. 133.
156 *Boyne*, Data Protection in the United States, S. 343.
157 *Boyne*, Data Protection in the United States, S. 343.

2.2.2 Recht auf Datenschutz / „Data Privacy“ bzw. „Data Protection“[158]

Das Recht auf Privatsphäre korrespondiert mit dem Recht auf Datenschutz.[159] Das Verhältnis zwischen den beiden Rechten ergibt sich aus der Tatsache, dass Datenschutz sich aus dem allgemeineren Recht auf Privatsphäre ableitet und ihm ,,dient“.[160] Es ist unmöglich, einer Person Privatsphäre zu gewähren, ohne ihre personenbezogenen Daten zu schützen.

Der Datenschutz ist von der Datensicherheit und der Informationssicherheit abzugrenzen (s. S→ 104-105). Die Datensicherheit garantiert im Grunde genommen den technischen Datenschutz. Ist die Rede von Informationssicherheit, ist der Schutz aller Daten, d. h. sowohl personenbezogener als auch nicht personenbezogener Daten gemeint, nicht aber den Schutz von Menschen oder ihrer Privatsphäre.

Ganz konkret: Wenn eine Person die Kontrolle über ihre Daten hat, bedeutet dies, dass ihre Datenschutz-Rechte geschützt sind; sind die Datenschutz-Rechte geschützt, ist die Privatsphäre garantiert; die Garantie der Privatsphäre schafft den Raum für die Ausübung der Persönlichkeitsrechte; sind die Persönlichkeitsrechte ausgeübt, sind die Menschenrechte gewährt.

Weltweit gibt es zwei große Ansätze für den Schutz personenbezogener Daten: Der ,,sektorale“ / ,,sectoral“ und der ,,umfassende“ / ,,comprehensive“ Ansatz. Bei dem **sektoralen** Ansatz legen verschiedene gesetzliche Regelungen die Normen und Vorschriften für einzelne Wirtschaftsbereiche fest.[161] Außerhalb dieser Bereiche wird der Schutz der Privatsphäre ausschließlich dem freien Markt überlassen, wobei die verschiedenen Gerichtsbarkeiten unterschiedliche Bereiche und Schutzniveaus regeln.[162]

Als Beispiel für den sektoralen Ansatz sind die USA zu nennen. Die Vereinigten Staaten haben den Schutz der Privatsphäre in verschiedenen Bereichen gesetzlich geregelt (u. a. in den Bereichen Telekommunikation, Gesundheitsinformationen und Kreditauskunft), aber es gibt wenig Einheitlichkeit hinsichtlich der Art des Datenschutzes, der in diesen Bereichen geboten wird.[163] Für die überwiegende Mehrheit der Unternehmen, die nicht in diese stärker regulierten Sektoren fallen, verfolgen die USA einen Ansatz des Verbraucherschutzes in Bezug auf den Datenschutz.[164]

158 Das Recht auf Datenschutz hat seinen Ursprung im deutschen Konzept der informationellen Selbstbestimmung, wie es vom Bundesverfassungsgericht 1983 entwickelt wurde. Es spiegelt die Idee wider, dass Personen als Eigentümer ihrer eigenen personenbezogenen Daten betrachtet werden können. S.: *Fuster/Hijmans*, Discussion paper: The EU rights to privacy and personal data protection: 20 years in 10 questions: Discussion paper, S. 6.

159 Datenschutz, abrufbar: https://edps.europa.eu/data-protection/data-protection_de, zuletzt abgerufen am 04.08.2023.

160 *Sharpson*, Schlussanträge der Generalanwältin Eleanor Sharpston vom 27. September 2018 Rechtssache C-345/17 (ECLI:EU:C:2018:780) – Rn. 30; *Fuster/Hijmans*, Discussion paper: The EU rights to privacy and personal data protection: 20 years in 10 questions: Discussion paper, S. 3.

161 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 152.

162 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 152.

163 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 152.

164 *McGeveran*, Arizona Law Review, 959, 959.

Kritiker argumentieren, dass dies Lücken im Gesetz hinterlässt und zu verwirrenden Unstimmigkeiten führt.[165] Den Datenchutz („Privacy Protection“) in diesen Lücken dem freien Markt zu überlassen, ist ineffektiv, da es große Unterschiede in der Verhandlungsmacht zwischen Einzelpersonen und großen Organisationen gibt, die personenbezogene Daten sammeln, nutzen oder weitergeben wollen.[166]

Eine andere Art von Ansatz für den Schutz personenbezogener Daten ist ein umfassender Ansatz. Ein **umfassendes** staatliches Engagement in Form von Datenschutzregelungen ist gerechtfertigt, da die Privatsphäre als ein Menschenrecht verstanden wird, das mit Individualität, Würde und Autonomie verbunden ist; robuste Datenschutzrechte können zwar wirtschaftliche Kosten verursachen, sind aber aufgrund der Werte, um die es geht, gerechtfertigt.[167]

Der Ursprung umfassender Datenschutzregelungen liegt in den Datenschutzleitlinien der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung / „Organisation for Economic Co-operation and Development Privacy Guidlines“ (OECD) aus dem Jahr 1980, die der Sammlung, Verwendung und Offenlegung personenbezogener Daten eine Richtung geben sollten.[168] Obwohl diese Leitlinien gemeinsam entwickelt wurden, gingen die EU und die USA in den folgenden Jahren hinsichtlich ihrer Anwendbarkeit in unterschiedliche Richtungen.[169] Europa verschärfte sie und machte sie direkt durchsetzbar, während die USA sie als einen Rahmen „nützlicher Leitlinien“ betrachteten, die von der Industrie frei übernommen werden konnten.[170] Aufgrund des gemeinsamen ideologischen Erbes weisen diese Regelungen in der Regel trotzdem einige allgemeine bzw. gemeinsame Merkmale auf.[171]

165 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 152.
166 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 152.
167 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 152.
168 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 152.
169 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 152.
170 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 152.
171 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 153.

2.2.2.1 Recht auf Datenschutz in der EU

In der EU ist das Recht auf Datenschutz ein in den europäischen Verfassungen verankertes Grundrecht,[172] das als wesentliches Element einer nachhaltigen Demokratie zu sehen ist.[173] Das Recht auf den Schutz personenbezogener Daten ist in Art. 8 GrCh festgelegt und in der DSGVO weiterentwickelt.[174] Gemäß Art. 16 AEUV hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.[175]

Die DSGVO befasst sich mit Fragen des Datenschutzes und der IT-Sicherheit und bildet die Grundlage für alle europäischen nationalen Gesetze.[176] Artikel 1 Abs. 2 DSGVO besagt: „Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten".

Wenn keine missbräuchliche Datenverarbeitung stattfindet, sind die personenbezogenen Daten geschützt. Der Schutz dieser Daten umfasst u. a. die folgenden Kriterien: Eine Person hat die Kontrolle über ihre Daten, sie bestimmt über deren Weitergabe bzw. Nichtweitergabe oder verlangt deren Löschung. Schließlich bedeutet dies, dass die Person nach ihrem Willen agieren und sich frei entfalten kann, was wiederum die Gewährleistung der Grundrechte darstellt.

Die Verarbeitung von Daten ist nur aus einem gesetzlich festgelegten Grund zulässig,[177] d. h. dass die Datenverarbeitung nicht erlaubt ist, es sei denn, es gibt eine klare gesetzliche Grundlage bzw. einen Erlaubnistatbestand.

Dieses Recht stützt sich auf eine Struktur mit drei Säulen bzw. Aspekten.[178] Es geht nämlich darum, 1. Verantwortlichen Verpflichtungen aufzuerlegen (Verpflichtungen des Verantwortlichen), 2. den Personen, über die Daten verarbeitet werden, subjektive Rechte zu gewähren (Rechte des Betroffenen) und 3. die unabhängige Kontrolle der Einhaltung der Pflichten und der Achtung der Rechte zu etablieren (Kontrolle).[179] Dieses Struktur beruht auf der grundlegenden Annahme, dass dieses Recht alle Daten über bestimmte oder bestimmbare Personen abdecken muß, unabhängig von ihrer Art oder ihrer möglichen Weiterverwendung.[180]

172 *Pell/Grace*, United States of America v. Microsoft Corporation: On Writ of Certiorari to the United States Court of Appeals for the Second Circuit, S. 3.

173 Datenschutz, abrufbar: https://edps.europa.eu/data-protection/data-protection_de, zuletzt abgerufen am 04.08.2023.

174 *Fuster/Hijmans*, Discussion paper: The EU rights to privacy and personal data protection: 20 years in 10 questions: Discussion paper, S. 6.

175 *Pell/Grace*, United States of America v. Microsoft Corporation: On Writ of Certiorari to the United States Court of Appeals for the Second Circuit, S. 4.

176 IT-Sicherheit und Datenschutz: Die Gesetzeslage in den USA und Deutschland im Vergleich, abrufbar: https://digitaleweltmagazin.de/it-sicherheit-und-datenschutz-die-gesetzeslage-in-den-usa-und-deutschland-im-vergleich/, zuletzt abgerufen am 04.08.2023.

177 *McGeveran*, Arizona Law Review, 959, 966.

178 *Fuster/Hijmans*, Discussion paper: The EU rights to privacy and personal data protection: 20 years in 10 questions: Discussion paper, S. 6.

179 *Fuster/Hijmans*, Discussion paper: The EU rights to privacy and personal data protection: 20 years in 10 questions: Discussion paper, S. 6.

180 *Fuster/Hijmans*, Discussion paper: The EU rights to privacy and personal data protection: 20 years in 10 questions:

2.2.2.2 Recht auf Datenschutz in den USA

In den USA existieren keine allgemeinen übergeordneten nationalen Regelungen in Bezug auf Datenschutz.[181] Die Datenschutzgesetze sind in hohem Maße von den Reaktionen der Regierung auf private Klagen sowie Vorfällen abhängig.[182] Es gibt nur Bundesdatenschutzgesetze bzw. -regulierungen, die sektorspezifisch sind oder sich auf bestimmte Arten von Daten konzentrieren.[183] So verlangt beispielsweise der CLOUD Act die Offenlegung von Inhalten, Aufzeichnungen oder anderen Informationen über einen Kunden oder Abonnenten im Falle einer strafrechtlichen Untersuchung.

Das allgemein geltende amerikanische Datenschutzrecht verfolgt einen „Verbraucherschutz"-Ansatz.[184] Die US-Regelungen wie CCPA und CPRA konzentrieren sich auf die Verbraucher. Eine Verbraucher-Schutzregelung erlaubt im Allgemeinen jede Verarbeitung personenbezogener Daten, es sei denn, sie ist ausdrücklich untersagt.[185]

Datenschutz regelt den ordnungsgemäßen Umgang mit personenbezogenen Daten bei der Datenverarbeitung vom Datenverarbeiter (1. Verpflichtungen des Datenverarbeiters). Weiterhin regelt der Datenschutz die Kontrolle durch einen Betroffenen über die Daten, die sich auf ihn beziehen[186] (2. Rechte des Einzelnen) und Überwachung der Einhaltung des Datenschutzvorschriften (3. Kontrolle).

Discussion paper, S. 6.

181 *Gabel u.a. - Podebrad/Gabel*, Rechtshandbuch Cyber-Security, S. 357.

182 IT-Sicherheit und Datenschutz: Die Gesetzeslage in den USA und Deutschland im Vergleich, abrufbar: https://digitaleweltmagazin.de/it-sicherheit-und-datenschutz-die-gesetzeslage-in-den-usa-und-deutschland-im-vergleich/, zuletzt abgerufen am 04.08.2023.

183 Data Protection Laws and Regulations USA 2023, abrufbar: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa, zuletzt abgerufen am 05.08.2023.

184 *McGeveran*, Arizona Law Review, 959, 966.

185 *McGeveran*, Arizona Law Review, 959, 966.

186 A Guide to the Federal and State Data Privacy Laws in the U.S., abrufbar: https://www.comparitech.com/data-privacy-management/federal-state-data-privacy-laws/, zuletzt abgerufen am 30.07.2023.

2.2.2.3 Vergleich des Rechts auf Datenschutz und in der EU und in den USA

Das Recht auf Datenschutz ist sowohl in der EU als auch in den USA gewährleistet. Es schützt die Daten, die einen Personenbezug aufweisen und garantiert damit die Grundrechte und Grundfreiheiten natürlicher Personen. Es ist jedoch erwähnenswert, dass die Datenschutzbestimmungen in der EU und in den USA unterschiedliche Ansätze verfolgen.

Die EU verfügen über einen umfassenden Datenschutzrahmen, wenn die USA einen sektoralen Ansatz verfolgen. In den USA ist die Datenverarbeitung normalerweise erlaubt, es sei denn, das Gesetz verbietet es, während es in der EU nicht erlaubt ist, es sei denn, das Gesetz gestattet es.[187] Der Datenschutz in der EU garantiert den Schutz jeder Person, während der Datenschutz in den USA bestimmte Daten schützt und sich weitgehend auf die Verbraucher konzentriert. US-Datenschutzgesetze sind in hohem Maße von den Reaktionen der Regierung auf private Klagen sowie von Vorfällen abhängig, was dazu führt, dass die Rechtslage in Bezug auf Datenschutz und IT-Sicherheit nur als ein „Framework" angesehen wird.[188] Infolgedessen ist ein zuverlässiger Schutz der Privatsphäre nicht gegeben.[189]

All dies beweist die folgende Aussage: „*However, in contrast to the European Union's data protection approach, which in many ways represents the gold standard of privacy protections, the dominant approach in the United States is grounded in consumer protection regulations.*"[190]

187 *McGeveran*, Arizona Law Review, 959, 966.

188 IT-Sicherheit und Datenschutz: Die Gesetzeslage in den USA und Deutschland im Vergleich, abrufbar: https://digitaleweltmagazin.de/it-sicherheit-und-datenschutz-die-gesetzeslage-in-den-usa-und-deutschland-im-vergleich/, zuletzt abgerufen am 04.08.2023.

189 IT-Sicherheit und Datenschutz: Die Gesetzeslage in den USA und Deutschland im Vergleich, abrufbar: abrufbar: https://digitaleweltmagazin.de/it-sicherheit-und-datenschutz-die-gesetzeslage-in-den-usa-und-deutschland-im-vergleich/, zuletzt abgerufen am 04.08.2023.

190 *Boyne*, Data Protection in the United States, S. 301.

2.2.3 Das Recht auf (informationelle) Selbstbestimmung[191]

Die Selbstbestimmung ist eine Art Überkategorie innerhalb des Persönlichkeitsrechts und beinhaltet viele Aspekte.[192] Sie beginnt mit der Selbstbestimmung über den eigenen Körper und betrifft den gesamten Bereich der medizinischen Behandlung und Patientenaufklärung.[193]

Das Selbstbestimmungsrecht, das erstmals in der UN Charta verankert wurde, garantiert den Menschen das Recht, ihren politischen Status frei zu bestimmen und u. a. ihre wirtschaftliche und soziale Entwicklung frei zu verfolgen.[194] In Art. 1 Abs. 2 UN Charta wird das Wort „Selbstbestimmung" / „Self Determination" ausdrücklich erwähnt.

Die informationelle Selbstbestimmung kommt ins Spiel, wenn über die Verfügungsgewalt über die eigenen personenbezogenen Daten gesprochen wird.[195] Die Erhebung dieser Daten, ohne dass die betroffene Person dies kontrollieren kann, schafft ein Gefühl der Überwachung. Fühlt man sich überwacht, verliert man die Möglichkeit, seine Freiheitsrechte auszuüben und seine Persönlichkeit frei zu entfalten. Deshalb muss jeder das Recht haben, über seine Daten selbst zu bestimmen. Aus diesem Grund wurde das Recht auf informationelle Selbstbestimmung, das seine besondere Ausprägung im Persönlichkeitsrecht findet, ständig gefordert.[196]

2.2.3.1 Das Recht auf informationelle Selbstbestimmung in der EU

Das Recht auf informationelle Selbstbestimmung ist ein von der Rechtsprechung entwickeltes Grundrecht, das in die Fallgruppe der allgemeinen Persönlichkeitsrechte fällt.[197] Es umfasst das Recht des Einzelnen, selbst zu entscheiden, wann und aus welchem Grund er wem gegenüber personenbezogene Daten bekannt macht.[198] Dieses Recht steht jeden Menschen zu[199] und ist in den meisten europäischen Staaten geregelt.[200]

---

191 Es wurde vom Bundesverfassungsgericht Deutschlands in seinem Urteil von 1983 als das Recht auf informationelle Selbstbestimmung bezeichnet. S.: Informational Self-Determination of Europe and Its Importance, abrufbar: https://legal-dialogue.org/informational-self-determination-of-europe-and-its-importance, zuletzt abgerufen am 30. 07.2023.

192 *Brüggemeier*, Personality Rights in European Tort Law, S. 574.

193 *Brüggemeier*, Personality Rights in European Tort Law, S. 574.

194 Self-determination, abrufbar: https://minorityrights.org/law/self-determination/, zuletzt abgerufen am 30.07.2023.

195 *Brüggemeier*, Personality Rights in European Tort Law, S. 574.

196 Die in diesem Abschnitt dargestellte Auffassung befindet sich in dem folgenden Artikel. S.: Das Recht auf informationelle Selbstbestimmung, abrufbar: https://www.bpb.de/themen/recht-justiz/persoenlichkeitsrechte/244837/das-recht-auf-informationelle-selbstbestimmung/, zuletzt abgerufen am 30.07.2023.

197 *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung: Die zivilrechtliche Erfassung des Datenhandels, S. 80.

198 *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung: Die zivilrechtliche Erfassung des Datenhandels, S. 80.

199 Das Recht auf informationelle Selbstbestimmung, abrufbar: https://www.bpb.de/themen/recht-justiz/persoenlichkeitsrechte/244837/das-recht-auf-informationelle-selbstbestimmung/, zuletzt abgerufen am 30.07.2023.

200 *Brüggemeier u.a.*, Personality Rights in European Tort Law, S. 574.

Das Recht auf informationelle Selbstbestimmung als Grundrecht führt dazu, dass der Staat, wenn er Informationen von seinen Bürgern haben will, immer eine Rechtsgrundlage benötigt, die ein angemessenes Gleichgewicht bzw. einen Ausgleich zwischen diesem Recht und den Interessen des Staates schafft.[201]

Werden personenbezogene Daten von privaten Unternehmen verarbeitet (z. B. Erhebung von personenbezogenen Daten zur Schaltung von individualisierter Werbung), müssen diese die zahlreichen Datenschutzgesetze einhalten, die das Recht auf informationelle Selbstbestimmung näher definieren.[202]

Das informationelle Selbstbestimmungsrecht wird nur bei Vorliegen eines überwiegenden öffentlichen Interesses eingeschränkt.[203]

2.2.3.2 Das Recht auf informationeller Selbstbestimmung in den USA

Ungeachtet der unterschiedlichen rechtlichen Strategien, damit umzugehen, ist Autonomie als Selbstbestimmung der eigenen Persönlichkeit in den USA wie in Europa der entscheidende Wert hinter der Privatsphäre.[204]

Die USA kennen den Begriff der „informationellen Selbstbestimmung“ als ein eigenständiges Recht nicht. Dort werden nur bestimmte Aspekte der Privatsphäre unter der Überschrift des Rechts auf Privatsphäre geschützt.[205] Die informationelle Selbstbestimmung spiegelt die Beschreibung der Privatsphäre von Alan F. Westins wider: *“The right of the individual to decide what information about himself should be communicated to others and under what circumstances.“*[206]

201 Das Recht auf informationelle Selbstbestimmung, abrufbar: https://www.bpb.de/themen/recht-justiz/persoenlichkeitsrechte/244837/das-recht-auf-informationelle-selbstbestimmung/, zuletzt abgerufen am 30.07.2023.

202 Das Recht auf informationelle Selbstbestimmung, abrufbar: https://www.bpb.de/themen/recht-justiz/persoenlichkeitsrechte/244837/das-recht-auf-informationelle-selbstbestimmung/, zuletzt abgerufen am 30.07.2023.

203 Informational Self-Determination of Europe and Its Importance, abrufbar: https://legal-dialogue.org/informational-self-determination-of-europe-and-its-importance, zuletzt abgerufen am 30.07.2023.

204 *Rouvroy/Poullet*, Right to informational self-determinationand the Value of Self-Development: Reassessing the Importance of Privacy for Democracy, S. 65.

205 *Rehm*, SSRN Electronic Journal 01.2000.

206 Empowering Resignation: There's an App for That, abrufbar: https://dl.acm.org/doi/fullHtml/10.1145/3411764.3445293, zuletzt abgerufen am 30.07.2023.

2.3 Die Zusammenfassung der Persönlichkeitsrechte

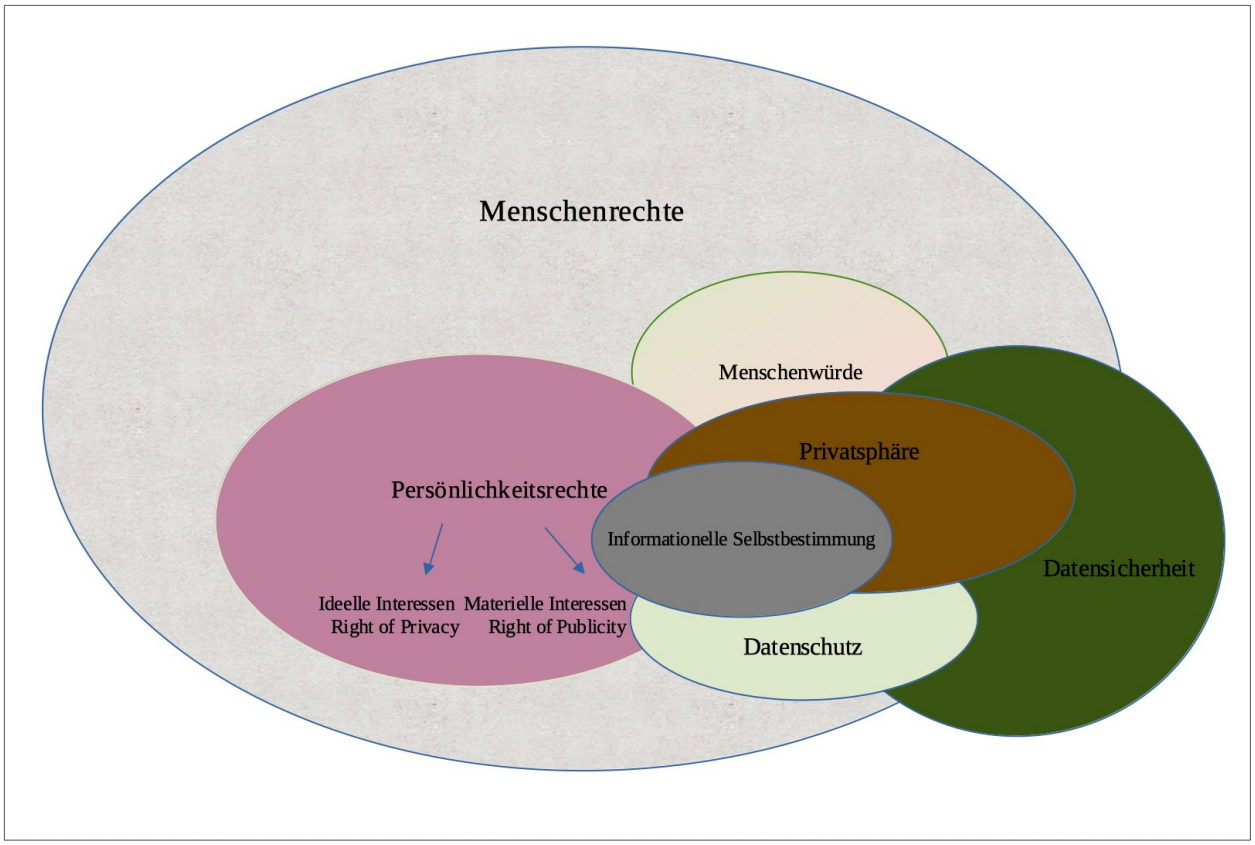

Abbildung 2.3 Persönlichkeitsrechte und ihre besonderen Ausprägungen

Der Gegenstand der oben beschriebenen Kapitel waren die Persönlichkeitsrechte. Die Persönlichkeit, die jeder Mensch von Geburt an in sich trägt und aufbaut, findet ihre Wurzeln in den alten lateinischen Sprache und wird in der Persönlichkeitspsychologie umfassend definiert. Ihr Schutz prägt die freiheitliche Demokratie, und damit ist ihre rechtliche Regulierung von entscheidender Bedeutung. Da der digitale Wandel diese Rechte stark beeinflusst, ist es die tägliche Aufgabe der Rechtswissenschaft, die Anforderungen zum Schutz der Persönlichkeitsrechte an die Realität anzupassen.

Durch die Darstellung der **Menschenrechte** wurde bestimmt, dass die moralischen Grundsätze, die seit den mosaischen Gesetzen festgehalten wurden, in jedem Land auf unterschiedliche Art und Weise anerkannt bzw. ratifiziert sind. Diese Regelungen schaffen die Grundlagen für die von ideellen Maßstäben geprägten Persönlichkeitsrechte, die den höchsten, unverletzlichen und unveräußerlichen Rechtsgütern[207] dienen. Die Gewährleistung dieser wird durch ideelle sowie materielle Interessen, das Recht auf Privatsphäre bzw. das Recht auf Öffentlichkeit, das Recht auf Datenschutz und durch das Recht auf informationelle Selbstbestimmung gewährleistet.

207 *Götting*, Persönlichkeitsrechte als Vermögensechte, S. 4.

Bei der Untersuchung des europäischen **ideellen und materiellen Interesses**, die dem amerikanischen Right of Privacy und Right of Publicity entsprechen, hat sich gezeigt, dass die Persönlichkeitsrechte sowohl in der EU als auch in den USA gewährleistet sind.

Wird das **Recht auf Privatsphäre** weiter im Detail auf beiden Ebenen betrachtet, so lässt sich feststellen, dass in vielen Bereichen der Persönlichkeitsrechte der Schutz dieses Rechts in den USA geringer sein könnte.

Während das EU-**Datenschutzrecht** einen grundrechtsbasierten Ansatz verfolgt, bei dem es in erster Linie um den Schutz der betroffenen Personen geht, basiert dieser in den USA auf dem Wirtschaftsrecht und bekommt daher weit weniger Relevanz.[208] Hierbei ist wichtig zu erwähnen, dass, wenn sich das EU-Datenschutzrecht auf natürliche Personen und Einzelpersonen in Europa konzentriert, im Mittelpunkt des modernen US-Datenschutzrecht der Verbraucher steht.

Wenn das **Recht auf informationelle Selbstbestimmung** in der EU als Grundrecht aufgenommen ist, berufen sich die USA auf das Recht auf Privatsphäre bezüglich dieses Recht. Es zeigt deutlich, dass die EU einen umfassenderen Schutz der informationeller Selbstbestimmung bietet, der letztlich die Möglichkeit schafft, die Persönlichkeit frei zu entfalten und alle Grundrechte und Grundfreiheiten auszuüben, anders als die USA.

Aus diesen Gründen ist festzustellen, dass die Persönlichkeitsrechte, auf die jede Person weltweit Anspruch hat, sowohl in der EU als auch in den USA anerkannt sind und durch unterschiedliche Ansätze umgesetzt werden. Wenn es um den Grad oder das Ausmaß des Schutzes geht, hat die EU einen wesentlichen Vorsprung vor den USA.

Die Bedeutung der Persönlichkeit und die Darstellung der damit verbundenen Rechte hat deutlich gezeigt, wie wichtig dieses Thema ist und welche Auswirkungen es auf das Leben eines jeden Menschen haben kann. Erwähnenswert ist auch, dass Personen und die sie betreffenden Daten kaum von der Technologie und der Digitalisierung zu trennen sind.

Wird festgestellt, dass die Persönlichkeitsrechte für die freie Entfaltung jedes Einzelnen von entscheidender Bedeutung sind, ist herauszufinden, was genau dies mit dem Datentransfer zu tun hat und wie sie in diesem Bereich geschützt werden könnten. Noch spannender wird das Thema, wenn es in einem internationalen Kontext durch das Zusammenspiel von europäischem und amerikanischem Recht betrachtet wird. All dies wird in den kommenden Kapiteln geschehen.

208 IONOS, Aktuelle Rechtslage zum US-Datentransfer unter besonderer Berücksichtigung des US CLOUD Act, S. 4.

3 (Internationaler) Datentransfer

3.1 Datentransfer – historische Entwicklung und heutige Ausprägung

Die digitale Welt ist viel älter, als die Menschen glauben.[209] Sie findet ihre Wurzeln zwischen 1646 und 1716, als der deutsche Philosoph und Mathematiker, Gottfried Wilhelm Leibniz, das Binärsystem entwickelte.[210]

Der Startschuss für die elektronische Datenübertragung geht auf das Jahr 1837 zurück, als der Amerikaner Samuel Morse den Telegraphen mit Morsezeichen erfand. Seitdem konnten Nachrichten in kodierter Form große Entfernungen überwinden. Kurze Zeit später, nämlich im Jahr 1843, wurde von dem Schotten Alexander Bain ein Telegraf mit Kopierfunktion entwickelt, mit dem Notizen und Zeichnungen elektronisch verschickt werden konnten. Dieses Gerät war der Vorläufer des Faxgeräts. Das erste Mal wurde 1928 ein Fax per Funk über den Atlantik übermittelt.[211]

In den späten 1930er und frühen 1940er Jahren war bereits die Rede davon, den Begriff „digital“[212] in seiner heutigen Bedeutung zu verwenden. Dies bringt die ersten Computer hervor, die digital, d. h. mit dem Binärsystem 1 und 0, rechneten. 1937 entwickelte der deutsche Ingenieur Konrad Zuse den Z1, der noch mechanisch aufgebaut war. Er ähnelte den bereits seit Jahrhunderten existierenden Rechenschiebern und war der erste, mit dem man mit binären Zahlen rechnen und gleichzeitig frei programmieren konnte.[213]

209 Was ist Digital? Einfach erklärt, abrufbar: https://praxistipps.chip.de/was-ist-digital-einfach-erklaert_41596, zuletzt abgerufen am 31.07.2023.

210 Was ist Digital? Einfach erklärt, abrufbar: https://praxistipps.chip.de/was-ist-digital-einfach-erklaert_41596, zuletzt abgerufen am 31.07.2023.

211 Dieser historische Fakt wird in dem folgenden Artikel beschrieben. S.: Sicherer Datenaustausch: Definition, Entwicklung und Formate,
abrufbar: https://teamdrive.com/blog-de/sicherer-datenaustausch-definition-entwicklung-und-formate, zuletzt abgerufen am 01.08.2023.

212 Das Wort „digital“ kommt vom lateinischen „digitus“, was „Finger, Zehe“ bedeutet, und bezieht sich auch auf das Abzählen unter 10 an den Fingern. Das Wort „digit“ steht in der englischen Sprache sowohl für „Finger“ als auch für „Zahl“. In diesem Sinne steht also 10 für 10 Finger und auch für eine Zahl, die aus 1 und 0 besteht. S.: Seit wann gibt es die Digitalisierung? Teil I: Eine Reise in die Geschichte des Computers und der Digitalisierung, abrufbar:https://www.wfb-bremen.de/de/page/stories/digitalisierung-industrie40/seit-wann-gibt-es-die-digitalisierung-geschichte-teil-eins, zuletzt abgerufen am 31.07.2023.

213 Dieser historische Schritt wird in dem folgenden Artikel beschrieben. S.: Seit wann gibt es die Digitalisierung? Teil I: Eine Reise in die Geschichte des Computers und der Digitalisierung, abrufbar:
https://www.wfb-bremen.de/de/page/stories/digitalisierung-industrie40/seit-wann-gibt-es-die-digitalisierung-geschichte-teil-eins, zuletzt abgerufen am 31.07.2023.

Der „Meilenstein für den Datenaustausch“ ist der 10.12.1969, die Geburt des Internets, als Nutzer an vier amerikanischen Universitäten zum ersten Mal Daten miteinander austauschten.[214] In den 1960-1970er Jahren wurden Computer immer häufiger zum Speichern und Durchsuchen von Regierungs- und Unternehmensdaten verwendet.[215] Das Aufkommen von sozialen Netzwerken, Plattformen und Messengern wie Facebook, YouTube oder WhatsApp hat den Datenaustausch nochmals beschleunigt.[216]

Im Jahr 2018 verbrachten Erwachsene in den USA durchschnittlich fast vier Stunden am Tag damit, auf ihr Telefon, ihren Computer oder ihr Tablet zu schauen.[217] Bis 2019 verbrachten Amerikaner durchschnittlich sechs Stunden und 31 Minuten pro Tag online.[218] Europäer und Amerikaner verbringen etwas weniger Zeit online als der befragte weltweite Durchschnitt von sechs Stunden und 42 Minuten.[219] Dennoch entsprechen sechs Stunden pro Tag im Laufe eines Lebens einem Viertel eines Lebens.[220]

Mittlerweile gibt es mehrere Plattformen, um Daten auszutauschen. Cloud Computing gewinnt sowohl im privaten als auch im beruflichen Umfeld zunehmend an Bedeutung. Die Speicherung und Verwaltung von Daten in der Cloud, deren Inhalte rund um die Uhr ortsunabhängig aus der Cloud abgerufen werden können, gehört zum Alltag. Der Datenaustausch erfolgt in Echtzeit, wobei das schnelle Internet für eine hohe Übertragungsgeschwindigkeit sorgt.[221] Diese Prozesse sind viel komplexer als im vergangenen Jahrhundert und ermöglichen einen schnellen und reibungslosen Datentransfer in jeden Winkel der Welt.

214 Sicherer Datenaustausch: Definition, Entwicklung und Formate, abrufbar: https://teamdrive.com/blog-de/sicherer-datenaustausch-definition-entwicklung-und-formate, zuletzt abgerufen am 01.08.2023.
215 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. XXVII.
216 Sicherer Datenaustausch: Definition, Entwicklung und Formate, abrufbar: https://teamdrive.com/blog-de/sicherer-datenaustausch-definition-entwicklung-und-formate, zuletzt abgerufen am 01.08.2023.
217 *Stucke*, Breaking Away: How to Regain Control Over Our Data, Privacy, and Autonomy, S. 227.
218 *Stucke*, Breaking Away: How to Regain Control Over Our Data, Privacy, and Autonomy, S. 227.
219 *Stucke*, Breaking Away: How to Regain Control Over Our Data, Privacy, and Autonomy, S. 227.
220 *Stucke*, Breaking Away: How to Regain Control Over Our Data, Privacy, and Autonomy, S. 227.
221 Diese historische Entwicklung wird in dem folgenden Artikel beschrieben. S.: Sicherer Datenaustausch: Definition, Entwicklung und Formate, abrufbar: https://teamdrive.com/blog-de/sicherer-datenaustausch-definition-entwicklung-und-formate, zuletzt abgerufen am 01.08.2023.

3.2 Internationaler Datentransfer

3.2.1 Internationaler Datentransfer – ihre Relevanz und ihr Bezug auf das Rechtswesen

„Netz- und Informationssysteme, sowie elektronische Kommunikationsnetze und -dienste spielen eine lebenswichtige Rolle in der Gesellschaft und sind mittlerweile zum Hauptmotor des Wirtschaftsraums geworden“ – stellt ErwGr. 1 S. 1 Rechtsakt zur Cybersicherheit[222] klar. Daten und ihr transatlantischer Transfer sind wesentliche Elemente vieler Prozesse, Geschäfte oder Aktivitäten, die weltweit täglich durchgeführt werden und jeden gesellschaftlichen Raum beeinflussen, sei es das tägliche Leben, die nationale Sicherheit oder die Wirtschaft.

Heutzutage treten Menschen in aller Welt mehr als je zuvor digital miteinander in Kontakt, tauschen von Home-Office oder anderen Orten Geschäftsunterlagen aus, führen Videotelefonate oder arbeiten an gemeinsamen Projekten online.[223] Durch solche fortschreitende Digitalisierung wird die Fähigkeit, große Datenmengen in Echtzeit sowie schnell über das Internet auszutauschen, immer wichtiger und ihre Handhabung immer komplexer.[224]

Seit 2015 wird häufig über einen besseren Schutz der EU-Außengrenzen diskutiert.[225] Um den Terrorismus besser zu bekämpfen und die Freizügigkeit zu wahren, sollte die EU Ein- sowie Ausreisen aller Drittstaatsangehörigen fehlerfrei biometrisch erfassen und Einreisegenehmigungen für visumfreie Reisende lückenlos elektronisch ausstellen.[226] Um Identitätsbetrug zu vermeiden und Ermittlungen zu beschleunigen, sollen die Polizei- sowie Grenzkontrollbehörden über besseren Zugang zu Daten aus verschiedenen EU-Datenbanken verfügen.[227] Dieses politische Thema bezieht sich auf intelligente Grenzen sowie Infrastrukturen für den transnationalen Datentransfer.[228]

222 Der vollständige Name des Aktes lautet wie folgt: VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit).

223 Bmwi, Sicherer Datenaustausch: Themenheft Mittelstand-Digital, 1, 2.

224 Datentransfer: So versenden Sie große Dateien sicher und einfach, abrufbar: https://www.dracoon.com/de/datentransfer, zuletzt abgerufen am 01.08.2023.

225 *Bossong*, SWP-Studie: Intelligente Grenzen und interoperable Datenbanken für die innere Sicherheit der EU: Umsetzungsrisiken und rechtsstaatliche Anforderungen, 5, 7.

226 *Bossong*, SWP-Studie: Intelligente Grenzen und interoperable Datenbanken für die innere Sicherheit der EU: Umsetzungsrisiken und rechtsstaatliche Anforderungen, 5, 7; vgl.: Europäischer Rat, Erklärung von Bratislava, 16.9.2016, S. 3 ff.

227 *Bossong*, SWP-Studie: Intelligente Grenzen und interoperable Datenbanken für die innere Sicherheit der EU: Umsetzungsrisiken und rechtsstaatliche Anforderungen, 5, 7.

228 *Bossong*, SWP-Studie: Intelligente Grenzen und interoperable Datenbanken für die innere Sicherheit der EU: Umsetzungsrisiken und rechtsstaatliche Anforderungen, 5, 5.

Der durch die Digitalisierung verursachte technologische Wandel schafft die Möglichkeiten, die Datenverarbeitung in fast allen Wirtschaftsbereichen zu revolutionieren.[229] Dadurch erreichen viele Unternehmen hohe Umsätze (z. B. Google oder Facebook).[230] Technische Innovationen der digitalen Wirtschaft und Erfassung sowie Nutzung von Daten bringen viele wirtschaftliche Vorteile, wie z. B. Effizienzgewinne und wettbewerbsfördernde Wirkung.[231] Darüber hinaus können Daten mit ihrer Kombinationsfähigkeit ein Persönlichkeitsbild schaffen und die Marktmacht von Unternehmen stärken.[232] Die Datenverarbeitung mit persönlichkeitsrechtsrelevanten Inhalten steigt.[233]

Die Datenverarbeitung bzw. der (internationale) Datentransfer, der viel Positives beinhaltet, bringt auch Negatives bzw. Komplexes mit sich. Der Austausch von vertraulichen Geschäftsdaten innerhalb eines Unternehmens oder mit anderen Organisationen stellt ein nicht zu unterschätzendes Hindernis dar.[234] Mehr digitale Verfahren verursachen Sicherheitsrisiken.[235] Das permanente Home-Office bringt neue Fragen der Datensicherheit mit sich, selbst für Unternehmen, die über eine gute digitale Infrastruktur verfügen.[236] Sensible Geschäftsdaten sollen sicher ausgetauscht werden, um Hackerangriffe zu verringern[237] und Geschäftsprozesse am Laufen zu halten. Kommt es zu einem Vorfall, sind sowohl personenbezogene Daten eines Betroffenen als auch Unternehmensdaten gefährdet, was viele tiefgravierenden Schäden (z. B. ungewünschte Veröffentlichung personenbezogener Daten oder Reputationsschäden eines Unternehmens) mit sich ziehen könnte.

Das Thema ,,Internationaler Datentransfer“ ist auf den ersten Blick ein technisches Thema, das viel u. a. zum Alltag, zur nationalen Sicherheit und zur Wirtschaft beitragen kann. Wird es jedoch im Zusammenhang mit einer sicheren oder rechtskonformen Verarbeitung, den Rechten der Menschen oder einem nachhaltigen Datenschutz genauer betrachtet, kommt sehr schnell Rechtswissenschaft ins Spiel.

229 Bundeskartellamt, Big Data und Wettbewerb: Schriftenreihe „Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft“, 1, 4.
230 Bundeskartellamt, Big Data und Wettbewerb: Schriftenreihe „Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft“, 1, 1.
231 Bundeskartellamt, Big Data und Wettbewerb: Schriftenreihe „Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft“, 1, 6.
232 Bundeskartellamt, Big Data und Wettbewerb: Schriftenreihe „Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft“, 1, 4.
233 *Specht/Mantz -Wieczorek,* Handbuch: Europäisches und deutsches Datenschutzrecht, S. 168.
234 Bmwi, Sicherer Datenaustausch: Themenheft Mittelstand-Digital, 1, 2.
235 Bmwi, Sicherer Datenaustausch: Themenheft Mittelstand-Digital, 1, 2.
236 Bmwi, Sicherer Datenaustausch: Themenheft Mittelstand-Digital, 1, 2.
237 Bmwi, Sicherer Datenaustausch: Themenheft Mittelstand-Digital, 1, 2.

Wenn die von einem Unternehmen verarbeiteten Daten von einer Behörde angefordert werden, stellt sich die Frage, wie weit eine Behörde in das Privatleben einer Person eindringen darf, um ihre Aufgaben zu erfüllen und die Sicherheit anderer Einwohner zu gewährleisten oder was die Rolle eines IT-Service-Providers bzw. Cloud-Service-Provider ist, der eine enorme Menge der Nutzerdaten verarbeitet. Das Thema wird noch komplexer, wenn es im internationalen Kontext betrachtet wird. Hier muss u. a. sichergestellt werden, unter welchen Umständen eine Behörde eines anderen Landes vom IT-Unternehmen die Herausgabe personenbezogener Daten einer Person eines anderen Landes verlangen kann oder nicht.

Es verdient, hervorgehoben zu werden, dass trotz aller erheblicher Vorteile die exzessive Datennutzung aus Verbrauchersicht als kritisch zu betrachten ist, da viele Verbraucher nicht wissen, welche ihrer Daten zu welchem Zweck benutzt und weitergegeben werden.[238] Werden die Daten unrechtmäßig und technisch ungeschützt transferiert, kann eine Person nicht in der Lage sein, sie zu verwalten, ihre Privatsphäre zu schützen und ggf. ihre Persönlichkeitsrechte auszuüben.

Um optimale Vorteile und Rechtssicherheit bei der digitalen Datenübermittlung anzubieten, müssen Themen wie z. B. die Zugriffskontrolle oder die Art und Weise des Datentransfers festgelegt werden. Dies ermöglicht einen effizienten und durchdachten Umgang mit digitalen Daten und verschafft den Unternehmen einen Wettbewerbsvorteil bei ihrer Digitalisierungsstrategie. Dabei sollen Informationen intelligent verwendet, Geschäftsprozesse standardisiert und die Effizienz in allen Prozessen gesteigert werden. Diese Prozesse sollten rechtskonform und technisch so abgesichert werden, dass die Benutzerfreundlichkeit nicht darunter leidet. Jegliche Verarbeitung personenbezogener Daten steht unter besonderem Schutz und soll diesbezüglich hohen Anforderungen gerecht werden,[239] die sowohl rechtliche als auch technische Themengebiete abdecken. All dies spielt bei dem internationalen Datentransfer eine zentrale Rolle, denn dadurch finden die persönlichkeitsrechtliche Merkmale entsprechende Berücksichtigung und werden die Rechte und Freiheiten jedes Einzelnen gewährleistet.

238 Bundeskartellamt, Big Data und Wettbewerb: Schriftenreihe „Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft“, 1, 4.

239 Diese Aussage ist in dem folgenden Artikel zu finden. S.: Datentransfer: So versenden Sie große Dateien sicher und einfach, abrufbar: https://www.dracoon.com/de/datentransfer, zuletzt abgerufen am 01.08.2023.

3.2.2 Internationaler Datentransfer – ihr Verhältnis mit den Persönlichkeitsrechten

Es wurde bereits festgestellt, dass die Persönlichkeitsrechte für jeden Mensch sehr bedeutend sind. Durch diese Rechte werden die Grundrechte und -freiheiten des Einzelnen garantiert und werden ihm die rechtlichen Mittel in die Hand gegeben, um seine Persönlichkeit und sein Wohlbefinden zu entwickeln und zu verbessern.

Darüber hinaus wurde festgestellt, dass der internationale Datentransfer sowohl für die Digitalisierung als auch in jeder Art von Sozialraum für jeden Einzelnen eine wesentliche Bedeutung hat. Außerdem beeinflusst er die technologische Entwicklung sowie jegliche Art der Arbeitsprozesse und geht tief in das Leben eines jeden Einzelnen.

Die Berührungspunkte sowie Verhältnisse zwischen diesen Themen, nämlich Persönlichkeitsrechte und internationaler Datentransfer, wurde auch bereits erwähnt. Sie stehen nebeneinander und sind voneinander abhängig. Nun stellt sich die Frage, wie genau sie miteinander kommunizieren, in welchem Verhältnis sie zueinander stehen oder welche charakteristischen Merkmale sie einander näher bringen.

Niemand kann beschließen, in der Welt ohne eigene Persönlichkeit zu leben. Die Persönlichkeit wird immer getragen und kontinuierlich (unbewusst) aufgebaut. So bestimmt jede Person ihr Wohlbefinden und manchmal sogar, ob sie überhaupt leben will. Das Leben und die Gesundheit eines jeden Menschen sind das Wichtigste und Bedeutendste. Dazu gehört das Recht, sich frei zu entfalten und ungestört von äußeren Einflüssen zu leben. Es gibt kein Recht, keine Sache oder Situation, die Vorrang hat. Aus diesem Grund ist es unerlässlich, die Persönlichkeitsrechte zu schützen und damit die Grundrechte und -freiheiten u. a. das Recht auf Leben und Gesundheit, zu gewährleisten.

Ist die Rede von der Persönlichkeit, steht das Thema ,,Technik“ oder ,,Digitalisierung“ gleich daneben. Es gibt kaum einen Menschen auf der Welt, der kein Handy, kein Tablet oder keinen Laptop hat. Jeden Tag werden zahlreiche Apps heruntergeladen und Inhalte ins Internet hochgeladen. Diese enthalten sehr viele vom einzelnen Personen abgeleitete Elemente. Die Welt hat sich so weit entwickelt, dass selbst eine Uhr, eine Waschmaschine oder ein Auto viel mehr Informationen enthält als eine Bibliothek, und diese Informationen werden ständig weitergegeben. Wie Aaron Franklin Brantly in seinem Buch beschreibte: ,,INFORMATION IS THE LIFEBLOOD of modern states.“[240]

240 *Brantly*, The decision of Attack: Military and Intelligence Cyber Decision-Making, S. 101.

Man spricht nicht mit jedem, den man auf der Straße trifft, über alles. Man sucht sich bestimmte Leute aus, mit denen man etwas gemeinsam unternehmen, über seine Probleme sprechen oder mit denen man zum Feiern gehen möchte. Genauso verhält es sich mit der Technik. Wenn man ein Foto mit seinem Handy gemacht hat, sollte das nicht bedeuten, dass der Hersteller des Handys es haben kann, oder wenn man ein Video mit einer bestimmten Software bearbeitet hat, sollte das nicht bedeuten, dass der Softwareentwickler sich es anschauen kann. Leider gelingt es nicht immer. Ein Beweis dafür sind die Worte von Googles CEO Eric Schmidt, die er 2010 sagte: *„We know where you are. We know where you've been. We can more or less know what you have been thinking about."*[241]

Aus diesem Grund ist es wichtig, diese beiden Dimensionen, nämlich Digitalisierung und Recht, gemeinsam zu betrachten und zu analysieren. Die Digitalisierung, die Datenverarbeitung bzw. deren Entwicklung ist bedeutsam und entscheidend für die Globalisierung und die weitere Entwicklung. Allerdings sollten diese entsprechend gesteuert und kontrolliert werden, wobei die Rechtswissenschaft dazu einen großen Beitrag leisten kann. Die Datenübermittlung unter besonderer Berücksichtigung der Persönlichkeitsrechte schafft Transparenz. Dadurch wird klar, welche Daten bzw. Informationen man aus seinem Alltag in die Software / Hardware eingebracht hat und welche Daten bzw. Informationen von der Software / Hardware an den Hersteller oder den Entwickler gehen werden.

Der Datentransfer zwischen einer Person und einem Softwareentwickler oder Hardwarehersteller ist ein einfaches Beispiel. Es kann so weit gehen, dass andere beteiligte Personen oder Einrichtungen ins Spiel kommen. Nehmen wir an, eine Regierungsbehörde hat einen Verdacht, dass eine Person sich unrechtmäßig verhalten hat oder ein Verbrechen begangen hat. Auch Behörden wissen, dass sie mit Hilfe der Technologie zeitnah und ungefiltert an die benötigten Informationen gelangen können. Daher versuchen sie zunehmend, die Informationen über eine Person von einer Organisation zu erhalten, die sofort zahlreiche Daten liefern kann, wie Amazon oder Google.

Noch kritischer wird das Thema, wenn es auf internationaler Ebene betrachtet wird. Hier kommen Gedanken auf wie z. B.: Darf eigentlich eine Behörde eines Landes in das Privatleben eines Bürgers eines anderen Landes eindringen? Wenn ja, wie weit darf sie gehen? Wer kontrolliert sie? Wer schützt die betroffene Person? Welches Landesrecht gilt in einem solchen Fall? Diese sind nur einige der Fragen, die bedacht, kritisch analysiert und bewertet werden sollten.

241 *Stucke*, Breaking Away: How to Regain Control Over Our Data, Privacy, and Autonomy, S. 14.

Damit der Datentransfer nicht unbeachtet bleibt und Transparenz bei jeder Übermittlung herrscht, ist es wichtig, das Thema „Internationaler Datentransfer“ gut zu kennen und seine rechtlichen Anforderungen genau zu regeln. Hierbei ist es wichtig, die technischen Anforderungen des digitalen Datentransfers genau zu betrachten.

Auf diese Weise kann ein Instrument entwickelt werden, das eine rechtskonforme und technisch machbare Option bietet, deren Einsatz auf internationaler Ebene möglich ist. Damit wird eine Lage geschaffen, in der Menschen ihre Rechte wahrnehmen, Organisationen ihre Aufgaben erfüllen und Behörden die nationale sowie internationale Sicherheit gewährleisten können – alles im Rahmen des Schutzes der Persönlichkeitsrechte bei dem Datentransfer.

3.3 Begrifflichkeiten und Eingrenzung des Untersuchungsgegenstands

Alle Gesellschaften der Industrieländer sind heute informationsgetriebener als früher.[242] Dieser Bedeutungszuwachs bezieht sich nicht nur auf Geschäftsgeheimnisse, sondern alle Arten von Informationen[243] von Nutzerdaten von Facebook bis hin zu Staatsgeheimnissen. Der Umgang mit Daten und deren Schutz ist ein preisunabhängiger Wettbewerbsparameter, der umso wichtiger wird, je mehr die Nutzer dem rücksichtsvollen Umgang mit ihren Daten große Bedeutung beimessen.[244] Um die Daten ordnungsgemäß zu verarbeiten und zu schützen, sollten auf Seiten der Verantwortlichen bzw. Auftragsverarbeiter bestimmte Anforderungen erfüllt werden, die wiederum die Ausübung der Persönlichkeitsrechte ermöglichen.

Um dies analysieren zu können, sollte zunächst bestimmt werden, was unter Daten und Informationen zu verstehen ist und wie sie einzuordnen sind (A. Daten und Informationen). Danach ist es festzustellen, was genau unter ihre Verarbeitung bzw. ihrem Transfer / ihrer digitalen Übermittlung gemeint ist (B. Untersuchungsgegenstand – internationaler Datentransfer). Dies wird in den folgenden Abschnitten näher erläutert und untersucht.

3.3.1 Daten und Informationen

3.3.1.1 Bedeutung von Daten und Informationen

Daten stellen Zeichen oder Zeichenketten dar, die interpretationsfreie Bestandteile von Sprache oder Schrift sind, und lassen sich durch Übertragung des gesprochenen Wortes auf einen Datenträger sichtbar voneinander unterscheiden.[245] Sie sind inhaltliche Komponenten von Informationen, die immer einen Kontext für die Interpretation benötigen.[246]

Nach der Filterung der Daten von einem Rezipienten durch die Interpretation kommt die Information im Gehirn an.[247] Informationen sind also die mit Bedeutung ausgestatteten Daten.[248] Sie sind wesentliche Elemente der Geschäftsprozesse einer Organisation, die durch den Kontext zu verwertbaren Informationen werden.[249] Aus Informationen ergibt sich das Wissen ,,als Ergebnis der Verarbeitung von Informationen durch das Bewusstsein“.[250]

242 *Ann u.a. -Ann*, Praxishandbuch: Know-how-Schutz, S. 4 ff.
243 *Ann u.a. -Ann*, Praxishandbuch: Know-how-Schutz, S. 4 ff.
244 Bundeskartellamt, Big Data und Wettbewerb: Schriftenreihe „Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft“, 1, 12.
245 *Specht*, CR 2016, 288, 290; vgl.: *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung: Die zivilrechtliche Erfassung des Datenhandels, S. 19; vgl. auch: Voßkuhle *u.a. -Albers*, Grundlagen des Verwaltungsrechts, § 22 Rn. 6.
246 *Hildebrand u.a.*, Daten- und Informationsqualität: Die Grundlage der Digitalisierung, S. 145.
247 *Specht*, CR 2016, 288, 290; vgl.: *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung: Die zivilrechtliche Erfassung des Datenhandels, S. 20 ff.
248 *Hildebrand u.a.*, Daten- und Informationsqualität: Die Grundlage der Digitalisierung, S. 5.
249 *Hildebrand u.a.*, Daten- und Informationsqualität: Die Grundlage der Digitalisierung, S. 145.
250 *Hildebrand u.a.*, Daten- und Informationsqualität: Die Grundlage der Digitalisierung, S. 7.

3.3.1.2 Arten von Daten

3.3.1.2.1 Personenbezogene Daten[251]

In der EU werden als personenbezogene Daten nach Art. 4 Nr. 1 DSGVO die Informationen betrachtet, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Solche Daten können objektive (z. B. Videos, Substanz im Blut oder Fingerabdrücke)[252] oder subjektive (z. B. Meinungen, Beurteilungen oder Einschätzungen)[253] Daten sein.

In den USA werden für personenbezogene Daten die Begriffe wie „Personally Identifiable Information (PII)", „Personal Data", „Personal Information" oder „Identifiable Information" verwendet. Sie bezeichnen unterschiedliche Merkmale der Daten und weisen divergente Feinheiten auf. Grundsätzlich sind diese Daten Informationen, die einen bestimmten Verbraucher oder Haushalt bzw. eine natürliche Person identifizieren, sich auf sie beziehen, sie beschreiben oder vernünftigerweise mit ihr in Verbindung gebracht werden können.[254] Solche Daten können z. B. die Sozialversicherungsnummer, der militärischer Rang, der Familienstand, die Rasse oder das Gehalt sein.[255] In den USA sind personenbezogene Daten nach den sektorspezifischen Gesetzen klassifiziert.[256]

3.3.1.2.2 Pseudonymisierte Daten

In der EU werden nach Art. 4 Nr. 5 DSGVO als pseudonymisiert die Daten betrachtet, deren Personenbezug nur durch zusätzliche Informationen wiederhergestellt werden kann. Sie sind so zu sagen potentielle personenbezogene Daten.[257]

In den USA sind pseudonyme Daten in den verschiedenen Gesetzen definiert. Beispielsweise sind nach 1798.140 (r) CCPA pseudonymisiert die personenbezogene Daten, die es ermöglichen, einen Personenbezug mit zusätzlichen Informationen wiederherzustellen.

---

251 In Bezug auf die Datenverarbeitung nach der DSGVO werden neben personenbezogenen Daten auch pseudonymisierte Daten betrachtet. In den USA gibt es, anders als in der EU, keine einheitliche Definition für den Umfang personenbezogener Daten. Daher kann in bestimmten Situationen und in Bezug auf bestimmte Staaten der unterschiedliche Umfang/die unterschiedliche Definition von personenbezogenen herangezogen werden. Aus diesem Grund wird in diesem Kapitel die Definition nach dem amerikanischen Recht nur allgemein vorgestellt. In der Dissertation wird der Begriff „personenbezogene Daten" sowohl auf deutscher als auch auf amerikanischer Ebene verwendet, um Ungereimtheiten zu vermeiden.

252 EuGH, Urt. v. 17.10.2013 – C-291/ 12, ZD 2013, 608 Rn. 27 – Schwarz.

253 Art.-29-Datenschutzgruppe, Stellungnahme 4/2007, WP 136, 20.6.2007, S. 7 ff.

254 Siehe eine Auflistung von Definitionen personenbezogener Daten in dem folgenden Artikel. S.: Comparing U.S. State Data Privacy Laws vs. The EU's GDPR, abrufbar: https://pro.bloomberglaw.com/brief/data-privacy-laws-in-the-u-s/, zuletzt abgerufen am 01.08.2023.

255 Defense Privacy and Civil Liberties Office, Introduction to the privacy Act, 1, 20.

256 Siehe Auflistung vom Definitionen, Klassifikationen sowie Verarbeitung der Informationen in: *Boyne,* Data Protection in the United States, 299, 302-304.

257 *Schantz/Wolff -Schantz*, Das neue Datenschutzrecht: Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, S. 101.

3.3.1.2.3 Nicht-personenbezogene Daten

Im Hinblick auf den internationalen Datentransfer werden geschäftskritische Daten, Metadaten, maschinengenerierte Daten, Big Data sowie gemischte Daten als nicht-personenbezogene Daten definiert und werden wie folgt klassifiziert:

1. Daten, die ursprünglich nicht personenbezogene Daten waren (z. B. die von Sensoren erzeugten Daten über Wetterbedingungen) und
2. Daten, die ursprünglich einen Personenzug hatten und später anonymisiert[258] wurden.[259]

3.3.1.2.3.1 Geschäftskritische Daten

Als geschäftskritische Daten zählen vertrauliche Informationen, die nur für bestimmten Personengruppen im Unternehmen zugänglich sind, wie z. B. Daten in den strategischen Dokumenten[260] bzw. Betriebsgeheimnisse. Sie sind in der Organisation als vertrauliche bzw. streng vertrauliche Informationen gekennzeichnet und verdienen einen besonderen Schutz.

3.3.1.2.3.2 Metadaten

Metadaten sind Informationen über den Inhalt von Daten, aber nicht deren Inhalt selbst. Solche Daten können u. a. Zeitstempel, IP-Adressen, Geräte, Browsersignaturen und E-Mail-Adressen umfassen. Zu den Metadaten gehört nicht der Inhalt des Internetverkehrs oder der Kommunikation wie E-Mails oder Textnachrichten.[261]

258 Anonymisierung von personenbezogenen Daten bedeutet, dass die anonymisierten Daten nicht mehr durch zusätzliche Informationen einer bestimmten Person zugeordnet werden können. S.: Europäische Kommission_COM(2019) 250 final, S. 5.

259 Europäische Kommission, COM(2019) 250 final, S. 5.

260 Definition: vertrauliche Daten, abrufbar: https://www.it.tum.de/it/vertrauliche-daten/definition-vertrauliche-daten/#c2421, zuletzt abgerufen am 01.08.2023.

261 Diese Definition des Begriffs „Metadaten“ ist in dem folgenden Artikel zu finden. S.: A breakdown of the Patriot Act, Freedom Act, and FISA, abrufbar: https://www.comparitech.com/blog/vpn-privacy/a-breakdown-of-the-patriot-act-freedom-act-and-fisa/, zuletzt abgerufen am 01.08.2023.

3.3.1.2.3.3 Maschinengenerierte Daten

Bei maschinengenerierten Daten handelt es sich um unternehmensbezogene Daten, die für bestimmte Transaktionen oder für den Maschinenbetrieb wertvoll sein könnten.[262] Der Begriff „maschinengenerierte Daten“ bezieht sich auf die Informationen, die von Hardware- sowie Software-Elementen, die an Maschinen angebracht sind, erzeugt und übertragen werden.[263] Mit diesen Informationen können Produkte überwacht und Optimierungspotenziale oder Fehlerquellen identifiziert werden.[264]

3.3.1.2.3.4 Big Data

Für „Big Data“ existiert noch keine allumfassende Definition; im Wesentlichen geht es darum, große Mengen verschiedener Datentypen in hoher Geschwindigkeit aus diversen Quellen zu erzeugen, diese mit neuen sowie leistungsfähigen Verfahren und Algorithmen zu verarbeiten und zu analysieren.[265]

Darüber hinaus wird der Begriff „Big Data“ verwendet, um aktuelle technische Entwicklungen insbesondere im IT-Bereich zu beschreiben (z. B. die immense Zunahme der Datenübertragungsgeschwindigkeit und -kapazität sowie ihre Folgen für die ökonomische Verwertbarkeit von Daten.)[266]

3.3.1.2.3.5 Gemischte Daten

Ein gemischter Datensatz stellt eine Mischung aus personenbezogenen und nicht-personenbezogenen Daten dar, von denen der größte Teil in der Datenwirtschaft benutzt wird und auf technologische Entwicklungen zurückzuführen ist, z. B. Internet der Dinge / „Internet of Things“ (IoT) oder künstliche Intelligenz / „Artificial Intelligence“ (KI / AI).[267]

262 Bundeskartellamt, Big Data und Wettbewerb: Schriftenreihe „Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft“, 1, 2 ff.
263 Bundeskartellamt, Big Data und Wettbewerb: Schriftenreihe „Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft“, 1, 2 ff.
264 Bundeskartellamt, Big Data und Wettbewerb: Schriftenreihe „Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft“, 1, 2 ff.
265 Bundeskartellamt, Big Data und Wettbewerb: Schriftenreihe „Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft“, 1, 3.
266 Bundeskartellamt, Big Data und Wettbewerb: Schriftenreihe „Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft“, 1, 3.
267 Europäische Kommission_COM(2019) 250 final, S. 8.

3.3.2 Detaillierte Beschreibung des Untersuchungsgegenstands

3.3.2.1 Bedeutung von Datentransfer

Der Begriff **„Datentransfer“** bezieht sich auf „alle Methoden, die Informationen von einem Sender […] zu einem Empfänger […] übermitteln“. Im Kern geht es um die Übertragung digitaler Daten und Informationen, deren Transfer über das Internet erfolgt.[268]

Wird über die Datenübermittlung zwischen Menschen und Geräten gesprochen, die auf Gegenseitigkeit beruht (z. B. Versand von Fotos oder Dokumenten), wird **Datenaustausch** gemeint.[269] Die Begriffe „Datenaustausch“ und „Datenübermittlung“ stammen aus dem Bereich der Datenverarbeitung.[270]

Werden Daten digital ausgetauscht, spielt es keine Rolle, wo der Standort des Absenders oder Empfängers liegt, da ein solcher Datenaustausch von überall erfolgen kann. Jeder Projektbeteiligte kann jederzeit und von jedem Ort auf relevante Informationen zugreifen und diese bearbeiten. Es gibt verschiedene Möglichkeiten, Daten digital auszutauschen, z. B. über eine E-Mail, einen Freigabelink, einen FTP-Server oder über einen Upload in die Cloud.[271]

Der Begriff „**Internationaler Datentransfer**“ bezeichnet die grenzüberschreitende digitale Übertragung von Daten über nationale Grenzen hinweg. Bei der Betrachtung dieses Phänomens verwendet Bastian Baumann die folgenden Begriffe: „Grenzüberschreitende[r] Datenaustausch“, „grenzüberschreitende[r] Datenfluss“, „grenzüberschreitende[r] Datenverkehr“ bzw. „Transborder Data Flows“ oder „International Data Flow“.[272] Sie sind austauschbar und ermöglichen es, das Phänomen sowie die nuancierten Unterschiede zu verdeutlichen.[273] Diese Begriffe werden in der Monographie als Synonyme verwendet.

268 Diese Definition wird in dem folgenden Artikel beschrieben. S.: Datentransfer: So versenden Sie große Dateien sicher und einfach, abrufbar: https://www.dracoon.com/de/datentransfer, zuletzt abgerufen am 01.08.2023.

269 Sicherer Datenaustausch: Definition, Entwicklung und Formate, abrufbar: https://teamdrive.com/blog-de/sicherer-datenaustausch-definition-entwicklung-und-formate, zuletzt abgerufen am 01.08.2023.

270 Hier geht es um „Datenaustausch“. S.: Sicherer Datenaustausch: Definition, Entwicklung und Formate, abrufbar: https://teamdrive.com/blog-de/sicherer-datenaustausch-definition-entwicklung-und-formate, zuletzt abgerufen am 01.08.2023. Hier geht es um „Datenübermittlung“. S.: Datentransfer und Datenaustausch, abrufbar: https://www.dracoon.com/de/datentransfer, zuletzt abgerufen am 01.08.2023.

271 Diese Erläuterung des digitalen Datenaustauschs wird in dem folgenden Artikel beschrieben. S.: Datentransfer und Datenaustausch, abrufbar: https://www.dracoon.com/de/datentransfer, zuletzt abgerufen am 01.08.2023.

272 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 41.

273 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 41.

3.3.2.2 Umfang des Datentransfers

Es wurde festgestellt, was Daten und ihrer (internationaler) Transfer / (transatlantische) digitale Übermittlung bedeuten. Es ist nun klarzustellen, was für ein Umfang dieser Prozess hat. Es stellt sich die Frage: **Wo bzw. zwischen wem werden Daten transferiert?**

Der Umfang des Datentransfers ist relativ vielfältig, da es kaum noch Prozesse gibt, die ohne digitale Datenübermittlung möglich sind. Grundsätzlich sind bei diesem Thema die folgenden Arten zu unterscheiden: Datenübermittlung zwischen 1. Unternehmen und Endkunde / Privatpersonen, 2. zwischen Unternehmen, 3. zwischen Unternehmen und seinen Mitarbeitern oder 4. zwischen Unternehmen und Behörden.

In dieser Monographie wird das Thema „Internationaler Datentransfer" im Kontext des Verhältnisses zwischen **Unternehmen und Behörden** sowie **zwischen Unternehmen** betrachtet, da dieses viele wichtige Punkte für die Entwicklung und Ausübung von Persönlichkeitsrechten aufweist. In diesem Zusammenhang verdient es derzeit sowohl im europäischen als auch im amerikanischen Rechtsraum große Aufmerksamkeit. Das Thema ist auch im technischen Bereich, durch den die rechtlichen Anforderungen umgesetzt werden, sehr aktuell.

Die rechtlichen und technischen Anforderungen in Bezug auf internationale digitale Datenübertragungen, ihre Problematik und die damit verbundenen Lösungsvorschläge sind für alle Organisationen bzw. Verantwortlichen oder Auftragsverarbeiter gleichermaßen relevant, die mit der Datenverarbeitung bzw. -transfer konfrontiert sind. Trotzdem wurden von den Unternehmenskategorien IT-Unternehmen bzw. IT-Dienstleister und Cloud-Service-Provider ausgewählt, da sie den digitalen Datentransfer prägen und damit eine entscheidende Rolle in der digitalen Welt spielen.

Cloud-Dienste sind Infrastrukturen, Plattformen oder Software, die von Drittanbietern gehostet und den Nutzern über das Internet zur Verfügung gestellt werden. Cloud-Dienste fördern die Entwicklung von Cloud-nativen Anwendungen und die Flexibilität der Arbeit in der Cloud. Für den Zugriff auf diese Dienste benötigen die Nutzer nichts weiter als einen Computer, ein Betriebssystem und eine Internet-Verbindung.[274] Cloud-Dienste werden oft für die Verarbeitung personenbezogener Daten (z. B. von Personaldaten) verwendet.[275]

274 Diese Beschreibung ist in dem folgenden Artikel zu finden. S.: What are cloud services? abrufbar: https://www.redhat.com/en/topics/cloud-computing/what-are-cloud-services, zuletzt abgerufen am 01.08.2023.

275 *Voigt/von dem Bussche,* EU-Datenschutz-Grundverordnung (DSGVO), S. 315.

3.4 Rechtliche Voraussetzungen zum internationalen Datentransfer

Die Datenübermittlung in außereuropäische Länder ist aus wirtschaftlicher Sicht unerlässlich, und daher dürfen die Hürden für solchen Transfer nicht zu hoch sein.[276] Die Datenübermittlung in den europäischen Raum ist ebenso wichtig, darf jedoch nicht unbeschränkt oder unzureichend geregelt bleiben. Werden Daten digital und transatlantisch übermittelt, sind zahlreiche gesetzliche Vorgaben einzuhalten. Sie sind sowohl auf europäischer als auch auf amerikanischer Ebene vorgeschrieben und implementiert.

Im Folgenden wird dieses Thema zunächst im europäischen (A. Internationaler Datentransfer aus der EU in die USA) und dann im amerikanischen Rechtssystem (B. Internationaler Datentransfer aus den USA in die EU) untersucht. Nachher wird die Problematik zwischen diesen Rechtssystemen betrachtet (C. Konflikte zwischen den Datenschutzbestimmungen der EU und der USA). Folglich wird analysiert, wie es derzeit gehandhabt wird und was unternommen wird, um die Rechtslage zu verbessern (D. Internationale Bemühungen). Die bestmöglichen Lösungen und Vorschläge sind abschließend, basierend auf der oben beschriebenen Untersuchung, präsentiert (E. Digitaler Datentransfer bei gleichzeitigem Zusammenspiel von EU- und US-Datenschutzvorschriften). All dies wird schließlich zusammengefasst (Kapitel 8 – Die Zusammenfassung des internationalen Datentransfers).

3.4.1 Internationaler Datentransfer aus der EU in die USA

Der grenzüberschreitende Transfer personenbezogener Daten aus der EU in die USA ist im Wesentlichen in der DSGVO[277] geregelt, die die Anforderungen vorschreibt, die einerseits die Datenschutzrechte sowie den damit verbundenen Schutz der Persönlichkeitsrechte gewährleisten und andererseits ein reibungsloses Funktionieren einer Organisation ermöglichen. Die DSGVO gilt seit 2018.

3.4.1.1 Ziel der DSGVO

Artikel 1 DSGVO stellt das Ziel der DSGVO klar, nämlich „[…] Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten […] und freien Verkehr solcher Daten“. Es schließt selbstverständlich auch den freien grenzüberschreitenden Datenverkehr ein. Bei der Verarbeitung personenbezogener Daten schafft die DSGVO einen einheitlichen Rechtsrahmen im Europäischen Raum (in der EU) und im Europäischen Wirtschaftsraum (in EWR).

276 *Kühling/Buchner -Schröder*, DSGVO/BDSG, Art. 44 Rn. 1.

277 Während die DSGVO einen Governance-Rahmen für personenbezogene Daten in der EU schafft, bieten der Data Governance Act und der vorgeschlagene The European Data Act einen zusätzlichen Rahmen für die Wiederverwendung, die Übermittlung und den Schutz von nicht personenbezogenen Daten. S.: *Wood/Lewis*, CSIS, 03.2023, 1, 4.

3.4.1.2 Räumliche Anwendung der DSGVO

Die DSGVO findet nach Art. 3 Abs. 1 und 2 DSGVO Anwendung, wenn ein Verantwortlicher oder ein Auftragsverarbeiter im Rahmen seiner Tätigkeit eine Niederlassung in der Union hat (**Niederlassungsprinzip**) oder in der Union tätig ist, nämlich wenn er Waren oder Leistungen aus einem Drittland[278] in der Union einer Person anbietet oder ihr Verhalten von dort beobachtet (**Marktortprinzip**).[279] Es ist nicht davon abhängig, wo die Datenverarbeitung stattgefunden hat oder wo die verarbeitende Stelle ihren Sitz hat.[280] Damit gilt die DSGVO für die Handlungen sowohl in der EU als auch bei international agierenden Gesellschaften, die die Daten europäischer Bürger verarbeiten.[281]

In diesen beiden Fällen liegt im Hinblick auf Betroffene in der EU keine völkerrechtlich bedenkliche Regelung rein ausländischer Sachverhalte vor.[282] Auch Unternehmen mit Sitz in Drittländern sind nicht generell an die DSGVO gebunden, sondern nur insoweit, als sie auf dem Markt in der EU tätig sind.[283] Daher liegt Extraterritorialität nicht vor.

Laut Art. 3 Abs. 3 DSGVO ist die DSGVO auch an einem Ort anwendbar, der sich außerhalb der Union befindet und „aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt“, wie z. B. konsularische oder diplomatische Vertretungen nach ErwGr. 25 DSGVO.

3.4.1.3 Sachliche Anwendung der DSGVO

Nach der DSGVO sind sowohl personenbezogene als auch pseudonymisierte Daten erfasst – d. h. die Daten, die sich nach Art. 4 Nr. 1 DSGVO auf identifizierte oder identifizierbare natürliche Personen beziehen oder die Daten, deren Personenbezug nach Art. 4 Nr. 5 DSGVO durch zusätzliche Informationen wiederhergestellt werden kann (s. → S. 42).

Die DSGVO legt keine konkrete Form der zu schützenden Daten fest. Nach Art. 2 S. 1 DSGVO gilt die Verordnung für: 1. „Die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten“ und 2. „die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen“. Damit bezieht sie sich sowohl auf elektronische als auch auf nicht-elektronische Daten.

278 Drittland bedeutet ein Land außerhalb der EU/des EWR.
279 *Däubler -Däubler*, EU-DSGVO und BDSG, Art. 3 Rn. 16.
280 DSK, Marktortprinzip: Regelungen für außereuropäische Unternehmen, Kurzpapier Nr. 7, 17.12.2018; *Däubler u.a.-Weichert*, EU-DSGVO und BDSG, S. 44 Rn. 27.
281 *Solmecke/Kocatepe*, DSGVO für Website-Betreiber: Ihr Leitfaden für die sichere Umsetzung der EU-Datenschutz-Grundverordnung, S. 18.
282 *Däubler -Däubler*, EU-DSGVO und BDSG, Art. 3 Rn. 16.
283 *Däubler -Däubler*, EU-DSGVO und BDSG, Art. 3 Rn. 16.

3.4.1.4 Adressanten der DSGVO

Die DSGVO gilt sowohl für den **Verantwortlichen** als auch für den Auftragsverarbeiter. Ein Verantwortlicher ist nach Art. 4 Nr. 7 Hs. 1 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder eine andere Stelle, die allein (eine einzige natürliche oder juristische Person[284]) oder gemeinsam (mehrere Beteiligte[285]) mit anderen (gemeinsamer Verantwortlicher nach Art. 26 DSGVO) über den Zweck sowie die Mittel der Verarbeitung der personenbezogenen Daten entscheiden kann.

Auftragsverarbeiter ist nach Art. 4 Nr. 8 DSGVO „jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet".

3.4.1.5 Voraussetzungen nach der DSGVO

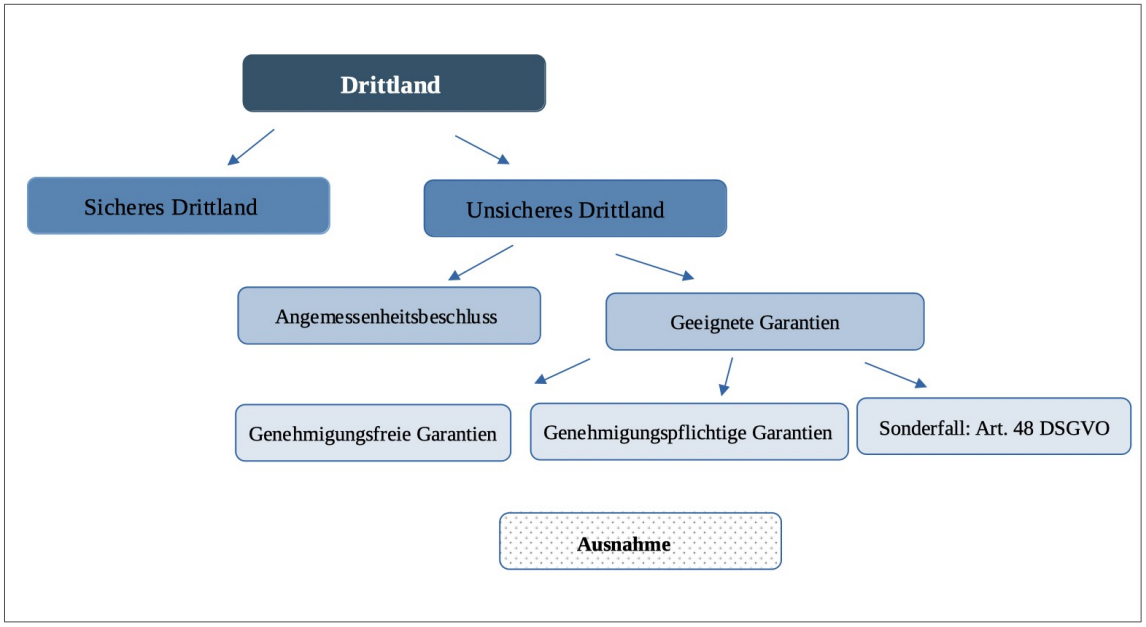

Abbildung 3.4.1.5 Voraussetzungen nach der DSGVO

Drittländer werden in zwei Kategorien unterteilt, nämlich: 1. Drittländer mit einem angemessenen Datenschutzniveau[286] (sog. „sichere Drittländer"[287]) und 2. Drittländer ohne einem angemessenen Datenschutzniveau (sog. „unsichere Drittländer"[288]).

284 EuGH, Urt. v. 10.7.2018 – C-25/17, ZD 2018, 469 Rn. 65 – Zeugen Jehovas.
285 EuGH, Urt. v. 10.7.2018 – C-25/17, ZD 2018, 469 Rn. 65 – Zeugen Jehovas.
286 Ein „angemessenes Schutzniveau" ist ein Schutzstandard, das vom Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen der Freiheiten und Grundrechte so gewährleistet wird, dass es in der EU auf Grund der DSGVO im Licht der GrCh gleichwertig ist. S.: EuGH, Urt. v. 06.10.2015 – C-362/14, NJW 2015, 3151, Rn. 73 – Schrems.
287 *Specht/Mantz -Wieczorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 169.
288 *Specht/Mantz -Wieczorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 169.

Jede Übermittlung oder Weiterübermittlung von personenbezogenen Daten durch einen Verantwortlichen oder einen Auftragsverarbeiter an ein Drittland oder eine internationale Organisation[289] unterliegt den Anforderungen von Kapitel V der DSGVO.[290] Für die Übermittlung personenbezogener Daten in Drittländer sind in Art. 44-49 DSGVO Sonderregelungen vorgeschrieben,[291] die sowohl für Verantwortliche als auch für Auftragsverarbeiter gelten. Findet eine solche Übermittlung statt, muss eine zweistufige Prüfung durch die Europäische Kommission durchgeführt werden,[292] um festzustellen, ob ein Drittland ein „angemessenes Schutzniveau" bietet.[293]

Zunächst muss überprüft werden, ob alle Anforderungen der DSGVO außer den Art. 45 ff. DSGVO eingehalten werden[294] (**Prüfung allgemeiner Zulässigkeitsvoraussetzungen**[295]). Wenn der Verarbeitung nach diesem Prüfschritt nichts im Wege steht, ist festzustellen, dass die spezifischen Voraussetzungen nach Art. 45 ff. DSGVO beachtet werden[296] (**Prüfung spezieller Vorschriften**[297]). Wurde auch dieser Schritt bejaht, ist die Datenübermittlung in dieses Land problemlos möglich[298] und bedarf keiner besonderen Genehmigung[299].

3.4.1.5.1 Datentransfer in ein sicheres Land

Nach Art. 45 DSGVO ist die Datenübermittlung in ein sicheres Land auf der Grundlage eines Angemessenheitsbeschlusses ungehindert möglich. Der Angemessenheitsbeschluss ist eines der Instrumente, die in der DSGVO für die Übermittlung personenbezogener Daten aus der EU in Drittländer vorgesehen sind, die nach Einschätzung der EU-Kommission ein vergleichbares Schutzniveau für personenbezogene Daten gewährleisten wie die Europäische Union.[300] Auf der Grundlage solcher Angemessenheitsentscheidungen können personenbezogene Daten aus dem EWR (d. h. den 27 EU-Mitgliedstaaten sowie Norwegen, Island und Liechtenstein) auf die gleiche Weise wie innerhalb der EU ohne weitere Bedingungen oder Genehmigungen frei und sicher in das jeweilige Drittland fließen.[301]

289 Eine Internationale Organisation ist gem. Art. 4 Nr. 26 DSGVO eine völkerrechtliche Organisation und eine ihr unterstellte Einrichtung oder eine Einrichtung, die durch oder aufgrund einer Übereinkunft zwischen zwei oder mehreren Staaten geschlossen wurde.
290 *Kühling/Buchner -Schröder*, DSGVO/BDSG, Art. 44 Rn. 16.
291 DSK, Datenübermittlung in Drittländer, Kurzpapier Nr. 4, 22.07.2019, S. 1.
292 DSK, Datenübermittlung in Drittländer, Kurzpapier Nr. 4, 22.07.2019, S. 1.
293 DSK, Datenübermittlung in Drittländer, Kurzpapier Nr. 4, 22.07.2019, S. 1.; vgl.: EuGH, Urt. v. 16.07.2020 – C-311/18, NJW 2020, 2613 Rn. 102 – Schrems II.
294 DSK, Datenübermittlung in Drittländer, Kurzpapier Nr. 4, 22.07.2019, S. 1.
295 *Specht/Mantz -Wieczorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 168.
296 DSK, Datenübermittlung in Drittländer, Kurzpapier Nr. 4, 22.07.2019, S. 1.
297 *Specht/Mantz -Wieczorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 168.
298 DSK, Datenübermittlung in Drittländer, Kurzpapier Nr. 4, 22.07.2019, S. 1.
299 *Specht/Mantz -Wieczorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 169.
300 Fragen und Antworten: Datenschutzrahmen EU-USA, abrufbar: https://ec.europa.eu/commission/presscorner/detail/de/qanda_23_3752, zuletzt abgerufen am 03.08.2023.
301 Fragen und Antworten: Datenschutzrahmen EU-USA, abrufbar:

Damit das Datenschutzsystem des Drittstaats als angemessen angesehen werden kann, muss es nicht mit dem der EU identisch sein. Erforderlich ist vielmehr ein im Wesentlichen gleichwertiges Schutzniveau. Zu diesem Zweck wird der Datenschutzrahmen eines Landes im Hinblick auf den Schutz personenbezogener Daten sowie auf die verfügbaren Kontrollmechanismen und Rechtsbehelfsverfahren umfassend bewertet. Die EU-Datenschutzbehörden haben eine Liste von Elementen erstellt, die berücksichtigt werden müssen: So müssen z. B. die wichtigsten Datenschutzgrundsätze, die Rechte des Einzelnen, eine unabhängige Aufsicht und wirksame Rechtsmittel gewährleistet sein.[302]

3.4.1.5.2 Prüfung allgemeiner Zulässigkeitsvoraussetzungen für die USA

Um festzustellen, ob die USA ein sicheres bzw. ein unsicheres Land sind, müssen allgemeine Zulässigkeitsvoraussetzungen nach Art. 45 ff. DSGVO durchgeprüft werden. Hierbei ist Folgendes zu beachten: Auf der Grundlage der nationalen Sicherheit erhalten die US-Behörden Zugriffsrechte nach Abschn. 702 FISA, E. O. 12333 sowie PPD-28 und überwachen Nicht-US-Personen, die sich außerhalb der Vereinigten Staaten befinden.[303]

Die **FISA-Bestimmungen** regeln, wann der wesentliche Zweck einer Untersuchung die Sammlung ausländischer Informationen ist.[304] Das Gesetz zielt darauf ab, dass der Kongress eine gerichtliche und kongressmäßige Aufsicht über ausländische Geheimdienstaktivitäten gewährleistet und die Geheimhaltung wahrt, die für eine wirksame Überwachung nationaler Sicherheitsbedrohungen erforderlich ist.[305] FISA wurde durch u. a. das USA PATRIOT Act (Das Akronym „PATRIOT“ steht für „Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism“[306]), durch das USA PATRIOT Additional Reauthorization Amendments Act von 2006 und das FISA Sunsets Extension Act geändert.[307] Abschnitt 702 FISA ergibt sich aus dem Amendement von 20.06.2008.

https://ec.europa.eu/commission/presscorner/detail/de/qanda_23_3752, zuletzt abgerufen am 03.08.2023.

302 Die EU-Kommission hat diese Erklärung in den folgenden Artikeln erläutert. S.: Fragen und Antworten: Datenschutzrahmen EU-USA, abrufbar: https://ec.europa.eu/commission/presscorner/detail/de/qanda_23_3752, zuletzt abgerufen am 03.08.2023.

303 EuGH kippt Privacy Shield: US-Dienste weiterhin nutzen – FAQ zu Schrems II, abrufbar: https://www.srd-rechtsanwaelte.de/blog/privacy-shield-schrems-ii/, zuletzt abgerufen am 01.08.2023.

304 *Boyne*, Data Protection in the United States, S. 328.

305 The Foreign Intelligence Surveillance Act of 1978 (FISA), abrufbar: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286, zuletzt abgerufen am 01.08.2023.

306 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 584.

307 The Foreign Intelligence Surveillance Act of 1978 (FISA), abrufbar: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286, zuletzt abgerufen am 01.08.2023.

Die **Executive Order 12333** (E. O. 12333) zielt nach E. O. 12333 Teil 2 (2.2) darauf ab, die personellen und technischen Erhebungsmethoden, insbesondere im Ausland, und die Beschaffung wichtiger ausländischer Informationen sowie die Aufdeckung und Bekämpfung von internationalen terroristischen Aktivitäten und Spionage durch ausländische Mächte zu verbessern.

Die am 17.01.2014 herausgegebene **Presidential Policy Directive 28 to Signals Intelligence Activities** (PPD-28) formuliert nach Abs. 1 S. 1 der Einführung PPD-28 Grundsätze, die bestimmen, warum, ob, wann und wie die Vereinigten Staaten Signals Intelligence Activities für genehmigte Zwecke der Auslandsaufklärung und Spionageabwehr durchführen.

Hier ist eine der wichtigsten Schwachstellen des amerikanischen Rechtssystems zu nennen: **Das Eindringen in die Privatsphäre** (diese beinhaltet natürlich auch Zugang zu den personenbezogenen Daten). Im Kapitel „Who Watches the Watchers?" skizziert Cyrus Farivar, dass die Rechtssachen Katz gegen die Vereinigten Staaten bis zu Riley gegen Kalifornien ein gemeinsames Thema haben: Die Maßnahmen der Strafverfolgungsbehörden wären zulässig gewesen, wenn die Behörden einfach einen Haftbefehl beantragt hätten.[308]

In der Rechtssache Lopez gegen die Vereinigten Staaten bewertete Chief Justice Earl Warren das Eindringen der US-Behörden in die Privatsphäre wie folgt: Die phantastischen Fortschritte im Bereich der elektronischen Kommunikation stellen eine große Gefahr für die Privatsphäre des Einzelnen dar; der wahllose Einsatz solcher Geräte bei der Strafverfolgung wirft schwerwiegende verfassungsrechtliche Fragen gemäß dem vierten und fünften Verfassungszusatz auf; und diese Erwägungen erlegen dem Gericht eine größere Verantwortung bei der Überwachung der Fairness der Verfahren im Bundesgerichtssystem auf.[309]

Nur selten werden die Strafverfolgungsbehörden von einem Richter abgewiesen, wenn sie einen hinreichenden Verdacht auf ein Verbrechen nachweisen können.[310] In jedem dieser Fälle wurde kein Durchsuchungsbefehl beantragt, und die Strafverfolgungsbehörden nutzten ihre Befugnisse, um das Gesetz neu auszulegen und neue Schleichwerbungstechnologien einzusetzen, versteckten aber Mikrofone oder Infrarotkameras.[311]

308 *Farivar*, habeas data, S. 228.
309 *Farivar*, habeas data, Einführung.
310 *Farivar*, habeas data, S. 228.
311 *Farivar*, habeas data, S. 228.

Der EuGH stellte fest, dass Abschn. 702 FISA und E. O. 12333, selbst in der durch PPD-28 eingeschränkten Form, nicht den Erforderlichkeits- und Verhältnismäßigkeitsstandards der DSGVO entsprechen und den betroffenen Personen in der EU keinen wirksamen gerichtlichen Rechtsbehelf bieten können.[312] Die US-Überwachungsprogramme sind nicht auf das absolut Notwendige beschränkt und bieten keinen EU-Recht entsprechenden und ausreichenden Rechtsschutz.[313] Dies verstößt gegen das Datenminimierungsprinzip nach Art. 5 Abs. 1 lit. c) DSGVO.

Hinsichtlich des Zugriffs durch öffentliche Sicherheitsbehörden äußerte die Art. 29-Datenschutzgruppe, dass die Verhältnismäßigkeit des Datenzugriffs in Frage gestellt werden sollte: Ein massenhafter verdachtsunabhängiger Zugriff auf Daten sei nach wie vor möglich.[314] Die zahlreichen Maßnahmen zur Sicherstellung der Kontrolle seien im Hinblick auf den nicht-staatlichen Umgang mit Daten ausreichend; dies gelte jedoch nicht für gewisse nachrichtendienstliche Tätigkeiten, die vom FISA-Gericht überwacht werden.[315]

Auch die Rechtsbehelfe werden häufig als unzureichend angesehen: So ist die Möglichkeit, Rechte vor einem amerikanischen Gericht geltend zu machen, davon abhängig, dass der US-Generalstaatsanwalt diese Rechte gewährt / einräumt und sie nicht im Einzelfall zurücknimmt.[316] Der Ombudsmann-Mechanismus ist nicht geeignet, die Defizite im Rechtsschutz zu kompensieren.[317]

Aus diesen Gründen war das Datenschutzniveau in den USA bis Anfang Juli 2023 als unangemessen angesehen. Dementsprechend wurde sie als **ein unsicheres Drittland** betrachtet, und es konnte kein Angemessenheitsbeschluss nach Art. 45 Abs. 3 DSGVO vorgelegt werden.

Diese Lage hat sich am 10.07.2023 mit dem Erlass des neuen Angemessenheitsbeschlusses zum EU-US Datenschutzrahmen / „EU-US Data Privacy Framework“ (EU-US DPF) geändert. Ab diesem Datum gelten die USA als **sicheres Land**, und Daten können weiterhin frei übermittelt werden. Der neue Angemessenheitsbeschluss zum EU-US DPF gilt für Datentransfer von öffentlichen und privaten Stellen im EWR an US-Unternehmen, die an diesem Datenschutzrahmen teilnehmen. [318] Dieser Beschluss, der neue Datenschutzrahmen sowie die erwarteten Auswirkungen werden in den kommenden Abschnitten behandelt (s. → S. 82-88).

312 *Linebaugh/Liu,* EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield, 1, 8.

313 EuGH kippt Privacy Shield: US-Dienste weiterhin nutzen – FAQ zu Schrems II, abrufbar: https://www.srd-rechtsanwaelte.de/blog/privacy-shield-schrems-ii/, zuletzt abgerufen am 01.08.2023.

314 *Kühling/Buchner -Schröder*, DSGVO/BDSG, Art. 45 Rn. 42.

315 *Kühling/Buchner -Schröder*, DSGVO/BDSG, Art. 45 Rn. 42.

316 *Kühling/Buchner -Schröder*, DSGVO/BDSG, Art. 45 Rn. 42.

317 EuGH kippt Privacy Shield: US-Dienste weiterhin nutzen – FAQ zu Schrems II, abrufbar: https://www.srd-rechtsanwaelte.de/blog/privacy-shield-schrems-ii/, zuletzt abgerufen am 01.08.2023.

318 Fragen und Antworten: Datenschutzrahmen EU-USA, abrufbar: https://ec.europa.eu/commission/presscorner/detail/de/qanda_23_3752, zuletzt abgerufen am 03.08.2023.

3.4.1.5.3 Datentransfer in ein unsicheres Land

Liegt kein Angemessenheitsbeschluss nach Art. 45 Abs. 3 DSGVO vor, darf eine Übermittlung in ein Drittland nach Art. 46 Abs. 1 DSGVO nur erfolgen, wenn der Verantwortliche oder der Auftragsverarbeiter **geeignete Garantien** bietet und der Betroffene über durchsetzbare Rechte und wirksame Rechtsbehelfe verfügt.

Geeignete Garantien sind Vereinbarungen zwischen Datenexporteuren aus der EU und Datenimporteuren in einem unsicheren Drittland, die das unzureichende Datenschutzniveau ausgleichen können.[319] Sie werden in genehmigungsfreie und genehmigungspflichtige Garantien unterteilt.

Darf die Datenübermittlung nicht nach angemessenen Garantien erfolgen, können personenbezogene Daten in ein unsicheres Land übermittelt werden, wenn es sich um einen Sonderfall nach Art. 48 DSGVO oder eine Ausnahme nach Art. 49 DSGVO handelt. Der Sonderfall nach Art. 48 DSGVO bezieht sich auf Übermittlungen oder Offenlegungen, die nach dem Unionsrecht nicht zulässig sind, und die Ausnahme nach Art. 49 DSGVO bezieht sich auf besondere Fälle (z. B. Übermittlungen aufgrund des öffentlichen Interesses).

3.4.1.5.3.1 Genehmigungsfreie Garantien

Zu den genehmigungsfreien Garantien gem. Art. 46 Abs. 2 DSGVO gehören die folgenden Dokumente:

1. Ein rechtlich bindendes und durchsetzbares Dokument zwischen den Behörden oder öffentlichen Stellen: Zu diesen Garantien gehören Verwaltungsvereinbarungen jeglicher Art im öffentlichen Bereich oder an internationale Organisationen (z. B. Gemeinsame Absicherungserklärungen nach ErwGr. 108 S. 5 DSGVO).[320]

2. Verbindliche interne Datenschutzvorschriften / „Binding Corporate Rules“ nach Art. 47 DSGVO: Sie werden von weltweit tätigen Unternehmensgruppen oder Gruppen von Unternehmen mit gemeinsamer wirtschaftlicher Tätigkeit bei der zuständigen Aufsichtsbehörde beantragt, um den internationalen Datentransfer in einem unsicheren Land zu rechtfertigen.[321] Sie können auf einzelne Mitglieder des Unternehmensverbundes, der Unternehmensgruppe oder auf eine bestimmte Kategorie der Daten beschränkt werden.[322]

319 *Specht/Mantz -Wieczorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 174.
320 *Specht/Mantz -Wieczorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 175.
321 *Specht/Mantz -Wieczorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 176.
322 *Specht/Mantz -Wieczorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 177.

3. Standarddatenschutzklauseln der europäischen Kommission: Es handelt sich um vorformulierte Verträge zwischen Datenexporteur und Datenimporteur, die von der EU-Kommission verabschiedet wurden.[323] Diese Klauseln verringern die Risiken für die Verantwortlichen bzw. die Auftragsverarbeiter, unzureichende Regelungen zu vereinbaren, und sorgen für einheitliche Regelungen, die jedoch gleichzeitig für die Parteien nicht mehr disponibel sind.[324] Wenn etwas an den Klauseln der einzelnen Verträge nicht geändert wird, muss dies von den Aufsichtsbehörden nicht genehmigt werden.[325] Die DSGVO äußert sich jedoch nicht dazu, ob die nationalen Aufsichtsbehörden weitergehende Anforderungen an den Transfer bestimmter Daten stellen und damit weiterreichende Sicherheitsvorkehrungen verlangen können.[326]

Neue Standardvertragsklauseln wurden von der Europäischen Kommission im Juni 2021 herausgegeben.[327] Sie sind wie die folgenden Module aufgebaut: 1. Verantwortlicher an Verantwortlichen, 2. Verantwortlicher an Auftragsverarbeiter, 3. Auftragsverarbeiter an (Unter-) Auftragsverarbeiter oder 4. Rückübermittlung des Auftragsverarbeiters in der EU an einen Verantwortlichen im Drittland.[328] Dies bedeutet, dass die neuen Klauseln zwischen diesen Beteiligten geschlossen werden (z. B. zwischen dem Verantwortlichen und dem Auftragsverarbeiter).

4. Standarddatenschutzklauseln der Aufsichtsbehörde: Werden sie von einer Aufsichtsbehörde mit geeigneten Garantien angenommen, bedürfen sie der Abstimmung im Kohärenzverfahren[329] [330] und der anschließenden Genehmigung von der europäischen Kommission.[331] Auf diese Weise bietet die DSGVO einen starken Anreiz, national geprüfte Klauseln bei der Kommission einzureichen, weil diese die Klauseln nach Abschluss des Überprüfungsverfahrens auf das gleiche Niveau wie die von ihr selbst verabschiedeten Standarddatenschutzklauseln heben kann.[332] Diese Standarddatenschutzklauseln schaffen die Möglichkeit, (nationale) Sonderanlagen (z. B. technologiespezifische) zu berücksichtigen.[333]

323 *Specht/Mantz -Wieczorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 184.
324 *Kühling/Buchner -Schröder*, DSGVO/BDSG, Art. 46 Rn. 25.
325 Interview mit Cornelia Sasse, im elektronischen Zusatzmaterial, Anlage 1, S. 2.
326 *Kühling/Buchner -Schröder*, DSGVO/BDSG, Art. 46 Rn. 33.
327 Standarddatenschutzklauseln der EU-Kommission oder einer Aufsichtsbehörde, abrufbar: https://www.datenschutz.rlp.de/de/themenfelder-themen/standarddatenschutzklauseln-der-eu-kommission-oder-einer-aufsichtsbehoerde/, zuletzt abgerufen am 02.08.2023.
328 Die in diesem Abschnitt dargestellte Aussage befindet sich in dem folgenden Artikel. S.: Standarddatenschutzklauseln der EU-Kommission oder einer Aufsichtsbehörde, abrufbar: https://www.datenschutz.rlp.de/de/themenfelder-themen/standarddatenschutzklauseln-der-eu-kommission-oder-einer-aufsichtsbehoerde/, zuletzt abgerufen am 02.08.2023.
329 Das Kohärenzverfahren ist in Kapitel VII Abschn. 2 Artt. 63-67 DSGVO beschrieben.
330 Artikel 63 DSGVO stellt klar, dass das Kohärenzverfahren zu einer einheitlichen Anwendung der DSGVO in der gesamten EU beitragen soll. Der Wortlaut von Art. 63 DSGVO bezieht sich auf die Zusammenarbeit zwischen den Aufsichtsbehörden. S.: *Kühling/Buchner -Caspar*, DSGVO/BDSG, Art. 63 Rn. 15.
331 *Kühling/Buchner -Schröder*, DSGVO/BDSG, Art. 46 Rn. 34.
332 *Kühling/Buchner -Schröder*, DSGVO/BDSG, Art. 46 Rn. 34.
333 *Specht/Mantz -Wieczorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 188.

5. Genehmigte Verhaltensregeln / „Code of Conducts“ (CoC): Nach Art. 40 Abs. 1 DSGVO handelt es sich dabei um bereichspezifische Regeln bzw. Richtlinien sowie Leitlinien für kleinste, kleine und mittlere Unternehmen. Die DSGVO erweitert die Verhaltensregeln für den grenzüberschreitenden Datentransfer, indem sie die branchenspezifischen Regelungen um die internationale Aspekte erweitert und damit auch für den internationalen Verkehr attraktiver gemacht werden.[334]
6. Genehmigter Zertifizierungsmechanismus: Zertifizierungen dienen dem Nachweis, dass die konkrete Datenverarbeitung dem geltenden Datenschutzrecht entspricht.[335] Der Gesetzgeber zeigt damit bedeutendes Vertrauen in private Zertifizierungsstellen, die sicherstellen müssen, dass ihre Zertifikate den hohen Anforderungen an angemessene Schutzmaßnahmen nach Art. 46 DSGVO erfüllen.[336]

3.4.1.5.3.2 Genehmigungspflichtige Garantien

Zu den genehmigungspflichtigen Garantien gem. Art. 46 Abs. 3 DSGVO gehören die folgenden Dokumente:
1. Ad-hoc-Vertragsklauseln: Dabei handelt es sich um Einzelverträge zwischen Datenexporteur und Datenimporteur in einem unsicheren Land, die von einer zuständigen Aufsichtsbehörde geprüft und ggf. genehmigt werden müssen.[337] Diese Klauseln bieten eine vernünftige Rechtfertigungsgrundlage für besondere / spezifische Datentransfers.[338]
2. Bestimmungen in Verwaltungsvereinbarungen: Dies sind individuelle Vereinbarungen zwischen Behörden oder öffentlichen Einrichtungen, die von einer zuständigen Aufsichtsbehörde geprüft und ggf. genehmigt werden müssen.[339] Sie sind, anders als Verwaltungsvereinbarungen nach Art. 46 Abs. 2 lit. a) DSGVO, nicht verbindlich.[340]

334 *Kühling/Buchner -Schröder*, DSGVO/BDSG, Art. 46 Rn. 36.
335 *Specht/Mantz -Wieczorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 190.
336 *Kühling/Buchner -Schröder*, DSGVO/BDSG, Art. 46 Rn. 38.
337 *Specht/Mantz -Wieczorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 192.
338 *Specht/Mantz -Wieczorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 193.
339 *Specht/Mantz -Wieczorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 193.
340 *Specht/Mantz -Wieczorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 193.

3.4.1.5.3.3 Sonderfall: Rechtshilfeabkommen bzw. internationale Übereinkünfte

Der Datentransfer auf der Grundlage von Rechtshilfeabkommen bzw. internationalen Übereinkünften ist als Sonderfall zu betrachten. Ein Ersuchen einer ausländischen Behörde stellt an sich keine Rechtsgrundlage für eine Übermittlung dar.[341] Eine Übermittlung oder Offenlegung personenbezogener Daten darf nur auf der Grundlage von Rechtshilfeabkommen oder internationalen Vereinbarungen (z. B. Mutual Legal Assistance Treaty – MLAT; s. → S. 76-82) nach Art. 48 DSGVO erfolgen, unbeschadet anderer Gründe für eine Übermittlung gem. Kapitel V der DSGVO.[342]

Artikel 48 DSGVO regelt den Zugriff auf personenbezogene Daten durch Gerichte und Behörden in Drittländern, die unter der DSGVO fallen, wodurch klargestellt wird, dass die Verordnung auch personenbezogener Daten aus hoheitlichen Handlungen von Drittländern schützt.[343] Dieser Artikel umfasst Urteile sowie Verwaltungsentscheidungen, und macht sie vom Bestehen eines Rechtshilfeabkommens abhängig, der diese Entscheidungen anerkennt.[344] Alle hoheitlichen Handlungen einer Stelle in einem Drittstaat sind damit abgedeckt, einschließlich z. B. einer Regierung.[345] Sie gilt jedoch nicht für Offenlegungsanträge privater Dritter, selbst wenn diese im Rahmen eines Gerichtsverfahrens gestellt werden, wie beispielsweise im Rahmen eines US-amerika-nischen „Pre-Trial-Discovery"-Verfahrens.[346] Sie werden Gegenstand einer hoheitlichen Handlung nach Art. 48 DSGVO, wenn das zuständige amerikanische Gericht eine entsprechende Anordnung erlässt.[347]

Der Verantwortliche ist verpflichtet, die betroffenen Personen über die (geplante) Datenübermittlung in ein Drittland zu unterrichten und ihnen Informationen über die angemessenen Sicherheitsvorkehrungen bereitzustellen.[348]

341 Edpb, ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence, S. 3; *Pearsall/Unikowsky*, BRIEF OF THE EUROPEAN COMMISSION ON BEHALF OF THE EUROPEAN UNION AS AMICUS CURIAE IN SUPPORT OF NEITHER PARTY, S. 14.

342 Edpb, ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence, S. 3.

343 *Kühling/Buchner -Schröder*, DSGVO/BDSG, Art. 48 Rn. 2.

344 *Kühling/Buchner -Schröder*, DSGVO/BDSG, Art. 48 Rn. 13.

345 *Kühling/Buchner -Schröder*, DSGVO/BDSG, Art. 48 Rn. 13.

346 *Kühling/Buchner -Schröder*, DSGVO/BDSG, Art. 48 Rn. 13.

347 *Kühling/Buchner -Schröder*, DSGVO/BDSG, Art. 48 Rn. 13.

348 IONOS, Aktuelle Rechtslage zum US-Datentransfer unter besonderer Berücksichtigung des US CLOUD Act, 2, 5.

3.4.1.5.3.4 Ausnahmen

Findet eine Übermittlung personenbezogener Daten nicht auf der Grundlage eines Angemessenheitsbeschlusses oder geeigneter Garantien statt, ist die Übermittlung nur in Ausnahmefällen gem. Art. 49 DSGVO erlaubt. Diese sind nach Art. 49 Abs. 1 DSGVO die folgenden:

1. Ausdrückliche Einwilligung (Art. 49 S. 1 lit. a) DSGVO): Dabei geht es um eine unmissverständliche, freiwillige sowie bestätigende Handlung eines Betroffenen, der sein Einverständnis mit der spezifischen Übermittlung zum Ausdruck bringt.[349] Sie kann weder stillschweigend noch konkludent erfolgen und ist jederzeit zu widerrufen.[350]

2. Verträge auf Antrag des Betroffenen (Art. 49 S. 1 lit. b) DSGVO): Bei dieser Ausnahme handelt es sich um einen Vertrag, der mit Betroffenen geschlossen wurde bzw. wird und einen Bezug auf ein Drittland aufweist.[351]

3. Verträge im Interesse des Betroffenen (Art. 49 S. 1 lit. c) DSGVO): Diese Ausnahme gilt im Falle einer Datenübermittlung zum Abschluss oder zur Erfüllung eines im Interesse des Betroffenen geschlossenen Vertrags.[352] Ein solcher Vertrag wurde mit einer anderen natürlichen oder juristischen Person und nicht mit dem Betroffenen selbst geschlossen.[353]

Ausnahmen im Falle einer ausdrücklichen Einwilligung, von Verträgen auf Antrag des Betroffenen oder von Verträgen im Interesse des Betroffenen gelten gem. Art. 49 Abs. 3 DSGVO nicht für Tätigkeiten, die von Behörden in Ausübung ihrer hoheitlichen Befugnisse durchgeführt werden.

4. Öffentliches Interesse (Art. 49 S. 1 lit. d) DSGVO): Dieser Fall bezieht sich auf wichtige Gründe des öffentlichen Interesses, das wiederum dem Schutz eines besonders wichtigen Rechtsgutes gilt (z. B. Austausch zwischen Zollbehörden).[354] Bei dem Stellenwert des öffentlichen Interesses nach Art. 49 Abs. 3 lit. d) DSGVO handelt es sich um einen Stellenwert des öffentlichen Interesses nach Art. 6 lit. e) DSGVO[355] (Datenverarbeitung auf der Grundlage des öffentlichen Interesses oder der Ausübung öffentlicher Gewalt).

5. Rechtsansprüche (Art. 49 S. 1 lit. e) DSGVO): Diese Ausnahme betrifft die Datenübermittlung zur Geltendmachung, Verteidigung oder Ausübung von Rechtsansprüchen, was sowohl in Pre-Trial-Discovery-Verfahren als auch vor Schiedsgerichten der Fall sein kann.[356]

---

349 *Specht/Mantz -Wiezorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 196.
350 *Specht/Mantz -Wiezorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 196.
351 *Specht/Mantz -Wiezorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 198; *Gola/Heckmann -Klug*, DSGVO/BDSG, Art. 49 Rn. 7.
352 *Specht/Mantz -Wiezorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 199.
353 *Specht/Mantz -Wiezorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 199.
354 *Specht/Mantz -Wiezorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 200.
355 *Specht/Mantz -Wiezorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 200.
356 *Kühling/Buchner -Schröder*, DSGVO/BDSG, Art. 49 Rn. 30.

6. Schutz lebenswichtiger Interessen: Ist lebenswichtiges Interesse einer Person zu schützen und ist sie körperlich oder rechtlich nicht in der Lage, ihre Einwilligung zu geben, dann können die sich auf sie beziehenden Daten nach Art. 49 Abs. 1 lit. f) DSGVO zum Schutz ihres lebenswichtigen Interesses in ein Drittland übermittelt werden.[357] Hier geht es um medizinische Daten (z. B. wenn es für eine medizinische Behandlung zum Schutz des Lebens einer Person notwendig ist, die Daten über diese Person an einen Arzt in einem Drittland zu übermitteln).[358]

7. Wahrung berechtigter Interessen: Haben Personen oder die gesamte Öffentlichkeit ein berechtigtes Interesse am Zugang zu Informationen aus dem öffentlichen Register und sind die Voraussetzungen für die Einsichtnahme im Einzelfall gegeben, so ist die Datenübermittlung in ein unsicheres Drittland gem. Art. 49 Abs. 1 lit. g) und Abs. 2 DSGVO möglich.[359] Dieses Register umfasst alle öffentlichen Informationen, die der gesamten Öffentlichkeit oder speziellen Personengruppen mit relativ geringeren Zugangsschwellen zugänglich gemacht werden (z. B. Handelsregister).[360]

3.4.2 Internationaler Datentransfer aus den USA in die EU

In den USA gelten keine geografischen Übertragungsbeschränkungen,[361] außer in Bezug auf die Speicherung einiger staatlicher Aufzeichnungen und Informationen.[362] US-Anbieter unterliegen dem PATRIOT Act, dem FREEDOM Act und dem USA CLOUD Act[363] (im Folgenden „CLOUD Act“[364]), die solche Beschränkungen bzw. Anforderungen vorschreiben. Der Patriot Act (insbesondere Abschn. 215) und der Freedom Act (insbesondere Abschn. 101) beziehen sich als zeitlich befristete Änderungsgesetze auf den FISA, der die Grundlage für die Sammlung von nachrichtendienstlichen Daten durch amerikanischen Behörden im Ausland darstellt.[365]

357 *Specht/Mantz -Wiezorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 202; *Gola/Heckmann -Klug*, DSGVO/BDSG, Art. 49 Rn. 11.

358 *Specht/Mantz -Wiezorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 202; *Gola/Heckmann -Klug*, DSGVO/BDSG, Art. 49 Rn. 11.

359 *Specht/Mantz -Wiezorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 202.

360 *Specht/Mantz -Wiezorek*, Handbuch: Europäisches und deutsches Datenschutzrecht, S. 202.

361 Data Protection Laws and Regulations USA 2023, abrufbar: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa, zuletzt abgerufen am 05.08.2023.

362 Data Protection Laws of the World: United States, abrufbar: https://www.dlapiperdataprotection.com/index.html?t=transfer&c=US, zuletze abgerufen am 05.08.2023.

363 Legal rift between the EU and USA: Data handling & data transfer and the implications for enterprises, abrufbar: https://blog.cryptshare.com/en/legal-rift-eu-usa-data-handling-data-transfer-implications-for-enterprises?hs_amp=true, zuletzt abgerufen am 02.08.2023.

364 Der CLOUD Act wurde in erster Linie als Ergebnis der Kontroverse um die Rechtssache USA gegen Microsoft in Bezug auf § 2703 SCA erlassen, auf die Frage einzugehen, ob den US-Strafverfolgungsbehörden nach dem ECPA erlaubt ist, einen Anbieter zur Herausgabe kommunikationsbezogener Inhaltsdaten zu zwingen, die nicht in den USA gespeichert wurden (in diesem Fall ging es um E-Mails, die in Irland gespeichert wurden). S.: Europäisches Parlament, 4. Arbeitsdokument (A), 11.03.2019, S. 7.

365 Wissenschaftliche Dienste des Deutschen Bundestages, WD 3 - 3000 – 181/20, 2, 4.

Nach den Anschlägen vom 11.09.2001 hat die Bundesregierung die FISA-Befugnisse drastisch ausgeweitet.[366] Das Gesetz enthält eine Reihe von Bestimmungen, die sich auf den FISA auswirken oder ihn ändern.[367] Vor allem **Abschn. 215 PATRIOT Act** erweiterte die Möglichkeiten der Regierung, Geschäftsunterlagen von Dritten einzuholen.[368]

Abschnitt 215 PATRIOT Act änderte **Abschn. 501 FISA** und erweiterte die Arten von Aufzeichnungen, die die Regierung erhalten konnte, während die Anforderung, dass die Untersuchung mit einer ausländischen Macht oder deren Agenten in Verbindung stehen muss, gelockert wurde, solange die Informationen keine US-Personen betrafen.[369] Die Regierung holte statt individueller gerichtlicher Anordnungen die FISA-Anordnungen ein, um die Massenerfassung von ,,Telefonie-Metadaten“ von Telekommunikationsunternehmen auf der Grundlage der FISA-Befugnisse für Pen-Register und Trap-and-Trace sowie der National Security Letter Statuten zu ermöglichen.[370]

Das FBI hatte das Recht, von den betreffenden Organisationen die Vorlage von Telekommunikationsdaten, Finanzdaten, Kreditdaten, und Verbraucherberichten zu verlangen, wenn diese Informationen für die Sammlung ausländischer Informationen oder für die Zwecke einer Terrorismusuntersuchung relevant waren, ohne dass ein wahrscheinlicher Grund nachgewiesen werden musste.[371] In den Jahren nach der Verabschiedung des PATRIOT Act hat die Verwendung von National Security Letters durch das FBI exponentiell zugenommen; das FBI hat zwischen 2003 und 2006 ca. 200 000 National Security Letters ausgestellt.[372] Zwei Jahre nach den Snowden-Enthüllungen hat der Kongress mit dem USA Freedom Act von 2015 die Massenerfassung von Metadaten verboten.[373]

366 *Boyne*, Data Protection in the United States, S. 329.
367 *Boyne*, Data Protection in the United States, S. 329.
368 *Boyne*, Data Protection in the United States, S. 329.
369 *Boyne*, Data Protection in the United States, S. 329.
370 *Boyne*, Data Protection in the United States, S. 329.
371 *Boyne*, Data Protection in the United States, S. 329 ff.
372 *Boyne*, Data Protection in the United States, 66, S. 330.
373 *Boyne*, Data Protection in the United States, S. 330.

Der **USA Freedom Act** (vollständige Bezeichnung: „Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015“) enthält drei wichtige Bestimmungen zum Schutz der Privatsphäre: Erstens wurde der National Security Agency (NSA) eine rechtliche Befugnis entzogen, die sie zur Massenerfassung von Telefon-Metadaten nutzte.[374] Statt der Massenerfassung von Daten durch die Regierung schreibt das Gesetz vor, dass Anträge der Regierung auf Anrufaufzeichnungen auf einem spezifischen Auswahlbegriff beruhen müssen, der eine Person, ein Konto, eine Adresse oder ein persönliches Gerät auf eine Art und Weise identifiziert, die den Umfang der gesuchten materiellen Dinge in Übereinstimmung mit dem Zweck der Suche nach den materiellen Dingen so weit wie möglich einschränkt.[375]
Zweitens wird eine größere Transparenz der Entscheidungen des Foreign Intelligence Surveillance Court (FISC) gefordert und die Ernennung von amicus curiae („Freunde des Gerichts“) genehmigt, die vor dem FISC rechtliche Argumente vorbringen, um den Schutz der Privatsphäre und der bürgerlichen Freiheiten zu fördern.[376] Drittens wurde Einzelpersonen und Unternehmen eine größere Freiheit eingeräumt, ihre Beteiligung bzw. Nichtbeteiligung an der Sammlung von Massendaten durch die Regierung zu melden oder offenzulegen.[377]
Seit 2018 gilt der CLOUD Act. Er ist von dem FISA, dem USA PATRIOT Act und dem USA Freedom Act abzugrenzen.[378] Er befasst sich mit einem anderen Sachverhalt: Anders als die nachrichtendienstliche Überwachung nach FISA, dem PATRIOT Act und dem Freedom Act regelt der CLOUD Act die Sammlung elektronischer Beweismittel für Strafverfahren.[379] Da der CLOUD Act beim Thema „Internationaler Datentransfer“ eine wichtige Rolle spielt, wird es im Folgenden näher betrachtet und analysiert.

3.4.2.1 Ziel des CLOUD Act

Abschnitt 102 (1) CLOUD Act stellt fest, dass der rechtzeitige Zugang zu elektronischen Daten, die sich im Besitz von Kommunikationsdiensteanbietern befinden, ein wesentlicher Bestandteil der staatlichen Bemühungen zum Schutz der öffentlichen Sicherheit und zur Bekämpfung schwerer Verbrechen ist. Laut dem US-Justizministeriums sind solche Daten für die Ermittlungen der schweren Verbrechen auf der ganzen Welt von entscheidender Bedeutung, die von Terrorismus und Gewaltverbrechen bis hin zur sexuellen Ausbeutung von Kindern und Cyberkriminalität reichen.[380]

374 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 613; *Boyne*, Data Protection in the United States, S. 330.
375 *Boyne*, Data Protection in the United States, S. 330.
376 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 613.
377 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 613.
378 Wissenschaftliche Dienste des Deutschen Bundestages, WD 3 - 3000 – 181/20, 2, 5.
379 Wissenschaftliche Dienste des Deutschen Bundestages, WD 3 - 3000 – 181/20, 2, 5.
380 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 10.

Darüber hinaus stellt das US-Justizministerium fest, dass in den letzten Jahren die Zahl der Rechtshilfeersuche, in denen die Vereinigten Staaten um elektronische Beweismittel ersucht werden, drastisch gestiegen ist, was die Ressourcen belastet und die Reaktionszeiten verlangsamt.[381] Hinzu kommt, dass bei vielen Rechtshilfeersuchen die Beweismittel zufällig von einem in den USA ansässigen Unternehmen verwahrt werden.[382]

Infolgedessen wurde als Ziel des Gesetzes eine effiziente Ermittlung durch die US-Strafverfolgungsbehörden festgelegt, und der CLOUD Act wurde vom US-Justizministerium mit den folgenden Worten als ein neues Paradigma bewertet: *„an efficient, privacy-protective approach to public safety by enhancing effective access to electronic data [...], [which] makes both the United States and its partners safer while maintaining high levels of protection of privacy and civil liberties.“*[383]

3.4.2.2 Räumliche Anwendung des CLOUD Act

Nach Abschn. 103 (a) (1), § 2713 Hs. 2 CLOUD Act ist es unerheblich, ob sich die Daten innerhalb oder außerhalb der Vereinigten Staaten befinden. Es reicht aus, dass sie von einem Anbieter verarbeitet werden, der dort ansässig oder geschäftlich tätig ist.[384] So können personenbezogene Daten, die von EU-Verantwortlichen verarbeitet werden, betroffen sein, wenn sie diese Daten an einen US-Anbieter weitergeben.[385]

Anders als die DSGVO verpflichtet der CLOUD Act Unternehmen mit (einem) Sitz in den USA, den Strafverfolgungsbehörden auch Informationen zu übermitteln, die bei ausländischen Tochtergesellschaften (z. B. in der EU), gespeichert sind.[386] Somit liegt die Extraterritorialität im Falle des CLOUD Act vor.

381 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 10.
382 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 10.
383 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 10.
384 IONOS, Aktuelle Rechtslage zum US-Datentransfer unter besonderer Berücksichtigung des US CLOUD Act, 2, 7.
385 IONOS, Aktuelle Rechtslage zum US-Datentransfer unter besonderer Berücksichtigung des US CLOUD Act, 2, 7.
386 *Däubler -Däubler*, EU-DSGVO und BDSG, Art. 3 Rn. 16.

3.4.2.3 Sachliche Anwendung des CLOUD Act

Laut Abschn. 103 (a) (1) Hs. 1 CLOUD Act sind folgende Daten betroffen: 1. Der Inhalt einer drahtgebundenen oder elektronischen Kommunikation, 2. alle Aufzeichnungen oder 3. sonstigen Informationen über einen Kunden oder Abonnenten, die sich im Besitz, im Gewahrsam oder unter der Kontrolle / „possession, custody, or control" dieses Anbieters befinden. Die Form dieser Daten wird in Abschn. 102 (1) CLOUD Act ausschließlich als elektronische Form definiert.

Anders als die DSGVO betrifft der CLOUD Act alle Arten von Daten einschließlich sensiblen Daten wie Geschäftsgeheimnissen,[387] die als nicht-personenbezogene Daten zu betrachten sind, gleichermaßen. Eine wahllose oder massenhafte Datenerfassung ist nicht zulässig.[388]

3.4.2.4 Adressaten des CLOUD Act

Der CLOUD Act gilt für alle US-Anbieter elektronischer Kommunikations- und Ferninformationsdienste (z. B. IT-Dienstleister, Cloud-Anbieter sowie Internet-Provider).[389] Mit dem CLOUD Act sind auch US-Anbieter betroffen, die mit dem EU-Dienstleister in Verbindung stehen (z. B. Unterauftragnehmer).[390]

Elektronischer Kommunikationsdienst / „Electronic Communication Service" ist nach 18 U.S.C. § 2510 (15) jeder Dienst, der seinen Nutzern die Möglichkeit bietet, drahtgebundene oder elektronische Nachrichten zu senden oder zu empfangen.[391]

Ferninformationsdienst / „Remote Computing Service" bedeutet nach 18 U.S.C § 2711 (2) die Bereitstellung von Computerspeicher- und -verarbeitungsdiensten für die Öffentlichkeit mittels eines elektronischen Kommunikationssystems.[392]

Das Gesetz gilt nicht für Unternehmen, die nur in irgendeiner Weise mit dem Internet interagieren (z. B. bestimmte E-Commerce-Seiten).[393]

387 IONOS, Aktuelle Rechtslage zum US-Datentransfer unter besonderer Berücksichtigung des US CLOUD Act, 2, 7.
388 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 15.
389 IONOS, Aktuelle Rechtslage zum US-Datentransfer unter besonderer Berücksichtigung des US CLOUD Act, 2, 6.
390 IONOS, Aktuelle Rechtslage zum US-Datentransfer unter besonderer Berücksichtigung des US CLOUD Act, 2, 7.
391 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 16.
392 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 16.
393 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 16.

3.4.2.5 Voraussetzungen nach dem CLOUD Act

Anders als die DSGVO ist der CLOUD Act kein eigenständiges Gesetz, sondern eine Ergänzung zu anderen Gesetzen, deren Voraussetzungen in den bestimmten Situationen gelten. Bei der Prüfung der Vorschriften des CLOUD Act sollten insbesondere die zwei folgenden Gesetze betrachtet werden.

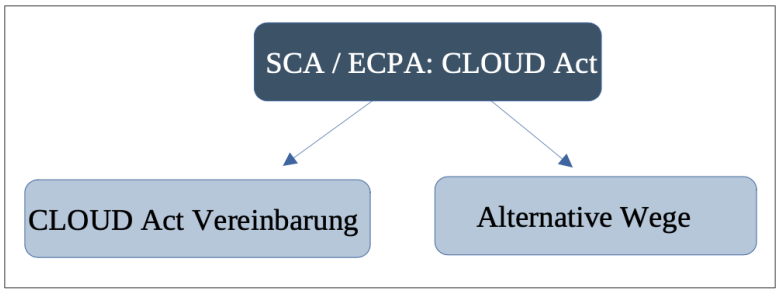

Abbildung 3.4.2.5 Voraussetzungen nach dem CLOUD Act

Der SCA (Stored Communications Act; 18 U.S.C. §§ 2701 ff.) regelt den Zugriff auf gespeicherte drahtgebundene und elektronische Kommunikation wie E-Mails und andere Online-Nachrichten, die von Dienstanbietern gespeichert werden.[394] Das SCA wurde als Titel II des ECPA (Electronic Communications Privacy Act von 1986) verabschiedet, der erlassen wurde, um Abhörmaßnahmen der Regierung und andere Fragen der Kommunikationsverfolgung zu regeln.[395] Das SCA verbietet Anbietern die Weitergabe elektronischer Kommunikation an Personen oder Einrichtungen.[396] Es enthält aber auch Ausnahmen, z. B. wenn die Regierung die Informationen erzwingt.[397]

Mit dem CLOUD Act wurde eine Meinungsverschiedenheit über den Anwendungsbereich des SCA beigelegt.[398] Es ging um die Entscheidung des US-Bundesgerichts vom 07.2016 über den Microsoft-Fall, in der erstmals festgestellt wurde, dass das SCA die Regierung nicht ermächtigt, die Offenlegung von im Ausland gespeicherten Daten von Unternehmen zu verlangen, die der US-Gerichtsbarkeit unterliegen.[399] Nach dieser Entscheidung hatten sich einige US-Anbieter geweigert, auf der Grundlage des SCA gerichtliche Anordnungen zur Herausgabe von auf Servern im Ausland gespeicherten Daten zu befolgen.[400]

394 *Balser*, Overview of Governmental Action Under the Stored Communications Act (SCA), S. 1.
395 *Balser*, Overview of Governmental Action Under the Stored Communications Act (SCA), S. 1.
396 *Balser*, Overview of Governmental Action Under the Stored Communications Act (SCA), S. 1.
397 *Balser*, Overview of Governmental Action Under the Stored Communications Act (SCA), S. 1.
398 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 7.
399 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 7.
400 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 7.

Das SCA regelt die elektronische Kommunikation und Aufzeichnungen, die sich in Ruhestand / „at Rest“ oder in elektronischer Form im Besitz von Anbietern befinden.[401] Andere Bestimmungen des ECPA, wie z. B. das Abhörgesetz (Wiretap Act), befassen sich mit der Kommunikation während der Übertragung.[402]

Der CLOUD Act ist ein Änderungsgesetz[403] / eine Ergänzung des SCA[404] (Abschn. 270310 ECPA) und schafft entsprechend keine neue Form von Anordnungen.[405] Er verdeutlicht lediglich die Verpflichtungen von US-Anbietern / „US-Provider“ im Rahmen des SCA.[406]

US-Strafverfolgungsbehörden können einen Durchsuchungsbefehl für die Daten einer US-Organisation ausstellen, und sofern eine der drei folgenden Voraussetzungen erfüllt ist, muss diese Organisation dem nachkommen:

1. Der US-Anbieter muss der US-Gerichtsbarkeit unterliegen.[407] Ob dies der Fall ist, ist von einer faktenabhängigen Analyse abhängig, bei der es darum geht, ob ein Unternehmen ausreichende Kontakte zu den USA hat, um die Ausübung der Gerichtsbarkeit zu ermöglichen.[408]

2. Es handelt sich um einen Anbieter von elektronischen Kommunikationsdiensten oder Ferninformationsdiensten.[409]

3. Die Organisation ist im Besitz, im Gewahrsam oder unter der Kontrolle / „possesion, custody, or control“ der gesuchten Daten.[410] Abschnitt 103 (a) (1), § 2713 Hs. 1 CLOUD Act verpflichtet US-Provider, die Daten, die sich im Besitz, im Gewahrsam oder unter der Kontrolle dieses Anbieters befinden, aufzubewahren, zu schützen und offenzulegen.

401 *Balser*, Overview of Governmental Action Under the Stored Communications Act (SCA), S. 1.
402 *Balser*, Overview of Governmental Action Under the Stored Communications Act (SCA), S. 1.
403 Wissenschaftliche Dienste des Deutschen Bundestages, WD 3 - 3000 – 181/20, 2, 5.
404 IONOS, Aktuelle Rechtslage zum US-Datentransfer unter besonderer Berücksichtigung des US CLOUD Act, 2, 6.
405 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 15.
406 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 15.
407 How to comply with both the GDPR and the CLOUD Act, abrufbar: https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/, zuletzt abgerufen am 03.08.2023; vgl.: The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 17.
408 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 17.
409 How to comply with both the GDPR and the CLOUD Act, abrufbar: https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/, zuletzt abgerufen am 03.08.2023.
410 How to comply with both the GDPR and the CLOUD Act, abrufbar: https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/, zuletzt abgerufen am 03.08.2023.

Der CLOUD Act hängt in Bezug auf den Zugang der Strafverfolgungsbehörden zu Daten nicht von der Frage des „Eigentums“ an den Daten ab.[411] Stattdessen wird die Offenlegung von Daten verlangt, die sich **im Besitz oder unter der Kontrolle** eines Dienstleistungserbringers befinden, in Übereinstimmung mit Art. 18 des Auszuges aus dem Erläuternden Bericht: 173 Budapester Übereinkommen.[412]

Laut Art. 18 des Auszuges aus dem Erläuternden Bericht: 173, S. 2 Budapester Übereinkommen beziehen jedoch „**Besitz oder Kontrolle**“ sich auf den physischen Besitz der betreffenden Daten im Hoheitsgebiet des Auftraggebers sowie auf Situationen, in denen sich die vorzulegenden Daten außerhalb des physischen Besitzes der Person befinden, diese Person aber dennoch die Vorlage der Daten vom Hoheitsgebiet des Auftraggebers aus frei kontrollieren kann.

Der CLOUD Act besagt nicht, wie lange der US-Provider die Daten aufbewahren soll. Dies wird jedoch in 18 U.S.C. § 2703 (a) S. 1 Hs. 1 mit 180 Tagen oder weniger konkretisiert.

Der CLOUD Act erlaubt es den US-Strafverfolgungsbehörden, Haftbefehle auszustellen, um Zugang zu Daten zu erhalten.[413] Sind die Daten verschlüsselt, hat die Strafverfolgungsbehörde keine Befugnis, Dienstanbieter zur Entschlüsselung der Kommunikation zu zwingen.[414] Ebenso wenig hindert es die Diensteanbieter daran, bei der Entschlüsselung zu helfen, oder die Länder daran, Entschlüsselungsanforderungen in ihren Gesetzen zu regeln.[415]

3.4.2.5.1 CLOUD Act Vereinbarungen

Abschnitt 102 (3) CLOUD Act sieht vor, dass ausländische Regierungen sich um den Zugang zu elektronischen Daten bemühen können, die von Kommunikationsdienstleistern in den USA gespeichert werden. Fordert eine ausländische Regierung die Freigabe elektronischer Daten an, deren Weitergabe den Anbietern nach US-Recht untersagt ist, kann dies nach Abschn. 102 (5) Hs. 1 CLOUD Act die US-Anbieter potenziell widersprüchlichen rechtlichen Verpflichtungen aussetzen. Entsprechend zögern Dienstleister, auf Datenanfragen ausländischer Behörden zu antworten, weil sie befürchten, dass sie gegen inländische Gesetze zum Schutz der Privatsphäre und des Datenschutzes verstoßen.[416]

411 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 16.
412 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 16.
413 How to comply with both the GDPR and the CLOUD Act, abrufbar: https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/, zuletzt abgerufen am 03.08.2023.
414 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 18.
415 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 18.
416 *Wood/Lewis*, CSIS, 03.2023, 1, 2.

Als Lösung solcher Situationen sieht Abschn. 102 (6) CLOUD Act internationale Vereinbarungen / CLOUD Act Vereinbarungen (sog. „Executive Agreements“) vor. Besteht eine solche Vereinbarung, können die Behörden des ausländischen Landes direkt verlangen, dass US-Anbieter Daten ohne weitere Prüfung herausgeben und umgekehrt:[417] Die US-Behörden können direkt verlangen, dass Anbieter aus ausländischen Staaten Daten ohne weitere Prüfung herausgeben. CLOUD Act Vereinbarungen werden als Reaktion auf ein Gerichtsverfahren verwendet.[418]

Die nach dem CLOUD Act erlassenen Anordnungen müssen dem Zweck dienen, Informationen im Zusammenhang mit der Verhinderung, Aufdeckung, Untersuchung oder Verfolgung schwerer Straftaten, die Terrorismus auslösen, zu erhalten und müssen einer Überprüfung oder Aufsicht durch eine Justizbehörde unterliegen.[419]

Abschnitt 105, § 2523 (b) CLOUD Act legt Anforderungen zu CLOUD Act Vereinbarungen fest. Auf dieser Grundlage können die ausländischen Behörden ihre inländischen Gerichtsverfahren nach ihrem eigenen Recht direkt an die Anbieter zustellen, und die Anbieter können die entsprechenden Daten direkt an die ausländischen Behörden weitergeben.[420] Hierbei ist **darauf zu vertrauen** („the authorities of each country may use their own domestic authority“), dass die rechtliche Forderung nicht gegen das Recht des anderen Landes verstößt.[421] Die im Rahmen des CLOUD Act vorgesehenen bilateralen Abkommen sollten die Konflikte beseitigen, wenn sowohl die anfragende als auch die liefernde Gerichtsbarkeit ähnliche Datenschutz- und Bürgerrechtsschutzbestimmungen haben.[422]

Die CLOUD Act Vereinbarungen sind als sehr kritisch zu betrachten. Die direkte Anfrage ausländischer Behörden bei US-Anbietern oder von US-Behörden bei EU-Anbietern bietet die Möglichkeit, bei jeder Gelegenheit weltweit Daten anzusammeln. Zudem ist die Transparenz nicht mehr gewährleistet, da die Behörde gegenüber einem Dritten (in diesem Fall einem Gericht) nicht nachweisen muss, warum und welche Daten sie genau erheben möchte. Es darf nicht vergessen werden, dass die Behörde nicht alle rechtlichen Vorgaben eines fremden Landes kennen kann. Dies kann in vielen Fällen bedeuten, dass die auf CLOUD Act Vereinbarungen basierenden Anfragen die Rechte anderer Personen verletzen können. Es reicht nicht aus, nur **„darauf zu vertrauen“**, dass die Anfrage nicht gegen das Recht des anderen Landes verstößt.

417 IONOS, Aktuelle Rechtslage zum US-Datentransfer unter besonderer Berücksichtigung des US CLOUD Act, 2, 7.
418 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 13.
419 *Wood/Lewis*, CSIS, 03.2023, 1, 2.
420 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 12.
421 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 12.
422 *Wood/Lewis*, CSIS, 03.2023, 1, 2.

Das CLOUD Act ersetzt nicht das Verfahren des Rechtshilfevertrags, sondern bietet vielmehr eine zusätzliche Methode des grenzüberschreitenden Datenzugriffs.[423] Die CLOUD Act Vereinbarungen schaffen keine Verpflichtungen oder Beschränkungen für Anbieter; sie beseitigen lediglich rechtliche Beschränkungen, die andernfalls der Einhaltung der erfassten Aufträge entgegenstehen würden.[424] Anbieter, die Aufträge nach der CLOUD Act Vereinbarung erteilen, unterliegen den innerstaatlichen Vorschriften des ausstellenden Landes.[425] Daher muss jede Durchsetzung nach dem Recht des Landes erfolgen, das die Offenlegung verlangt.[426] Ein US-Anbieter, der eine ausländische Anordnung zur Offenlegung von Informationen erhält, kann nach dem Recht des ausländischen Staates anfechten, soweit es nach diesem Recht zulässig ist.[427]

Anordnungen ausländischer Regierungen, die Gegenstand von Vereinbarungen sind, dürfen nicht auf Daten von **Personen der Vereinigten Staaten** oder in den USA ansässigen Personen abzielen.[428] Den ausländischen Regierungen steht es dennoch frei, in **Verhandlungen ähnliche Beschränkungen** anzustreben.[429]

Der Begriff „Person der Vereinigten Staaten“ / „United States Person“ bezeichnet nach Abschn. 105, § 2523 (a) (2) CLOUD Act einen Bürger oder Staatsangehörigen der USA, einen Ausländer, der rechtmäßig zum ständigen Aufenthalt zugelassen ist, eine nicht rechtsfähige Vereinigung, bei der eine wesentliche Anzahl der Mitglieder US-Bürger oder Ausländer sind, die rechtmäßig zum ständigen Aufenthalt zugelassen sind, oder eine in den USA gegründete Gesellschaft.

423 *Wood/Lewis*, CSIS, 03.2023, 1, 2.
424 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 14.
425 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 14.
426 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 14.
427 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 14.
428 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 12.
429 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 12.

Die USA und andere Länder können weiterhin ihre bestehenden rechtlichen Verfahren nutzen, um Daten außerhalb dieser Vereinbarungen abzufragen, sind aber unter diesen Umständen möglicherweise mit einem Rechtskonflikt konfrontiert.[430] Sollte die US-Regierung versuchen, die Anordnung trotz eines Konflikts mit ausländischem Recht durchzusetzen, **ist davon auszugehen** („can be expected"), dass die US-Gerichte die geltenden US-amerikanischen und internationalen Grundsätze in Bezug auf Rechtskonflikte anwenden und eine mehrstufige Abwägungsprüfung durchführen, bei der die Interessen sowohl der USA als auch des ausländischen Staates berücksichtigt werden.[431]

Die Sprache, die das US-Justizministerium hier verwendet, ist viel zu weich. Die Worte „**ist davon auszugehen**" vernachlässigen die Bedeutung der Anwendung internationaler Grundsätze und einer mehrstufigen Abwägungsprüfung. Wenn es um Rechtskonflikte zwischen Ländern geht, muss klar formuliert werden, was zu tun ist, was genau vom Gericht oder der Behörde erwartet wird und wie sie sich daran halten sollen. Es muss deutlich gemacht werden, dass die Anwendung internationaler Grundsätze und eine mehrstufige Abwägungsprüfung unverzichtbar sind und in jedem Fall durchgeführt werden sollten, um die (Persönlichkeits-) Rechte und die dahinter stehenden Menschen bestmöglich zu schützen.

Nach Abschn. 105, § 2523 (b) (1) CLOUD Act sollte das innerstaatliche Recht der ausländischen Regierung sowie die Umsetzung dieses Rechts einen soliden materiell- und verfahrensrechtlichen Schutz der **Privatsphäre** und der **bürgerlichen Freiheiten** in Anbetracht der Datenerhebung und der Aktivitäten der ausländischen Regierung bieten. Die ausländische Regierung muss **Rechenschaft** über die Erhebung und Verwendung elektronischer Daten ablegen und für angemessene Transparenz sorgen.[432] Die Vereinbarung nach dem CLOUD Act erfordert eine Bewertung des innerstaatlichen Rechts des fremden Landes, um sicherzustellen, dass es den materiellen und verfahrenstechnischen Schutz der Privatsphäre und der bürgerlichen Freiheiten respektiert und die Zielgruppe einschränkt.[433] Wie sie umgesetzt werden soll, ist nicht im ClOUD Act vorgeschrieben.

430 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 12.
431 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 16.
432 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 13.
433 *Wood/Lewis*, CSIS, 03.2023, 1, 2.

Es verdient, hervorgehoben zu werden, dass dieser Vorbehalt gem. Abschn. 105, § 2523 (b) (1) CLOUD Act als positiv zu bewerten ist. Wenn ein Land zeigt, dass es die Privatsphäre und die Freiheiten seiner Bürger schützt, ist das natürlich gut; wenn es dafür Rechenschaft über die Erhebung und Verwendung elektronischer Daten ablegen muss, ist dies noch besser. Aber wie kann es gewährleistet werden? Wie soll ein Land nachweisen, dass es seine Bürger schützt? Wie kann eine angemessene Transparenz gemessen werden? Wird es in Zukunft einen internationalen Mechanismus dafür geben? Muss ein Land die US-Vorschriften und -Anforderungen befolgen oder reicht es aus, wenn es dies nach seinen eigenen Vorschriften und Anforderungen tut?

Die Untersuchung der Persönlichkeitsrechte und ihrer besonderen Ausprägungen, die in den vorangegangenen Kapiteln beschrieben wurden, hat deutlich gezeigt, dass es trotz vieler Ähnlichkeiten auch zahlreiche Unterschiede zwischen den Rechtssystemen der EU und der USA gibt. Wie werden diese Unterschiede bei der Rechenschaft über die Erhebung und Verwendung elektronischer Daten abgedeckt? Das CLOUD Act gibt hierauf derzeit keine genaue Antwort, und es bleibt abzuwarten, wie es in der Rechtsprechung ausgelegt wird.

Hat der Anbieter Bedenken hinsichtlich der Anwendbarkeit des Abkommens auf einen bestimmten Produktionsauftrag, kann er sich mit der benannten Behörde des Landes, das den Auftrag erteilt, beraten.[434] Darüber hinaus hat die benannte Behörde des anderen Landes die Möglichkeit, das Abkommen in einem bestimmten Fall unanwendbar zu machen, wenn sie der Ansicht ist, dass es unrechtmäßig in Anspruch genommen wurde.[435]

Anbieter **dürfen** Kontoinhaber über Abfragen aufgrund einer gerichtlichen Anordnung informieren, es sei denn, ein unabhängiger Richter hat eine Schutzanordnung erlassen.[436] Da die Unterrichtung des Kontoinhabers kein Pflicht ist (die Anbieter dürfen den Kontoinhaber informieren; müssen aber nicht), ist es sehr unwahrscheinlich, dass die Anbieter dies immer tun werden. Dadurch verliert der User die Kontrolle über seine Daten, und die Persönlichkeitsrechte werden beeinträchtigt.

434 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 14.

435 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 14.

436 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 18.

3.4.2.5.2 Alternative Wege

Wenn kein CLOUD Act-Abkommen besteht, könnte die Befolgung einer gerichtlichen Anordnung in den USA durch ein Unternehmen mit dem Gesetz eines anderen Landes kollidieren, das die Herausgabe von Daten verbietet.[437] In solchen Fällen könnte die US-Regierung alternative Wege beschreiten (z. B. **die Einschränkung** oder **Änderung eines Ersuchens**), um den Konflikt zu vermeiden.[438]

Das Gericht kann das Gerichtsverfahren gem. Abschn. 103, § 2713 (h) (2) (B) CLOUD Act abändern oder aufheben, wenn es feststellt, dass 1. die geforderte Offenlegung dazu führen würde, dass der Anbieter gegen die Gesetze einer qualifizierten ausländischen Regierung verstößt, 2. aufgrund der Gesamtheit der Umstände die Interessen der Justiz eine Änderung oder Aufhebung des Gerichtsverfahrens erfordern und 3. der Kunde oder Abonnent kein Person der Vereinigten Staaten / „United States Person" ist und nicht dort ansässig ist.

Darüber hinaus hat eine Partei eine Alternative nach wie vor zum **MLA-Verfahren**[439] bzw. MLAT-Verfahren. Es wird weiterhin eine Option sein, um Daten zu erhalten, die nicht durch ein CLOUD Act Abkommen abgedeckt sind oder wenn es kein solches Abkommen gibt.[440]

3.4.3 Konflikte zwischen den Datenschutzbestimmungen der EU und der USA

Die jüngsten Konflikte zwischen den Datenschutzbestimmungen der EU und der USA in Bezug auf internationale Datenübertragungen sind weitgehend auf den CLOUD Act zurückzuführen. Daher ist es zielführend, zunächst zu verstehen, warum bzw. wofür das Gesetz geschaffen wurde. Dies wird von Georgia Woods und James A. Lewis vom Center for Strategic and International Studies ausführlich beschrieben.

3.4.3.1 Entstehung des CLOUD Act

Es wurde bereits erwähnt, dass sich die Strafverfolgungsbehörden in vielen Ländern seit Jahren über die Langsamkeit der herkömmlichen Verfahren beschweren.[441] Eine Überprüfung der US-Regierung aus dem Jahr 2013 ergab, dass die Beantwortung von Anfragen etwa zehn Monate dauerte, wobei einige Anfragen noch länger dauerten.[442]

---

437 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 15 ff.

438 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 16.

439 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 11 ff.

440 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 11.

441 *Wood/Lewis*, CSIS, 03.2023, 1, 1.

442 *Wood/Lewis*, CSIS, 03.2023, 1, 1.

Im Jahr 2013 legten die Vereinigten Staaten Microsoft Ireland einen Haftbefehl zur Herausgabe von Daten vor, die in einem Rechenzentrum in Dublin gespeichert waren.[443] Microsoft argumentierte, dass das US-Gericht nicht befugt sei, eine Ermächtigung für im Ausland gespeicherten Daten zu erlassen, und forderte es auf, die Anordnung aufzuheben.[444] Die Begründung, dass die materielle Kontrolle über die Daten – unabhängig davon, wo sie gespeichert sind – für den südlichen Bezirk von New York ausreichend war, besagte, dass Microsoft der Anordnung nachkommen könne.[445] Das US-Berufungsgericht für den zweiten Gerichtsbezirk entschied jedoch, dass es sich in diesem Fall um eine unzulässige extraterritoriale Anwendung von US-Recht handelte.[446] Die Vereinigten Staaten legten beim Obersten Gerichtshof Berufung ein und verwiesen darauf, dass andere Gerichte zuvor festgestellt hatten, dass die Verpflichtung von US-Unternehmen zur Einhaltung von SCA außerhalb der USA eine inländische Anwendung des Gesetzes sei.[447] Bevor der Oberste Gerichtshof entschied, verabschiedete der Kongress den CLOUD Act.[448]

Mit dem CLOUD Act wurde das SCA geändert, um klarzustellen, dass Kommunikationsdienstanbieter Datenanfragen der US-Regierung nachkommen müssen, unabhängig davon, ob sich die Daten innerhalb oder außerhalb der Vereinigten Staaten befinden.[449] Diese löste in der Europäischen Union Bedenken hinsichtlich der extraterritorialen Anwendung des US-Rechts aus.[450]

3.4.3.2 Problematik

Digitale Souveränität oder die Kontrolle über die Technologie, die unter der eigenen Gerichtsbarkeit betrieben wird, ist ein zentrales Ziel der EU-Mitgliedstaaten.[451] Aufbauend auf dem Misstrauen gegenüber der Privatsphäre und dem Datenschutz der Nutzer, das teilweise durch die Snowden-Enthüllungen über die Überwachung verschärft wurde, stieß der CLOUD Act auf Kritik und Bedenken von EU-Behörden, die befürchteten, dass er die digitale Souveränität Europas verletzen würde.[452] Ohne ein Abkommen zwischen der EU und den USA über den Zugang zu elektronischen Beweismitteln bleiben Konflikte zwischen der DSGVO und dem CLOUD Act bestehen.[453] Diese Konflikte und Herausforderungen sind aber nicht neu.

443 *Wood/Lewis*, CSIS, 03.2023, 1, 2.
444 *Wood/Lewis*, CSIS, 03.2023, 1, 2.
445 *Wood/Lewis*, CSIS, 03.2023, 1, 2.
446 *Wood/Lewis*, CSIS, 03.2023, 1, 2.
447 *Wood/Lewis*, CSIS, 03.2023, 1, 2.
448 *Wood/Lewis*, CSIS, 03.2023, 1, 2.
449 *Wood/Lewis*, CSIS, 03.2023, 1, 2.
450 *Wood/Lewis*, CSIS, 03.2023, 1, 2.
451 *Wood/Lewis*, CSIS, 03.2023, 1, 2.
452 *Wood/Lewis*, CSIS, 03.2023, 1, 2.
453 *Wood/Lewis*, CSIS, 03.2023, 1, 3.

Nach den Anschlägen vom 11.09.2001 haben die Vereinigten Staaten eine Vielzahl von Sicherheitsgesetzen erlassen, um die Sicherheit vor Terrorismus und anderen Bedrohungen zu erhöhen.[454] Diese Gesetze ermöglichen häufig den Zugriff auf Daten von Privatunternehmen für die anschließende Datenanalyse.[455] Die US-Vorschriften zur Erhöhung der Sicherheit werden als „**trojanisches Pferd**" bezeichnet, das vor allem versucht, die EU-Datenschutzfestungen anzugreifen.[456] Da der PATRIOT Act und andere Gesetze den Zugriff auf Daten von Personen ermöglichen, die sich nicht in den USA aufhalten, stellt dies eine weitere Herausforderung dar.[457]

Der Ansatz einer **Vielzahl von Rechtsordnungen** führt zu Herausforderungen in Bezug auf das anwendbare Recht: Es besteht beispielsweise die Gefahr, dass bei Einzelpersonen unrealistische Erwartungen geweckt werden, dass ihre Daten bei der Verarbeitung außerhalb ihrer eigenen Rechtsordnung denselben Rechtsschutz genießen.[458]

Darüber hinaus ergeben sich Herausforderungen für Unternehmen, wenn sie bei der Datenverarbeitung **den Rechtsordnungen verschiedener Länder** unterliegen, oder für die Länder selbst, wenn sie z. B. unterschiedliche internationale Verträge abschließen und die jeweiligen Regelungen nicht übereinstimmen.[459] Die bestehenden Anwendungen der Datenschutzgesetze verschiedener Länder führen daher zu einer Vielzahl von Regelungen und Konflikten, für die offenbar noch keine geeignete, zufriedenstellende Lösung gefunden wurde.[460]

454 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 75 ff.
455 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 75 ff.
456 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 75 ff.
457 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 75 ff.
458 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 79.
459 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 79.
460 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 79.

Die Bewertung von den EU-Behörden über Kompatibilität zwischen dem EU-Rechtsrahmen und CLOUD Act ergab, dass der größte potenzielle Konflikt in Art. 48 DSGVO über **unzulässige Übermittlungen oder Offenlegungen** nach EU-Recht zu finden ist.[461] Artikel 48 DSGVO besagt, dass Urteile eines Gerichts eines Drittlands oder Entscheidungen einer Verwaltungsbehörde eines Drittlands nur dann anerkannt oder vollstreckt werden dürfen, wenn sie (unbeschadet andere Gründe für die Übermittlung nach Kapitel V der DSGVO) auf eine in Kraft befindliche internationale Übereinkunft zwischen dem ersuchenden Drittland und der EU oder einem EU-Mitgliedstaat gestützt sind. Sind sie auf diesem Übereinkunft gestützt, darf von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt werden. Die EU-Kommission argumentierte im Microsoft-Fall, dass Art. 48 DSGVO klar stellte, dass ein ausländischer Gerichtsbeschluss eine Übermittlung als solche unrechtmäßig im Sinne der DSGVO macht.[462]

Artikel 49 DSGVO legt die Bedingungen fest, unter denen eine internationale Übermittlung erfolgen könnte, wenn kein internationales Abkommen[463] bzw. kein Angemessenheitsbeschluss oder keine geeignete Garantien bestehen. Unter anderem sind es die folgenden Szenarien: 1. Die Übertragung „aus wichtigen Gründen des öffentlichen Interesses“ nach Art. 49 Abs. 1 lit. d) DSGVO und 2. die Übertragung nach Art. 49 Abs. 1 lit. f) DSGVO, wenn die Übermittlung im „Schutz lebenswichtigen Interesse“ des Betroffenen selbst[464] oder anderer Person liegt.

Sollten diese als Grund für eine Datenübermittlung in die USA ohne internationale Abkommen verstanden werden? Sicherlich nicht – das ließe sich vielleicht nur in Einzelfällen, aber nicht in allen Fällen rechtfertigen. Die Überschrift von Art. 49 DSGVO erklärt diese bereits: „Ausnahmen für bestimmte Fälle“. Mit dieser Logik sind alle Strafverfahren wichtig für das öffentliche und vitale Interesse, aber wenn die digitale Souveränität und die technologische Kontrolle eines anderen Landes im Wege stehen, sollten immer internationale Vereinbarungen getroffen werden. Es sollten nicht einfach irgendwelche Daten bei Internet-Anbietern oder IT-Dienstleistern abgegriffen werden dürfen, weil eine Behörde einen Verdacht hat.

461 *Wood/Lewis*, CSIS, 03.2023, 1, 3.
462 *Wood/Lewis*, CSIS, 03.2023, 1, 3.
463 *Wood/Lewis*, CSIS, 03.2023, 1, 3.
464 *Wood/Lewis*, CSIS, 03.2023, 1, 3.

Alles, was oben beschrieben wurde, beweist dass die DSGVO und der CLOUD Act unvereinbar sind. Jegliche Datenübermittlung in die USA nach dem CLOUD Act steht grundsätzlich im Widerspruch zu den grundlegende Prinzipien der DSGVO. Für die Datenübermittlung fehlt die von der DSGVO geforderte Rechtsgrundlage zum Schutz der informationellen Selbstbestimmung des Einzelnen.[465] Es wäre nicht richtig, alle Ersuchen der US-Behörden als Ausnahmefälle zu sehen und sie so zu betrachten – es wäre keine korrekte Auslegung dieses Artikels.

Der Fortschritt bei einem CLOUD Act-Abkommen zwischen der EU und den USA wurde durch EuGH-Entscheidungen erschwert.[466] Seit den Snowden-Enthüllungen von 2013, die Massenüberwachung durch die NSA (National Security Agency) zum Zwecke der Terrorismusbekämpfung aufdeckten, gibt es in Europa zunehmende Besorgnis über den Zugriff der US-Regierung auf Daten von EU-Bürgern.[467] Darüber hinaus gibt es Bedenken, dass das CLOUD Act negative Auswirkungen auf die Persönlichkeitsrechte haben könnte. Das Gesetz erschwert den Betroffenen die Kontrolle über personenbezogene Daten.

Im Jahr 2015 erklärte der EuGH das Safe-Harbor-Datenschutzabkommen zwischen der EU und den USA in der ,,Schrems I"-Entscheidung für ungültig.[468] In dieser Entscheidung führte der EuGH an, dass die Snowden-Enthüllungen eine erhebliche Übergriffigkeit seitens der NSA und anderer Bundesbehörden zeigten und dass Datenübermittlungen in die Vereinigten Staaten gegen Art. 7 GrCh (Achtung des Privat- und Familienlebens) verstoßen könnten.[469]

Nach Schrems I begannen die Arbeiten zur Wiederherstellung der rechtlichen Grundlage für den transatlantischen Datenverkehr.[470] Dies führte zum erneuerten Abkommen zwischen der EU und den USA über Datenschutzgrundsätze, nämlich ,,Privacy Shield".[471] 2020 erklärte der EuGH diesen in der ,,Schrems II"-Entscheidung für ungültig.[472] In dieser Entscheidung befasste sich der EuGH hauptsächlich mit US-Vorschriften, die bestimmte Signalaufklärungsaktivitäten ermöglichen.[473] Die Entscheidung bezog sich auf Abschn. 702 FISA, der es der US-Regierung erlaubt, Kommunikationsdienstleister zu verpflichten, bei der Überwachung ausländischer Personen außerhalb des Landes zu helfen, und auf die E. O. 12333, die festlegt, wann Geheimdienste im Ausland tätig werden dürfen (Geheimdienstüberwachung im Ausland).[474]

---

465 Diese Meinung wird in dem folgenden Artikel geäußert. S.: Wie sicher sind Ihre Daten vor dem US CLOUD Act? abrufbar: https://www.plusserver.com/blog/cloud-act, zuletzt abgerufen am 02.08.2023.
466 *Wood/Lewis*, CSIS, 03.2023, 1, 3 ff.
467 *Wood/Lewis*, CSIS, 03.2023, 1, 3 ff.
468 *Wood/Lewis*, CSIS, 03.2023, 1, 3 ff.
469 *Wood/Lewis*, CSIS, 03.2023, 1, 3 ff.
470 *Wood/Lewis*, CSIS, 03.2023, 1, 4.
471 *Wood/Lewis*, CSIS, 03.2023, 1, 4.
472 *Wood/Lewis*, CSIS, 03.2023, 1, 4.
473 *Wood/Lewis*, CSIS, 03.2023, 1, 4.
474 *Wood/Lewis*, CSIS, 03.2023, 1, 4.

Welche Folgen kann die Missachtung des Sicherheitsniveaus für die USA haben? Werden beispielsweiße Standardvertragklauseln[475] nicht unterzeichnet, können Geldbußen verhängt werden; werden die Geldbußen nicht gezahlt, erhält eine Organisation Sanktionen.[476] Wie sich die Sanktionen auf eine Organisation auswirken können, lässt sich am Beispiel sanktionierter Unternehmen beim Krieg zwischen Russland und der Ukraine beurteilen. Daher ist es wichtig zu wissen, welche Anforderungen befolgt werden müssen, um rechtmäßig zu agieren.

Derzeit ist es so: Hält eine Organisation die DSGVO ein, verstößt sie gegen den CLOUD Act, wenn sie aufgefordert wird, personenbezogene Daten an die Behörden eines anderes Landes weiterzugeben bzw. offenzulegen. Hält eine Organisation den CLOUD Act ein und gibt Daten weiter oder legt sie offen, verstößt sie gegen die DSGVO. Daraus ergibt sich die Frage: Ist es möglich, Daten zwischen der EU und den USA auf eine Weise zu transferieren, die nicht gegen diese Gesetze verstößt? – Die Antwort lautet: Ja, es ist möglich.

3.4.4 Internationale Bemühungen

Sowohl in der EU als auch in den USA wird viel getan, um einen reibungslosen internationalen Datenaustausch zu gewährleisten. Einige der Ergebnisse dieser Bemühungen sind das MLAT-Verfahren, der neue EU-US Datenschutzrahmen und andere länderübergreifende Verordnungen oder Beschlüsse.

3.4.4.1 MLAT-Verfahren

Die Bekämpfung von schweren Straftaten wie organisierter Kriminalität, Korruption oder Terrorismus ist eine wachsende grenzüberschreitende Herausforderung.[477] Die Staaten müssen Zugang zu grundlegenden und einfachen Informationen haben, um ihre Aufgaben zu erfüllen.[478] Dafür ist die Rechtshilfe eine Form der Zusammenarbeit zwischen verschiedenen Ländern zum Zweck der Sammlung und des Austauschs von Informationen.[479] Die EU-Kommission besagt, dass die Behörden eines Landes Beweismittel aus einem anderen Land anfordern sowie für dieses zur Verfügung stellen können, um strafrechtliche Ermittlungen oder Verfahren in einem anderen Land zu unterstützen.[480]

475 Standardvertragsklauseln sind ab 07.2023 nicht mehr verbindlich. Sie werden hier lediglich als Beispiel genannt.
476 Diese Meinung wurde auf der Global GRC, Data Privacy & Cyber Security ConfEx am 31.05.2023 in NY/USA geäußert.
477 G2012 MEXIKO, REQUESTING MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS FROM G20 COUNTRIES, A STEP-BY-STEP-Guide, Foreword.
478 G2012 MEXIKO, REQUESTING MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS FROM G20 COUNTRIES, A STEP-BY-STEP-Guide, Foreword.
479 Mutual legal assistance and extradition, abrufbar: https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en, zuletzt abgerufen am 02.08.2023.
480 Mutual legal assistance and extradition, abrufbar: https://ec.europa.eu/info/law/cross-border-cases/judicial-

Rechtshilfe / „Judicial Assistance“ kann in der Vollstreckung eines von einem Gericht eines anderen Staates erlassenen Urteils oder in anderen Maßnahmen zur Unterstützung eines laufenden Gerichtsverfahrens in dem Staat bestehen, der um die Zusammenarbeit mit dem ausländischen Gericht ersucht. In einem Rechtshilfeersuchen wird ein ausländisches Gericht ersucht, bestimmte gerichtliche Maßnahmen zu ergreifen, z. B. eine Vorladung zuzustellen, die Vorlage von Dokumenten zu erzwingen oder eine Beweisaufnahme durchzuführen. Zwischen den Ländern können Verträge geschlossen werden, um regelmäßige Verfahren für die Übermittlung dieser Ersuchen festzulegen und die gegenseitige Behandlung bei der Gewährung von Rechtshilfe zu gewährleisten.[481]

Zwischen der EU und den USA wurden nach den Terroranschlägen am 11.09.2001[482] mindestens acht wichtige Abkommen[483] zur Strafverfolgung geschlossen. Im Jahr 2003 wurden die ersten internationalen Abkommen im Bereich Justiz und Inneres von der EU unterzeichnet.[484] [485] Trotzdem sind im Laufe der Zeit neue Anforderungen entstanden, und die Aushandlung eines Abkommens über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln wurde als besonders wichtig erachtet.[486]

Die meisten Ersuche werden im Rahmen des MLATs gestellt, das Gesetzeskraft hat und im Allgemeinen schneller und zuverlässiger als Rechtshilfeersuche / „Letters Rogatory“ ist.[487] Das MLAT regelt die Verpflichtung zur Amtshilfe, den Umfang der Amtshilfe sowie den Inhalt des Ersuchens und kann Beweisbestimmungen enthalten, die von den Bundesbeweisregeln abweichen.[488] Gemäß Art. 1 EU-US MLAT verpflichten sich die EU und die USA, MLAT-Verpflichtungen zur Stärkung der Zusammenarbeit und gegenseitigen Rechtshilfe zu erfüllen.

---

cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en, zuletzt abgerufen am 02.08.2023.

481 Der Begriff „Rechtshilfe“ wird im folgenden Artikel definiert. S.: Judicial Assistance, abrufbar: https://www.encyclopedia.com/law/encyclopedias-almanacs-transcripts-and-maps/judicial-assistance, zuletzt abgerufen am 02.08.2023.

482 Mutual legal assistance and extradition, abrufbar: https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en, zuletzt abgerufen am 02.08.2023.

483 *Christakis/Terpan*, IDPL, Vol. 11, Nr. 2, 2021, 81, 83.

484 Mutual legal assistance and extradition, abrufbar: https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en, zuletzt abgerufen am 02.08.2023.

485 Das Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Rechtshilfe (EU-US MLAT bzw. MLAT-Abkommen) gilt ab 19.07.2003.

486 *Christakis/Terpan*, IDPL, Vol. 11, Nr. 2, 2021, 81, 83.

487 276. TREATY REQUESTS, abrufbar: https://www.justice.gov/archives/jm/criminal-resource-manual-276-treaty-requests, zuletzt abgerufen am 02.08.2023.

488 276. TREATY REQUESTS, abrufbar: https://www.justice.gov/archives/jm/criminal-resource-manual-276-treaty-requests, zuletzt abgerufen am 02.08.2023.

Das MLAT-Abkommen gilt sowohl für das Strafrecht als auch für das Verwaltungsverfahren zur Untersuchung von Handlungen im Hinblick auf ihre strafrechtliche Verfolgung, betrifft jedoch nur „die Zusammenarbeit und Rechtshilfe zwischen staatlichen Behörden".[489] Gemäß Art. 12 Abs. 1 EU-US MLAT findet das MLAT-Abkommen für Straftaten Anwendung, die vor oder nach seinem Inkrafttreten begangen wurden. Die Europäische Union und die Vereinigten Staaten von Amerika stellen gem. Art. 3 S. 1 EU-US MLAT sicher, dass das MLAT-Abkommen in Bezug auf die bilateralen Verträge über Rechtshilfe Anwendung findet, die zum Zeitpunkt des Inkrafttretens des Abkommens zwischen die EU und den USA in Kraft sind.

Für die Verwendung von Informationen, die durch ein Ersuchen erlangt wurden, gibt es Grenzen.[490] Sie dürfen nicht für die folgenden Zwecke verwendet werden: 1. Politische Ermittlungen sowie Strafverfolgungen, 2. militärische Straftaten, die außerhalb des Militärdienstes nicht illegal sind und 3. jeglicher Ermittlungs- oder Strafverfolgungszweck, der nicht im Ersuchen enthalten ist.[491]

Nach Art. 3 Abs. 5 S. 2 Hs. 2 EU-US MLAT haben die MLAT-Bestimmungen nicht die Wirkung, anderes nationales Recht zu erweitern oder zu beschränken. In Einzelfällen kann der ersuchte Staat jedoch zusätzliche Bedingungen stellen und den ersuchenden Staat auffordern, Angaben über die Nutzung der Beweismittel sowie Informationen zu liefern.[492]

In Ermangelung eines bilateralen Rechtshilfeabkommens ist das Rechtshilfeabkommen zwischen der EU und den USA direkt auf alle Angelegenheiten im Zusammenhang mit der Rechtshilfe anwendbar.[493] Nach Art. 3 Abs. 5 S. 2 Hs. 1 EU-US MLAT begründen die MLAT-Bestimmungen keine Rechte für eine Privatperson, Beweise zu beschaffen, zu beseitigen, auszuschließen oder die Durchführung eines Ersuchens zu verhindern.

Staatsanwälte, die in einem anderen Land nach Informationen suchen, greifen auf das Rechtshilfeabkommen / MLAT zurück.[494] Es dient als eine Ergänzung bilateraler Rechtshilfe-abkommen zwischen den EU-Mitgliedstaaten und den USA,[495] die es Staatsanwälten ermöglicht, die Ermittlungsbehörden eines anderen Landes in Anspruch zu nehmen, um Beweise zur Verwendung in Strafverfahren zu sichern, indem sie um Rechtshilfe bitten.[496]

489 Europäisches Parlament, 4. Arbeitsdokument (A), 11.03.2019, S. 2 ff.
490 MLAT Subpoenas: What EU Service Providers Need to Know, abrufbar: https://revisionlegal.com/internet-law/privacy/mlat-subpoenas/, zuletzt abgerufen am 02.08.2023.
491 MLAT Subpoenas: What EU Service Providers Need to Know, abrufbar: https://revisionlegal.com/internet-law/privacy/mlat-subpoenas/, zuletzt abgerufen am 02.08.2023.
492 Europäisches Parlament, 4. Arbeitsdokument (A), 11.03.2019, S. 3.
493 Europäisches Parlament, 4. Arbeitsdokument (A), 11.03.2019, S. 2.
494 *Rush/Kephart*, LEGAL INSIGHT, 1, 1.
495 Europäisches Parlament, 4. Arbeitsdokument (A), 11.03.2019, S. 2.
496 *Rush/Kephart*, LEGAL INSIGHT, 1, 1.

MLAT erleichtert die grenzüberschreitende Zusammenarbeit bei der Strafverfolgung, verringert Konflikte, sorgt für einen kohärenten Überwachungsprozess, hilft dazu, dass geeignete rechtliche Kanäle für die Anforderung personenbezogener Daten genutzt werden, und reduziert das rechtliche Risiko für eine Organisation.[497] Die EU-Kommission hat dieses Abkommen als sehr nützlich und erfolgreich bewertet.[498] Die G20-Arbeitsgruppe zur Korruptionsbekämpfung hat anerkannt, dass die Rechtshilfe ein wesentliches Instrument im weltweiten Kampf gegen die grenzüberschreitende Kriminalität ist.[499]

Als **Nachteil** des MLAT-Verfahrens ist die lange Verfahrensdauer zu erwähnen.[500] Die für die Bearbeitung von MLAT-Anfragen zuständigen Stellen sind „häufig unterfinanziert und personell unterbesetzt".[501] Die EU-Kommission wies darauf hin, dass für Maßnahmen im Rahmen der gegenwärtigen justiziellen Zusammenarbeit bei der Rechtshilfe (auch mit den USA) im Durchschnitt zehn Monate benötigt und teilweise unverhältnismäßig viele Ressourcen aufgewendet würden.[502] Infolgedessen kommt es zu enormen Verzögerungen bei der Beantwortung der Anträge.[503]

Darüber hinaus ist es bei der Abfassung des Ersuchens klar anzugeben, auf welchen Vertrag, welches Übereinkommen oder welche andere Form der Zusammenarbeit sich das Ersuchen bezieht.[504] Andernfalls ist es nicht möglich, nachzuvollziehen, worauf die Anfrage beruht, was wiederum viel Zeit in Anspruch nimmt. Wenn das Ersuchen nicht die erforderlichen Informationen enthält, kann es nicht effizient oder überhaupt nicht ausgeführt werden.[505]

Gemäß Art. 14 EU-US MLAT ist das MLAT-Abkommen kein Hindernis für den Abschluss bilateraler Abkommen zwischen einem EU-Mitgliedstaat und den USA, die mit diesem Abkommen in Einklang stehen. So trat 2016 das Rahmenabkommen über den Datenschutz beim Informationsaustausch zwischen Polizei und Strafverfolgungsbehörden der EU und der USA (sog. „**Umbrella Agreement**") in Kraft.

---

497 IWGDPT, Arbeitspapier zu Standards für den Datenschutz und den Schutz der Privatsphäre bei grenzüberschreitenden Datenanforderungen zu Strafverfolgungszwecken, 63. Sitzung, 09 - 10.04.2018, S. 1.

498 Europäisches Parlament, 4. Arbeitsdokument (A), 11.03.2019, S. 4.

499 G2012 MEXIKO, REQUESTING MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS FROM G20 COUNTRIES, A STEP-BY-STEP-Guide, Foreword.

500 *Rush/Kephart*, LEGAL INSIGHT, 1, 8.

501 IWGDPT, Arbeitspapier zu Standards für den Datenschutz und den Schutz der Privatsphäre bei grenzüberschreitenden Datenanforderungen zu Strafverfolgungszwecken, 63. Sitzung, 09 - 10.04.2018, S. 1.

502 Europäisches Parlament, 4. Arbeitsdokument (A), 11.03.2019, S. 6.

503 IWGDPT, Arbeitspapier zu Standards für den Datenschutz und den Schutz der Privatsphäre bei grenzüberschreitenden Datenanforderungen zu Strafverfolgungszwecken, 63. Sitzung, 09 - 10.04.2018, S. 1.

504 G2012 MEXIKO, REQUESTING MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS FROM G20 COUNTRIES, A STEP-BY-STEP-Guide, S. 40.

505 G2012 MEXIKO, REQUESTING MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS FROM G20 COUNTRIES, A STEP-BY-STEP-Guide, Foreword.

Das Umbrella Agreement umfasst alle personenbezogenen Daten, die zwischen der EU und den USA zum Zwecke der Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten, einschließlich Terrorismus, ausgetauscht werden.[506] Das Ziel des Abkommens ist der Schutz personenbezogener Daten bei der Übermittlung durch Strafverfolgungsbehörden (Polizei und Strafjustiz).[507] Außerdem soll es die Zusammenarbeit der Strafverfolgungsbehörden zwischen der EU und den USA fördern.[508]

Das Abkommen stellt keine Rechtsgrundlage für die Übermittlung personenbezogener Daten zwischen der EU und den USA zum Zwecke der Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten, einschließlich Terrorismus, dar.[509] Es legt lediglich den rechtlichen Rahmen fest.

3.4.4.1.1 MLAT-Verfahren in der EU

Der Zugriff von US-Behörden auf die Daten, die in der EU gespeichert sind, wird durch das MLAT durchgesetzt, wobei die nationalen Behörden einzubeziehen sind. Eine **Ermächtigung** zu einer solchen Datenübermittlung ist in **Art. 48 DSGVO** enthalten. Handelt es sich beispielsweise um einen Cloud-Dienst (z. B. Microsoft Office 365), muss zwischen dem Kunden und dem Anbieter ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO geschlossen werden. Nach Art. 83 Abs. 5 lit. c) DSGVO würde diese Datenübermittlung ohne das MLAT-Verfahren einen Verstoß gegen Art. 48 DSGVO darstellen und sowohl für den Verantwortlichen, der die Verantwortung für das Fehlverhalten des Auftragsverarbeiters übernehmen muss, als auch für den Auftragsverarbeiter (in diesem Fall Microsoft) selbst eine Geldstrafe nach Art. 28 Abs. 10 DSGVO zur Folge haben.[510]

506 European Commission, Fact Sheet, Questions and Answers on the EU-US data protection "Umbrella agreement", S. 1.

507 *Christakis/Terpan*, IDPL, Vol. 11, Nr. 2, 2021, 81, 84; EU-US agreement on personal data protection, abrufbar: https://eur-lex.europa.eu/EN/legal-content/summary/eu-us-agreement-on-personal-data-protection.html, zuletzt abgerufen am 02.08.2023.

508 EU-US agreement on personal data protection, abrufbar: https://eur-lex.europa.eu/EN/legal-content/summary/eu-us-agreement-on-personal-data-protection.html, zuletzt abgerufen am 02.08.2023.

509 Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses, aburfbar: https://www.consilium.europa.eu/en/documents-publications/treaties-agreements/ratification/?id=2016043&partyid=UE&doclanguage=en, zuletzt abgerufen am 02.08.2023.

510 Die Erläuterung und Auslegung, die in diesem Abschnitt dargestellt wird, ist in dem folgenden Artikel zu finden. S.: Datenschutzkonformer Einsatz von Office 365 nach Cloud Act, abrufbar: https://www.dr-datenschutz.de/datenschutzkonformer-einsatz-von-office-365-nach-cloud-act/, zuletzt abgerufen am 03.08.2023.

Die zwischen den USA und der EU geschlossenen MLATs werden zwar unabhängig voneinander ausgehandelt,[511] haben aber im Allgemeinen einen ähnlichen Rahmen.[512] Daher ist jedes Land, das das Abkommen unterzeichnet hat, selbst für das MLAT-Verfahren verantwortlich. Beispielsweise ist in Deutschland dafür das **Bundesamt für Justiz** zuständig. Es ist u. a. für die Entscheidung über die Zulassung ein- sowie ausgehender strafrechtlicher Anträge um Vollstreckungshilfe, Auslieferung oder sonstige Rechtshilfe zuständig, soweit dies nicht den Ländern übertragen wurde.[513] Darüber hinaus beteiligt sich das Bundesamt für Justiz an der weltweiten Zusammenarbeit in einzelnen Strafrechtshilfe-Fällen, wenn diplomatische Instrumente oder Kanäle zu ausländischen Justizministerien offen sind.[514]

3.4.4.1.2 MLAT-Verfahren in den USA

Aus der Sicht des US-Rechts ist die **Ermächtigung** für ein Ersuchen um strafrechtliche Übergabe durch US-Ermittlungsbehörden der sog. „**Search Warrant**“, basierend auf dem SCA (18 U.S.C. § 2703) sowie dem ECPA (18 U.S.C. § 2510 ff.).[515] Um Informationen zu erhalten, die sich im Besitz von Einrichtungen befinden, die unter § 2703 SCA fallen, müssen die Strafverfolgungsbehörden einen Durchsuchungsbefehl, einen Gerichtsbeschluss oder eine Vorladung einholen.[516]

MLATs werden in den Vereinigten Staaten von einer zentralen Behörde, dem Amt für internationale Angelegenheiten / „Office of International Affairs“ (OIA) des US-Justizministeriums / „Department of Justice“ (DoJ), verwaltet.[517] Das OIA koordiniert das MLAT-Verfahren und bearbeitet alle ein- und ausgehenden Ersuche, die im Rahmen von MLATs gestellt werden.[518]

511 Sie werden also mit jedem einzelnen EU-Mitgliedstaat abgeschlossen.
512 LIFTING THE VEIL ON THE MLAT PROCESS: A GUIDE TO UNDERSTANDING AND RESPONDING TO MLA REQUESTS, abrufbar: https://www.klgates.com/Lifting-the-Veil-on-the-MLAT-Process-A-Guide-to-Understanding-and-Responding-to-MLA-Requests-01-20-2017, zuletzt abgerufen am 03.08.2023.
513 Internationale Rechtshilfe in Strafsachen, abrufbar: https://www.bundesjustizamt.de/DE/Themen/InternationaleZusammenarbeit/Strafsachen/Rechtshilfe/Rechtshilfe_node.html, zuletzt abgerufen am 02.08.2023.
514 Internationale Rechtshilfe in Strafsachen, abrufbar: https://www.bundesjustizamt.de/DE/Themen/InternationaleZusammenarbeit/Strafsachen/Rechtshilfe/Rechtshilfe_node.html, zuletzt abgerufen am 02.08.2023.
515 Datenschutzkonformer Einsatz von Office 365 nach Cloud Act, abrufbar: https://www.dr-datenschutz.de/datenschutzkonformer-einsatz-von-office-365-nach-cloud-act/, zuletzt abgerufen am 03.08.2023.
516 *Balser*, Overview of Governmental Action Under the Stored Communications Act (SCA), S. 2.
517 LIFTING THE VEIL ON THE MLAT PROCESS: A GUIDE TO UNDERSTANDING AND RESPONDING TO MLA REQUESTS, abrufbar: https://www.klgates.com/Lifting-the-Veil-on-the-MLAT-Process-A-Guide-to-Understanding-and-Responding-to-MLA-Requests-01-20-2017, zuletzt abgerufen am 03.08.2023.
518 LIFTING THE VEIL ON THE MLAT PROCESS: A GUIDE TO UNDERSTANDING AND RESPONDING TO MLA REQUESTS, abrufbar: https://www.klgates.com/Lifting-the-Veil-on-the-MLAT-Process-A-Guide-to-Understanding-and-Responding-to-MLA-Requests-01-20-2017, zuletzt abgerufen am 03.08.2023.

3.4.4.1.3 Abgrenzung zwischen MLAT-Abkommen und CLOUD Act

Der CLOUD Act bzw. die CLOUD Act Vereinbarungen können theoretisch den internationalen Datentransfer für Strafverfahren regeln. Da es aber keine Rechtshilfeabkommen zwischen der EU mit den USA unter dem CLOUD Act gibt, wird durch das MLAT die Datenoffenlegung in Strafverfahren durchgeführt.[519]

Das MLAT ist wesentlich vom CLOUD Act dadurch abzugrenzen, dass die US-Regierung im Rahmen des MLAT-Verfahrens eher als Vermittler auftritt und die Rechtshilfeersuchen ausländischer Regierungen überprüft, bevor sie an ein US-Gericht weitergeleitet werden.[520] Damit kann die US-Behörde die personenbezogene Daten nicht direkt bei dem US-Anbieter stellen.[521] Der CLOUD Act hat diesen Weg verkürzt.[522] Die US-Behörden können sich nun direkt an den betreffenden US-Anbieter wenden.[523] Hierfür sind nur Gerichtsbeschlüsse oder Haftbefehle ausreichend.[524]

3.4.4.2 Die neue EU-US Data Privacy Framework

Es wurde bereits erwähnt, dass Angemessenheitsbeschlüsse die Übermittlung personenbezogener Daten aus der EU in ein Drittland ohne weitere Schutzmaßnahmen ermöglichen (s. → S. 50-51).[525] Nachdem der EuGH den vorhergehenden Angemessenheitsbeschluss zum EU-US-Datenschutzschild / „EU-US Privacy Shield“ für ungültig erklärt hatte, begannen die EU-Kommission und die US-Regierung mit Gesprächen über einen neuen Rahmen, um die vom EuGH geäußerten Bedenken auszuräumen.[526]

Im März 2022 gaben die Präsidentin der EU-Kommission Ursula von der Leyen und der Präsident der USA Joe Biden „eine grundsätzliche Einigung über einen neuen transatlantischen Rahmen für Datenübermittlungen“ bekannt.[527]

519 IONOS, Aktuelle Rechtslage zum US-Datentransfer unter besonderer Berücksichtigung des US CLOUD Act, 2, 6.
520 IONOS, Aktuelle Rechtslage zum US-Datentransfer unter besonderer Berücksichtigung des US CLOUD Act, 2, 6.
521 IONOS, Aktuelle Rechtslage zum US-Datentransfer unter besonderer Berücksichtigung des US CLOUD Act, 2, 6.
522 IONOS, Aktuelle Rechtslage zum US-Datentransfer unter besonderer Berücksichtigung des US CLOUD Act, 2, 6.
523 IONOS, Aktuelle Rechtslage zum US-Datentransfer unter besonderer Berücksichtigung des US CLOUD Act, 2, 6.
524 U.S. CLOUD Act vs. GDPR, abrufbar: https://www.activemind.legal/guides/us-cloud-act/, zuletzt abgerufen am 03.08.2023.
525 Europäische Kommission, Pressemitteilung: Datenschutz: Kommission leitet Verfahren zur Annahme eines Angemessenheitsbeschlusses für einen sicheren Datenverkehr mit den USA ein.
526 Europäische Kommission, Pressemitteilung: Datenschutz: Kommission leitet Verfahren zur Annahme eines Angemessenheitsbeschlusses für einen sicheren Datenverkehr mit den USA ein.
527 Europäische Kommission, Pressemitteilung: Datenschutz: Kommission leitet Verfahren zur Annahme eines Angemessenheitsbeschlusses für einen sicheren Datenverkehr mit den USA ein.

Am 07.10.2022 wurde eine Anordnung über die Verbesserung der Schutzmaßnahmen für die Aktivitäten der US-Signaldienste (Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities; E. O. 14086) erlassen, in der die Schritte festgelegt sind, die die Vereinigten Staaten unternehmen werden, um die im März 2022 angekündigten Verpflichtungen im Rahmen des Datenschutzes zwischen der EU und den USA (**EU-US Datenschutzrahmen** / „EU-US Data Privacy Framework"; EU-US DPF) umzusetzen.[528] Die E. O. 14086 wurde durch eine Verordnung des US Attorney General ergänzt.[529]

Im Dezember 2022 stellte die **EU-Kommission** in der Pressemitteilung fest, dass die beiden Dokumente die von den USA eingegangenen Verpflichtungen in amerikanisches Recht umsetzen und die entsprechenden Verpflichtungen der US-Unternehmen ergänzen.[530] Auf dieser Grundlage legte die EU-Kommission den Entwurf eines Angemessenheitsbeschlusses über den EU-US-Datenschutzrahmen vor.[531]

Die EU-Kommission stellte in der Pressemitteilung von 13.12.2022 fest, dass die E. O. 14086 die Möglichkeit schafft, die beiden vom EuGH im „Schrems II"-Urteil geäußerten Kritikpunkte aufzugreifen und den Datenverkehr zwischen der EU und den USA wiederherzustellen.[532] Die Schrems II-Entscheidung skizzierte zwei notwendige Maßstäbe dafür, dass die transatlantischen Datenströme im Einklang mit EU-Recht stehen: 1. US-Überwachungsaktivitäten sollten auf das Notwendige und Verhältnismäßige beschränkt werden und 2. gerichtlichen Rechtsbehelfen unterliegen.[533] Der Beschlussentwurf kam zu dem Schluss, dass die USA ein angemessenes Schutzniveau für die aus der EU an US-Unternehmen zu transferierenden personenbezogene Daten garantieren.[534] Dabei wurden insbesondere die folgenden Punkte hervorgehoben:

528 FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework, abrufbar: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/, zuletzt abgerufen am 02.08.2023.

529 Europäische Kommission, Pressemitteilung: Datenschutz: Kommission leitet Verfahren zur Annahme eines Angemessenheitsbeschlusses für einen sicheren Datenverkehr mit den USA ein.

530 Siehe dazu: Pressemitteilung der Europäischen Kommission v. 13.12.2022, Datenschutz: Kommission leitet Verfahren zur Annahme eines Angemessenheitsbeschlusses für einen sicheren Datenverkehr mit den USA ein.

531 Europäische Kommission, Pressemitteilung: Datenschutz: Kommission leitet Verfahren zur Annahme eines Angemessenheitsbeschlusses für einen sicheren Datenverkehr mit den USA ein.

532 Europäische Kommission, Pressemitteilung: Datenschutz: Kommission leitet Verfahren zur Annahme eines Angemessenheitsbeschlusses für einen sicheren Datenverkehr mit den USA ein; vgl.: Transatlantische Datentransfers: aktueller Stand zwischen EU und USA, abrufbar: https://www.dataguard.de/blog/update-transatlantische-datentransfer-bedeutung-fuer-eu-unternehmen, zuletzt abgerufen am 03.08.2023.

533 *Wood/Lewis*, CSIS, 03.2023, 1, 4.

534 Europäischen Kommission, Pressemitteilung: Datenschutz: Kommission leitet Verfahren zur Annahme eines Angemessenheitsbeschlusses für einen sicheren Datenverkehr mit den USA ein.

1. Die Beschränkung des Zugangs der US-Geheimdienste zu EU-Daten auf das absolut Notwendige:[535] Laut White Haus fügt die E. O. 14086 weitere Schutzmaßnahmen für US-Signalaufklärungstätigkeiten / „Signal Intelligence Activities“ hinzu, einschließlich der Anforderung, dass solche Tätigkeiten nur im Rahmen definierter nationaler Sicherheitsziele durchzuführen sowie die Privatsphäre und die bürgerlichen Freiheiten aller Personen unabhängig von ihrer Staatsangehörigkeit oder ihrem Wohnsitzland zu berücksichtigen sind. Sie werden nur dann durchgeführt, wenn diese notwendig sind, um eine bestätigte Aufklärungspriorität voranzubringen, und nur in dem Umfang und auf eine Weise, die dieser Priorität angemessen sind.[536]

2. Ein unabhängiger und unparteiischer Rechtsbehelf für EU-Bürger:[537] Laut White House Schafft die E. O. 14086 einen mehrstufigen Mechanismus für Einzelpersonen aus qualifizierten Staaten und Organisationen der regionalen Wirtschaftsintegration. Betroffene können eine Beschwerde 1. bei der betreffenden zertifizierten Organisation, 2. bei einer von dieser Organisation benannten unabhängigen Beschwerdestelle, 3. bei den Datenschutzaufsichtsbehörden in der EU, 4. beim DOC oder 5. bei der FTC einreichen.[538] Konnte der Beschwerde nicht durch einen dieser Rechtsbehelfe abgeholfen werden, können die Betroffenen ein verbindliches Schiedsverfahren einleiten.[539] Die Betroffenen können einen oder alle der vorgenannten Rechtsbehelfe in Anspruch nehmen; es besteht kein Alternativverhältnis zwischen den Rechtsbehelfen, und es muss keine Reihenfolge eingehalten werden.[540] Lediglich das Schlichtungsverfahren erfordert, dass gewisse Rechtsbehelfe vor der Durchführung ausgeschöpft werden müssen.[541]

Der Rechtsbehelf für den Zugriff auf personenbezogene Daten und deren Verwendung zu Strafverfolgungszwecken ist Aufgabe eines unabhängigen und unparteiischen Gerichts.[542] Unter anderem bietet ECPA betroffenen Personen Rechtsmittel gegen eine Behörde oder einen Beamten, wenn diese personenbezogene Daten verarbeiten.[543]

535 EuGH, Urt. v. 16.07.2020 – C-311/18, NJW 2020, 2613 Rn. 176 – Schrems II.

536 Dieser Schritt wird auf der Website des Weißen Hauses in dem folgenden Merkblatt beschrieben. S.: FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework, abrufbar: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/, zuletzt abgerufen am 02.08.2023.

537 EuGH, Urt. v. 16.07.2020 – C-311/18, NJW 2020, 2613 Rn. 91 – Schrems II.

538 DSK, Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023, 04.09.2023, S. 22.

539 DSK, Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023, 04.09.2023, S. 22.

540 DSK, Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023, 04.09.2023, S. 22.

541 DSK, Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023, 04.09.2023, S. 22.

542 DSK, Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023, 04.09.2023, S. 25 ff.

543 DSK, Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023, 04.09.2023, S. 26.

Der neue Rechtsbehelf im Zusammenhang mit dem Zugang zu und der Verwendung von personenbezogenen Daten für Zwecke der nationalen Sicherheit ersetzt das bisherige Ombudsmannsystem durch ein zweistufiges Verfahren.[544] Als **erster Schritt** führt der Beauftragte für den Schutz der bürgerlichen Freiheiten / „Civil Liberties Protection Officer" (CLPO) die erste Untersuchung der eingegangenen Beschwerden durch, um festzustellen, ob gegen die E. O. 14086 oder andere geltende US-Gesetze verstoßen wurde. Falls dies der Fall ist, bestimmt sie die entsprechenden Abhilfemaßnahmen.[545]

Als **zweiter Schritt** ermächtigt die E. O. 14086 den Beschwerdeführer oder die entsprechende US-Behörde binnen 60 Tagen nach Erhalt der CLPO-Entscheidung, vor dem Datenschutz-Überprüfungsgericht / „Data Protection Review Court" (DPRC) diese Entscheidung anzufechten.[546] Die Richter des DPRC werden von außerhalb der US-Regierung ernannt, verfügen über einschlägige Erfahrungen auf dem Gebiet des Datenschutzes und der nationalen Sicherheit, überprüfen die Fälle unabhängig und sind vor Abberufung geschützt. Die Entscheidungen des DPRC darüber, ob ein Verstoß gegen geltendes US-Recht vorliegt und welche Abhilfemaßnahmen ggf. zu ergreifen sind, sind verbindlich.[547]

Der **Europäische Datenschutzausschuss** (EDSA) / „The European Data Protection Board" (EDPB) hat die Verbesserungen im Zusammenhang mit dem EU-US DPF begrüßt. Der EDSA hat zum Ausdruck gebracht, dass die Beschränkung der Datenverarbeitung durch die US- Nachrichtendienste auf ein notwendiges und verhältnismäßiges Maß sowie der neue Rechtsbehelfmechanismus als positiv angesehen werden.[548]

544 DSK, Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023, 04.09.2023, S. 26.

545 Dieser Schritt wird auf der Website des Weißen Hauses in dem folgenden Merkblatt beschrieben. S.: FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework, abrufbar: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/, zuletzt abgerufen am 02.08.2023.

546 DSK, Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023, 04.09.2023, S. 27.

547 Dieser Schritt wird auf der Website des Weißen Hauses in dem folgenden Merkblatt beschrieben. S.: FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework, abrufbar: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/, zuletzt abgerufen am 02.08.2023.

548 Der EDSA begrüßt Verbesserungen durch EU-US-Datenschutzrahmen, auch wenn nicht alle Bedenken ausgeräumt wurden, abrufbar: https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_de, zuletzt abgerufen am 03.08.2023.

Gleichzeitig äußerte er jedoch Bedenken hinsichtlich bestimmter Betroffenenrechte, der Weiterübermittlung, des Umfangs der Ausnahmen, der vorübergehenden Sammelerhebung von Daten sowie der praktischen Funktionsweise des Rechtsbehelfsverfahrens. Dementsprechend hat er ausgeführt, dass der Angemessenheitsbeschluss sowohl von der Annahme als auch von der praktischen Umsetzung von E. O. 14086 abhängig gemacht werden sollte. Die EDSA empfahl der EU-Kommission, diese aktualisierten Strategien sowie Verfahren zu bewerten und ihr die Bewertung mitzuteilen.[549] Damit stand die EDSA dieser Entscheidung weniger kritisch gegenüber als das EU-Parlament.

Das **Europäische Parlament** erinnerte sich daran, dass es noch in seiner Entschließung vom 20.05.2021 die europäische Kommission aufforderte, keinen neuen Angemessenheitsbeschluss anzunehmen, wenn die USA nicht sinnvolle Reformen einführen, insbesondere für die nationale Sicherheit und nachrichtendienstliche Zwecke.[550]

Das EU-Parlament brachte zum Ausdruck, dass der neue Angemessenheitsbeschluss nicht aussagekräftig genug ist.[551] Es kam zu dem Schluss, dass das EU-US DPF keine wesentliche Gleichwertigkeit herstellt, und forderte die EU-Kommission auf, die Verhandlungen mit den USA über das Rahmenwerk fortzusetzen und erst dann eine Entscheidung zu treffen, wenn alle in der Entschließung und der EDSA-Stellungnahme enthaltenen Empfehlungen vollständig umgesetzt sind.[552]

Das EU-Parlament forderte die EU-Kommission ferner auf, im Interesse der EU-Unternehmen und -Bürger zu handeln, indem sie sicherstellt, dass das EU-US DPF eine solide, ausreichende und zukunftsorientierte Rechtsgrundlage für Datenübermittlungen zwischen der EU und den USA bietet.[553] Es betonte, dass die EU-Kommission dafür verantwortlich wäre, wenn ein Angemessenheitsbeschluss angenommen und vom EuGH wieder für ungültig erklärt würde, da dies ein Versagen beim Schutz der Rechte der EU-Bürger wäre.[554]

549 Der EDSA begrüßt Verbesserungen durch EU-US-Datenschutzrahmen, auch wenn nicht alle Bedenken ausgeräumt wurden, abrufbar: https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_de, zuletzt abgerufen am 03.08.2023.

550 Resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework, 2023/2501(RSP) – 11.05.2023.

551 Resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework, 2023/2501(RSP) – 11.05.2023.

552 Resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework, 2023/2501(RSP) – 11.05.2023.

553 Resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework, 2023/2501(RSP) – 11.05.2023.

554 Resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework, 2023/2501(RSP) – 11.05.2023.

Am 03.07.2023 gab das US-Handelsministerium bekannt, dass die US-Handelsministerin Gina Raimondo die Erklärung zum EU-US Datenschutzrahmen abgegeben hat, d. h. dass die Vereinigten Staaten ihre Verpflichtungen zur Umsetzung des EU-US DPF, die im März 2022 von Präsident Biden und der Präsidentin von der Leyen angekündigt wurde, erfüllt haben.[555] Einige Tagen später stimmten 24 EU-Mitgliedstaaten für das EU-US DPF und gaben damit zu verstehen, dass sie der Meinung sind, dass dieser ein angemessenes Schutzniveau für personenbezogene Daten bietet.[556]

Am 10.07.2023 hat die EU-Kommission den Angemessenheitsbeschluss für den EU-US DPF verabschiedet. Diese kommt zu dem Schluss, dass die USA im Vergleich zu der EU ein angemessenes Schutzniveau für personenbezogene Daten garantieren. Im Art. 1 EU-US DPF wurde spezifiziert, dass die Vereinigten Staaten ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die von der Union an Organisationen in den Vereinigten Staaten übermittelt werden, die in der vom US-Handelsministerium geführten und öffentlich zugänglichen „Data Privacy Framework List" gem. Anhang I Abschn. I.3 aufgeführt sind. Daher dürfen personenbezogene Daten aus der EU an US-Unternehmen übermittelt werden, wenn diese an der EU-US DPF teilnehmen[557] bzw. sich zertifizieren lassen.

Alle von der US-Regierung eingeführten nationalen Sicherheitsvorkehrungen, einschließlich des Rechtsbehelfsverfahrens, gelten für alle Datenübermittlungen im Sinne der DSGVO an US-Unternehmen, unabhängig von den verwendeten Übertragungsmechanismen. Sie erleichtern die Verwendung anderer Instrumente wie Standardvertragsklauseln sowie verbindlicher unternehmensinterner Vorschriften.[558]

555 Statement from U.S. Secretary of Commerce Gina Raimondo on the European Union-U.S. Data Privacy Framework, abrufbar: https://www.commerce.gov/news/press-releases/2023/07/statement-us-secretary-commerce-gina-raimondo-european-union-us-data, zuletzt abgerufen am 03.08.2023.

556 The latest on the EU-US Data Privacy Framework, abrufbar: https://iapp.org/news/a/the-latest-on-the-eu-us-data-privacy-framework/, zuletzt abgerufen am 03.08.2023.

557 Diese Erklärung der EU-Kommission wird in dem folgenden Artikel beschrieben. S.: Fragen und Antworten: Datenschutzrahmen EU-USA, abrufbar: https://ec.europa.eu/commission/presscorner/detail/de/qanda_23_3752, zuletzt abgerufen am 03.08.2023.

558 Diese Erklärung der EU-Kommission wird in dem folgenden Artikel beschrieben. S.: Fragen und Antworten: Datenschutzrahmen EU-USA, abrufbar: https://ec.europa.eu/commission/presscorner/detail/de/qanda_23_3752, zuletzt abgerufen am 03.08.2023.

Damit eine US-amerikanische Organisation unter die EU-US DPF fällt, muss sie durch ein Selbstzertifizierungsverfahren des US-Handelsministeriums / „Department of Commerce“ zertifiziert werden. Diese Zertifizierung muss jedes Jahr erneuert werden. Das US-Handelsministerium erklärte, dass der Prozess der Selbstzertifizierung und der jährlichen Neuzertifizierung grundsätzlich derselbe bleibt.[559] Das Ministerium wird gem. Anhang I (III) (6) (a) EU-US DPF eine Organisation auf die Datenschutz-Rahmenliste setzen, wenn es festgestellt hat, dass die erste Selbstzertifizierung der Organisation vollständig ist. Sie wird die Organisation in folgenden Fällen von dieser Liste streichen: 1. Wenn sie sich freiwillig zurückzieht; 2. wenn sie die jährliche Neuzertifizierung nicht abschließt; oder 3. wenn sie die Grundsätze der EU-US DPF dauerhaft nicht einhält.

Bei der Betrachtung und Bewertung der EU-US DPF muss Folgendes berücksichtigt werden: Eine E. O. ist viel einfacher umzusetzen und zu revidieren, da sie ausschließlich auf einer Entscheidung des amtierenden US-Präsidenten beruht. Sie kann nicht durch den US-Kongress außer Kraft gesetzt werden. Sollte Präsident Biden die nächsten Präsidentschaftswahlen verlieren, kann sein Nachfolger die E. O. aufheben oder ändern. Dies könnte sich auf die Vereinbarungen zwischen der EU und den USA über den internationalen Datenverkehr auswirken.[560] Der Regierungswechsel kann zu weiteren Verzögerungen sowie Unsicherheiten in der internationalen Datenübertragung führen und entsprechende Risiken aufgrund fehlender Rechtssicherheit mit sich bringen.[561]

Eine massenhafte Datenerhebung („Bulk Collection“) ist nach der EU-US DPF in der Regel nur dann zulässig, wenn der beabsichtigte Zweck im Einzelfall nicht durch eine gezielte Erhebung erreicht werden kann.[562] Bezüglich der vorherigen unabhängigen Genehmigung von Überwachungsmaßnahmen gem. Abschn. 702 FISA zur gerichtlichen Aufsicht über Nachrichtendienste bedauerte der EDSA, dass die Einhaltung von E. O. 14086 bei der Zertifizierung ausländischer Überwachungsprogramme nicht prüfen wird, obwohl die Geheimdienste, die das Programm durchführen, daran gebunden sind.[563]

559 Die in diesem Abschnitt dargestellte Auffassung wird in dem folgenden Artikel beschrieben. S.: Privacy Shield 2.0: Datentransfer in die USA, abrufbar: https://www.e-recht24.de/datenschutz/13085-eu-us-data-privacy-framework.html, zuletzt abgerufen am 03.08.2023.

560 Die Beschreibung einer E. O. ist in dem folgenden Artikel zu finden. S.: Transatlantische Datentransfers: aktueller Stand zwischen EU und USA, abrufbar: https://www.dataguard.de/blog/update-transatlantische-datentransfer-bedeutung-fuer-eu-unternehmen, zuletzt abgerufen am 03.08.2023.

561 Interview mit Cornelia Sasse, im im elektronischen Zusatzmaterial, Anlage 1, S. 2.

562 DSK, Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023, 04.09.2023, S. 18.

563 Die in diesem Abschnitt dargestellte Auffassung ist in dem folgenden Artikel zu finden. S.: Der EDSA begrüßt Verbesserungen durch EU-US-Datenschutzrahmen, auch wenn nicht alle Bedenken ausgeräumt wurden, abrufbar: https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_de, zuletzt abgerufen am 03.08.2023.

Gegen Entscheidungen des Gerichts (DPRC) kann kein Rechtsmittel eingelegt werden. Dem Beschwerdeführer wird entweder mitgeteilt, dass keine erfassten Verstöße festgestellt wurden, oder dass eine angemessene Abhilfe angeordnet wurde.[564] Dieses neu etablierte Gericht ist keine echte Judikative, und es bleibt abzuwarten, ob der EuGH dieses Gremium akzeptieren wird.[565]

Die Tatsache, dass innerhalb weniger Tage bereits Tausende von Organisationen im Rahmen der EU-US DPF zertifiziert wurden, wirft die Frage auf, ob sie ausreichend auf Datenschutzkonformität geprüft wurden.

Außerdem, wie der EDSA feststellte, bleiben einige der Grundsätze gegenüber dem Privacy Shield im Wesentlichen unverändert. Daher bleiben Bedenken bestehen, *wie „in Bezug auf Ausnahmen vom Zugangsrecht, das Fehlen von wichtigen Begriffsdefinitionen, die mangelnde Klarheit über die Anwendung der Grundsätze des Datenschutzrahmens auf Auftragsverarbeiter, die breite Ausnahme vom Recht auf Zugang zu öffentlich zugänglichen Informationen und das Fehlen spezifischer Vorschriften für automatisierte Entscheidungsfindung und Profilerstellung“*.[566]

Abschließend sollte klargestellt werden, dass dieser neue Mechanismus grundsätzlich als positiv zu bewerten ist, da er eindeutig signalisiert, dass die USA die Verbesserung des Datenschutzes und die Vereinfachung des internationalen Datentransfers anstreben. Allerdings enthalten diese bereits einige Schwachstellen, die nicht zu übersehen sind. Es bleibt abzuwarten, wie der EUGH darauf reagieren wird und welche Auswirkungen dies letztlich für die Betroffenen haben wird.

3.4.4.3 Weitere internationale Bemühungen

Im September 2019 kündigten die EU und die USA in einer gemeinsamen Erklärung den Beginn formeller Verhandlungen über ein Abkommen zur Erleichterung des Zugangs zu elektronischen Beweismitteln bei strafrechtlichen Ermittlungen an.[567] Diese Verhandlungen sollten parallel zum EU-Framework der E-Beweis-Verordnung, stattfinden.[568] Interne Unstimmigkeiten in der EU verhinderten jedoch die Verabschiedung der Verordnung und die Fortsetzung der Verhandlungen mit den USA.[569]

564 Die in diesem Abschnitt dargestellte Auffassung ist in dem folgenden Artikel zu finden. S.: Der EDSA begrüßt Verbesserungen durch EU-US-Datenschutzrahmen, auch wenn nicht alle Bedenken ausgeräumt wurden, abrufbar: https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_de, zuletzt abgerufen am 03.08.2023.

565 Interview mit Cornelia Sasse, im elektronischen Zusatzmaterial, Anlage 1, S. 1.

566 Der EDSA begrüßt Verbesserungen durch EU-US-Datenschutzrahmen, auch wenn nicht alle Bedenken ausgeräumt wurden, abrufbar: https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_de, zuletzt abgerufen am 03.08.2023.

567 *Wood/Lewis*, CSIS, 03.2023, 1, 3.

568 *Wood/Lewis*, CSIS, 03.2023, 1, 3.

569 *Wood/Lewis*, CSIS, 03.2023, 1, 3.

Im Januar 2023 einigten sich der EU-Rat und das EU-Parlament mit ähnlichen Behörden wie dem CLOUD Act auf den **Verordnungsentwurf** und den **Richtlinienentwurf** zum grenzüberschreitenden Zugang zu elektronischen Beweismitteln.[570] Die vorgeschlagenen Vorschriften ergeben sich aus zwei Legislativvorschläge: 1. Der Verordnung über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen und 2. der Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren.[571] Der Rat bestätigte am 25.01.2023 die Einigung mit dem EU-Parlament über die beiden Gesetzgebungsvorschläge.[572] Dies signalisiert die Fortschritte bei der Erzielung eines Abkommens über elektronische Beweismittel zwischen der EU und den USA.[573]

Die vereinbarten Texte ermöglichen es den zuständigen Behörden, gerichtliche Anordnungen für elektronische Beweismittel direkt an Dienstleister in einem anderen Mitgliedsstaat zu richten. Damit soll ein alternativer Mechanismus zu den bestehenden Instrumenten der internationalen Zusammenarbeit und der Rechtshilfe eingeführt werden. Sie befassen sich insbesondere mit den Problemen, die sich aus dem flüchtigen Charakter elektronischer Beweismittel und dem Aspekt des „Verlusts des Standorts“ ergeben, indem sie neue Verfahren für einen schnellen, effizienten und wirksamen grenzüberschreitenden Zugang einführt.[574]

Am 12.07.2023 trat die Verordnung 2023/1543 des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren in Kraft und gilt ab 18.08.2026.

Der Rat hat am 14.02.2023 einen Beschluss angenommen, mit dem die Mitgliedstaaten ermächtigt werden, das **zweite Zusatzprotokoll zum Übereinkommen über Computerkriminalität** (Budapester Konvention) im Interesse der EU zu ratifizieren. Es zielt darauf ab, den internationalen Zugang zu elektronischen Beweismitteln zur Verwendung in Strafverfahren zu verbessern und zu vereinfachen. Es wird dazu beitragen, Computerkriminalität sowie andere Formen der Kriminalität weltweit wirksamer zu bekämpfen, ein hohes Schutzniveau für jedes Einzelnen zu garantieren und sicherzustellen, dass den EU-Datenschutzstandards eingehalten wird.

570 *Wood/Lewis*, CSIS, 03.2023, 1, 3.

571 Besserer Zugang zu elektronischen Beweismitteln für die Bekämpfung der Kriminalität, abrufbar: https://www.consilium.europa.eu/de/policies/e-evidence/, zuletzt abgerufen am 03.08.2023.

572 Besserer Zugang zu elektronischen Beweismitteln für die Bekämpfung der Kriminalität, abrufbar: https://www.consilium.europa.eu/de/policies/e-evidence/, zuletzt abgerufen am 03.08.2023.

573 *Wood/Lewis*, CSIS, 03.2023, 1, 3.

574 Die in diesem Abschnitt dargestellte Auffassung wird in dem folgenden Artikel ausführlich beschrieben. S.: Electronic evidence: Council confirms agreement with the European Parliament on new rules to improve cross-border access to e-evidence, abrufbar: https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/, zuletzt abgerufen am 03.08.2023.

34 Länder (darunter 18 EU-Mitgliedstaaten) haben das Protokoll bereits unterzeichnet. Das Protokoll ergänzt den internen EU-Rahmen für den Zugang zu elektronischen Beweismitteln, der kürzlich vom EU-Rat und dem EU-Parlament vereinbart wurde.[575]

3.4.5 Digitaler Datentransfer bei gleichzeitigem Zusammenspiel von EU- und US-Vorschriften

Mechanismen, die den transatlantischen Zugriff auf Daten erleichtern, sollen den Datenschutz und die Sicherung der Privatsphäre des Einzelnen gewährleisten und eine rasche bzw. adäquate Bearbeitung rechtmäßiger grenzüberschreitender Datenanfragen fördern.[576] Sie verdienen besondere Aufmerksamkeit, weil sie tiefgreifende Konsequenzen für die Grundrechte und -freiheiten wie die Persönlichkeitsrechte haben und einen reibungslosen Geschäftsbetrieb jeder Organisation ermöglichen.

Die EU und die USA befinden sich in einer Übergangsphase ihrer transatlantischen digitalen Beziehungen.[577] Wird sowohl der europäische als auch der amerikanische Raum betrachtet, so wird deutlich, dass in dieser Hinsicht bereits viel getan wurde. Zu nennen sind u. a. DSGVO, CLOUD Act, MLAT-Abkommen, zahlreiche Arbeitspapiere und andere Rechtsdokumente. Es wird viel über dieses Thema geschrieben, aber auch viel darüber gesprochen und diskutiert. Ist man im Bereich Datenschutz und / oder Informationssicherheit beruflich tätig, sieht man deutlich, dass Unternehmen, Behörden, Rechtsanwälte, Gesetzgeber oder andere Personen sowie Institutionen sich bemühen, zur Verbesserung der rechtlichen und technischen Lage für den internationalen Datentransfer etwas beizutragen.

Außerdem sind zahlreiche Handlungsempfehlungen, Projekten, Schulungen oder Konferenzen noch ein Beweis dafür, dass die EU und die USA nach den bestmöglichen Lösungen suchen. In der EU ist es spürbar, dass dort sehr viel Wert auf die Aufrechterhaltung und Verbesserung des Datenschutzniveaus gelegt wird. Diskutiert man mit den US-amerikanischen Fachleuten, merkt man sofort, dass dort intensiv darauf geachtet wird, ein einheitliches Datenschutzniveau zu erreichen und weiterzuentwickeln. Ein Beispiel dafür ist die Global GRC, Data Privacy & Cyber Security ConfEx am 31.05.2023 in NY / USA, auf der die Schwachstellen des US-amerikanischen Datenschutzsystems deutlich angesprochen und Abhilfemöglichkeiten angeboten wurden.

---

575 Die in diesem Abschnitt dargestellte Auffassung wird in dem folgenden Artikel ausführlich beschrieben. S.: Zugang zu elektronischen Beweismitteln: Rat ermächtigt Mitgliedstaaten, internationales Übereinkommen zu ratifizieren, abrufbar: https://www.consilium.europa.eu/de/press/press-releases/2023/02/14/access-to-e-evidence-council-authorises-member-states-to-ratify-international-agreement/, zuletzt abgerufen am 03.08.2023.

576 IWGDPT, Arbeitspapier zu Standards für den Datenschutz und den Schutz der Privatsphäre bei grenzüberschreitenden Datenanforderungen zu Strafverfolgungszwecken, 63. Sitzung, 09 - 10.04.2018, S. 5.

577 *Wood/Lewis*, CSIS, 03.2023, 1, 1.

Die Amerikaner, die die Gesetze schreiben, und auch die, die diese umsetzen, verstehen die Notwendigkeit und den Bedarf des rechtlich sauber geregelten internationalen Datenschutzes und versuchen, diese im Datenschutz-Alltag umsetzen. Europa bemüht sich ebenfalls, mit den USA so zusammenzuarbeiten, dass die Persönlichkeitsrechte geschützt werden und die Wirtschaft sowie die nationale und internationale Sicherheit nicht vernachlässigt werden. Das ist aber der schwierigste Teil und gelingt derzeit nicht immer perfekt. Hierbei ist zu erwähnen, dass es noch keine einheitlichen sowie praxisorientierten Wege gibt. Wie bereits beschrieben wurde, ergeben sich dementsprechend Lücken oder gegensätzliche Herausforderungen, die nur schwer, wenn überhaupt, zu regeln sind. Die daraus resultierenden Folgen sind nicht zu unterschätzen.

Dabei darf nicht vergessen werden, dass die EU und die USA füreinander die wichtigsten Handelspartner sind[578] und dass globale Unternehmen ein starkes wirtschaftliches Interesse am Datenaustausch zwischen der EU und den USA haben.[579] Durch die transatlantischen Beziehungen und die Datenübertragungsbeziehung entsteht eine Wirtschaftsbeziehung im Wert von 7,1 Billionen US-Dollar, sodass dies kein geringes Problem darstellt.[580] Alle Seiten wollen Lösungen finden, die den digitalen Handel weiterhin ermöglichen und den für die Strafverfolgung im digitalen Zeitalter notwendigen Beweisprozess vereinfachen.[581]

Im Folgenden werden einige Vorschläge als Lösungen dargelegt, die in den verschiedenen Dimensionen zu analysieren sind. Der Grund dafür liegt in der Natur der Sache: Wenn das Thema „transatlantischer Datenzugriff bzw. -transfer“ bereichsübergreifend ist, kann die Lösung nicht auf einen Bereich (z. B. nur im Recht oder nur in der IT) beschränkt werden. Dies findet seine Ausprägung im Recht (Lösung I: Rechtliche Schritte) sowie in dem organisatorischen (Lösung II: Organisatorische Gestaltung der Organisation) und technischen Aufbau einer Organisation (Lösung III: Technische Gestaltung der Organisation). Darüber hinaus kann die Antwort auch in der praktischen Vorgehensweise (Lösung IV: Praktische Schritte) gefunden werden.

578 *Wood/Lewis*, CSIS, 03.2023, 1, 1; *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 268.
579 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 268.
580 *Wood/Lewis*, CSIS, 03.2023, 1, 1.
581 *Wood/Lewis*, CSIS, 03.2023, 1, 1.

3.4.5.1 Lösung I: Rechtliche Schritte

Grundsätzlich gilt: Wenn zwei Gesetze nicht miteinander übereinstimmen, muss eine unternehmerische Risikoentscheidung getroffen werden.[582] Unternehmen bzw. Organisationen müssen entscheiden, welches Gesetz sie einhalten wollen, und müssen überlegen, welche Konsequenzen eine Nichteinhaltung haben kann. Es wird dazu empfohlen, dass, wenn zwei Gesetze nicht miteinander übereinstimmen, das strengste gewählt und umgesetzt werden sollte, damit das Unternehmen auf der sicheren Seite bleibt.[583] Aber gibt es noch andere Möglichkeiten?

3.4.5.1.1 Einheitliches MLAT-Abkommen und einfaches MLAT-Verfahren

Zu spät erhaltene Informationen sind demnach nicht zielführend und schaffen langwierige Ermittlungsverfahren, durch die die gesuchte Person nicht mehr auffindbar ist, die gesetzlichen Fristen bereits abgelaufen sind oder eine schwere Straftat bereits begangen wurde, die eigentlich vermieden werden konnte. Es ist immer unbedingt erforderlich, rechtzeitig zu klären, ob eine Übermittlung der Informationen zwischen der EU und den USA zulässig ist.

Die Mitgliedsländer sollten nach Art. 20 Abs. 1 GPP[584] sicherstellen, dass die Verfahren für den grenzüberschreitenden Fluss personenbezogener Daten sowie zum Schutz der Privatsphäre und der individuellen Freiheiten **einfach** und mit denen anderer Mitgliedsländer, die diese Richtlinien einhalten, kompatibel sind. Das Wort „einfach“ hat hier die entscheidende Bedeutung.

Das MLAT-Verfahren wird sowohl in der EU als auch in den USA angewendet und hat bereits gezeigt, dass es ein effektives Instrument ist. Es wurde aber auch festgelegt, dass es zu vielen Verzögerungen führt und sehr oft zu lange dauert (im Durchschnitt zehn Monate[585]). Dieser Zeitraum ist in Strafverfahren tatsächlich unangemessen. Daher wäre es zu überlegen, das Abkommen zu vereinheitlichen und das Verfahren zu vereinfachen.

Derzeit gibt es ein EU-US-MLAT und MLATs zwischen entsprechenden EU-Mitgliedstaaten und den USA (wie DSGVO in der EU und BDSG in Deutschland, so auch EU-US-MLAT und DEU-US-MLAT). Diese länderspezifischen MLATs sind jedoch als Ergänzungen zum EU-US MLAT zu betrachten (vgl. Art. 11 EU-US-MLAT und Art. 24 DEU-US-MLAT). Sie haben nicht den gleichen Charakter wie die länderspezifischen Datenschutzgesetze der EU (z. B. BDSG).

582 Diese Meinung wurde auf der Global GRC, Data Privacy & Cyber Security ConfEx am 31.05.2023 in NY/USA geäußert.

583 Diese Empfehlung wurde auf der Global GRC, Data Privacy & Cyber Security ConfEx am 31.05.2023 in NY/USA geäußert.

584 Bei den GPP handelt es sich um unverbindliche Leitlinien der OECD, die von den Mitgliedsländern erlassen wurden. Sie verfolgen das doppelte Ziel, die Akzeptanz bestimmter Mindeststandards für den Schutz der Privatsphäre und den Schutz personenbezogener Daten zu erreichen und Faktoren, die Länder dazu veranlassen könnten, den grenzüberschreitenden Datenverkehr einzuschränken, so weit wie möglich zu beseitigen. Mitglieder der OECD sind u.a. viele europäische Länder und die USA. S.: *Kuner*, Transborder Data Flows and Data Privacy Law, S. 35.

585 Europäisches Parlament, 4. Arbeitsdokument (A), 11.03.2019, S. 6.

Das MLAT-Abkommen kann vereinheitlicht werden, indem alle MLAT-Voraussetzungen in einem Dokument (in einem EU-US-MLAT) klar definiert werden, das sowohl in allen EU-Mitgliedstaaten als auch in den USA gilt. Das EU-US-MLAT sollte alle Anforderungen enthalten, die für jedes EU-Mitgliedsland sowie für jeden Staat in Amerika gelten. Länder- bzw. staatenstspezifische MLATs sollten nur die Spezifikationen oder Ausnahmen des jeweiligen Landes oder Staates enthalten. Dadurch wird das Verfahren verständlicher, schneller und leichter umsetzbar.

Derzeit beinhaltet das MLAT-Verfahren die folgende Schritte: 1. Prüfung des Antrags durch die ausländische Gegenseite, 2. Antrag auf Erlass einer gerichtlichen Anordnung, 3. Erteilung der Anordnung zur Datenweitergabe sowie 4. Beschaffung der Daten durch die ausländische Regierung und Übermittlung an die ersuchende Regierung.[586] Diese sollten wie folgt geändert werden: 1. Prüfung des Ersuchens durch das Gericht, 2. Erlass der Anordnung zur Offenlegung der Daten an das betreffende Unternehmen und 3. Beschaffung der Daten durch das betreffende Unternehmen und Übermittlung an die ersuchende Regierung.

In Art. 7 EU-US-MLAT („Beschleunigte Übermittlung von Ersuchen“) ist die Rede von einer Beschleunigung des MLAT-Verfahrens durch Übermittlung von Daten per Fax oder E-Mail. Dieser Artikel könnte dahingehend ergänzt werden, dass das Verfahren von dem Gericht bzw. von einer spezifischen Stelle beim Gericht innerhalb einer bestimmten Frist bearbeitet werden muss.

Dementsprechend sollte in jedem Land bzw. jeder Stadt das Gericht das Verfahren übernehmen, oder es sollte eine spezifische Stelle beim Gericht nur für dieses Verfahren geben, die die Anträge sofort entgegennimmt, prüft und vom Gericht genehmigen bzw. ablehnen lässt. Dies würde auch die Suche vereinfachen, welches Amt in welchem Land zuständig ist und welches Formular, welches Verfahren oder welche Vereinbarung zu welchem Fall passt. Dies würde wiederum eine Menge Zeit und Ressourcen sparen.

Soweit eine Vereinfachung und Beschleunigung des Verfahrens nicht möglich ist, dürfen Daten nur auf Verlangen der Behörden nicht weitergegeben oder offengelegt werden. Allein das Argument, das Verfahren laufe langsam, reicht nicht aus. Mit dieser Logik sollten alle Verdächtigen direkt ins Gefängnis geschickt werden, da Gerichtsverfahren in der Regel lange dauern. Es ist wichtig, dass das Verfahren schnell abläuft, aber wenn dies nicht der Fall ist, sollten die Rechte des Einzelnen nicht gefährdet oder missachtet werden. Mit dem hier vorgestellten Vorschlag ist eine zügige Bearbeitung des Strafverfahrens jedoch realistisch.

586 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 3.

3.4.5.1.2 „Verhandlung ähnlicher Beschränkungen“

Wie bereits erwähnt, dürfen Anordnungen ausländischer Regierungen, die Gegenstand von CLOUD Act Vereinbarungen sind, nicht auf Daten von US-Bürgern oder in den USA ansässigen Personen abzielen.[587] Den ausländischen Regierungen steht es dennoch frei, ,,Verhandlungen ähnlicher Beschränkungen“ anzustreben.[588]

Dies könnte von Europa genutzt werden. Zumindest vorübergehend dürfte die Lösung darin bestehen, dass nur Daten von US-Bürgern, die in der EU ansässig sind, von der EU angefordert werden können. Natürlich sind die Daten aller in der EU ansässigen Personen nach der DSGVO schützenswert. So kann beispielsweise ein US-Bürger, der in Deutschland studiert, seine Datenschutzrechte in Europa wahrnehmen. Daher werden die Daten von US-Bürgern durch die ,,Verhandlung ähnlicher Beschränkungen“ nicht vernachlässigt. Dieser Vorschlag schützt zumindest vorübergehend die Daten von in der EU ansässigen Nicht-US-Bürgern.

Diese Beschränkung wäre auch nach Art. 17 Abs. 1 GPP gerechtfertigt. Darin heißt es, dass ein Mitgliedstaat auch Beschränkungen in Bezug auf bestimmte Kategorien personenbezogener Daten auferlegen kann, für die seine nationalen Datenschutzgesetze aufgrund der Art dieser Daten besondere Vorschriften enthalten und für die der andere Mitgliedstaat keinen gleichwertigen Schutz bietet.

Es sollte aber dabei erwähnt werden, dass, wenn die EU diese Beschränkungen vornehmen möchte, sie wahrscheinlich zuerst das Rechtshilfeabkommen gem. dem CLOUD Act unterzeichnen sollte. Es wäre wiederum kein günstiger Ansatz für dieses Thema.

587 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 12 ff.

588 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 12 ff.

3.4.5.1.3 Melde- und Konsultationspflicht

Als eine weitere Lösung wären Melde- und Konsultationspflichten zu überlegen. Es wäre zu regeln, dass der EU- bzw. US-Anbieter im Falle einer Anfrage einer Behörde verpflichtet wird, sich bei der Datenschutzbehörde zu melden und sich von ihr beraten zu lassen. Auf diese Weise könnte jeder internationale Datentransfer zum Zwecke der Strafverfolgung kontrolliert werden.

Außerdem gibt die Melde- und Konsultationspflicht eine Möglichkeit, schnell festzustellen, ob die Datenübermittlung unrechtmäßig bzw. rechtmäßig ist oder ob sie doch nur teilweise durchgeführt werden dürfte. Dies hilft einerseits dem Diensteanbieter, diese wichtige Entscheidung nicht allein zu treffen, schützt andererseits jede einzelne Person davor, dass die sie betreffenden Daten nicht unrechtmäßig verarbeitet werden und dass sie weiterhin ihre Persönlichkeitsrechte sowie andere ihr zustehende Rechte wahrnehmen kann.

Als Beispiel für eine solche Verpflichtung kann die Verpflichtung zur Meldung einer Datenschutzverletzung gem. Art. 33 DSGVO genannt werden. Analog dazu könnte beispielsweiße eine 72-stündige Benachrichtigungspflicht, und Konsultationspflicht vor einer Datenweitergabe oder -offenlegung an US-Behörden vorgeschrieben werden.

3.4.5.2 Lösung II: Organisatorische Gestaltung einer Organisation

Erhält ein US-Anbieter von einer US-Strafverfolgungsbehörde ein Ersuchen für Daten, die in seiner in der EU ansässigen Tochtergesellschaft gespeichert sind und die Informationen über EU-Personen enthalten, hängt es zum Teil von der Organisationsstruktur des US-Unternehmens ab, ob diese Daten weitergegeben werden müssen oder nicht.

3.4.5.2.1 Duplizierte hierarchische Trennung und Segmentierung

Wenn die US-Anbieter im Besitz, im Gewahrsam oder unter der Kontrolle / ,,possession, custody, or control“ der gesuchten Daten sind, müssten diese Daten laut dem CLOUD Act herausgegeben werden. Daher soll festgestellt werden, ob die in den USA ansässige Mutter- oder Tochtergesellschaft möglicherweise ,,Besitz, Gewahrsam oder Kontrolle“ über die Daten hat, die von den nicht in den USA ansässigen Tochtergesellschaften gehalten werden.[589]

Wenn in einer Organisation die duplizierte hierarchische Trennung besteht und die Segmentierung vorhanden ist,[590] wären die bei der EU gespeicherten Daten den US-Behörden nach dem CLOUD Act mit hoher Wahrscheinlichkeit nicht zugänglich. Damit dies geschieht, sollten die folgenden Fakten zutreffen:

589 Diese Meinung, die in diesem Abschnitt beschrieben wird, ist in dem folgenden Artikel zu finden. S.: How to comply with both the GDPR and the CLOUD Act, abrufbar: https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/, zuletzt abgerufen am 03.08.2023.

590 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 20 ff.

a) Die EU-Tochtergesellschaft hat alle ihre Büros in dem betreffenden EU-Land, führt keine Geschäfte in den USA durch sowie arbeitet unabhängig von ihrer Muttergesellschaft.[591]
b) Das in der EU-Tochtergesellschaft eingerichtete Computernetz ist vollständig von den Netzen der Muttergesellschaft abgetrennt / segmentiert (z. B. die genutzte Server befinden sich in der europäische Union[592]).[593]
c) Das europäische IT-Team ist von dem amerikanischen IT-Team getrennt,[594] so dass z. B. der technische Support vor Ort geleistet wird.
d) Für das Personal der US-Muttergesellschaft ist es technisch unmöglich, in die Telekommunikationsinfrastruktur der EU-Tochtergesellschaft einzudringen, um Daten zu erhalten.[595]

3.4.5.2.2 Umgang mit dem Dienstleister

Hat eine Organisation einen Dienstleister im Einsatz, soll sie als der Dienstleistungsempfänger versuchen, die Vereinbarungen mit den Dienstleistern so zu ändern, dass der Zugriff der USA auf die Daten, die in der EU gespeichert sind, eingeschränkt[596] bzw. abgeschafft wird. Die Vereinbarungen mit US-Dienstleistern sollen dahingehend überprüft werden, ob Daten, die außerhalb der USA gehalten werden, in den USA zugänglich sind.[597] In den Vereinbarungen mit den Dienstleistern sollte klargestellt werden, dass die Daten außerhalb der USA physisch und logisch getrennt gespeichert werden und von den USA aus nicht zugänglich sind.[598]
All oben beschriebene Punkte sollten zuerst auf organisatorischer Ebene geregelt werden. Sie sind essentiell und müssen immer klar definiert, niedergeschrieben und dokumentiert werden. Darüber hinaus ist aber eine technische Umsetzung ebenso wichtig.

591 How to comply with both the GDPR and the CLOUD Act, abrufbar: https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/, zuletzt abgerufen am 03.08.2023.
592 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 20.
593 How to comply with both the GDPR and the CLOUD Act, abrufbar: https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/, zuletzt abgerufen am 03.08.2023.
594 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 21.
595 How to comply with both the GDPR and the CLOUD Act, abrufbar: https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/, zuletzt abgerufen am 03.08.2023.
596 How to comply with both the GDPR and the CLOUD Act, abrufbar: https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/, zuletzt abgerufen am 03.08.2023.
597 How to comply with both the GDPR and the CLOUD Act, abrufbar: https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/, zuletzt abgerufen am 03.08.2023.
598 How to comply with both the GDPR and the CLOUD Act, abrufbar: https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/, zuletzt abgerufen am 03.08.2023.

3.4.5.3 Lösung III: Technische Gestaltung der Organisation

Diejenigen, die Daten verarbeiten, sind verpflichtet, deren Sicherheit jederzeit zu gewährleisten. In Fällen, in denen kritische Daten, u. a. urheberrechtlich geschützter, vertraulicher Informationen oder personenbezogener Daten, in der Cloud gespeichert werden, sollte der neueste Stand der Sicherheit / „State-of-the-Art Security", einschließlich Verschlüsselung im Ruhezustand sowie bei der Übertragung verwendet werden.[599] Darüber hinaus sollten der Zugang zu Daten und die Segmentierung von Netzwerken in Betracht gezogen werden.

3.4.5.3.1 Verwaltung des Verschlüsselungsschlüssels

Die **Verwaltung des Verschlüsselungsschlüssels** muss in jedem Fall unter der vollständigen Kontrolle des Dienstleistungsempfängers stehen und darf dem US-Cloud-Dienstleister ohne Erlaubnis des für die Daten Verantwortlichen nicht zugänglich sein.[600] Den Schlüssel sollte an einem verschlossenen Ort aufbewahrt werden, auf den der Cloud-Dienstanbieter nicht zugreifen kann.[601] Nur die Person, die für die Speicherung der Daten in der Cloud verantwortlich ist, sollte Zugang zum Schlüssel haben.[602]

Gemäß Abschn. 105 (a), § 2523 (b) (3) CLOUD Act schaffen die Bedingungen des Abkommens keine Verpflichtung, den Anbieter zur Entschlüsselung der Daten zu verpflichten oder ihn an der Entschlüsselung der Daten zu hindern. Direkte Anfragen ausländischer Behörden dürfen in solchem Fall abgelehnt werden.

Der Cloud-Dienstleister ist für die Infrastruktur, die Integration mit dieser Infrastruktur, die Datenübertragung und die Datensicherheit verantwortlich.[603] Außerdem muss er sicherstellen, dass die Daten während der Übertragung und im Ruhezustand verschlüsselt sind.[604] Für die Daten selbst ist er nicht verantwortlich.

599 How to comply with both the GDPR and the CLOUD Act, abrufbar: https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/, zuletzt abgerufen am 03.08.2023.
600 How to comply with both the GDPR and the CLOUD Act, abrufbar: https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/, zuletzt abgerufen am 03.08.2023.
601 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 21.
602 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 29.
603 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 22.
604 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 22.

3.4.5.3.2 Zugang und Segmentierung

Die Datensicherheit für die Daten, die von dem Verantwortlichen und Auftragsverarbeiter verarbeitet werden, sollte von dem Verantwortlichen und dem Auftragsverarbeiter gewährleistet werden. Das bedeutet, dass auch die in der Cloud gespeicherten Daten von dem Verantwortlichen bzw. dem Auftragsverarbeiter geschützt werden müssen. Der Cloud-Anbieter kümmert sich ausschließlich um die Cloud-Infrastruktur. Daher benötigt er keinen **Zugang zu den Daten**, die von dem Verantwortlichen oder dem Auftragsverarbeiter verarbeitet werden.

Darüber hinaus soll die **Segmentierung / Abtretung der Netzwerke**, die in der organisatorischen Gestaltung des Unternehmens vorgenommen wurde, auch tatsächlich umgesetzt werden. Die Segmentierung bietet die Möglichkeit, dass die in einer in der EU ansässigen Gesellschaft oder Einheit verarbeiteten Daten in der EU verbleiben und die in einer in den USA ansässigen Gesellschaft oder Einheit verarbeiteten Daten in den USA verbleiben. Wenn dies nicht möglich ist, muss ein Unternehmen Möglichkeiten der Anonymisierung bis zu einem Grad prüfen, in dem es rechtlich als DSGVO-konform angesehen wird.[605]

Die Segmentierung sorgt dafür, dass die Kommunikation getrennt bzw. gesperrt wird. So kann sichergestellt werden, welche Einheit in welchem Land Zugang zu welchen Informationen hat. Eine absolute Kommunikationssperre unterbricht den gesamten Informationsfluss, so dass die Kommunikation mit dem entfernten Rechner vollständig unterbrochen ist.[606] Damit ist der Client-Rechner im Subnetz (und damit seine Benutzer) auch von weiteren Informationen über die betreffenden Server bzw. der Kommunikation mit dort registrierten Benutzern vollständig isoliert, so dass in der Regel alle Kommunikationsmöglichkeiten unterbunden werden.[607]

3.4.5.4 Lösung IV: Praktische Schritte

Traditionelle grenzüberschreitende Mechanismen wie Rechtshilfevereinbarungen werden als zu langsam und schwerfällig angesehen,[608] da sie mit vielen Verzögerungen verbunden sind, obwohl der Mechanismus selbst beispielsweise von der EU-Kommission oder der G20-Arbeitsgruppe positiv bewertet wurde (s. → S. 79). Darüber hinaus hat die internationale Gruppe zum Datenschutz in der Telekommunikation geäußert, dass die für MLAT-Anträge zuständige Stellen häufig „unterfinanziert und personell unterbesetzt“ sind.[609]

605 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 21.
606 *Greve*, Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, S. 122.
607 *Greve*, Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, S. 122.
608 *Christakis/Terpan*, IDPL, Vol. 11, Nr. 2, 2021, 81, 85.
609 IWGDPT, Arbeitspapier zu Standards für den Datenschutz und den Schutz der Privatsphäre bei grenzüberschreitenden Datenanforderungen zu Strafverfolgungszwecken, 63. Sitzung, 09 - 10.04.2018, S. 1.

Wenn nicht genügend Ressourcen für das Verfahren zur Verfügung gestellt werden, wird das Verfahren sicherlich länger dauern als geplant. Anstatt ein neues Gesetz zu erlassen, ist es daher besser, mehrere Personen einzustellen und genügend Zeit und Finanzen bereitzustellen. Dies wird eine schnelle und professionelle Bearbeitung der Anfragen ermöglichen. All dies sollte jedoch zielgerichtet eingesetzt werden – vorzugsweise werden die zeitlichen und monetären Ressourcen von Personen genutzt, die sich mit der Materie gut auskennen.

Es ist unerlässlich, zu kooperieren und Zeit zu gewinnen, um bestimmte Bedingungen für das Anbieten von Beweisen oder Einschränkungen für die Verwendung dieser Beweise zu erfüllen.[610] In jedem Fall ist es entscheidend, dass die Anwälte das betreffende Abkommen gründlich prüfen und verstehen, wie das Verfahren funktioniert.[611] Wenn die betreffende Partei oder Behörde das MLAT erst dann versucht zu verstehen, wenn sie eine Anfrage erhält, kann dies definitiv nicht reibungslos und hochprofessionell ablaufen. Dieses Wissen muss an eine ausreichende Anzahl von Mitarbeitern weitergegeben werden, damit der MLAT-Prozess reibungslos funktionieren kann.

Entsprechend wurden u. a. die folgende Handlungsempfehlungen in dem Arbeitspapier des EU-Parlaments definiert: 1. Mehr materielle, personelle sowie technische Ressourcen, um elektronische Beweismittel deutlich zeiteffizienter bereitstellen zu können,[612] 2. eine bessere Ausbildung des mit der Rechtshilfeangelegenheiten befassten Personals sowie 3. die Herausgabe von Leitlinien.[613]

610 *Rush/Kephart*, LEGAL INSIGHT, 1, 8.
611 *Rush/Kephart*, LEGAL INSIGHT, 1, 8.
612 Europäisches Parlament, 4. Arbeitsdokument (A), 11.03.2019, S. 6.
613 Europäisches Parlament, 4. Arbeitsdokument (A), 11.03.2019, S. 6.

3.5 Die Zusammenfassung des (internationalen) Datentransfers

Historische Entwicklung sowie heutige Ausprägung des (internationalen) Datentransfers / der (grenzüberschreitenden) digitalen Datenübermittlung haben ihre Relevanz sowohl im Alltag als auch in der nationalen Sicherheit oder Wirtschaft deutlich gemacht. Ihre zentrale Rolle in vielen Prozessen, Geschäften oder Aktivitäten schafft eine Bedeutung dieses Themas, das sich nicht nur auf den rechtlichen Rahmen beschränkt und ihre Ergänzung in den technischen sowie organisatorischen Bereichen findet. Die vorangegangenen Kapitel haben auch deutlich gemacht, dass das Thema „Internationaler Datentransfer" in einem sehr engen Verhältnis mit den Persönlichkeitsrechten steht.

Das Thema „Internationaler Datentransfer" ist sowohl im EU- als auch im US-Rechtssystem grundsätzlich im Bereich des Datenschutzes (eine besondere Ausprägung der Persönlichkeitsrechte) angesiedelt. Der Datenschutz gewährleistet die rechtmäßige Verarbeitung personenbezogener Daten vor, während und nach der Übermittlung. Dazu gehört auch die Übermittlung oder Offenlegung von Daten für wirtschaftliche Zwecke oder an die Behörden für Strafverfahren. Das Hauptgesetz hierfür ist die DSGVO in der EU und der CLOUD Act in den USA. Obwohl sie zur gleichen Zeit kamen, verfügen sie über einen sehr unterschiedlichen Rechtscharakter, dienen unterschiedlichen Zwecken und haben dementsprechend unterschiedliche und manchmal sogar widersprüchliche Folgen.

Die DSGVO versucht, die Integrität des Einzelnen zu schützen und den Menschen Macht über ihre Daten zu geben, während der CLOUD Act die Herausgabe der Daten fordert, indem er US-Interessen über ausländische Gesetze stellt.[614] Dies wurde wie folgt bewiesen: Werden die Daten in die USA oder weltweit exportiert, bietet die DSGVO mehrere Lösungen, um die Einhaltung ihrer Vorschriften zu gewährleisten.[615] Insbesondere ist Art. 48 DSGVO zu erwähnen, wenn EU-Daten von einer US-Strafverfolgungsbehörde angefordert werden.[616] Bezüglich des Datentransfers außerhalb des Landes haben die USA jedoch keine ausreichende Beschränkungen vorgeschrieben.[617] Sie verfügen über kein landesweites und allumfassendes Datenschutzgesetz.

614 U.S. CLOUD Act vs. GDPR, abrufbar: https://www.activemind.legal/guides/us-cloud-act/, zuletzt abgerufen am 03.08.2023.

615 European Privacy Framework, abrufbar: https://www.privacy-europe.com/european-privacy-framework.html, zuletzt abgerufen am 03.08.2023.

616 How to comply with both the GDPR and the CLOUD Act, abrufbar: https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/, zuletzt abgerufen am 03.08.2023.

617 *Hubbard*, The NATIONAL LAW REVIEW, 1, 1-2.

Der Ursprung der fragmentarischen Regelung liegt im Gesamtkonzept des Datenschutzes in den USA.[618] Sie haben kein allumfassendes gesetzliches Datenschutzsystem, sondern setzen auf die Selbstregulierung der Privatwirtschaft, die sektorspezifisch durch gesetzliche Regelungen auf Bundes- und Landesebene unterstützt wird.[619] So scheint die Erhebung neuer Daten und ihre Weiterverarbeitung nur geringen Einschränkungen zu unterliegen.[620]

Christopher Kuner identifizierte die betroffenen Parteien im amerikanischen Rechtssystem und bewertete die extraterritorialen Wirkungen des Datenschutzes wie folgt: *„Individuals, who become confused about which regulation applies to the processing of their data; data controllers, which are placed in the middle of contradictory requirements; and the law itself, which can lose respect when it makes contradictory demands or has no practical chance of being enforced. The increasing extraterritorial application of data protection law is another sign of the fragmentation of trans-border data flow regulation.“*[621]

Während die DSGVO den Schutz natürlicher Personen und den freien Datenverkehr zum **Ziel** hat, zielt der CLOUD Act auf effizientere Ermittlungen durch rechtzeitigen Zugriff auf elektronische Daten ab. Insbesondere zielt er auf das Ersetzen der MLAT-basierte Rechtshilfeersuchen durch CLOUD Act Vereinbarungen ab.[622] Dies zeigt, dass auf amerikanischer Seite weniger Interesse an den Persönlichkeitsrechten besteht als auf europäischer Seite.

Wird sowohl die **räumliche als auch die sachliche Anwendung** betrachtet, so lässt sich feststellen, dass, wenn die DSGVO personenbezogene und pseudonymisierte Daten in der EU schützt, der CLOUD Act den freien Zugang von US-Behörden zu jeder Art von Daten sowohl innerhalb als auch außerhalb der USA gewährleistet.

Die **Adressaten** werden im Rahmen der DSGVO breiter erfasst als im CLOUD Act. Die DSGVO betrifft alle Verantwortlichen und Auftragsverarbeiter, die in den räumlichen Anwendungsbereich der DSGVO fallen, wenn unter dem CLOUD Act nur elektronische Kommunikationsdienste und Ferninformationsdienste fallen. Es ist jedoch erwähnenswert, dass diese enge Erfassung der Adressaten positiv zu bewerten ist. Der CLOUD Act kann Unternehmen schädigen oder ihre Prozesse beeinträchtigen, z. B. indem sie verpflichtet werden, Daten unter Verstoß gegen die DSGVO herauszugeben. Da der Adressaten-Kreis des CLOUD Act eng gefasst ist, bedeutet dies, dass nur eine geringe Anzahl von Unternehmen von diesen schädlichen Folgen betroffen ist.

618 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 182.
619 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 182.
620 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 182.
621 *Kuner*, Transborder Data Flows and Data Privacy Law, S. 142.
622 Datenschutzkonformer Einsatz von Office 365 nach Cloud Act, abrufbar: https://www.dr-datenschutz.de/datenschutzkonformer-einsatz-von-office-365-nach-cloud-act/, zuletzt abgerufen am 03.08.2023.

Die **Voraussetzungen** nach der DSGVO sind komplexer und strenger als nach dem CLOUD Act. Dies ist sowohl an der Struktur als auch an der Komplexität der Prüfung des Datenschutzniveaus in einem Drittland nach der DSGVO zu erkennen. Demgegenüber können laut dem CLOUD Act die Anfragen auf Offenlegung personenbezogener Daten von US-Behörden direkt an den Dienstleister gerichtet werden.[623] Hierdurch nimmt der US-Kongress eine Praxis in US-Recht auf, die geeignet ist, das zwischen der EU und den USA geltende Abkommen über die Rechtshilfe in Strafsachen (MLAT) zu umgehen.[624]

Ist von **MLAT** die Rede, sind unterschiedliche Bewertungen zu nennen. Grundsätzlich wird das MLAT-Verfahren als hilfreich und zielführend eingeschätzt. Es muss aber betont werden, dass es viel Zeit in Anspruch nimmt und daher oft keine zeitgerechten Ergebnisse liefert. Dadurch wird das Strafverfahren verlangsamt. Weitere internationale Bemühungen wie die E-Beweis-Verordnung versuchen, dieses Problem zu lösen.

Mit der Unterschrift von Präsident Biden auf der E. O. 14086 erlauben sich die USA einen für das Land untypischen Eingriff in die eigene Gesetzgebung. Damit signalisieren sie ihre Bereitschaft, sich den Datenschutzvorgaben der EU anzunähern und zeigen, dass sie bereit sind, sich datenschutzrechtlich zu verbessern.[625] Der neue Datenschutzrahmen (EU-US DPF), der viele positive Aspekte enthält, wirft auch viele Datenschutzfragen auf und löst in der EU Besorgnis aus. Diese Rahmenbestimmungen werden bereits angewandt, und es bleibt abzuwarten, wie sich die Datenschutzsituation entwickelt.

Entsprechend der oben beschriebenen Situation wurden einige **Lösungen** präsentiert, die einen Ausweg in den verschiedenen Dimensionen findet. Rechtliche Schritte zeigen deutlich, dass durch die Vereinfachung des MLAT-Verfahrens, durch die „Verhandlungen ähnlicher Beschränkungen“ sowie durch die Melde- und Konsultationspflicht eine deutliche Verbesserung der (rechtliche) Lage möglich ist.

623 Edpb, ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence, S. 1.

624 Edpb, ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence, S. 1.

625 Diese Auffassung wird in dem folgenden Artikel beschrieben. S.: Transatlantische Datentransfers: aktueller Stand zwischen EU und USA, abrufbar: https://www.dataguard.de/blog/update-transatlantische-datentransfer-bedeutung-fuer-eu-unternehmen, zuletzt abgerufen am 03.08.2023.

Die **organisatorische Gestaltung** einer Organisation ermöglicht es, die aktuelle Situation so zu gestalten, dass jeder Verantwortliche sowie Auftragsverarbeiter die Bestimmungen der DSGVO so umsetzen kann, dass er nicht gegen den CLOUD Act verstößt und die Bestimmungen des CLOUD Act so erfüllen kann, dass er nicht gegen die DSGVO verstößt. Um dem bestmöglich zu entsprechen, sollten alle technisch-organisatorischen Maßnahmen auch tatsächlich gelebt werden. Dies wird durch die richtige **technische Gestaltung** einer Organisation ermöglicht.

Praktische Schritte verdeutlichen, was genau zu tun ist, um die Umsetzung aller oben beschriebenen Lösungen fristgerecht und hochprofessionell zu ermöglichen. Dieser Schritt deckt alle drei oben beschriebenen Lösungen ab. Ressourcen, Kapazitäten, Wissen oder Bereitschaft sind universelle Schlüssel für jeden Erfolg, ebenfalls für den Erfolg im internationalen Datentransfer und für den Schutz der Persönlichkeitsrechte.

Wird beschlossen, Daten zu verarbeiten bzw. grenzüberschreitend zu transferieren, soll die Lage entsprechend vorbereitet werden, um die Daten schützen, die Gesetze einhalten und den Geschäftsbetrieb aufrechterhalten bzw. in dem Ermittlungsprozess fortfahren zu können. Außerdem sollten die Betroffenen keinen Zweifel daran haben, dass ihre Daten rechtmäßig verarbeitet werden und ihre Rechte nicht verletzt werden.

Dies kann jedoch nicht allein durch IT- und / oder Informationssicherheit gewährleistet werden. Sicherheit und Datenschutz überschneiden sich oft, aber enthalten auch viele Unterschiede; es können gleichzeitig Informationen geschützt werden, aber Privatsphäre[626] und dadurch (Betroffenen-) und / oder Persönlichkeitsrechte verletzt werden. Um dies zu vermeiden, sollen zahlreiche Anforderungen und Maßnahmen erfüllt werden. Wie dies in der Praxis aussehen sollte, wird in den folgenden Kapiteln behandelt.

626 Diese Meinung wurde auf der Global GRC, Data Privacy & Cyber Security ConfEx am 31.05.2023 in NY/USA geäußert.

4 Präventive Maßnahmen

4.1 Präventive Maßnahmen – Platzierung und Relevanz

4.1.1 Einführung

Daten sind für jeden wichtig, unabhängig davon, ob sie aus dem Alltags- oder Berufsleben stammen oder in einem Strafverfahren entstanden sind. Nutzer, die großen Wert auf einen rücksichtsvollen Umgang mit den sie betreffenden Daten legen, neigen dazu, Anbieter zu wählen, die einen besonderen Schutz der Privatsphäre der Nutzer bieten oder die verarbeiteten Daten sensibel behandeln.[627] Darüber hinaus sollten die Mitgliedländer gem. Art. 16 GPP alle notwendigen und geeigneten Maßnahmen ergreifen, um sicherzustellen, dass der grenzüberschreitende Verkehr personenbezogener Daten, einschließlich des Transits durch ein Mitgliedsland, ununterbrochen und sicher ist. Aus diesen Gründen sollte sich jede Organisation (Unternehmen und Behörde) darüber im Klaren sein, wie sie den Datenschutz und die Informationssicherheit bei der Datenverarbeitung aufrechterhalten und verbessern kann.

Der **Datenschutz** schützt Bürger vor missbräuchlicher Verarbeitung der auf sie bezogenen Daten.[628] Er korrespondiert mit dem Recht auf Privatsphäre,[629] das unter die Persönlichkeitsrechte fällt[630]. Diese Rechte und die damit verbundenen Daten müssen von jedem Einzelnen geschützt und beachtet werden. Hierdurch werden Privatsphäre und das Recht auf informationelle Selbstbestimmung gewährleistet.[631]

Landen diese Daten in einer Organisation, kommt die **Informationssicherheit** ins Spiel, die jede Organisation dazu verpflichtet, alles zu tun, um die (personenbezogene) Daten zu schützen. Um dies zu ermöglichen, muss diese innerhalb der Organisation eingeführt und aufrechterhalten werden. Informationssicherheit ist darauf gerichtet, Risiken auf ein Niveau zu reduzieren, das für die Organisation akzeptabel ist.[632]

627 Bundeskartellamt, Big Data und Wettbewerb: Schriftenreihe „Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft“, 1, 12.

628 Was unterscheidet Datenschutz von Informationssicherheit? abrufbar: https://www.haufe.de/compliance/management-praxis/was-unterscheidet-datenschutz-von-informationssicherheit_230130_482568.html, zuletzt abgerufen am 04.08.2023.

629 Datenschutz, abrufbar: https://edps.europa.eu/data-protection/data-protection_de, zuletzt abgerufen am 04.08.2023.

630 *Brüggemeier u.a.*, Personality Rights in European Tort Law, S. 6.

631 Was unterscheidet Datenschutz von Informationssicherheit? abrufbar: https://www.haufe.de/compliance/management-praxis/was-unterscheidet-datenschutz-von-informationssicherheit_230130_482568.html, zuletzt abgerufen am 04.08.2023.

632 Grundlegende Begriffe und Schutzziele der Informationssicherheit, abrufbar: https://www.rst-beratung.de/themen/informationssicherheit, zuletzt abgerufen am 04.08.2023.

Der Begriff „Informationssicherheit“ bezieht sich auf alle „technischen und organisatorischen Maßnahmen zur Sicherung aller Daten in Systemen von Unternehmen[633] und Organisationen“ sowohl in technischen als auch nicht-technischen Systemen und stellen die folgenden Schutzziele sicher: **Vertraulichkeit / „Confidentiality“, Integrität / „Integrity“ und Verfügbarkeit / „Availability“[634] (CIA)**. Diese Eigenschaften bzw. Schutzziele können als die primären Schutzziele betrachtet werden, deren Einhaltung die Informationssicherheit schafft.[635]

Die DSGVO hat auch den Grundsatz der Belastbarkeit / „Resilience“ aufgenommen, der inzwischen international ergänzt wurde.[636] Weitere Eigenschaften bzw. Schutzziele wie **Authentizität, Zurechenbarkeit, Nichtabstreitbarkeit und Verlässlichkeit** sind ebenfalls zu berücksichtigen.[637]

Wie oben beschrieben wurde, besteht der größte Unterschied zwischen Datenschutz und Informationssicherheit darin, dass durch den Datenschutz Menschen bzw. betroffene Personen geschützt werden, wenn durch die Informationssicherheit Informationen bzw. Daten geschützt werden. Weiterhin ist die Umsetzung des Datenschutzes mit strengen gesetzlichen Auflagen verbunden, während bei der Informationssicherheit diverse Konzepte einzuführen und durchzusetzen sind.[638]

Zur Informationssicherheit gehören auch die Datensicherheit und IT-Sicherheit. **Datensicherheit** ist ein Teilbereich der Informationssicherheit[639] [640] und schützt alle Art der Daten sowohl personenbezogene (z. B. IP-Adresse) als auch nicht-personenbezogene Daten wie geschäftskritische Daten oder Metadaten. Datensicherheit zielt darauf ab, Sicherheitsrisiken entgegenzuwirken und Daten vor Verlust, Manipulation sowie unberechtigter Zugriff zu schützen.[641]

Unter **IT-Sicherheit** wird der Schutz der technischen Verarbeitung von Informationen sowie der fehlerfreien Funktion und Zuverlässigkeit von IT-Systemen verstanden. IT-Sicherheit bezieht sich grundsätzlich auf IT-Systeme und Informationen, die elektronisch gespeichert werden.[642]

---

633 Was unterscheidet Datenschutz von Informationssicherheit? abrufbar: https://www.haufe.de/compliance/management-praxis/was-unterscheidet-datenschutz-von-informationssicherheit_230130_482568.html, zuletzt abgerufen am 04.08.2023.

634 Was ist der Unterschied zwischen Datenschutz und Informationssicherheit? abrufbar: https://www.vialevo.de/unterschied-zwischen-datenschutz-und-informationssicherheit/, zuletzt abgerufen am 04.08.2023.

635 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 3.

636 *Auernhammer -Kramer/Meints,* DSGVO BDSG, Art. 32 Rn. 22.

637 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 3.

638 Was unterscheidet Datenschutz von Informationssicherheit? abrufbar: https://www.haufe.de/compliance/management-praxis/was-unterscheidet-datenschutz-von-informationssicherheit_230130_482568.html, zuletzt abgerufen am 04.08.2023.

639 Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 5.

640 In der Praxis werden die Begriffe Datensicherheit und Informationssicherheit als Synonyme verwendet. S: Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 5.

641 Was ist der Unterschied zwischen Datenschutz und Informationssicherheit? abrufbar: https://www.vialevo.de/unterschied-zwischen-datenschutz-und-informationssicherheit/, zuletzt abgerufen am 04.08.2023.

642 Die in diesem Abschnitt dargestellte Definition befindet sich in dem folgenden Artikel. S.: Was ist der Unterschied

Wenn eine Organisation eine strukturierte Herangehensweise zur effektiven Verwaltung der Informationssicherheit umsetzen möchte, führt praktisch kein Weg an der Normenreihe ISO/IEC 27000 vorbei.[643] ISO/IEC 27000 ist eine Reihe von Dokumenten, die verschiedene Aspekte des Informationssicherheitsmanagements behandeln.[644] Das zentrale und entscheidende Dokument in dieser Reihe ist ISO/IEC 27001[645]. Diese Normen legen nahe, dass die Organisation das Informationssicherheitsmanagementsystem (ISMS) führen soll.[646] Die Hauptaufgabe dieses Managementsystems ist die Planung, Umsetzung, Überprüfung und Verbesserung von Informationssicherheitskonzepten (s. → S. 152-153).[647]

Wenn Datenschutz und Informationssicherheit nebeneinander erwähnt werden, sollte betont werden, dass Schutz personenbezogener Daten bzw. Privatsphäre und Sicherheit eng miteinander verbunden sind, sich aber oft voneinander unterscheiden.[648] Es kann vorkommen, dass jemand Daten und Informationen schützt, aber die Privatsphäre verletzt.[649] Um dies zu verhindern, sollten geeignete Maßnahmen ergriffen werden.

Im Folgenden wird beschrieben, was genau die Informationssicherheit bezweckt und gewährleistet (B. Präventive Schutzziele der Informationssicherheit und C. Weitere Eigenschaften bzw. Schutzziele der Informationssicherheit). Wenn sichergestellt wird, was zu schützen ist, muss festgelegt werden, wie dies zu unternehmen ist. Aus diesem Grund ist zunächst das Thema „Risiko“ im Bereich der Risiko-Beurteilung zu betrachten (Kapitel – 10 Risiko-Beurteilung). Es ermöglicht die Einschätzung der Risiken, die mit der Datenverarbeitung verbunden sind.

Sind Risiken festgelegt und beurteilt, müssen sie behandelt bzw. eliminiert werden. Dies ist durch präventive Maßnahmen möglich, die in zwei Dimensionen zu unterteilen sind: Zum einen in obligatorische gesetzliche Maßnahmen (Kapitel – 11 Präventive rechtliche Maßnahmen) und zum anderen in normative Maßnahmen (Kapitel 12 – Präventive normative Maßnahmen). Die DIN ISO/IEC 27001:2022 (im Folgenden ISO/IEC 27001) wurde für die Untersuchung ausgewählt, weil es sich um eine internationale und sehr weit verbreitete Norm handelt, deren Anwendung sowohl in der EU als auch in den USA das allgemeine Niveau der Informationssicherheit in der Organisation und damit den internationalen Datentransfer erhöhen kann.

---

zwischen Datenschutz und Informationssicherheit? abrufbar: https://www.vialevo.de/unterschied-zwischen-datenschutz-und-informationssicherheit/, zuletzt abgerufen am 04.08.2023.

643 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 1.

644 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 1.

645 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 1.

646 *Auernhammer -Kramer/Meints,* DSGVO BDSG, Art. 32 Rn 26.

647 *Auernhammer -Kramer/Meints,* DSGVO BDSG, Art. 32 Rn 27.

648 Diese Meinung wurde auf der Global GRC, Data Privacy & Cyber Security ConfEx am 31.05.2023 in NY/USA geäußert.

649 Diese Meinung wurde auf der Global GRC, Data Privacy & Cyber Security ConfEx am 31.05.2023 in NY/USA geäußert.

4.1.2 Primäre Schutzziele der Informationssicherheit

4.1.2.1 Vertraulichkeit

Unter dem Begriff „Vertraulichkeit“ wird der Schutz vor unbefugter Kenntnisnahme von Informationen verstanden.[650] Sie bezieht sich auf die Eigenschaft, dass Informationen für Unbefugte nicht zugänglich sind und nicht von diesen offengelegt werden.[651] Die Vertraulichkeit wird verletzt, wenn z. B. ein Angreifer eine Kommunikation abfängt.[652]

Die Verschlüsselung von Daten ist einer der geeigneten Mechanismen zur Gewährleistung der Vertraulichkeit (z. B. Festplattenverschlüsselung bei der Datenspeicherung).[653]

4.1.2.2 Integrität

Der Begriff „Integrität“ bezieht sich auf eine Eigenschaft, die die Korrektheit und Vollständigkeit von Informationen gewährleistet.[654] Die Integrität soll eine unbemerkte Veränderung oder Manipulation der Daten verhindern.[655] Dazu gehört u. a. das Einfügen oder Löschen von Daten ebenso wie das Wiedereinspielen, Umordnen oder Duplizieren von Nachrichten.[656]

Die Integrität wird z. B. bei einem Man-in-the-Middle-Angriff (s. → S. 162) verletzt. In einem solchen Fall tritt ein Angreifer als „Vermittler“ auf und manipuliert Inhalte, um das beabsichtigte Ziel zu erreichen und die Datenintegrität zu gefährden. Eine Integritätsprüfung dieser Nachrichten oder digitaler Informationen wird verwendet, um jegliche Änderung zu erkennen.[657]

Es wird zwischen starker und schwacher Integrität unterschieden. Bei **starker Integrität** ist es unmöglich, die unbefugten Datenmanipulation / Datenänderungen (d. h. verändern, löschen oder einfügen von Daten) vorzunehmen. Bei **schwacher Integrität** können Änderungen vorgenommen werden, aber sie müssen bemerkt werden, damit sie nachvollziehbar sind.[658]

650 *Federrath*, Mitt. Math. Ges. Hamburg 34/2014, 21, 25.
651 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 3 ff.
652 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 3 ff.
653 *Federrath*, Mitt. Math. Ges. Hamburg 34/2014, 21, 25.
654 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 4.
655 Was ist Informationssicherheit - eine Definition, abrufbar: https://www.haufe.de/compliance/management-praxis/informationssicherheit/was-ist-informationssicherheit-eine-defintion_230130_483132.html, zuletzt abgerufen am 04.08.2023.
656 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 4.
657 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 4.
658 Dieser Unterschied, der in dem Abschnitt dargestellt wird, wird in dem folgenden Artikel detailliert beschrieben. S.: Schutzziele der Informationssicherheit, abrufbar: https://www.kryptowissen.de/schutzziele.php, zuletzt abgerufen am 04.08.2023.

4.1.2.3 Verfügbarkeit

Der Begriff „Verfügbarkeit“ bezieht sich auf die Eigenschaft, die Informationen bzw. Werte für einen autorisierten Benutzer verfügbar und anwendbar zu machen, wenn er sie anfordert.[659] Hierbei ist kein permanenter Zugang erforderlich.[660] Es reicht aus, wenn er dann hergestellt wird, wenn der Benutzer dies beabsichtigt hat[661] (z. B. die in Service Level Agreements geregelten Anforderungen an Server oder Rechenzentren).[662]

Eine Beeinträchtigung der Verfügbarkeit liegt z. B. bei Katastrophen oder DoS- Angriffen (Denial-of-Service) (s. → S. 163-164) vor,[663] wenn Daten entweder durch Naturkatastrophen oder durch Überlastung der Systeme durch Angreifer nicht mehr verfügbar sind.

Die Verfügbarkeit kann durch zwei Techniken sichergestellt werden,[664] nämlich durch Redundanz und Diversität. **Redundanz**, also die „mehrfache Auslegung von Systemkomponenten“, sorgt dafür, dass die redundante Komponente die Funktion der ausgefallenen Komponente übernimmt und das Gesamtsystem verfügbar bleibt.[665]

Bestehen Konstruktionsfehler oder werden sie während des Betriebs entdeckt, kann die Redundanz nicht in Anspruch genommen werden.[666] In diesem Fall werden IT-Systeme durch **Diversität**, d. h. Vielfalt der Herkunft, vor unentdeckten systematischen Designfehlern geschützt.[667]

4.1.2.4 Belastbarkeit

Die DSGVO greift ein neues Konzept der Belastbarkeit als Schutzziel auf.[668] Dies bezieht sich auf die Fähigkeit eines Systems, sich auf sich ändernde Umstände vorzubereiten, um sich rechtzeitig an solche veränderten Bedingungen anzupassen.[669]

Außerdem geht es um die Reaktion der Organisation auf Störungen und Cyberangriffe, um diese zu überstehen und die Ausgangsbedingungen schnell wiederherzustellen.[670] Sie stellt die Fähigkeit der technischen Systeme sowie der Organisation dar, Datensicherheit selbst bei einem Ausfall oder unbeabsichtigten Angriffen auf die Datensicherheit zu garantieren.[671]

---

659 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 4 ff.
660 Grundlegende Begriffe und Schutzziele der Informationssicherheit, abrufbar: https://www.rst-beratung.de/themen/informationssicherheit, zuletzt abgerufen am 04.08.2023.
661 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 4 ff.
662 Grundlegende Begriffe und Schutzziele der Informationssicherheit, abrufbar: https://www.rst-beratung.de/themen/informationssicherheit, zuletzt abgerufen 04.08.2023.
663 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 5.
664 *Federrath,* Mitt. Math. Ges. Hamburg 34/2014, 21, 22.
665 *Federrath,* Mitt. Math. Ges. Hamburg 34/2014, 21, 22 ff.
666 *Federrath,* Mitt. Math. Ges. Hamburg 34/2014, 21, 23.
667 *Federrath,* Mitt. Math. Ges. Hamburg 34/2014, 21, 23.
668 *Auernhammer -Kramer/Meints,* DSGVO BDSG, Art. 32 Rn. 32.
669 *Auernhammer -Kramer/Meints,* DSGVO BDSG, Art. 32 Rn. 32.
670 *Auernhammer -Kramer/Meints,* DSGVO BDSG, Art. 32 Rn. 32.
671 *Auernhammer -Kramer/Meints,* DSGVO BDSG, Art. 32 Rn. 22.

4.1.3 Weitere Eigenschaften bzw. Schutzziele der Informationssicherheit

Neben den primären Schutzzielen der Informationssicherheit gibt es weitere Schutzziele, die sowohl Daten als auch Systeme vor bösartigen Angriffen schützen.

4.1.3.1 Authentizität / „Authenticity“ und Authentifizierung / „Authentication“

Authentizität ist ,,die Eigenschaft einer Entität, das zu sein, was sie vorgibt zu sein“.[672] Sie bezieht sich also auf ,,die Echtheit und Überprüfbarkeit von Daten.“[673] Angenommen, Person A behauptet, das Konto B gehöre ihr. Dies muss IT-technisch durch Authentifizierung überprüft werden.

Authentifizierung ist der Prozess der Identifizierung und Verifizierung einer Einheit oder eines erforderlichen Merkmals einer Einheit.[674] Der Begriff wird für die Überprüfung der Identität von Personen, für IT-Komponenten oder Anwendungen verwendet.[675] Bei der Identitätsüberprüfung bzw. Authentifizierung wird die Verbindung zwischen dem Benutzer und seiner digitalen ID sichergestellt, z. B. durch die Eingabe eines nur dem Nutzer bekannten Passworts.[676] Wenn Person A dem Konto B das richtige Passwort eingibt, kann er es problemlos benutzen.

4.1.3.2 Nichtabstreitbarkeit / „Non-Repudiation“ und Verbindlichkeit

Bei der Nichtabstreitbarkeit steht die Beweisbarkeit gegenüber Dritten im Vordergrund.[677] Damit soll sichergestellt werden, dass das Senden und Empfangen von Daten nicht verweigert werden kann.[678] [679] Die Sicherheitsziele Nichtabstreitbarkeit und Authentizität werden unter Verbindlichkeit zusammengefasst.[680]

672 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 5.
673 Was ist Informationssicherheit - eine Definition, abrufbar: https://www.haufe.de/compliance/management-praxis/informationssicherheit/was-ist-informationssicherheit-eine-defintion_230130_483132.html, zuletzt abgerufen am 04.08.2023.
674 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 5.
675 Grundlegende Begriffe und Schutzziele der Informationssicherheit, abrufbar: https://www.rst-beratung.de/themen/informationssicherheit, zuletzt abgerufen am 04.08.2023.
676 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 5.
677 Grundlegende Begriffe und Schutzziele der Informationssicherheit, abrufbar: https://www.rst-beratung.de/themen/informationssicherheit, zuletzt abgerufen am 04.08.2023.
678 Grundlegende Begriffe und Schutzziele der Informationssicherheit, abrufbar: https://www.rst-beratung.de/themen/informationssicherheit, zuletzt abgerufen am 04.08.2023.
679 Personen können aus einer Vielzahl von Gründen leugnen, bestimmte Handlungen begangen zu haben. Wenn sie z.B. gegen Anweisungen oder Gesetze verstoßen oder einen Termin vergessen haben, werden sie leugnen, dass sie benachrichtigt wurden. S.: BSI, Elementare Gefährdungen, S. 40.
680 Grundlegende Begriffe und Schutzziele der Informationssicherheit, abrufbar: https://www.rst-beratung.de/themen/informationssicherheit, zuletzt abgerufen am 04.08.2023.

Die Verbindlichkeit bezieht sich auf den Prozess, durch den das Eintreten eines Ereignisses bzw. einer Handlung und die dafür verantwortliche Stelle zweifelsfrei nachgewiesen werden können.[681] Dadurch wird sichergestellt, dass jeglicher Datenzugriff nachvollziehbar ist.[682] Im Falle der Datenübertragung bedeutet dies, dass die Quelle der Information ihre Identität nachgewiesen hat und das Erhalten der Nachricht nicht bestritten werden kann.[683]

Ein Beispiel für diese Schutzziele ist das Identitätsmanagement, bei dem Aktionen immer deutlichen Identitäten zugewiesen sind und den Benutzern nachvollziehbar sowie verbindlich zugeordnet werden können, so dass deren Verweigerung nicht möglich ist.[684]

4.1.3.3 Verlässlichkeit / „Reliability“

Der Begriff ,,Verlässlichkeit“ bezeichnet die Eigenschaft, ,,ein konsistentes und bestimmungsgemäßes Verhalten zu zeigen“ und entsprechende Ergebnisse zu beschaffen.[685] Da sich dieses Schutzziel auf die technische Funktionalität von IT-Systemen sowie -Komponenten bezieht, kann es in Fällen mit schwerwiegenden Abhängigkeiten von IT-Systemen auch beim Schutzziel der Verfügbarkeit berücksichtigt werden.[686]

Die Verlässlichkeit wird verletzt, wenn z. B. eine Verschlüsselungssoftware jede dritte Nachricht nicht verschlüsselt und auf diese Weise überträgt.[687] In einem solchen Fall ist die Verlässlichkeit nicht mehr gewährleistet, und es ist leichter, diese Nachrichten zu manipulieren als die anderen, die nach Stand der Technik ausreichend verschlüsselt sind.

4.1.3.4 Zurechenbarkeit / „Accountability“

Die Verantwortung, Vermögenswerte zuzuweisen oder zu übertragen, sind die Grundsätze des Standards, die nur dann umgesetzt werden können, wenn es Mechanismen zur technischen Umsetzung der Zurechenbarkeit bzw. Rechenschaftspflicht gibt.[688] Durch die Zurechenbarkeit wird die Verantwortlichkeit einer Einheit für ihre Entscheidungen sowie ihre Handlungen realisiert.[689]

---

681 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 5.
682 Was ist Informationssicherheit - eine Definition, abrufbar: https://www.haufe.de/compliance/management-praxis/informationssicherheit/was-ist-informationssicherheit-eine-defintion_230130_483132.html, zuletzt abgerufen am 04.08.2023.
683 Grundlegende Begriffe und Schutzziele der Informationssicherheit, abrufbar: https://www.rst-beratung.de/themen/informationssicherheit, zuletzt abgerufen am 04.08.2023.
684 Grundlegende Begriffe und Schutzziele der Informationssicherheit, abrufbar: https://www.rst-beratung.de/themen/informationssicherheit, zuletzt abgerufen am 04.08.2023.
685 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 5.
686 Grundlegende Begriffe und Schutzziele der Informationssicherheit, abrufbar: https://www.rst-beratung.de/themen/informationssicherheit, zuletzt abgerufen am 04.08.2023.
687 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 5.
688 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 6.
689 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 6.

Ein Beispiel für dieses Schutzziel ist die Zuordnung einer sicherheitsrelevanten Handlung zu einer Person, die die entsprechende Handlung ausgeführt hat.[690] Wenn Person A für die Handlung B verantwortlich ist und dies klar geregelt sowie dokumentiert ist, ist es einfacher, die Zurechenbarkeit in dem Prozess zu ermöglichen.

690 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 6.

4.2 Risiko-Beurteilung

Um die Schutzziele der Informationssicherheit gewähren zu können, sollte zunächst die Risiko-Beurteilung durchgeführt werden. Bei dem internationalen Datentransfer findet dies am besten nach dem internationalen Standard wie ISO/IEC 27001 statt. Dazu gibt jedoch rechtliche Aspekte, die in der EU und in den USA teilweise unterschiedlich ausgeprägt sind.

4.2.1 Internationaler Standard

Die Risiko-Beurteilung ist im Zusammenhang mit dem Risikomanagement zu betrachten. In Abschn. 6 ISO/IEC 27001[691] wird dieser Aspekt in der ersten Planungsphase des PDCA-Zyklus (planen / ,,plan“, umsetzen / ,,do“, überprüfen / ,,check“ und handeln bzw. verbessern / ,,act“; PDCA) bei der Einführung eines ISMS behandelt (s. → S.152-153).[692]

Die Risikobeurteilung besteht aus drei Phasen, nämlich 1. die Risikoidentifikation, 2. die Risikoanalyse und 3. die Risikoabstufung bzw. Risikobewertung.[693] Die **Risikoidentifikation** umfasst die Erkennung und Beschreibung eines Risikos sowie die Korrelation von Schwachstellen und Bedrohungen im Zusammenhang mit den Werten.[694] Die Identifizierung von Datenschutz-Risiken beantwortet die Fragen: 1. Welchen Schaden die Datenverarbeitung für die betroffene Person haben kann; 2. welche Ereignisse diesen Schaden verursachen können und 3. welche Handlungen bzw. Umstände diese Ereignisse bewirken können.[695]

Bei der **Risikoanalyse** werden für das identifizierte Risiko eine Eintrittswahrscheinlichkeit und mögliche Auswirkungen / Schwere bzw. Schaden bei Risikoeintritt ermittelt, was quantitativ oder qualitativ erfolgen kann.[696]

Die Eintrittswahrscheinlichkeit beschreibt die Wahrscheinlichkeit, mit der ein bestimmtes Ereignis eintritt und die Wahrscheinlichkeit, mit der Folgeschäden auftreten können.[697] Wird beispielsweise die sexuelle Ausrichtung einer Person ungewollt offengelegt, sollte als Wahrscheinlichkeit diese Offenlegung sowie die daraus resultierender Schäden betrachtet werden.[698]

---

691 Es gibt weitere Normen, die sich ausschließlich mit dem Thema ,,Risiko“ befassen. Das Cybersecurity Framework des NIST ist eines der bekanntesten Rahmenwerke zur Risikobewertung. Es bietet einen strukturierten Ansatz für Organisationen, um ihre Cybersicherheitsrisiken zu bewerten und Maßnahmen zur Verringerung dieser Risiken zu priorisieren. S.: Cybersecurity Risk Assessments, abrufbar: https://www.itgovernanceusa.com/cyber-security-risk-assessments, zuletzt abgerufen am 04.08.2023. Das NIST CSF ist eine Reihe von Richtlinien, die Unternehmen bei der Verwaltung ihrer Cybersicherheitsrisiken unterstützen. S.: Guide to the NIST CSF (Cybersecurity Framework), abrufbar: https://www.itgovernanceusa.com/nist-cybersecurity-framework, zuletzt abgerufen am 04.08.2023.

692 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 46.

693 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 50.

694 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 50.

695 DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, 26.04.2018, S. 2.

696 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 50.

697 DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, 26.04.2018, S. 4.

698 DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, 26.04.2018, S. 4.

Die quantitative Analyse umfasst die Multiplizierung der Eintrittswahrscheinlichkeit mit dem Auswirkungswert (z. B. Prozent- und Eurozahlen).[699] Die qualitativen Analyse umfasst die Bestimmung des Risikoniveaus durch eine Risikomatrix.[700]

Bei der **Risikobewertung** wird festgelegt, ob das Risiko, das zu analysieren ist, die Akzeptanzkriterien erfüllt, und es wird eine Priorität vergeben, um die Bedeutung der Risikobehandlung im Vergleich zu anderen identifizierten Risiken anzugeben.[701] Mit der Bewertungsstufen („gering", „mittel", „hoch") und einer Multiplikation von „Eintrittswahrscheinlichkeit x Schwere" ergibt sich das Gesamtrisiko.[702]

4.2.2 Risiko-Beurteilung des rechtmäßigen Zugangs durch ausländische Behörden

Zur besseren Veranschaulichung des oben beschriebenen Themas wird die Beispielvorlage für die Risikobeurteilung von iapp (International Association of Privacy Professionals) bei rechtmäßigem Zugang durch ausländische Behörden am Beispiel des Cloud Computing[703] präsentiert. Der Bogen ist für die Beurteilung eines einzelnen Landes sowie für mehrere Länder gedacht und kann sowohl in der EU als auch in den USA verwendet werden.

Der **erste Schritt** besteht darin, die Ausgangslage für die Risiko-Beurteilung festzulegen. Hierbei sind folgende Punkte zu berücksichtigen: 1. Die vor staatlichem Zugriff zu schützenden Daten, 2. Cloud-Anwendung, mit der die Daten verarbeitet werden, 3. Betrachtungszeitraum für die Risikobeurteilung und 4. relevantes ausländisches Recht.

Der **zweite Schritt** besteht darin, die Wahrscheinlichkeit zu ermitteln, dass eine ausländische Behörde einen Anspruch auf die Daten hat und diesen gegen den Anbieter durchsetzen würde. Hierbei ist u. a. die Zahl der Fälle pro Jahr zu ermitteln, in denen eine Behörde in dem betreffenden Land während des Berichtszeitraums schätzungsweise versucht, einschlägige Daten mit legalen Mitteln zu beschaffen.

Als **dritter Schritt** ist die Wahrscheinlichkeit festzulegen, dass der Anspruch erfolgreich durchgesetzt wird. Hierbei sind Art. 18 Abs. 1 CCC (Convention of Cybercrime von 23.11.2001) und analoge Bestimmungen wie CLOUD Act Anforderungen für die Risiko-Beurteilung als Rechtsgrundlage heranzuziehen.

699 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 50.
700 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 50.
701 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 51.
702 Risiko-Beurteilung nach DSGVO in der Praxis, abrufbar: https://www.datenschutz-praxis.de/grundlagen/risikobeurteilung-nach-dsgvo-in-der-praxis/, zuletzt abgerufen am 04.08.2023.
703 Cloud-Computing ist ein Trend in der Datenverarbeitung, bei dem Datenhardware und -software über ein virtuelles Netzwerk zusammenarbeiten, um Nutzern überall auf der Welt On-Demand-Selbstbedienung zu bieten. S.: *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 89.

In **Schritt vier** wird die Wahrscheinlichkeit eines rechtmäßigen Zugangs durch eine ausländische Massenüberwachung bestimmt. Dabei sind Abschn. 702 FISA sowie E. O. 12333 bei der Risiko-Beurteilung heranzuziehen.

Im letzten, **fünften Schritt** soll eine Gesamtbewertung vorgelegt werden. Dabei sind folgende Aspekte zu berücksichtigen: 1. Wahrscheinlichkeit der Stellung des Ersuchens, 2. Wahrscheinlichkeit des rechtmäßigen Zugriffs ausländischer Behörden trotz Gegenmaßnahmen und weiterer rechtmäßiger Zugriff „durch einen ausländischen Nachrichtendienst ohne Rechtsweg-Garantie“ trotz Gegenmaßnahmen.[704]

Cloud-Computing: Risikobeurteilung eines Lawful Access durch ausländische Behörden — iapp — Eine Version als DSGVO TIA gibt es hier: https://bit.ly/2Wz1b0e

Bogen zur Beurteilung eines einzelnen Lands — Autor: David Rosenthal (Originalversion unter www.rosenthal.ch) *(Lizenz: Siehe unten)*

Version 5.04 (1. September 2021) (grün Text = ein Beispiel für die Schweiz)

Schritt 1: Ausgangslage der Risikobeurteilung definieren

a)	Unternehmen:	XYZ AG		Datum:	[Datum]
b)	Daten, die vor dem Behördenzugriff zu schützen sind und um die es hier geht:	Kundendaten		Mitwirkende:	[Namen; für die Prozentwerte sollte optimalerweise das Mittel der Schätzung jedes Mitwirkenden verwendet werden; die Musterwerte vorher löschen. Siehe "Delphi" rechts]
c)	Cloud-Anwendung, mit welcher die Daten bearbeitet werden sollen:[3)]	ACME CloudOffice		Rechtsberater:	[Name]
d)	Betrachtungszeitraum der Risikobeurteilung in Jahren:	5		Verantwortlich:	[Name]
e)	Relevante ausländische Rechtsordnung:	USA			

Schritt 2: Wahrscheinlichkeit, dass eine ausländische Behörde Anspruch auf die Daten hat und ihn gegen den Provider durchsetzen will[1)]

		Wahrscheinlichkeit pro Fall* **	Fälle pro Jahr	Fälle verbleibend	Begründung
a)	Anzahl der Fälle pro Jahr, in welchen eine Behörde im Land im Betrachtungszeitraum schätzungsweise versuchen wird, auf dem Rechtsweg an relevante Daten zu gelangen[2)]		0.50		*Wir hatten in den letzten zehn Jahren nur gerade zwei Fälle, in welchen ausländische Behörden von uns Daten verlangt haben, und sie betrafen nur in einem Fall die hier relevanten Daten. Selbst bei konservativer Betrachtung gehen wir von diesem Land nicht mehr als einem Fall alle zwei Jahre aus.*
b)	Anteil der Fälle, in welchen die Herausgabe der Verfolgung von Fällen dient, die im betreffenden Staat einen Herausgabebefehl grundsätzlich auch gegenüber einem Provider erlauben	25%	0.13		*Wir gehen davon aus, dass die grosse Mehrheit der Fälle nicht schwerwiegende Straftaten, sondern aufsichts- und zivilrechtliche Streitigkeiten betreffen, welche im Rahmen des US CLOUD Act und Stored Communications Act keine Herausgabebefehle an Provider erlauben.*
c)	Wahrscheinlichkeit, dass es in den verbleibenden Fällen gelingt, die Behörde nach ihrem eigenen Recht oder sonst von ihrem Vorhaben, an die Daten im Klartext zu gelangen, abzubringen[3)]	20%	0.10		*In den meisten Fällen werden wir nicht in der Lage sein, uns nach US-Recht gegen die Herausgabe zu wehren. In seltenen Fällen wird es uns gelingen, die Behörde mit geschwärzten Daten zu befriedigen.*
d)	Wahrscheinlichkeit, dass in den verbleibenden Fällen die Daten in der einen oder anderen Weise geliefert werden (z.B. mit Einwilligung oder über Rechts- oder Amtshilfe)[4)]	75%	0.03		*In den hier relevanten Fällen der Verfolgung von schweren Straftaten wird typischerweise auch die Rechtshilfe offenstehen. Sie wird für die ausländische Behörde in der Regel einfacher sein als den Zugriff über den Provider zu versuchen.*
e)	Wahrscheinlichkeit, dass die Behörde in den verbleibenden Fällen die Daten trotzdem für so wichtig erachtet, dass sie einen anderen Weg suchen wird, um an sie heranzukommen	50%	0.01	0.01	*Die Durchsetzung eines Lawful Access über den Provider zwecks Zugriff auf Daten eines seiner Unternehmenskunden (wo er Auftragsbearbeiter ist) ist wesentlich schwieriger als im Falle von Daten von Privatpersonen (wo er Verantwortlicher ist). Sie dauert zudem länge. Daher glauben wir, dass die Behörden diese Mühe nur in besonders wichtigen Fällen auf sich nehmen werden, was die Anzahl der relevanten Fälle weiter senkt.*

Anzahl der Fälle pro Jahr, in welchen sich die Frage eines lawful access durch eine ausländische Behörde stellt	0.01
Anzahl Fälle im Betrachtungszeitraum	0.06

Schritt 3: Wahrscheinlichkeit, dass eine ausländische Behörde den Anspruch über den Provider erfolgreich durchsetzt

Für die vorliegende Beurteilung herangezogene Rechtsgrundlage:	Art. 18 Abs. 1 Cybercrime Convention (CCC) und analoge Bestimmungen, wie z.B. im US CLOUD Act umgesetzt

Abbildung 4.2.2. Auszug des Fragebogens zur Risikobeurteilung.

Quelle: iapp, Transfer Impact Assessment Templates, https://iapp.org/resources/article/transfer-impact-assessment-templates/.

704 Diese fünf Schritte sind im Fragebogen beschrieben, der unter dem folgenden Link als Excel-Datei verfügbar ist. S.: Transfer Impact Assessment Templates: Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities, abrufbar: https://iapp.org/resources/article/transfer-impact-assessment-templates/, zuletzt abgerufen am 04.08.2023.

4.2.3 Risiko-Beurteilung nach dem EU-Datenschutzrecht

Die DSGVO verfolgt einen risikobasierten Ansatz.[705] Um diesen umzusetzen, muss eine Risikoanalyse durchgeführt werden, auf die sich die entsprechenden Datenschutzmaßnahmen stützen sollten.[706] Nach ErwGr. 75 DSGVO ist eine Verarbeitung risikobehaftet, wenn sie dem Betroffenen einen materiellen oder immateriellen Schaden zufügt (z. B. Diskriminierung oder Identitätsdiebstahl).[707] Um die Sicherheit aufrechtzuerhalten und eine gegen die DSGVO verstoßende Verarbeitung zu verhindern, sollte der Verantwortliche bzw. der Auftragsverarbeiter laut ErwGr. 83 DSGVO die Risiken ermitteln, die mit der Verarbeitung verbunden sind und Maßnahmen zu deren Eindämmung ergreifen.[708]

Nach der Ermittlung / Identifizierung der Risiken müssen sie analysiert werden. Die Verpflichtung zur Durchführung einer Risikoanalyse entsteht mittelbar aus Art. 32 DSGVO, wonach sich die Sicherheitsmaßnahmen am Risiko orientieren müssen.[709] Dementsprechend ist eine Risikoanalyse durchzuführen, um u. a. die technische und organisatorische Maßnahmen (TOM) entsprechend dem Risikoprofil auszuwählen oder der Rechenschaftspflicht des Verantwortlichen nachzukommen.[710]

Der Begriff **Datenschutz-Risiko** ist in der DSGVO nicht definiert.[711] Laut DSK (Datenschutzkonferenz) kann diese Definition nach den ErwGr. 75 und 94 S. 2 DSGVO abgeleitet werden: *„Ein Risiko im Sinne der DS-GVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann.“*[712]

705 Risikoanalyse im Datenschutz, abrufbar: https://www.datenschutzexperte.de/datenschutz-risikoanalyse/, zuletzt abgerufen am 04.08.2023.
706 Rechenschaftspflichten bei der Datenverarbeitung, abrufbar: https://www.activemind.de/magazin/rechenschaftspflicht-dsgvo/, zuletzt abgerufen am 04.08.2023.
707 *Auernhammer -Brüggemann*, DSGVO BDSG, Art. 25 Rn. 18.
708 *Auernhammer -Kramer*, DSGVO BDSG, S. 475.
709 Muster für eine Risikoanalyse nach DSGVO, abrufbar: https://dsgvo-vorlagen.de/muster-fuer-eine-datenschutz-folgenabschaetzung-dsfs-nach-dsgvo, zuletzt abgerufen am 04.08.2023.
710 Muster für eine Risikoanalyse nach DSGVO, abrufbar: https://dsgvo-vorlagen.de/muster-fuer-eine-datenschutz-folgenabschaetzung-dsfs-nach-dsgvo, zuletzt abgerufen am 04.08.2023.
711 Risikoanalyse im Datenschutz, abrufbar: https://www.datenschutzexperte.de/datenschutz-risikoanalyse/, zuletzt abgerufen am 04.08.2023.
712 DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, 26.04.2018, S. 1.

Eine DSGVO-Risikoanalyse bedeutet eine Beurteilung, ob ein Risiko für die Rechte und Freiheiten des Betroffenen durch eine unrichtige oder fehlerhafte Datenverarbeitung entstehen kann. Aus Betroffenensicht müssen alle Risiken kontinuierlich ermittelt, beurteilt und schlussendlich dokumentiert werden. Die Besonderheit einer Datenschutz-Risikoanalyse liegt im Gegensatz zur herkömmlichen Risikoanalyse in der Fokussierung auf den Betroffenen.[713] *„Die Risikobeurteilung muss sozusagen durch dessen Brille erfolgen.“*[714]

Eine Datenschutz-Risikoanalyse, wie eine herkömmliche Risikoanalyse zur Beurteilung, besteht aus zwei Dimensionen: 1. Die Wahrscheinlichkeit des Eintretens des Ereignisses sowie der Folgeschäden und 2. die Schwere des Schadens.[715] Nach ErwGr. 76 S. 1 DSGVO sind Eintrittswahrscheinlichkeit und die Schwere des Risikos zu bestimmen, wobei insbesondere die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung zu berücksichtigen sind.

Nach ErwGr. 75 S. 1 Hs. 1 DSGVO sind physische, materielle und immaterielle Schäden voneinander zu unterscheiden. Schäden können aus planmäßiger Verarbeitung, Eigenverschulden oder Fremdschäden (z. B. Naturkatastrophe oder Hardwaredefekt) entstehen.[716] In ErwGr. 75 DSGVO werden einige Schäden ausdrücklich erwähnt, nämlich u. a. Diskriminierung, Identitätsdiebstahl bzw. -betrug, finanzieller Verluste oder Rufschädigung.

Insbesondere die folgenden Faktoren sind bei der Bestimmung der Schwere des Schadens zu berücksichtigen: 1. Die Verarbeitung besonderer Kategorien personenbezogener Daten oder personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten; 2. die Verarbeitung personenbezogener Daten von Personengruppen, die eines besonderen Schutzes bedürfen, wie z. B. Kinder; 3. die automatisierte Verarbeitung einschließlich Profiling; 4. die Verarbeitung, die eine systematische Überwachung ermöglicht; 5. die Anzahl der Betroffenen sowie Datensätze und 6. der geografische Erfassungsbereich der verarbeiteten Daten.[717]

Bei der Beurteilung der Schwere eines Betroffenenrisikos (Auswirkung) sind die Einflussfaktoren als gesundheitliche, finanzielle und / oder soziale Auswirkungen sowie Auswirkungen auf das informationelle Selbstbestimmungsrecht zu klassifizieren.[718]

---

713 Die in diesem Abschnitt dargestellte Aussage befindet sich in dem folgenden Artikel. S.: Risikoanalyse im Datenschutz, abrufbar: https://www.datenschutzexperte.de/datenschutz-risikoanalyse/, zuletzt abgerufen am 04.08.2023.

714 Risiko-Beurteilung nach DSGVO in der Praxis, abrufbar: https://www.datenschutz-praxis.de/grundlagen/risikobeurteilung-nach-dsgvo-in-der-praxis/, zuletzt abgerufen am 04.08.2023.

715 DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, 26.04.2018, S. 1.

716 DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, 26.04.2018, S. 2.

717 DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, 26.04.2018, S. 5.

718 Risiko-Beurteilung nach DSGVO in der Praxis, abrufbar: https://www.datenschutz-praxis.de/grundlagen/risikobeurteilung-nach-dsgvo-in-der-praxis/, zuletzt abgerufen am 04.08.2023.

Nach der Bestimmung der Eintrittswahrscheinlichkeit und der Schwere der möglichen Schäden müssen diese in die Risikostufen „geringes Risiko“, „Risiko“ und „hohes Risiko“ eingeteilt werden.[719] Diese Abstufung wird in der DSGVO nicht im Detail beschrieben.[720] Die DSGVO verwendet die Begriffe „**Risiko**“ („nicht zu einem Risiko […] führt“ – Art. 27 Abs. 2 lit. a) und Art. 33 Abs. 1 DSGVO) und „hohes Risiko“ („ein Risiko oder ein hohes Risiko birgt“ – ErwGr. 76 DSGVO),[721] aber kein „geringes Risiko“. Da es keine völlig risikofreie Verarbeitung gibt, wird der Ausdruck „nicht zu einem Risiko [...]“ als „zu einem geringen Risiko“ verstanden.[722]

Das Risiko der Verarbeitung ist durch Abhilfemaßnahmen zu mindern, die grundsätzlich durch TOMs (technisch-organisatorische Maßnahmen) erreicht werden.[723] Diese Maßnahmen sollten nach dem Stand der Technik konzipiert worden sein und die Rechte und Freiheiten des Betroffenen sicherstellen.[724] Sie sind im Hinblick auf den Schutz des Betroffenen und nicht der für die Verarbeitung Verantwortlichen zu bewerten[725] und müssen für jede betroffene Person einzeln festgelegt werden.[726]

Sind die Abhilfemaßnahmen umgesetzt worden, müssen sie auf die Effektivität geprüft und systematisch überwacht werden, da bei der Umsetzung der Maßnahmen herausgestellt werden kann, dass es noch andere Risiken gibt, die ebenfalls angegangen werden müssen.[727] Das Risiko, das nach der Umsetzung der TOM verbleibt, wird als **Restrisiko** beschrieben.[728] Wird dies als hoch eingestuft, besteht nach Art. 36 DSGVO eine Verpflichtung zur vorherigen Konsultation.[729]

719 DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, 26.04.2018, S. 2.
720 DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, 26.04.2018, S. 2.
721 DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, 26.04.2018, S. 2.
722 DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, 26.04.2018, S. 2.
723 DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, 26.04.2018, S. 6
724 DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, 26.04.2018, S. 6.
725 DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, 26.04.2018, S. 6.
726 *Auernhammer -Brüggemann*, DSGVO BDSG, Art. 25 Rn. 18.
727 DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, 26.04.2018, S. 6.
728 DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, 26.04.2018, S. 6.
729 DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, 26.04.2018, S. 6.

4.2.4 Risiko-Beurteilung nach dem US-Datenschutzrecht

Das Thema Risiko ist in den USA bekannt und wird in vielen Bereichen angewendet. Beispielsweise setzen lokale, staatliche und bundesstaatliche Strafverfolgungsbehörden zunehmend auf datengestützte Entscheidungsfindung bei der Überwachung, Verwaltung und Behandlung von Personen, die mit der Justiz zu tun haben.[730] Ein Eckpfeiler dieser Beurteilung ist die Risiko-Beurteilung, die in verschiedenen Phasen des Gerichtsverfahrens durchgeführt wird, um z. B. Entscheidungen über die Freilassung oder die Inhaftierung zu treffen.[731] Ein risikobasierter Ansatz ist auch laut NIST im Allgemeinen der Schlüssel zu effektiver Sicherheit.[732] Das Risikomanagement ist ein Grundprinzip der Cybersicherheit,[733] das natürlich eine Risiko-Beurteilung beinhaltet.

Die rechtliche Verpflichtung zur Durchführung einer Risiko-Beurteilung ist in **HIPAA, PCI, FISMA, Sarbanes-Oxley und Gramm-Leach-Bliley** vorgeschrieben.[734] Sie regeln, wie die verschiedenen Datentypen und die Systeme, die diese Daten verwalten, zu sichern sind, und verlangen regelmäßige Bewertungen der Sicherheitslage.[735]

Diese Gesetze sind jedoch sektorspezifisch und daher nicht in allen Bereichen des Datenschutzes oder der Informationssicherheit verbindlich. Die Risikomanagementpraktiken der US-Regierung im Bereich der Cybersicherheit basieren auf dem **FISMA** (Federal Information Security Management Act) und dem damit verbundenen **RMF** (Risk Management Framework), das von NIST entwickelt wurde.[736]

730 What Is Risk Assessment, abrufbar: https://bja.ojp.gov/program/psrac/basics/what-is-risk-assessment, zuletzt abgerufen am 04.08.2023.

731 What Is Risk Assessment, abrufbar: https://bja.ojp.gov/program/psrac/basics/what-is-risk-assessment, zuletzt abgerufen am 04.08.2023.

732 National Institute of Standards and Technology (NIST), abrufbar: https://www.itgovernanceusa.com/nist, zuletzt abgerufen am 04.08.2023.

733 *Lipner/Lampson W.,* Risk Management and the Cybersecurity of the U.S.: Government Input to the Commission on Enhancing National Cybersecurity 1, 1.

734 *Randall/Kroll,* US LAW, Fall/Winter 2017.

735 *Randall/Kroll,* US LAW, Fall/Winter 2017.

736 *Lipner/Lampson,* Risk Management and the Cybersecurity of the U.S.: Government Input to the Commission on Enhancing National Cybersecurity 1, 1-2.

Obwohl die Durchführung der Risiko-Beurteilung nicht in allen Bereichen gesetzlich vorgeschrieben ist, bemühen sich viele Unternehmen dennoch, diese durchzuführen. Viele Firmenkunden verlangen von den Unternehmen, in ihren Ausschreibungen ausdrücklich anzugeben, welche Datensicherheitsprogramme sie eingeführt haben, bevor sie ihre Dienste in Anspruch nehmen.[737] Es ist als ein sehr wichtiges Instrument angenommen, das in jedem Bereich eingesetzt werden soll.[738] So haben beispielsweise große Finanzinstitute wie J.P. Morgan Chase & Co, Bank of America Corp. und UBS AG externe Anwaltskanzleien einer genaueren Prüfung ihre Cybersicherheit unterzogen.[739]

Der Begriff „Risiko" wird im CLOUD Act einmal bei der Verpflichtung des Anbieters während des eingeleiteten Gerichtsverfahrens erwähnt. Wenn ein Anbieter nach dem CLOUD Act verpflichtet ist, den Inhalt der drahtgebundenen oder elektronischen Kommunikation eines Teilnehmers oder Kunden vor Gericht offenzulegen, kann er einen Antrag nach Abschn. 103 (a), § 2713 (B) (2) (ii) CLOUD Act auf Änderung oder Aufhebung des Verfahrens stellen, wenn er davon ausgeht, dass die geforderte Offenlegung ein erhebliches Risiko schaffen würde, dass der Anbieter die Gesetze einer qualifizierten ausländischen Regierung verletzt.

Der CLOUD Act definiert nicht, was ein Risiko bedeutet oder wie ein erhebliches Risiko zu bewerten ist. Unter der Risiko-Beurteilung der Cybersicherheit ist im Grunde genommen eine Beurteilung der Fähigkeit einer Organisation zu verstehen, ihre Informationen und Informationssysteme vor Cyberbedrohungen zu schützen.[740] Diese Beurteilung ist am besten mit den richtigen Ansprechpartnern und den in der Organisation bestehenden Richtlinien durchzuführen.[741]

Der Zweck einer Cybersicherheitsrisiko-Beurteilung besteht darin, die Risiken für Informationen und Informationssysteme zu identifizieren, zu bewerten und nach Prioritäten zu ordnen. Dies hilft einer Organisation wiederum, Bereiche zu identifizieren und zu priorisieren, in denen ihr Cybersecurity-Programm verbessert werden könnte. Außerdem hilft diese Beurteilung der Organisation, ihre Risiken den Interessengruppen mitzuteilen und fundierte Entscheidungen über die Zuweisung von Ressourcen zur Verringerung dieser Risiken zu treffen.[742]

737 *Randall/ Kroll*, US LAW, Fall/Winter 2017.

738 Diese Meinung wurde auf der Global GRC, Data Privacy & Cyber Security ConfEx am 31.05.2023 in NY/USA geäußert.

739 *Randall/Kroll*, US LAW, Fall/Winter 2017.

740 Cybersecurity Risk Assessments, abrufbar: https://www.itgovernanceusa.com/cyber-security-risk-assessments, zuletzt abgerufen am 04.08.2023.

741 Diese Meinung wurde auf der Global GRC, Data Privacy & Cyber Security ConfEx am 31.05.2023 in NY/USA geäußert.

742 Die Beschreibung des Zweckes der Cybersicherheitsrisiko-Beurteilung, die in dem Abschnitt beschrieben wird, findet sich in dem folgenden Artikel. S.: Cybersecurity Risk Assessments, abrufbar: https://www.itgovernanceusa.com/cyber-security-risk-assessments, zuletzt abgerufen am 04.08.2023.

Im Zusammenhang mit Cyber-Risiken erfordert eine Risiko-Beurteilung von Unternehmen folgende Aufgaben: 1. Bewertung von Netzwerkschwachstellen; 2. Empfehlungen zur Behebung potenzieller Schwachstellen; 3. Überprüfung der Cyber-Richtlinien und -Verfahren; und 4. Überprüfung des internen Netzwerks.[743]

Im Rahmen des FISMA und der RMF stufen die Behörden ihre Systeme auf der Grundlage einer Bewertung der Sensibilität der verarbeiteten Informationen und der möglichen Folgen eines Verlusts als niedrig, mittel oder hoch ein.[744] Sobald die Kategorie bestimmt wurde, wird von den Behörden erwartet, dass sie die für diese Kategorie erforderlichen Sicherheitsmaßnahmen gem. der NIST SP 800-53 (National Institute of Standards and Technology: Special Publication 800-53) umsetzen.[745]

Laut NIST SP 800-53, Rev. 5: 1.1 werden in der NIST SP 800-53 Maßnahmen für Systeme und Organisationen festgelegt und können in jeder Organisation bzw. jedem System implementiert werden, das Informationen verarbeitet, speichert oder überträgt. Die Verwendung dieser Maßnahmen ist nach NIST SP 800-53, Rev. 5: 1.1 für Informationssysteme des Bundes gem. dem Rundschreiben A-130 des Office of Management and Budget (OMB A-130) und den Bestimmungen des FISMA, der die Implementierung von Mindestmaßnahmen zum Schutz von Informationen und Informationssystemen des Bundes vorschreibt, obligatorisch.

4.2.5 Vergleich der Risiko-Beurteilung in der EU und in den USA

Das Thema Risiko-Beurteilung ist sowohl in der EU als auch in den USA bekannt und folgt im Wesentlichen nach einem internationalen Standard. Sie ist in der ISO/IEC 27001 geregelt und beinhaltet die drei Phasen, nämlich Risikoidentifikation, Risikoanalyse und Risikobewertung. Bei der Risikoidentifikation werden Schwachstellen und Bedrohungen erkannt und beschrieben. Die Risikoanalyse erfolgt durch die Bestimmung der Eintrittswahrscheinlichkeit und der Schwere. Schließlich wird das Ergebnis bzw. das Risiko als niedrig, mittel oder hoch eingestuft.

Wenn eine Organisation in der EU oder in den USA die Risiken vor der Datenverarbeitung einschätzen möchte, sollte sie die Risiko-Beurteilung auf diese Weise durchführen. Es ist jedoch wichtig zu beachten, dass ISO/IEC 27001 eine Norm und kein Gesetz ist. Daher ist es wichtig fest-zustellen, welche rechtlichen Anforderungen in dem betreffenden Bereich von einer Organisation erfüllt werden müssen.

743 *Randall/Kroll*, US LAW, Fall/Winter 2017.

744 *Lipner/Lampson*, Risk Management and the Cybersecurity of the U.S.: Government Input to the Commission on Enhancing National Cybersecurity 1, 2.

745 *Lipner/Lampson*, Risk Management and the Cybersecurity of the U.S.: Government Input to the Commission on Enhancing National Cybersecurity 1, 3.

In der EU ist das Thema „Risiko-Beurteilung“ mittelbar in der DSGVO geregelt. Die Verpflichtung zu ihrer Durchführung ergibt sich indirekt aus Art. 32 DSGVO, der entsprechende Sicherheitsmaßnahmen zu ihrer Beseitigung vorsieht. Darüber hinaus sind weitere Schritte wie die Risikoanalyse und die Bestimmungen über die Schwere des Schadens sowie dessen Bewertung in der DSGVO zu finden. All dies liefert umfangreiche Informationen darüber, was genau gesetzlich vorgeschrieben ist und wie diese Maßnahmen einzuhalten sind. Darüber hinaus werden damit personenbezogene Daten sowie die dahinter stehende Menschen in dem Mittelpunkt gestellt und nicht lediglich Daten (z. B. Betriebsgeheimnisse oder Konstruktionspläne).

In den USA ist das Thema ebenfalls gesetzlich geregelt. Es ist jedoch erwähnenswert, dass das Thema nicht in einem allumfassenden Gesetz sondern in den sektorspezifischen Vorschriften vorgeschrieben ist. Der CLOUD Act erwähnt den Begriff „Risiko“ einmal, definiert ihn aber nicht und sieht keine weiteren Schritte zur Durchführung der Risikoanalyse vor. Fällt die Risiko-Beurteilung nicht unter diese Gesetze, so wird sie nur von der Organisation durchgeführt, die selbst diese Bewertung vornehmen möchte, oder wenn eine andere Organisation dies verlangt. Zu erwähnen ist auch, dass die Risiko-Beurteilung von Daten und Informationen in den USA grundsätzlich Teil der Cybersicherheit ist, was wiederum bedeutet, dass personenbezogene Daten und die Menschen dahinter nicht im Mittelpunkt stehen.

Zusammenfassend lässt sich feststellen, dass in der EU mehr Wert auf die Risiko-Beurteilung gelegt wird als in den USA. Im weiteren Sinne lässt sich festlegen, dass die Risiken in Bezug auf die Wahrnehmung der Persönlichkeitsrechte in der EU besser gehandhabt werden als in den USA.

4.3 Präventive rechtliche Maßnahmen

Nach der Beurteilung der Risiken sollen diese behandelt bzw. beseitigt werden. Da dies im Hinblick auf den (internationalen) Datentransfer in Verbindung mit Hard- und Softwarekomponenten geschieht, ist neben den Begriffen „Datenschutz“ und „Informationssicherheit“ auch der Begriff „Cyber“ und „Cybersicherheit“ zu nennen. Cybersicherheit umfasst nach Art. 2 S. 1 Rechtsakt zur Cybersicherheit alle Aktivitäten, die zum Schutz von Netz- und Informationssystemen, der Nutzer dieser Systeme und anderer von Cyberbedrohungen betroffenen Personen erforderlich sind. Diese bedeutet, dass die Cybersicherheit durch den Schutz der Hardware- und Software-Komponenten die Nutzer dieser Komponenten schützen soll. Dies wiederum geschieht durch ordnungsgemäß umgesetzte rechtliche und normative Maßnahmen, die zum Teil unterschiedlich ausgeprägt sind.

4.3.1 Präventive rechtliche Maßnahmen nach dem europäischen Recht

Die DSGVO garantiert Cybersicherheit durch drei Dimensionen: Prävention, Detektion und Reaktion. Die Präventionsmaßnahmen müssen ihre Wirksamkeit beweisen und ihre Umsetzung belegen. Die Aufgabe der Detektion besteht darin, eine Verletzung der Sicherheit durch geeignete Maßnahmen festzustellen. Wenn ein Vorfall eingetreten ist, wird durch Reaktion festgelegt, wie der Verantwortliche auf die Sicherheitsverletzung reagieren soll.[746]

Geeignete Maßnahmen können alle Maßnahmen im Zusammenhang mit der Datenverarbeitung sein, die ein angemessenes Datenschutzniveau im Sinne der DSGVO in Bezug auf die betroffenen personenbezogenen Daten gewährleisten.[747] Diese Maßnahmen sollten ein Schutzniveau sicherstellen, das den mit der Datenverarbeitung verbundenen Risiken und der schützenswerte Datenart angemessen ist, wobei der Stand der Technik und die Umsetzungskosten zu berücksichtigen sind.[748] Die Risiken für die Ziele der Informationssicherheit, die IT-Systeme sowie die Geschäftsprozesse sind mit Hilfe von technischen und organisatorischen Maßnahmen (TOM) einzudämmen.[749]

746 Diese Dimensionen werden in dem folgenden Artikel beschrieben. S.: Aufgabe und Herausforderung des Datenschutzes, abrufbar: https://www.euroforum.de/datenschutz-kongress/aufgabe-und-herausforderung-des-datenschutzes/, zuletzt abgerufen am 04.08.2023.

747 *Voigt/von dem Bussche*, EU-Datenschutz-Grundverordnung (DSGVO), S. 48.

748 *Auernhammer*, DSGVO BDSG, S. 475 ff.

749 Aufgabe und Herausforderung des Datenschutzes, abrufbar: https://www.euroforum.de/datenschutz-kongress/aufgabe-und-herausforderung-des-datenschutzes/, zuletzt abgerufen am 04.08.2023.

Um die Rechte und Freiheiten natürlicher Personen bei der Datenverarbeitung zu schützen, ist es unerlässlich, angemessene TOM zu ergreifen und damit sicherzustellen, dass den Anforderungen der DSGVO nachgekommen wird.[750] TOM im Bereich Datenschutz sind verschiedene Vorkehrungen, die von dem Verantwortlichen in der Organisation zu treffen sind.[751]

Die Verpflichtungen aus Artt. 25 und 32 DSGVO sind eng miteinander verknüpft.[752] Artikel 25 DSGVO (Datenschutz durch Technikgestaltung / „Privacy by Design" bzw. „Data Protection by Design" und Datenschutz durch datenschutzfreundliche Voreinstellungen / „Privacy by Default" bzw. „Data Protection by Default") verlangt von den Unternehmen eine proaktive Gestaltung ihrer Verarbeitungen durch umfassende Datenschutz- und Sicherheitskonzepte, die sich nicht lediglich auf TOM beschränken, sondern ihnen einen weiten Ermessensspielraum bei der Umsetzung lassen und gleichzeitig wirtschaftliche Belange eines Unternehmens einbeziehen.[753]

TOM nach Art. 32 DSGVO (Sicherheit der Verarbeitung) sind integraler Bestandteil von Datenschutz- und Sicherheitskonzepten zur Minimierung von Haftungsrisiken.[754] Während der Datenschutz durch Technikgestaltung im Vorfeld von Verarbeitungstätigkeiten sicherzustellen ist, werden TOM während des Verarbeitungsprozesses getroffen.[755]

4.3.1.1 Privacy by Design und Privacy by Default

Die Grundsätze des Datenschutzes durch Technikgestaltung / „Privacy by Design" und des Datenschutzes durch datenschutzfreundliche Voreinstellungen / „Privacy by Default" gewährleisten, dass der Verantwortliche die DSGVO einhält, indem er seine interne Strategie feststellt und die erforderlichen Maßnahmen ergreift.[756] Diese Grundsätze verfolgen unterschiedliche Ziele: Der „Data Protection by Design" soll den Datenschutz stärken; der „Data Protection by Default" verbessert die Position des Betroffenen.[757]

750 *Auernhammer -Brüggemann*, DSGVO BDSG, S. 408.
751 Technisch organisatorische Maßnahmen (TOM), abrufbar: https://www.datenschutzexperte.de/technisch-organisatorische-massnahmen/, zuletzt abgerufen am 06.08.2023.
752 *Auernhammer -Brüggemann*, DSGVO BDSG, Art. 25 Rn. 2 und 7.
753 *Auernhammer -Brüggemann*, DSGVO BDSG, Art. 25 Rn. 2.
754 *Auernhammer -Brüggemann*, DSGVO BDSG, Art. 25 Rn. 2.
755 *Voigt/von dem Bussche*, EU-Datenschutz-Grundverordnung (DSGVO), S. 47.
756 *Auernhammer -Brüggemann*, DSGVO BDSG, S. 408.
757 *Auernhammer -Brüggemann*, DSGVO BDSG, Art. 32 Rn. 1.

Der Adressat des Art. 25 DSGVO ist der Verantwortliche, nicht jedoch der Hersteller bzw. der Anbieter der verwendeten Softwareprodukte oder Dienstleistungen, es sei denn dass der Verantwortliche und der Hersteller oder der Anbieter identisch sind.[758] Der Auftragsverarbeiter ist nur mittelbarer Adressat des Art. 25 DSGVO.[759] Nach Art. 32 Abs. 1 DSGVO im Vergleich mit Art. 28 Abs. 1 DSGVO ist der Auftragsverarbeiter verpflichtet, die dem Verarbeitungsrisiko angemessenen TOM zu ergreifen, allerdings nur gemeinsam mit dem Verantwortlichen.[760]

Das Prinzip des „Data Protection by Design" beruht auf der Idee eines komplementären Verhältnisses zwischen Recht und Technik, die sich gegenseitig ergänzen.[761] Der rechtliche Rahmen beeinflusst die Art und den Umfang der obligatorischen technischen Sicherheitsmaßnahmen, und die technische Sicherheit wiederum wirkt auf den rechtlichen Rahmen bei der Beurteilung der Rechtmäßigkeit der Datenverarbeitung ein.[762] Privacy by Design bedeutet, dass alle datenschutzrechtlichen Anforderungen bereits bei der Planung der Datenverarbeitung oder der Softwareerstellung berücksichtigt werden.[763]

Dem Prinzip des „Data Protection by Default" liegt die Idee zugrunde, dass die Souveränität der Betroffenen im Umgang mit den sie betreffenden Daten durch u. a. Gestaltungsmöglichkeiten gestärkt und damit der Bedarf an externer Kontrolle verringert werden soll.[764] Er erstreckt sich auf den gesamten Lebenszyklus eines Produkts bzw. einer Dienstleistung, d. h., dass er bereits in der Planungsphase angewandt und zu Beginn sowie während der gesamten Verarbeitungskette überprüft werden sollte.[765] Privacy by Default bedeutet, dass die datenschutzfreundlichen Einstellungen vor der Anwendung direkt im Tool vorgenommen werden können.[766]

758 *Paal/Pauly -Martini,* DSGVO BDSG, Art. 25 Rn. 25; *Auernhammer -Brüggemann,* DSGVO BDSG, Art. 32 Rn. 6.
759 *Auernhammer -Brüggemann*, DSGVO BDSG, Art. 32 Rn. 7.
760 *Auernhammer -Brüggemann*, DSGVO BDSG, Art. 32 Rn. 7.
761 *Auernhammer -Brüggemann*, DSGVO BDSG, S. 409.
762 *Auernhammer -Brüggemann*, DSGVO BDSG, S. 409 ff.
763 Interview mit Cornelia Sasse, im elektronischen Zusatzmaterial, Anlage 1, S. 3.
764 *Auernhammer -Brüggemann*, DSGVO BDSG, S. 410.
765 *Auernhammer -Brüggemann*, DSGVO BDSG, Art. 25 Rn. 9.
766 Interview mit Cornelia Sasse, im elektronischen Zusatzmaterial, Anlage 1, S. 3.

Bei datenschutzfreundlichen Voreinstellungen geht es im Wesentlichen darum, dass durch Voreinstellungen nur Daten verarbeitet werden, die für den jeweiligen konkreten Verarbeitungszweck unbedingt notwendig sind.[767] Nach Art. 25 Abs. 2 S. 1 DSGVO unterliegt die Auswahl der Voreinstellungen durch den Verantwortlichen dem Grundsatz der Zweckbindung gem. Art. 5 Abs. 1 lit. b) DSGVO.[768] Ein Produkt oder ein Dienst sollte bereits über die datenschutzfreundlichen Einstellungen und Komponenten (z. B. die Privatsphäreeinstellungen durch den Nutzer) verfügen, wenn der Nutzer es zum ersten Mal einschaltet oder aufruft.[769]

Zur wirksamen Umsetzung der allgemeinen Verarbeitungsgrundsätze nach Art. 5 DSGVO ist es notwendig zu prüfen, ob die getroffenen TOM angemessen sind.[770] Die folgenden Kriterien des Art. 25 Abs. 1 DSGVO sind dabei zu berücksichtigen: 1. Stand der Technik, 2. Implementierungskosten bzw. wirtschaftliche Interesse des Verantwortlichen bezüglich der Verarbeitung, 3. Art, Umfang, Umstände sowie die Zwecke der Verarbeitung und 4. Risiken für die Rechte und Freiheiten des Betroffenen, die mit der Verarbeitung verbunden sind.[771]

Gemäß Art. 25 DSGVO (ebenso wie nach Art. 24 DSGVO) ist der Verantwortliche verpflichtet, TOM zu ergreifen, um die DSGVO-Bestimmungen einzuhalten und die Rechte und Freiheiten natürlicher Personen zu gewährleisten.[772] Darüber hinaus gibt es erhebliche Querverweise auf die Verpflichtung der Datenschutz-Folgenabschätzung in Artt. 35 und 36 DSGVO, die ebenfalls auf dem Grundprinzip der Risiko-Beurteilung vor der Datenverarbeitung sowie der Verpflichtung, im Falle eines hohen Risikos risikominimierende Maßnahmen zu ergreifen und nachweisen zu können, beruht.[773]

Der Gesetzgeber hat die Maßnahmen bewusst nicht in Art. 25 DSGVO weiter spezifiziert, um Raum für technische Entwicklungen zu schaffen.[774] Um die oben dargestellte Grundsätze einzuhalten, sollten nach Art. 32 Abs. 1 DSGVO bestimmte Maßnahmen getroffen werden.[775] Diese werden im Folgenden detailliert beschrieben und analysiert.

767 *Auernhammer -Brüggemann*, DSGVO BDSG, Art. 25 Rn. 24.
768 *Auernhammer -Brüggemann*, DSGVO BDSG, Art. 25 Rn. 24.
769 *Kühling/Buchner -Hartung*, DSGVO/BDSG, Art. 25 Rn. 24 ff.
770 *Auernhammer -Brüggemann*, DSGVO BDSG, Art. 25 Rn. 10.
771 *Auernhammer -Brüggemann*, DSGVO BDSG, Art. 25 Rn. 10.
772 *Kühling/Buchner -Hartung*, DSGVO/BDSG, Art. 25 Rn. 10.
773 *Kühling/Buchner -Hartung*, DSGVO/BDSG, Art. 25 Rn. 10.
774 *Auernhammer -Brüggemann*, DSGVO BDSG, Art. 25 Rn. 13.
775 Technisch organisatorische Maßnahmen (TOM), abrufbar: https://www.datenschutzexperte.de/technisch-organisatorische-massnahmen/, zuletzt abgerufen am 06.08.2023.

4.3.1.2 Sicherheit der Verarbeitung nach EU-Vorschriften

Die Sicherheit der Verarbeitung im Sinne der DSGVO bezieht sich auf die Datensicherheit im Zusammenhang mit dem Schutz der personenbezogenen Daten.[776] Die Verletzung der Sicherheit wird als Verletzung des Schutzes personenbezogener Daten in Art. 4 Nr. 12 DSGVO definiert.[777] Datensicherheitsmaßnahmen stellt die DSGVO als technische und organisatorische Maßnahmen dar.[778]

Unter **technischen Maßnahmen** sind nach Artt. 24 und 25 DSGVO alle Vorkehrungen des physischen und logischen Zugangs-, der Zugriffs- und Übertragungskontrolle zu verstehen.[779] Dies bedeutet, dass eine geeignete physische Umgebung sowie Hard- und Software verwendet werden, um sicherzustellen, dass personenbezogene Daten, die durch die DSGVO und andere Datenschutzvorschriften geschützt sind, nicht unbeabsichtigt weitergegeben, zerstört oder verändert werden.[780]

Organisatorische Maßnahmen betreffen in erster Linie die äußeren Rahmenbedingungen sowie die konkrete Ausgestaltung des Verarbeitungsverfahrens, insbesondere solche, die die Umsetzung der Betroffenenrechte sicherstellen.[781] Darunter lassen sich geeignete prozess- und anweisungsbasierte Verfahren vorstellen.[782]

Die zentrale Bestimmung zu TOM ist Art. 32 DSGVO.[783] Er spezifiziert die in Art. 24 DSGVO allgemein geregelten Datensicherheitsmaßnahmen bei der Verarbeitung personenbezogener Daten und ergänzt sie durch entsprechende rechtliche Verpflichtungen des Auftragsverarbeiters.[784] Gemäß Art. 32 Abs. 1 S. 1 DSGVO sind diese Verpflichtungen sowohl durch den Verantwortlichen als auch durch Auftragsverarbeiter zu treffen.[785] Die Verantwortung für die Datensicherheit wird auf den Auftragsverarbeiter ausgedehnt, im Gegensatz zur Verantwortung für die Zulässigkeit der Datenverarbeitung.[786]

776 *Auernhammer -Kramer/Meints*, DSGVO BDSG, Art. 32 Rn. 9.
777 *Auernhammer -Kramer/Meints*, DSGVO BDSG, Art. 32 Rn. 9.
778 *Auernhammer -Kramer/Meints*, DSGVO BDSG, Art. 32 Rn.11.
779 *Auernhammer -Brüggemann*, DSGVO BDSG, Art. 25 Rn. 11.
780 *Auernhammer -Brüggemann*, DSGVO BDSG, Art. 32 Rn. 13.
781 *Auernhammer -Brüggemann*, DSGVO BDSG, Art. 25 Rn. 11.
782 *Auernhammer -Brüggemann*, DSGVO BDSG, Art. 32 Rn. 13.
783 Was sind Technisch und organisatorische Maßnahmen (TOM)? abrufbar: https://www.dr-datenschutz.de/was-sind-technisch-und-organisatorische-massnahmen-tom/, zuletzt abgerufen am 04.08.2023.
784 *Auernhammer -Kramer/Meints*, DSGVO BDSG, Art. 32 Rn. 3.
785 *Auernhammer*, DSGVO BDSG, Art. 32, Rn. 4; *Kühling/Buchner -Jandt*, DSGVO/BDSG, Art. 32 Rn. 4.
786 *Kühling/Buchner -Jandt*, DSGVO/BDSG, Art. 32 Rn. 4.

Um die oberste Pflicht des Verantwortlichen zu erfüllen, nämlich personenbezogene Daten datenschutzkonform zu verarbeiten, ist der Verantwortliche nach Art. 24 Abs. 1 S. 1 DSGVO aufgefordert, u. a. die geeigneten TOM anzuwenden und deren Einhaltung nachzuweisen.[787] Artikel 24 Abs. 1 DSGVO hat drei Ziele: 1. Er schafft eine neue rechtliche Verpflichtung für den für die Verarbeitung Verantwortlichen; 2. er führt den sog. risikobasierten Ansatz ein; und 3. der Verantwortliche muss sicherstellen, dass die Verarbeitung, für die er verantwortlich ist, mit der DSGVO übereinstimmt, indem er die TOM umsetzt.[788]

Da sich der Umfang von Datensicherheitsmaßnahmen immer erweitert, gibt es keinen a-priori-Katalog dieser Maßnahmen.[789] Diese Liste von Datensicherheitsmaßnahmen ist auf eine ständige Überprüfung und Erweiterung ausgelegt.[790] Das Gesetz bildet lediglich einen Mindestmaßnahmenkatalog in Art. 32 Abs. 1 lit. a) - d) DSGVO und schreibt den primären Anforderungsstandard als ,,Stand der Technik“ vor.[791]

Darüber hinaus präzisiert Art. 32 Abs. 1 lit. d) DSGVO die verfahrensrechtlichen Datensicherheitspflichten, indem er ,,Verfahren zur regelmäßigen Überwachung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“ vorschreibt.[792]

4.3.1.3 Mindestanforderungen nach EU-Vorschriften

Nachstehend sind die in Art. 32 DSGVO vorgesehenen Maßnahmen bzw. Mindestanforderungen aufgeführt. Es ist unbedingt erforderlich, diese zu erfüllen und aufrechtzuerhalten. Dies schließt jedoch nicht aus, dass der Verantwortliche bzw. Auftragsverarbeiter auch weitere entsprechende Maßnahmen in Angriff nimmt und umsetzt.

787 Kühling/Buchner -*Hartung*, DSGVO/BDSG, Art. 24 Rn. 1; *Gola/Heckmann -Piltz*, DSGVO/BDSG, Art. 24 Rn. 1.
788 *Gola/Heckmann -Piltz*, DSGVO/BDSG, Art. 24 Rn. 4.
789 *Auernhammer -Kramer/Meints*, DSGVO BDSG, Art. 32 Rn. 12.
790 *Auernhammer -Kramer/Meints*, DSGVO BDSG, Art. 32 Rn. 12.
791 *Auernhammer -Kramer/Meints*, DSGVO BDSG, Art. 32 Rn. 13.
792 *Auernhammer -Kramer/Meints*, DSGVO BDSG, Art. 32 Rn. 2.

4.3.1.3.1 Pseudonymisierung: Art. 32 Abs. 1 lit. a) DSGVO

Die Pseudonymisierung dient der Umsetzung des Prinzips der Datenminimierung.[793] Der Grundsatz der Datenminimierung erfordert nach Art. 5 Abs. 1 lit. c) DSGVO, dass die Verarbeitung personenbezogener Daten dem Zweck angemessen und erheblich sein muss. Sie muss sich auf das beschränken, was für die Zwecke der Datenverarbeitung erforderlich ist. Laut ErwGr. 28 DSGVO verringert die Pseudonymisierung das Risiko für die Rechte und Freiheiten natürlicher Personen im Falle des Verlusts, der unbefugten Weitergabe oder des unbefugten Zugriffs auf pseudonymisierte Daten.[794]

Artikel 4 Nr. 5 Hs. 1 DSGVO definiert den Begriff ,,Pseudonymisierung“ ausdrücklich. Demnach bedeutet Pseudonymisierung die Verarbeitung personenbezogener Daten in einer solchen Weise, dass sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer bestimmten Person zugeordnet werden können. Die anderen Informationen dienen als ,,Schlüssel“, mit dem eine Zuordnung der Daten zu einer Person möglich ist.[795] Gemäß Art. 4 Nr. 5 Hs. 2 DSGVO müssen diese Informationen getrennt aufbewahrt und TOM unterliegen, die sicherstellen, dass sie nicht einer identifizierten oder identifizierbaren natürlichen Person zugeordnet werden können.

Eine andere Möglichkeit, die Daten zu pseudonymisieren, ist die Verwendung komplexer mathematischer Formeln (sog. Hash-Funktionen).[796] Sie ermitteln aus den personenbezogenen Daten einen spezifischen Code, der sowohl für einen konkreten Datensatz als auch für die Person gilt, die dahinter steht.[797] Die Beschreibung der Pseudonymisierung kann sich auch auf anonymisierte Daten nach ErwGr. 26 S. 3 DSGVO beziehen, wenn diese trotz bestehender Identifizierungsmöglichkeiten nicht dazu genutzt werden, die natürliche Person nach allgemeinem Ermessen unmittelbar oder mittelbar zu identifizieren.[798]

Hashing ist eine mathematische Funktion, die eine Eingabe annimmt und eine Zeichenkette von unbestimmter Größe ausgibt, die nicht mit der Eingabe in Verbindung gebracht werden kann, es sei denn, sie wird zurückentwickelt / ,,reverse engineered“.[799] Daher ist dazu eine Anonymisierung erforderlich.[800] Es reicht also nicht aus, nur die Werte zu hashen.[801] Wären Daten enthasht / ,,unhashed“, darf es nicht möglich sein, sie einer Person zuzuordnen.[802]

---

793 *Kühling/Buchner -Jandt*, DSGVO/BDSG, Art. 32 Rn. 17.
794 *Auernhammer -Kramer/Meints*, DSGVO BDSG, Art. 32 Rn. 16.
795 Pseudonymisierung, abrufbar: https://ascon-datenschutz.de/datenschutz-abc/pseudonymisierung/, zuletzt abgerufen am 04.08.2023.
796 *Auernhammer -Kramer/Meintz*, DSGVO BDSG, Art. 32 Rn. 15.
797 *Auernhammer -Kramer/Meintz*, DSGVO BDSG, Art. 32 Rn. 15.
798 *Auernhammer -Kramer/Meintz*, DSGVO BDSG, Art. 32 Rn. 15.
799 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 23.
800 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 23.
801 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 23.
802 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 23.

4.3.1.3.2 Verschlüsselung: Art. 32 Abs. 1 lit. a) DSGVO

Die Verschlüsselung von Daten wird in Art. 32 Abs. 1 lit. a) DSGVO als eine Maßnahme zur Gewährleistung der Sicherheit der Verarbeitung vorgeschrieben. Sie ist für den Verantwortlichen und Auftragsverarbeiter vorteilhaft.[803] Nach einer Datenpanne muss diese den Datenschutzbehörden gemeldet werden, und die Betroffenen müssen über den Vorfall informiert werden[804] (s. → S. 176-181). Geht ein Datenträger verloren oder wird eine E-Mail kompromittiert / gefährdet, auf der gespeicherte Daten nach dem Stand der Technik verschlüsselt sind, entfällt die Benachrichtigungspflicht aus Art. 34 Abs. 3 lit. a) DSGVO gegenüber den Betroffenen; er muss nicht informiert werden.[805] Außerdem berücksichtigen die Aufsichtsbehörden bei der Entscheidung über eine Sanktion nach Art. 83 Abs. 2 lit. c) DSGVO positiv jede vorgenommene Verschlüsselung.[806]

4.3.1.3.3 Verfügbarkeit / Backup: Art. 32 Abs. 1 lit. c) DSGVO

Verfügbarkeit nach Art. 32 Abs. 1 lit. c) DSGVO ergänzt die Verfügbarkeit aus Art. 32 Abs. 1 lit. b) DSGVO.[807] Dies bedeutet, dass die Verfügbarkeit im Sinne der DSGVO nicht nur aus notwendigen Präventivmaßnahmen besteht, sondern auch alle Maßnahmen umfasst, die eine schnelle Wiederherstellung von Daten im Falle eines Zwischenfalls ermöglichen.[808]

Der Verantwortliche und Auftragsverarbeiter müssen sich daher auf Zwischenfälle vorbereiten, indem sie über bewährte Verfahren für solche Fälle verfügen (z. B. Notfallmanagement oder Business Continuity Management).[809] Darüber hinaus müssen Risikoanalysen durchgeführt werden, um potenzielle Schadensfälle zu erkennen und Abhilfemaßnahmen vorzubereiten.[810]

803 Verschlüsselung, abrufbar: https://dsgvo-gesetz.de/themen/verschluesselung/, zuletzt abgerufen am 04.08.2023.
804 Die DSGVO und die E-Mail-Verschlüsselung, abrufbar: https://www.e-recht24.de/artikel/datenschutz/11284-dsgvo-und-e-mail-verschluesselung.html, zuletzt abgerufen 04.08.2023.
805 Die DSGVO und die E-Mail-Verschlüsselung, abrufbar: https://www.e-recht24.de/artikel/datenschutz/11284-dsgvo-und-e-mail-verschluesselung.html, zuletzt abgerufen am 04.08.2023; vgl.: Verschlüsselung, abrufbar: https://dsgvo-gesetz.de/themen/verschluesselung/, zuletzt abgerufen am 04.08.2023.
806 Verschlüsselung, abrufbar: https://dsgvo-gesetz.de/themen/verschluesselung/, zuletzt abgerufen am 04.08.2023.
807 *Auernhammer -Kramer/Meints*, DSGVO BDSG, Art. 32 Rn. 33.
808 *Auernhammer -Kramer/Meints*, DSGVO BDSG, Art. 32 Rn. 33.
809 *Auernhammer -Kramer/Meints*, DSGVO BDSG, Art. 32 Rn. 33.
810 *Auernhammer -Kramer/Meints*, DSGVO BDSG, Art. 32 Rn. 33.

4.3.1.3.4 Gewährleistung der Sicherheit der Verarbeitung: Art. 32 Abs. 1 lit. d) DSGVO

„Die Herstellung der Datensicherheit ist keine einmalige Aufgabe"; die Systeme müssen kontinuierlich auf neue Störungen und Angriffe vorbereitet werden.[811] Dieser Ansatz war bereits obligatorisch, aber nicht ausdrücklich gesetzlich geregelt.[812] In der DSGVO ist nun eindeutig in Art. 32 Abs. 1 lit. d) vorgeschrieben, dass „ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen" angewandt werden muss, um die Sicherheit der Verarbeitung zu gewährleisten.

Dieses Verfahren muss rechtlich und technisch ordnungsgemäß durchgeführt werden. Es ist heute jedoch nicht ungewöhnlich, dass eine Organisation mit eigenem Personal nicht in der Lage ist, vollständige verfahrenstechnische Datensicherheit herzustellen.[813] So werden die de facto Ausweitung auf Zertifizierungen,[814] Verhaltensregeln sowie die Schulung bzw. Sensibilisierung der Mitarbeiter entscheidend.

4.3.1.3.5 Genehmigte Verhaltensregeln: Art. 32 Abs. 3 DSGVO

Genehmigte Verhaltensregeln / „Code of Conducts" (CoC) aus Art. 40 DSGVO können europaweit (genehmigt durch den EU-Datenschutzausschuss) oder national bzw. in einem Mitgliedsstaat (genehmigt durch die zuständige nationale Datenschutzaufsichtsbehörde) gelten.[815]

COC ist ein besonders hilfreiches Instrument für Branchen, die sensible Daten oder große Datenmengen verarbeiten.[816] Sie dienen als Nachweis der Einhaltung datenschutzrechtlicher Pflichten aus der DSGVO.[817] Als eine Alternative für CoC können die Zertifizierungen angesehen werden.[818]

811 *Auernhammer -Kramer/Meints*, DSGVO BDSG, Art. 32 Rn. 34.
812 *Auernhammer -Kramer/Meints*, DSGVO BDSG, Art. 32 Rn. 34.
813 *Auernhammer -Kramer/Meints*, DSGVO BDSG, Art. 32 Rn. 34.
814 *Auernhammer -Kramer/Meints*, DSGVO BDSG, Art. 32 Rn. 34.
815 Dokumentationspflichten und Rechenschaftspflicht, abrufbar: https://www.frankfurt-main.ihk.de/recht/uebersicht-alle-rechtsthemen/datenschutzrecht/dokumentationspflichten-und-rechenschaftspflicht-5192962, zuletzt abgerufen am 04.08.2023.
816 Interwiew mit Cornelia Sasse, im Anhang S. 193.
817 Dokumentationspflichten und Rechenschaftspflicht, abrufbar: https://www.frankfurt-main.ihk.de/recht/uebersicht-alle-rechtsthemen/datenschutzrecht/dokumentationspflichten-und-rechenschaftspflicht-5192962, zuletzt abgerufen am 04.08.2023.
818 Interwiew mit Cornelia Sasse, im Anhang S. 193.

4.3.1.3.6 Genehmigte Zertifizierungen: Art. 32 Abs. 3 DSGVO

In Art. 42 DSGVO ist das Thema „Zertifizierung“ geregelt. In Bezug auf die Zertifizierungsverfahren heißt es in Art. 42 Abs. 1 S. 1 DSGVO lediglich, dass die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss sowie die Kommission die Einführung von datenschutzspezifischen Zertifizierungen, insbesondere auf Unionsebene, fördern.[819] Es ist noch nicht klar, wer die Zertifizierungen entwickeln soll.[820]

Die Einhaltung von CoC und Zertifizierungsverfahren genügt nicht automatisch der Verpflichtung, die Sicherheit der Verarbeitung zu gewährleisten.[821] Sie sollen dem Verantwortlichen neben der Nachweismöglichkeit als Anleitungen dienen, um ihn bei seinen Auswahlentscheidungen zu unterstützen.[822] Die Zertifizierung nach ISO 27001 und ISO 27701 kann eine erste Anlaufstelle für eine Organisation sein, um ihren Dokumentationspflichten nachzukommen, zumal es noch keine gleichwertige Zertifizierung gibt.[823]

Bei der ISO 27701[824] handelt es sich um eine Erweiterung von ISO 27001.[825] Diese soll die Zertifizierung für Informations- und Datensicherheit vereinheitlichen.[826] Dies deutet darauf hin, dass es um eine Zertifizierung im Bereich des ISMS geht und nicht um eine unabhängige Zertifizierung nach der DSGVO.[827]

Die Norm ISO 27701 entspricht nicht vollumfänglich den Anforderungen der DSGVO. Zudem entspricht die ISO 27701-Zertifizierung nicht Art. 43 DSGVO, der eine Akkreditierung der Zertifizierungsstellen nach ISO 17065 vorschreibt.[828]

819 *Kühling/Buchner -Jandt*, DSGVO/BDSG, Art. 32 Rn. 36.
820 *Kühling/Buchner -Jandt*, DSGVO/BDSG, Art. 32 Rn. 36.
821 *Kühling/Buchner -Jandt*, DSGVO/BDSG, Art. 32 Rn. 36.
822 *Kühling/Buchner -Jandt*, DSGVO/BDSG, Art. 32 Rn. 36.
823 Datenschutz Zertifizierung, abrufbar: https://keyed.de/blog/datenschutz-zertifizierung/, zuletzt abgerufen am 04.08. 2023.
824 Der Vollständige Name der ISO/ICE 27701-Norm lautet: „Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management- Requirements and guidelines“.
825 Was ist der Unterschied zwischen Datenschutz und Informationssicherheit? abrufbar: https://www.vialevo.de/unterschied-zwischen-datenschutz-und-informationssicherheit/, zuletzt abgerufen am 04.08. 2023.
826 Datenschutz Zertifizierung, abrufbar: https://keyed.de/blog/datenschutz-zertifizierung/, zuletzt abgerufen am 04.08. 2023.
827 Datenschutz Zertifizierung, abrufbar: https://keyed.de/blog/datenschutz-zertifizierung/, zuletzt abgerufen am 04.08. 2023.
828 Die in diesem Abschnitt dargestellte Aussage befindet sich in dem folgenden Artikel. S.: Datenschutz Zertifizierung, abrufbar: https://keyed.de/blog/datenschutz-zertifizierung/, zuletzt abgerufen am 04.08.2023.

4.3.1.3.7 Mitarbeiteranweisungen: Art. 32 Abs. 4 DSGVO

Die DSGVO erweitert die Verpflichtung zur Regelung einer Verschwiegenheitspflicht.[829] Demnach müssen der Verantwortliche und der Auftragsverarbeiter Maßnahmen ergreifen, um sicherzustellen, dass die Mitarbeiter personenbezogene Daten „nur auf Anweisung des Verantwortlichen verarbeiten".[830] Gemäß Art. 32 Abs. 4 DSGVO umfasst diese Verpflichtung die Pflicht, dafür zu sorgen, dass natürliche Personen, die dem Verantwortlichen und dem Auftragsverarbeiter unterstellt sind, personenbezogene Daten nur auf Weisung des Verantwortlichen verarbeiten.[831] Dies geschieht in der Regel durch sog. Mitarbeiteranweisungen bzw. Arbeitsanweisungen, die vom Arbeitgeber herausgegeben und vom Arbeitnehmer unterschrieben werden.

Diese Anweisungen sind für den „datenschutzkonformen Umgang mit personenbezogenen Daten" durch nachgeordnete Personen, die Zugang zu diesen Daten haben, zu erstellen und deren Umsetzung auf ihre Effektivität zu überprüfen.[832] Eine Information der Mitarbeiter reicht nur dann aus, wenn die Technik eine missbräuchliche oder die Datensicherheit verletzende Datenverarbeitung absolut verhindert.[833] In der Praxis ist dies jedoch nur selten der Fall.

Der Verantwortliche hat die möglichen Zugriffe der Mitarbeiter seines Auftragsverarbeiters über die Arbeitsanweisungen im Auftragsverarbeitungsvertrag zu regeln und damit ein Weisungsrecht auszuüben.[834] Er muss auch sicherstellen, dass die Mitarbeiter ihres Auftragsverarbeiters ihre Arbeitsanweisungen zum Datenschutz einhalten.[835] Dies kann auf verschiedene Weise geschehen.

Der Verantwortliche kann beispielsweise den Auftragsverarbeiter auditieren und überprüfen, ob die im Auftragsverarbeitungsvertrag unterzeichneten Bestimmungen im Arbeitsalltag auch tatsächlich gelebt werden. Ein Audit kann mündlich / über online Call oder schriftlich erfolgen, wobei der Verantwortliche vom Auftragsverarbeiter alle notwendigen Informationen über die Einhaltung der Datenschutzbestimmungen bei der Datenverarbeitung erhält. Er kann sich aber auch selbst vor Ort davon überzeugen, wie alles aussieht und wie die Prozesse ablaufen.

829 *Auernhammer -Kramer/Meints,* DSGVO BDSG, Art. 32 Rn. 60.
830 *Auernhammer -Kramer/Meints,* DSGVO BDSG, Art. 32 Rn. 60.
831 *Voigt/von dem Bussche,* EU-Datenschutz-Grundverordnung (DSGVO), S. 47.
832 *Auernhammer -Kramer/Meints,* DSGVO BDSG, Art. 32 Rn. 60.
833 *Auernhammer -Kramer/Meints,* DSGVO BDSG, Art. 32 Rn. 60.
834 *Auernhammer -Kramer/Meints,* DSGVO BDSG, Art. 32 Rn. 61.
835 *Auernhammer -Kramer/Meints,* DSGVO BDSG, Art. 32 Rn. 61.

4.3.2 Präventive rechtliche Maßnahmen nach dem amerikanischen Recht

Wie bereits erwähnt, verfolgt der Datenschutz in den USA einen sektorspezifischen Ansatz. Das bedeutet, dass auch präventive rechtliche Maßnahmen sektorspezifisch zu betrachten sind. In den USA gibt es kein allumfassendes Bundesgesetz, das Unternehmen zum Ergreifen der geeigneten Sicherheitsmaßnahmen zwingt.[836] Dort variieren die Gesetze für Unternehmen je nach Industriezweig und geografischer Lokation.[837] Erwähnenswert ist jedoch in diesem Zusammenhang der **Cybersecurity Enhancement Act von 2014**, der als ein Bundesgesetz aufgenommen wurde.[838] Er verpflichtet das NIST (National Institute of Standards and Technology), branchenspezifische Richtlinien sowie bewährte Verfahren für Privatunternehmen weiterzuentwickeln.[839] Das Dokument enthält die zwanzig Schritte, die von jedem Unternehmen zu befolgen sind, um die kontinuierliche IT-Sicherheit zu ermöglichen.[840]

Im Bereich des Datentransfers stellt sich die Lage z. B. bei der Strafverfolgung wie folgt dar: Die Architektur des Informationsaustauschs in der Strafverfolgung ist komplex.[841] Die Strafverfolgungsbehörden benötigen in zunehmendem Maße hochentwickelte Informationstechnologie zur Unterstützung ihrer Arbeit.[842] Selbst auf der höchsten Ebene gibt es mehr als 50 gewünschte Schnittstellen zwischen RMS- (Aktenverwaltungssystemen, die die Fallgeschichten der Behörden verwalten) und CAD- (computergestützte Dispositionssystemen, die die Anrufe der Behörden und die Historie der Anrufbeantwortung verwalten) Systemen.[843] Nur ein Bruchteil dieser Schnittstellen wird durch Normen abgedeckt, die sich häufig überschneiden und im Widerspruch zueinander stehen; die Infrastruktur für die Entwicklung und Prüfung von Normen ist unvollständig.[844]

836 IT-Sicherheit und Datenschutz: Die Gesetzeslage in den USA und Deutschland im Vergleich, abrufbar: https://digitaleweltmagazin.de/it-sicherheit-und-datenschutz-die-gesetzeslage-in-den-usa-und-deutschland-im-vergleich/, zuletzt abgerufen am 04.08.2023.

837 IT-Sicherheit und Datenschutz: Die Gesetzeslage in den USA und Deutschland im Vergleich, abrufbar: https://digitaleweltmagazin.de/it-sicherheit-und-datenschutz-die-gesetzeslage-in-den-usa-und-deutschland-im-vergleich/, zuletzt abgerufen am 04.08.2023.

838 IT-Sicherheit und Datenschutz: Die Gesetzeslage in den USA und Deutschland im Vergleich, abrufbar: https://digitaleweltmagazin.de/it-sicherheit-und-datenschutz-die-gesetzeslage-in-den-usa-und-deutschland-im-vergleich/, zuletzt abgerufen am 04.08.2023.

839 IT-Sicherheit und Datenschutz: Die Gesetzeslage in den USA und Deutschland im Vergleich, abrufbar: https://digitaleweltmagazin.de/it-sicherheit-und-datenschutz-die-gesetzeslage-in-den-usa-und-deutschland-im-vergleich/, zuletzt abgerufen am 04.08.2023.

840 IT-Sicherheit und Datenschutz: Die Gesetzeslage in den USA und Deutschland im Vergleich, abrufbar: https://digitaleweltmagazin.de/it-sicherheit-und-datenschutz-die-gesetzeslage-in-den-usa-und-deutschland-im-vergleich/, zuletzt abgerufen am 04.08.2023.

841 *Hollywood/Winkelman,* Improving Information-Sharing Across Law Enforcement, 1, 2.

842 *Hollywood/Winkelman,* Improving Information-Sharing Across Law Enforcement, 1, 1.

843 *Hollywood/Winkelman,* Improving Information-Sharing Across Law Enforcement, 1, 1-2.

844 *Hollywood/Winkelman,* Improving Information-Sharing Across Law Enforcement, 1, 2.

Aus diesem Grund wird das Thema zunächst unter SCA und seiner Ergänzung im CLOUD Act präsentiert. Wenn die Gesetze keine entsprechenden oder ausreichenden Regelungen enthalten, wird es nach CCPA und seiner Änderung CPRA präsentiert, da diese der DSGVO ähnlich sind. Ist auch dort nichts zu finden oder, ist es dort nicht ausführlich dargestellt, so werden ggf. weitere Gesetze oder Normen genannt.

Die folgenden Maßnahmen basieren auf den DSGVO-Bestimmungen, da sie ein ausreichendes Datenschutzniveau garantieren. Dies wird auch den abschließenden Vergleich der präventiven Maßnahmen auf EU- und US-Ebene vereinfachen.

4.3.2.1 Privacy by Design, Privacy by Default

Die Begriffe „Privacy by Design" und „Privacy by Default" werden weder im CLOUD Act / SCA noch im CCPA / CPRA erwähnt. Der Begriff „Privacy by Design" ist jedoch bei der Bundeshandelskommission (Federal Trade Commission; FTC) zu finden. Die FTC verwendet den Begriff „Privacy by Design" in ihrer Rahmenregelung[845] und empfiehlt „Privacy by Design"-Praktiken[846] zu implementieren. Hierbei ist zu betonen, dass diese Regelungen von der FTC also von der Bundeshandelskommission stammen, was bedeutet, dass sie für ein Unternehmen gelten und nicht für alle Organisationen, einschließlich Behörden.

Die FTC ist eine unabhängige Bundesbehörde, die in erster Linie für die Bereiche Wettbewerb und Verbraucherschutz zuständig ist.[847] Ihre Aufgabe im Bereich des Datenschutzes besteht darin, Selbstregulierung zu fordern und den Datenschutz im Allgemeinen durchzusetzen.[848]

Die Selbstregulierung ist ein Verzicht des Staates auf die Ausübung seiner Regelungskompetenz.[849] Dieses Konzept ist in den USA besonders stark ausgeprägt.[850] Wenn die Selbstregulierung an ihre Grenzen stößt und keine Lösungen für bestehende Probleme bietet oder die vorgegebenen Lösungen ein Problem nicht wirksam lösen können, greift der Staat ein, um negative Folgen für den Bürger und die Lage des Staates abzuwenden.[851]

845 *Ramirez,* Remarks of Commissioner Edith Ramirez Privacy by Design Conference: Privacy By Design and the New Privacy Framework of the U.S. Federal Trade Commission, 1, 2.
846 Data Protection Laws and Regulations USA 2023, abrufbar: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa, zuletzt abgerufen am 05.08.2023.
847 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 229 ff.
848 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 229 ff.
849 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 228.
850 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 228.
851 *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. 229.

Laut diese Rahmenregelung sollten Unternehmen in erster Linie den Datenschutz und die Sicherheit von Anfang an in ihre Produkte und Dienstleistungen einbeziehen.[852] Zweitens sollten Unternehmen nur die Daten erheben, die sie für einen bestimmten Geschäftszweck[853] bzw. für einen bestimmten Transaktion) benötigen oder wenn die Datenerhebung gesetzlich vorgeschrieben bzw. ausdrücklich erlaubt ist.[854] Die Daten sind sicher zu entsorgen, wenn der Zweck erfüllt ist.[855] Drittens sollten Unternehmen angemessene Sicherheitsvorkehrungen treffen, um Verbraucherdaten zu schützen.[856]
Der Begriff „Privacy by Default" ist im Bereich des Datenschutzes und der Informationssicherheit in den USA nicht bekannt. Deren Fehlen kann als fehlendes Regelungsstück des Persönlichkeitsrechts angesehen werden. Privacy by Design und Privacy by Default sollen eng miteinander verbunden sein. Sie gehören zusammen.[857] Ein starkes Privacy by Design sorgt für weniger Aufwand bei der Gestaltung der Privacy by Default.[858] Je besser eine Organisation plant, desto einfacher und rechtskonformer wird die datenschutzfreundliche Anwendung später sein.[859]

4.3.2.2 Sicherheit der Verarbeitung nach US-Vorschriften

Der CLOUD Act verlangt in Abschn. 105 (b) (1), dass das innerstaatliche Recht der ausländischen Regierung einen soliden materiellen und verfahrensrechtlichen Schutz der Privatsphäre, der bürgerlichen Freiheiten und der Menschenrechte im Hinblick auf die Datenerhebung und die Aktivitäten der ausländischen Regierung, die Gegenstand des Abkommens sind, bietet. Das bedeutet, dass ein Land innerhalb seines Rechtsrahmens angemessene Standards und Kontroll-mechanismen zum Schutz der Privatsphäre, der bürgerlichen Freiheiten und der Menschenrechte einführen muss.[860] Allerdings ist im **CLOUD Act** und im **SCA** der Begriff „technische und organisatorische Maßnahmen" (TOM) nicht erwähnt. Darüber hinaus bezieht sich die Anforderung gem. Abschn. 105 (b) (1) CLOUD Act auf ausländisches und nicht nicht auf inländisches Recht.

852 *Ramirez,* Remarks of Commissioner Edith Ramirez Privacy by Design Conference Hong Kong: Privacy By Design and the New Privacy Framework of the U.S. Federal Trade Commission, 1, 2.
853 *Ramirez,* Remarks of Commissioner Edith Ramirez Privacy by Design Conference Hong Kong: Privacy By Design and the New Privacy Framework of the U.S. Federal Trade Commission, 1, 2.
854 Data Protection Laws and Regulations USA 2023, abrufbar: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa, zuletzt abgerufen am 05.08.2023.
855 *Ramirez,* Remarks of Commissioner Edith Ramirez Privacy by Design Conference Hong Kong: Privacy By Design and the New Privacy Framework of the U.S. Federal Trade Commission, 1, 2.
856 *Ramirez,* Remarks of Commissioner Edith Ramirez Privacy by Design Conference Hong Kong: Privacy By Design and the New Privacy Framework of the U.S. Federal Trade Commission, 1, 2.
857 Interview mit Cornelia Sasse, im elektronischen Zusatzmaterial, Anlage 1, S. 3.
858 Interview mit Cornelia Sasse, im elektronischen Zusatzmaterial, Anlage 1, S. 3.
859 Interview mit Cornelia Sasse, im elektronischen Zusatzmaterial, Anlage 1, S. 3.
860 The United States Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2, 5.

CPRA verpflichtet in 1798.130 (3) (A) S. 4 einem Dienstleister bzw. Auftragnehmer, der personenbezogene Daten aufgrund eines schriftlichen Vertrags mit einem Unternehmen sammelt, die CPRA-Anforderungen durch geeignete TOM einzuhalten, wobei die Art der Verarbeitung zu berücksichtigen ist.

Unter TOM sind Funktionen, Prozesse, Kontrollen, Systeme, Verfahren und Maßnahmen zu verstehen, die Organisationen einführen können, um die sichere Verarbeitung und Speicherung personenbezogener Daten zu fördern, Datenschutzverletzungen zu vermeiden und die Einhaltung der einschlägigen Datenschutzpflichten zu erleichtern. Beispielsweise gehören Pseudonymisierung und Verschlüsselung zu technischen Maßnahmen, Datenschutz-Folgeabschätzung und Informationssicherheitsrichtlinien zu organisatorischen Maßnahmen.[861]

4.3.2.3 Mindestanforderungen nach US-Vorschriften

4.3.2.3.1 Pseudonymisierung: 1798.140 (aa) CPRA

Der Begriff „Pseudonymisierung" wird im CLOUD Act weder erwähnt noch definiert. „Pseudonymisieren" bzw. „Pseudonymisierung" bedeutet nach 1798.140 (aa) Hs. 1 CPRA die Verarbeitung personenbezogener Daten in einer Weise, die dazu führt, dass die personenbezogenen Daten ohne Verwendung zusätzlicher Informationen nicht mehr einem bestimmten Verbraucher zugeordnet werden können. 1798.140 (aa) Hs. 2 CPRA setzt voraus, dass die zusätzlichen Informationen getrennt aufbewahrt und TOM unterlegt werden sollten, die sicherstellen, dass die personenbezogenen Daten nicht einem identifizierten oder identifizierbaren Verbraucher zugeordnet werden können.

Außer der Verwendung der in 1798.140 (aa) Hs. 1 CPRA erwähnten „zusätzlicher Informationen" als „Schlüssel" sollten auch die Hash-Funktionen als eines der Mittel zur Pseudonymisierung verstanden werden (s. → S. 128).

4.3.2.3.2 Verschlüsselung: CLOUD Act / SCA, CCPA / CPRA

Das Thema „Verschlüsselung" ist natürlich auf amerikanischer Ebene bekannt und wird dort angewendet, ist aber nicht gesetzlich geregelt. Die Verschlüsselung wird weder im CLOUD Act / SCA noch im CCPA / CPRA erwähnt. Das bedeutet, dass jede Organisation selbst entscheiden sollte, ob sie die von ihr verarbeiteten Daten verschlüsselt. Wenn sie sie vornehmen möchte, kann sie die normative Regelungen abrufen und die Daten gemäß ISO/IEC 27001 verschlüsseln.

861 Diese Definition der TOM findet sich in dem folgenden Artikel. S.: Technical and organisational measures, abrufbar: https://content.next.westlaw.com/practical-law/document/I8d24008059ec11e89bf199c0ee06c731/Technical-and-organisational-measures?originationContext=document&transitionType=DocumentItem&ppcid=45562d1e38a344b2b385a1f4739a475b&contextData=(sc.Category)&firstPage=true&viewType=FullText, zuletzt abgerufen am 04.08.2023.

Sollte gesetzlich vorgeschrieben werden, die Daten zu verschlüsseln, wird sich dies wahrscheinlich auf die Anwendung des CLOUD Act auswirken. Nach dem CLOUD Act unterliegen verschlüsselte Daten nicht der Offenlegung gegenüber der Regierung. Das heißt, wenn jede Organisation ihre Daten verschlüsselt, bleibt dann auch nichts mehr offenzulegen.

4.3.2.3.3 Verfügbarkeit / Backup: Abschn. 103 (a) (1), § 2713 CLOUD Act / 18 U.S.C. § 2704 (a) (1)-(3) SCA

Ein Anbieter von elektronischen Kommunikationsdiensten oder Ferninformationsdiensten muss nach Abschn. 103 (a) (1), § 2713 CLOUD Act den Inhalt einer drahtgebundenen oder elektronischen Kommunikation und alle Aufzeichnungen oder sonstigen Informationen über einen Kunden oder Subskribenten, die sich im Besitz, im Gewahrsam oder unter der Kontrolle des Anbieters befinden, aufbewahren, sichern / ,,back up“ oder offenlegen.

Eine staatliche Stelle kann nach 18 U.S.C. § 2704 (a) (1) S. 1 SCA in ihrer Vorladung oder gerichtliche Anordnung die Anforderung aufnehmen, dass der Diensteanbieter, an den das Ersuchen gerichtet ist, eine Sicherungskopie des Inhalts der angeforderten elektronischen Kommunikation anfertigt, um diese Kommunikation aufzubewahren. Der Diensteanbieter erstellt nach 18 U.S.C. § 2704 (a) (1) S. 2 und 3 SCA eine Sicherungskopie so bald wie möglich (innerhalb von zwei Arbeitstagen nach Eingang der Vorladung oder des Gerichtsbeschlusses) im Einklang mit seinen üblichen Geschäftspraktiken und bestätigt der staatlichen Stelle, dass eine solche Sicherungskopie erstellt wurde.

Der Dienstleister darf den Teilnehmer oder Kunden über eine solche Vorladung oder gerichtliche Anordnung nicht in Kenntnis setzen; die staatliche Stelle benachrichtigt sie nach 18 U.S.C. § 2704 (a) (2) SCA innerhalb von drei Tagen nach Erhalt einer solchen Bestätigung, es sei denn, die Benachrichtigung wird gem. 18 U.S.C. § 2705 (a) SCA aufgeschoben.

Der Diensteanbieter darf die Sicherungskopie gem. 18 U.S.C. § 2704 (a) (3) SCA erst dann vernichten, wenn die Informationen übermittelt wurden oder wenn ein Verfahren (einschließlich eines Berufungsverfahrens), bei dem es um eine Vorladung oder einen Gerichtsbeschluss der Regierung geht, abgeschlossen wurde.

4.3.2.3.4 Gewährleistung der Sicherheit der Verarbeitung: 1798.140 (j) (1) (C) CPRA

Die Verfahren zur Gewährleistung der Sicherheit der Verarbeitung sind weder im CLOUD Act noch im SCA nicht geregelt.

Ergänzend zum CCPA fügt jedoch CPRA die Bedeutung des Auftragnehmers hinzu, wobei die Gewährleistung der Sicherheit der Datenverarbeitung thematisiert wird. CPRA verlangt, dass der Dienstleister oder der Auftragnehmer dem betroffenen Unternehmen erlaubt, die Einhaltung seiner vertraglichen Verpflichtungen zu überwachen.[862]

1798.140 (j) (1) (C) CPRA setzt voraus, dass der Auftragnehmer zur Einhaltung des Vertrags zwischen dem Verantwortlichen und dem Auftragnehmer Überwachungsmaßnahmen wie manuelle Überprüfungen, automatische Scans sowie regelmäßige Bewertungen, Audits oder andere technische und betriebliche Tests mindestens alle 12 Monate durchführt. Das CPRA besagt, dass bei Dienstleistern eine solche Überwachung vertraglich vorgeschrieben werden kann, aber nicht muss.[863]

4.3.2.3.5 Verhaltensregeln: CLOUD Act / SCA, CCPA / CPRA

Verhaltensregeln („Code of Conduct" – CoC) werden in dem CLOUD Act / SCA sowie CCPA / CPRA nicht erwähnt und dementsprechend auch nicht aufgefordert, diese abzuschließen und einzuhalten.

Wie bereits erwähnt, kann CoC als ein besonders hilfreiches Instrument für Branchen, die sensible Daten oder große Datenmengen verarbeiten, dienen.[864] Daher kann der Schluss gezogen werden, dass die Implementierung eines CoC für diese Kategorie von Organisationen eine gute Garantie für den Schutz personenbezogener Daten sein sollte.

862 The CPRA & Third Parties, abrufbar: https://www.sixfifty.com/blog/the-cpra-third-parties/, zuletzt abgerufen am 04.08.2023.

863 The CPRA & Third Parties, abrufbar: https://www.sixfifty.com/blog/the-cpra-third-parties/, zuletzt abgerufen am 04.08.2023.

864 Interwiew mit Cornelia Sasse, im Anhang S. 193.

4.3.2.3.6 Genehmigte Zertifizierungen: 1798.140 (j) (1) (A) und (B) CPRA

Derzeit existieren keine konkreten CLOUD Act- oder CCPA-Zertifizierungen. Die Zertifizierung bzw. Bescheinigung wird nur durch das CPRA bei den Verpflichtungen des Auftragsverarbeiters geregelt. Zusätzlich zu den vertraglichen Voraussetzungen für Dienstleister und Auftragnehmer müssen Auftragnehmer Datenverträge mit einigen zusätzlichen Anforderungen haben.[865] Nach dem CPRA muss ein Auftragnehmer bescheinigen, dass er seine Pflichten versteht.[866] 1798.140 (j) (1) (B) CPRA verlangt, dass der dem Auftragnehmer vorgelegte Vertrag eine Bescheinigung des Auftragnehmers enthält, dass er die Beschränkungen gem. 1798.140 (j) (1) (A) CPRA kennt und einhalten wird. Diese Bescheinigung ist als eine Zertifizierung / „Certification" zu verstehen.

Wenn eine Organisation eine Zertifizierung nach z. B. ISO/IEC 27001 anstrebt, gelten die gleichen Anforderungen, die auch für eine europäische Organisation gelten würden. Eine Besonderheit wäre nur, dass eine Organisation, die sich in den USA nach ISO/IEC 27001 oder ISO/IEC 27701 zertifizieren lässt, die amerikanischen Datenschutzgesetze einhalten muss, eine Organisation in Europa die europäischen Datenschutzbestimmungen.

4.3.2.3.7 Mitarbeiteranweisungen: CLOUD Act, CCPA

Nach Abschn. 105 (b) (4) (F) CLOUD Act muss die ausländische Regierung unverzüglich das im Rahmen des Abkommens gesammelte Material prüfen und alle nicht geprüften Mitteilungen in einem sicheren System speichern, zu dem nur die Personen Zugang haben, die in den einschlägigen Verfahren geschult sind.

Nach 1798.130 (a) (6) CCPA müssen alle Personen, die mit den Voraussetzungen des CCPA in der Firma arbeiten, trainiert werden. Das Ziel ist es, mit Verbraucheranfragen sicher und rechtmäßig umzugehen.[867] Gehen Vertreter des Verbraucherservices durch Telefonate oder Bedienstete bei der Registrierkasse auf die Fragen über die Datenschutzpraktiken des Unternehmens ein, müssen sie sich mit den Kernpunkten des CCPA gut auskennen.[868] Das bedeutet, dass die Beschäftigte, die mit den personenbezogenen Daten arbeiten, entsprechende Anweisungen erhalten haben sollten, um diese Daten jederzeit rechtskonform verarbeiten zu können.

865 The CPRA & Third Parties, abrufbar: https://www.sixfifty.com/blog/the-cpra-third-parties/, zuletzt abgerufen am 04.08.2023.

866 The CPRA & Third Parties, abrufbar: https://www.sixfifty.com/blog/the-cpra-third-parties/, zuletzt abgerufen am 04.08.2023.

867 CCPA training requirement – Section 1798.130(a)(6) compliance, abrufbar: https://www.clarip.com/data-privacy/ccpa-training/, zuletzt abgerufen am 04.08.2023.

868 CCPA training requirement – Section 1798.130(a)(6) compliance, abrufbar: https://www.clarip.com/data-privacy/ccpa-training/, zuletzt abgerufen am 04.08.2023.

4.3.3 Vergleich der präventiven rechtlichen Maßnahmen

Präventive rechtliche Maßnahmen, die vor oder während einem Datentransfer ergriffen werden müssen, finden sich sowohl im europäischen als auch im amerikanischen Rechtssystem. Sie schreiben Anforderungen vor, die nach der Risiko-Beurteilung die Beseitigung von Risiken und die sichere Verarbeitung bzw. den Transfer von (personenbezogenen) Daten gewährleisten. Diese Maßnahmen werden in der Regel in Form von technischen und organisatorischen Maßnahmen vorgesehen. Sie dienen als geeignete Maßnahmen für eine sichere Datenverarbeitung.

Auf europäischer Ebene sollten zunächst der **Privacy by design** und **Privacy by Default** in Betracht gezogen werden. Datenschutz durch Technikgestaltung stärkt den Datenschutz; datenschutzfreundliche Voreinstellungen verbessern die Position der betroffenen Personen.[869] In den USA ist derzeit nur der erste Grundsatz bekannt und wird angewandt.

Die **Sicherheit der Verarbeitung** durch technischen und organisatorischen Maßnahmen umfasst viele Aspekte, u. a. Pseudonymisierung, Verschlüsselung, Verfügbarkeit / Backup, Gewährleistung der Sicherheit der Verarbeitung, genehmigte Verhaltensregeln, genehmigte Zertifizierungen und Mitarbeiteranweisungen. Dies sind Punkte, die in der DSGVO genau aufgelistet und geregelt sind. Die meisten dieser Vorschriften finden sich auch in den USA, jedoch in recht begrenztem Umfang. Außerdem sind diese Themen in den sektorspezifischen Gesetzen festgelegt. Sie sind entsprechend nur in den spezifischen Fällen geregelt und nicht allumfassend. Sie betreffen nicht alle Kategorien personenbezogener Daten, sondern nur bestimmte Datenkategorien sowie spezifische Prozesse und Bereiche.

Wenn es um den digitalen Datentransfer geht, ist vor allem der CLOUD Act zu nennen. In diesem Gesetz werden nur wenige technische und organisatorische Maßnahmen erwähnt, wobei diese oft dennoch das Ausland und nicht eine inländische Struktur betreffen. Am Beispiel des CCPA / CPRA wurde festgestellt, dass die Datenschutzgesetze, die mit der DSGVO identisch sind, sicherstellen, dass die TOM-Thematik in den USA gesetzlich geregelt ist, aber nicht so umfassend wie in der EU. Weitere Anforderungen, die z. B. von NIST oder FTC zur verfügung gestellt werden, sind teilweise nicht verpflichtend oder regeln nur sektorspezifische Bereiche.

Alle oben beschriebene Vorschriften finden sich zusätzlich in den internationalen Standards, die es Organisationen ermöglichen, auf freiwilliger Basis eine Lage in der Organisation zu schaffen, in der alle rechtlichen Anforderungen erfüllt werden und eine sichere Datenverarbeitung implementiert sowie aufrechterhalten wird. Darüber hinaus bieten diese Standards genaue Schritte für eine ordnungsgemäße Umsetzung, Handlungsempfehlungen und zielgerichtete Anleitungen. Diese werden im Folgenden erörtert.

869 *Auernhammer -Brüggemann*, DSGVO BDSG, Art. 25. Rn. 1.

4.4 Präventive normative Maßnahmen

Sicherheit ist eines der ersten Dinge, die vergessen oder übersehen werden können.[870] Daher ist es unerlässlich, präventive normative Maßnahmen zu ergreifen, um die Organisation sicher zu halten und eine sichere Datenübertragung zu gewährleisten.

Zu den normativen Maßnahmen nach ISO/IEC 27001 gehören organisatorische Maßnahmen, personenbezogene Maßnahmen, physische Maßnahmen und technische Maßnahmen. Im Folgenden werden die Maßnahmen vorgestellt, die insbesondere für den Datentransfer gelten, nämlich die entsprechenden Punkte der organisatorischen, der personenbezogenen und der technischen Maßnahmen. Außerdem wird die PDCA-Methodik betrachtet, die die vollständige Umsetzung diese Maßnahmen ermöglicht.

4.4.1 Organisatorische Maßnahmen / „Organizational Controls“

4.4.1.1 Erkenntnisse zur Bedrohungslage

ISO/IEC 27001: A.5.7 verlangt, dass Informationen über die Gefährdungs- bzw. Bedrohungslage der Informationssicherheit gesammelt und analysiert werden müssen, um einen Überblick über die Bedrohungslage zu bekommen. Dadurch kann sichergestellt werden, auf Bedrohungen zu reagieren bzw. sie zu verhindern (z. B. Informationssicherheitsereignisse zu bewerten oder die Angriffs-erkennungssysteme zu konfigurieren).[871] Wird die Bedrohungslage rechtzeitig erkannt und bewertet, kann rechtzeitig reagiert werden, um sicherzustellen, dass kein Unbefugter Zugriff auf Daten erhält.

4.4.1.2 Übertragung oder Transport von Informationen

Gemäß ISO/IEC 27001: A.5.14 müssen Regeln, Verfahren bzw. Vereinbarungen festgesetzt werden, wenn Informationen innerhalb der Organisation oder zwischen der Organisation und anderen Parteien übertragen oder transportiert werden.

Daten und Informationen werden auf verschiedenen Wegen (z. B. elektronisch, physisch oder mündlich) und zwischen unterschiedlichen internen und externen Einrichtungen ausgetauscht.[872] Dementsprechend müssen grundlegende Anforderungen in einer themenspezifischen Richtlinie definiert und entsprechende Regelungen wie Vertraulichkeitsvereinbarungen, Anweisungen oder Hinweise (z. B. Regeln für die Verwendung elektronischer Signaturen) schriftlich festgehalten werden.[873]

870 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 25.
871 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 79.
872 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 83.
873 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 83.

Damit der digitale Datentransfer sicher ist, ist es wichtig, alle Ebenen / „Layers“ zu verwalten.[874] Es muss sichergestellt werden, dass sie gesichert sind.[875] Wenn davon die Rede ist, dass die Daten während der Übertragung zu verschlüsseln sind, ist damit bereits die Netzwerkschicht / „Network Layer“ gemeint.[876] Dabei handelt es sich um die eigentlichen Pakete, die zwischen dem Server und der Maschine gesendet werden.[877]

Die Verschlüsselung bei der Übertragung spielt keine Rolle, wenn jemand Fernzugriff auf einen IT-Arbeitsplatz hat und alles, was in der Organisation geschieht, verfolgt und aufzeichnet.[878] Auf jeder Ebene gibt es im Grunde einen Weg, sich Zugang zu verschaffen, wenn jemand die Sicherheitsmaßnahmen umgehen und auf Daten zugreifen will, deren Zugriff von der Organisation nicht erwünscht ist.[879] Es ist daher unerlässlich, diese Maßnahmen zu verschriftlichen und ihre Einhaltung zu überprüfen.

4.4.1.3 Zugangssteuerung

Gemäß ISO/IEC 27001: A.5.15 sollte der physische und logische Zugang zu Informationen sowie zu anderen damit verbundenen Werten bzw. Assets geregelt und umgesetzt werden. Da die Sicherheit vollständig vom Zugang abhängt,[880] ist es unerlässlich, diesen niederzuschreiben und in einer Organisation entsprechend umzusetzen. Dabei sollten für besonders schützenswerte Informationen Prinzipien wie „Need-to-Know“ oder „Least Privilege“ Anwendung finden.[881]

Das Need-to-know-Prinzip beim **physischen Zugang** ist z. B. gewährleistet, wenn nur eine begrenzte Anzahl von Personen Zugang zum Serverraum hat. So dürfen beispielsweise nur ein IT-Leiter und sein Vertreter die Schlüssel zum Serverraum haben, weil sie diese u. a. zur Überwachung und Wartung des Server-Racks, der Sensoren oder der Hardware benötigen.

Wenn es um die Zugangsverwaltung im Zusammenhang mit dem Datentransfer geht, ist dazu der **logische Zugang** in Betracht zu ziehen. Wenn beispielsweise ein neuer Mitarbeiter eingestellt wird oder jemand die Abteilung wechselt, muss immer darauf geachtet werden, welche Zugänge auf welche Informationen er erhält und welche Daten er wohin übertragen kann.

874 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 24.
875 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 24.
876 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 24.
877 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 24.
878 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 24.
879 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 24.
880 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 21.
881 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 84.

4.4.1.4 Informationssicherheit bei der Verwendung von Cloud-Diensten

ISO/IEC 27001: A.5.23 setzt voraus, dass die Prozesse, die einen Bezug zu Cloud-Diensten haben, in Übereinstimmung mit den Informationssicherheitsanforderungen der Organisation eingerichtet werden müssen. Hierbei sollte die Organisation eine Cloud-Strategie ausbauen und diese allen relevanten Parteien mitteilen.[882] Die Cloud-Service-Verträge sind einer Informationssicherheits-risikoanalyse zu unterziehen, und verbleibende Risiken sind zu identifizieren und zu akzeptieren.[883] Dadurch werden die Risiken transparent, und es werden geeignete Maßnahmen ergriffen.

Die Cloud-Nutzung kann gemeinsame Verantwortlichkeiten und kooperative Dienste zwischen Cloud-Anbieter und Cloud-Kunde beinhalten.[884] Dabei ist es unerlässlich, die Verantwortlichkeiten klar zu definieren und entsprechend umzusetzen.[885] Wer verantwortlich ist und wer Zugriff auf welche Daten und Systeme hat, muss vor der Nutzung der Cloud-Umgebung klar definiert werden. Dies gilt natürlich auch für die Testphase (sog. Pilot Phase), d. h. wenn das Produkt noch nicht gekauft oder die Umgebung noch nicht vollständig genutzt wird und nur getestet wird.

4.4.2 Personenbezogene Maßnahmen / „People Controls“

4.4.2.1 Sensibilisierung, Ausbildung und Schulung für Informationssicherheit

Der Datentransfer ist das Thema, wobei die Mitarbeiter viel falsch machen können.[886] Der Einsatz einschlägiger Dritter (z. B. eines Dienstleisters) kann auch eine Rolle spielen. Daher müssen Mitarbeiter und relevante Dritte nach ISO/IEC 27001: A.6.3 für die Informationssicherheit sensibilisiert, ausgebildet, geschult und über die Informationssicherheitspolitik und -verfahren informiert werden. Dadurch wird sichergestellt, dass sich die Mitarbeiter stets ihrer Pflichten und Verantwortlichkeiten in Bezug auf die Informationssicherheit bewusst sind und verstehen, was zu tun ist.[887]

Die Schulungen bzw. das Training sollten allgemeine Grundlagen sowie Spezifika der eigenen Organisation beinhalten und die Hintergründe sowie Ziele vermitteln, um ein tieferes Verständnis zu erreichen.[888] Dies ist sehr wichtig, insbesondere wenn eine Richtlinie oder Leitlinie in der Organisation veröffentlicht wird. Wenn dies gewährleistet ist, kann eine Organisation die ordnungsgemäße Einhaltung der einschlägigen Gesetze sicherstellen, was wiederum die Vermeidung von Strafen ermöglicht und Gesetzesverstöße verringert.[889]

882 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 89.
883 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 89.
884 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 89.
885 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 89.
886 Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 6.
887 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 101.
888 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 101.
889 Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 6.

Die Schulungen sind regelmäßig und abwechselnd durchzuführen.[890] Es ist unerlässlich, verschiedene Kanäle und Medien zu nutzen (z. B. Newsletter, Intranet-Website, E-Learning-Plattform oder Quiz), um die kontinuierliche Beschäftigung mit der Materie zu fördern.[891] Darüber hinaus gibt es Ablaufpläne und Inhaltsvorlagen der europäischen ENISA (European Union Agency for Cybersecurity) oder der US-amerikanischen CISA (Cybersecurity and Infrastructure Security Agency), die Anleitungen bieten und die Möglichkeit schaffen, das Thema mit eigenen Inhalten einzurichten.[892]

4.4.2.2 Disziplinarverfahren

Halten sich Mitarbeiter und Dritte nicht an die Informationssicherheitsrichtlinie, muss ein Verfahren gem. ISO/IEC 27001: A.6.4 eingerichtet werden, um disziplinarische Maßnahmen zu ermöglichen. Dieses Verfahren soll eine gerechte Behandlung gewährleisten und darf nicht ohne vorherige Prüfung des mutmaßlichen Verstoßes eingeleitet werden.[893] Hierbei sind u. a. die Schwere des Verstoßes sowie Sensibilisierungsmaßnahmen zu berücksichtigen.[894] Disziplinarmaßnahmen sind wichtig, damit das Thema ernst genommen wird.[895] Zusätzlich zu den disziplinarischen Maßnahmen kann ein Belohnungssystem eingeführt werden. Durch dieses System werden die Mitarbeiter zu verbindlichem Verhalten und aktivem Engagement motiviert.[896]

Ob ein Disziplinarverfahren oder ein Belohnungssystem effektiver ist, wird bei der Sicherheitsgemeinschaft nicht einheitlich beurteilt.[897] Die Befürworter eines Belohnungssystems glauben, dass es zu vorbildlichem Verhalten und aktivem Engagement motiviert. Die Befürworter von Disziplinarmaßnahmen sind der Meinung, dass Verstöße gegen die Datenübertragungsrichtlinie genauso eingestuft werden sollten wie Diebstahl oder Arbeitsverweigerung. Wenn Mitarbeiter nicht dafür belohnt werden, dass sie nicht stehlen, sollten sie auch nicht für die rechtmäßige Übertragung von Daten belohnt werden.[898]

890 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 101.
891 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 101 ff.
892 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 101 ff.
893 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 102.
894 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 102.
895 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 102.
896 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 102.
897 Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 6.
898 Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 6.

Das Thema „Disziplinarmaßnahmen“ muss mit Sorgfalt behandelt werden. Wenn ein Mitarbeiter bei der Datenübermittlung einen Fehler macht, der zu einem Gesetzesverstoß oder einem Datenschutzvorfall führt, muss eine Ursachenanalyse durchgeführt werden.[899] Es ist wichtig, mit dem Geschäftsführer zu sprechen, mögliche Schwachstellen nachzuarbeiten[900] und den Mitarbeiter gezielt zu schulen, um ihm zu helfen, sich zu verbessern und den Fehler zu beseitigen. Wenn dies nicht gelingt und der Mitarbeiter denselben Fehler wiederholt, sollten geeignete weitere Maßnahmen eingeleitet werden, einschließlich einer Abmahnung und Kündigung.[901]

4.4.3 Technische Maßnahmen / „Technological Controls“

4.4.3.1 Einschränkung des Zugangs zu Informationen

Die Maßnahmen, die zur Verhinderung von Datenlecks in Betracht gezogen werden sollten, bestehen im Wesentlichen darin, den Zugang zu beschränken.[902] Die Zugriffe, die in einer Richtlinie nach ISO/IEC 27001: A.5.15 geregelt werden sollen, sind nach ISO/IEC 27001: A.8.3 einzuschränken. Dies ist das Konzept der geringsten Anzahl von Rechten.[903]

Beispielsweise sichert Entität A ihre Daten, die an Standort C gehen müssen.[904] In diesem Fall sollte die Entität A die Möglichkeit haben, die Daten zu lesen, und am Standort C nur die Möglichkeit bestehen, die Backups zu sichern.[905] Diese Möglichkeit muss zeitlich begrenzt sein.[906] Um sicher zu sein, dass dieser Prozess tatsächlich funktioniert, muss dies mit einem Session-Token geschehen.[907] Es gibt also einen asymmetrischen Schlüssel, und daraus kann ein Token generiert werden, das für eine bestimmte Zeit verwendet werden kann und danach nicht mehr gültig ist.[908] Auf diese Weise lässt sich der Zugang begrenzen und Benutzern sowie Systeme ermöglichen, die von ihnen benötigte Arbeit zu verrichten, aber auf eine Weise, die kontrolliert, verwaltbar und nachvollziehbar ist.[909]

899 Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 7.
900 Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 7.
901 Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 7.
902 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 26.
903 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 27.
904 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 27.
905 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 27.
906 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 27.
907 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 27.
908 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 27.
909 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 27.

4.4.3.2 Konfigurationsmanagement

ISO/IEC 27001: A.8.9 macht die Festlegung, Dokumentation, Umsetzung und Überwachung sowie Überprüfung der (Sicherheits-) Konfigurationen von Hardware, Software, Diensten und Netzwerken erforderlich. Da der sichere Betrieb von IT-Systemen mit ihrer Konfiguration beginnt, sollte bereits bei der Installation auf ihre Sicherheit geachtet, bewährte Verfahren zur Systemhärtung befolgt (z. B. Einsatz einer Firewall oder Deaktivierung nicht benötigter Services) und die Regelungen in eigenen Richtlinien berücksichtigt werden.[910]

Von Mitarbeitern (inklusive IT-Mitarbeitern) kann nur dann erwartet werden, dass sie sich korrekt verhalten, Updates installieren oder die Systeme konfigurieren, wenn klar geregelt ist, was erwartet wird.[911]

Sicherheit wird jedoch nicht nur durch ein Blatt Papier erreicht.[912] Das ist nur der erste Schritt,[913] der aber unerlässlich ist. Dazu ist es sehr wichtig, auf die sich ändernden Bedingungen zu reagieren, die Konfigurationen kontinuierlich zu überprüfen und ggf. anzupassen.[914]

4.4.3.3 Vermeidung von Datenabfluss

Die Anforderung der ISO/IEC 27001 in Bezug auf die Datenübermittlung betrifft die Maßnahmen nach ISO/IEC 27001: A.8.12 zur Verhinderung von Datenlecks / Datenabfluss. Diese Maßnahmen müssen auf alle Systeme, Netzwerke und Geräte verwendet werden, auf denen sensible Informationen verarbeitet bzw. übertragen werden.

Es könnten Tools zur Verhinderung von Datenlecks / „**Data Leakage Prevention Tools**“, zur Überwachung von Kommunikationsverhalten und zur Meldung verdächtiger Aktivitäten oder zur Blockierung deren Transfer eingesetzt werden.[915] Hierbei handelt es sich um Systeme, die bestimmte Handlungen auf der Grundlage einer bestimmten Logik verhindern.[916]

910 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 123.
911 Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 7.
912 Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 7.
913 Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 7.
914 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 123.
915 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 125.
916 Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 8.

Data Leakage Prevention bzw. Data Loss Prevention (DLP) besteht im Wesentlichen aus zwei Teilen: 1. der Identifizierung von Daten / Ressourcen und 2. deren Verfolgung.[917] Die **Identifizierung** erfolgt in der Regel entweder durch Prüfsummen / „Checksums“ oder digitale Signaturen von Dateien, die als wichtig erachtet werden.[918] Bei einer Prüfsumme handelt es sich um eine Hash-Funktion, die eine Eingabe annimmt und mit den andern Daten vergleicht.[919] Sie beschaffen sich also nicht die Datei selbst; sie geben der Datei lediglich einen Namen.[920]

Bei der **Verfolgung** wird der Internetverkehr in erster Linie daraufhin überwacht, ob sich diese vertrauliche Datei auf dem Computer eines Endbenutzers befindet, ob er über diese Datei verfügen darf und ob er versucht, sie irgendwo hin zu senden.[921] Die Organisation sollte die Kommunikation über VPN oder über Zero-Trust-Network-Access verfolgen.[922] Alles, was sehr vertraulich oder geschützt ist, sollte nur über dieses Transportmittel zugänglich sein.[923]

Es ist erwähnenswert, dass sich DLP weitgehend auf zufällige Lecks konzentriert, denn wenn z. B. jemand versucht, ein Bild von einem Firmengeheimnis zu machen, um es zu verkaufen, kann man nichts dagegen tun.[924] Wenn jedoch jemand ein Dokument fälschlicherweise hochlädt oder weiterleitet, kann DLP dies erkennen und verhindern.

4.4.3.4 Datensicherung / „Backup“

Die Erstellung und Speicherung von Sicherungskopien der Daten ist ein wichtiger Bestandteil einer Notfallwiederherstellungsstrategie.[925] Laut ISO/IEC 27001: A.8.13 sind Backups von Informationen, Software sowie Systemen in einer Richtlinie zu thematisieren und regelmäßig zu testen. Nur eine vernünftige Datensicherung, die belastbar ist, kann sicherstellen, dass die Verfügbarkeit gewährt wird.[926]

917 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 25.
918 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 25.
919 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 25.
920 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 25.
921 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 26.
922 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 26.
923 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 26.
924 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 26.
925 Information Commissioner’s Office, Encryption, 2, 24.
926 Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 9.

Um die Verfügbarkeit von Informationen zu gewährleisten, sollten Sicherungskopien der Daten erstellt werden.[927] Grundsätzlich werden sie auf Band, Festplatte oder anderen physischen Medien aufgezeichnet.[928] Die Organisation muss festlegen, welche Daten gesichert werden sollen, wie oft dies geschehen soll und wo sie gespeichert werden sollen.[929] Vor allem Systeme, die für den Geschäftsbetrieb unerlässlich sind, und die „Kronjuwelen" / „Crown Jewels" einer Organisation müssen vorrangig gesichert werden.[930]

Daten sollten in verschiedenen Orten gesichert werden und auf unterschiedliche Weise zugänglich sein.[931] Durch das Speichern der Kopie an verschiedenen Orten wird ein Medienbruch erzeugt und damit die Fernverwaltung sowie das Fernlöschen aller Backups durch den Hacker geschützt.

Außerdem muss festgelegt werden, ob die Datensicherungen zu verschlüsseln sind und wie Wiederherstellungstests durchzuführen sind.[932] Wenn die Daten in einem verschlüsselten Format gespeichert werden, sind sie vor unberechtigtem Zugriff geschützt.[933] Im Falle einer langfristigen Sicherung oder Archivierung ist sicherzustellen, dass der Zugriff auf die Daten weiterhin möglich ist und dass die verwendete Verschlüsselung auch im Laufe der Zeit angemessen bleibt.[934]

Es sollte möglich sein, die Daten wieder zu verwenden.[935] Ansonsten wird das eigentliche Ziel, warum die Backups gemacht werden, nicht erreicht.[936] Es muss getestet werden, ob die Daten wiederhergestellt werden können.[937] Viele Unternehmen setzen heute auf Cloud-Speicher, da die manuelle Verwaltung von Serverfirmen und Backup-Standorten zeit- und kostenintensiv ist.[938] Es ist erwähnenswert, dass ein Cloud Backup nicht weniger sicher ist als die Anmietung von Rackspace in einem Rechenzentrum.[939] Entscheidend ist dabei, dass diese Backups angemessen abgesichert sind.

Der Anwendungsfall für die Cloud ist typischerweise dann gegeben, wenn die Organisation klein ist und entweder nicht über die Mittel oder die Arbeitskraft verfügt, um seine Datensicherung selbst zu verwalten.[940] Es ist aber auch möglich, einen hybriden Ansatz zu verfolgen, bei dem etwas „on Premise" und etwas in der Cloud (z. B. auf AWS) gespeichert wird.[941]

927 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 125.
928 Information Commissioner's Office, Encryption 2, 24.
929 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 125.
930 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 45.
931 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 28.
932 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 125.
933 Information Commissioner's Office, Encryption, 2, 24.
934 Information Commissioner's Office, Encryption, 2, 24.
935 Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 10.
936 Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 10.
937 Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 10.
938 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 28.
939 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 29.
940 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 29.
941 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 29.

4.4.3.5 Einsatz von Kryptographie / Verschlüsselung

ISO/IEC 27001: A.8.24 stellt klar, dass Regeln für die Verwendung von Verschlüsselung, einschließlich der Verwaltung kryptographischer Schlüssel, festgestellt und umgesetzt werden sollten. Die zu verschlüsselnden Daten hängen vom Grund und vom Ziel ab.[942] Befindet sich der Computer beispielsweise in einem Home-Office, sollte die Verschlüsselung der Daten als zusätzliche Sicherheit gegen die Folgen eines möglichen Zugriffs durch Dritte eingesetzt werden, da in einem solchen Fall die Möglichkeit der Zugriffskontrolle für die Organisation stark eingeschränkt ist.[943] [944]

Da es möglich ist, Daten mit dem richtigen Schlüssel zu entschlüsseln, sind verschlüsselte Daten nicht als anonyme, sondern als pseudonyme Daten zu betrachten.[945] Der Personenbezug kann unter bestimmten Bedingungen wiederhergestellt werden.[946]

Ob verschlüsselte Daten tatsächlich geschützt sind oder nicht, hängt von der gewählten Verschlüsselungsmethode und dem Stand der Technik ab. Technisch gesehen kann eine starke Verschlüsselung, die dem neuesten Stand der Technik entspricht, die Identifizierung von Personen durch Unbefugte unmöglich machen, da die so verschlüsselten Daten keinen Personenbezug mehr aufweisen. Wird die Verschlüsselung im Laufe der Zeit schwach (z. B. durch die von Angreifern entwickelten Methoden zum Brechen einer Verschlüsselung, die zuvor als stark galt), dann werden die verschlüsselten Daten wieder personenbezogen und erfordern weitere Maßnahmen, um sie angemessen zu schützen.[947] Beispiele von Verschlüsselungsprogrammen:

- BitLocker – Verschlüsselung für die gesamte Windows;
- VeraCrypt – Verschlüsselung für Daten, Ordner und Laufwerke;
- Boxcryptor – Ende-zu-Ende-Verschlüsselung für Cloud-Speicher;
- Zip-Ordner – Verschlüsselung einzelner Dateien mit einem Passwort.[948]

942 Verschlüsselung von Dateien: Stolperfallen beim Datenschutz, abrufbar: https://www.mein-datenschutzbeauftragter.de/blog/20170908-verschluesselung-von-dateien-stolperfallen-beim-datenschutz/, zuletzt abgerufen am 04.08.2023.

943 Verschlüsselung von Dateien: Stolperfallen beim Datenschutz, abrufbar: https://www.mein-datenschutzbeauftragter.de/blog/20170908-verschluesselung-von-dateien-stolperfallen-beim-datenschutz/, zuletzt abgerufen am 04.08.2023.

944 Um die Datenschutzrisiken zu minimieren, ist es sinnvoll, alle personenbezogenen Daten, die sogar in speziellen, durch Zugangskontrollen gesicherten Räumen aufbewahrt werden, zu verschlüsseln. S.: Verschlüsselung von Dateien: Stolperfallen beim Datenschutz, abrufbar: https://www.mein-datenschutzbeauftragter.de/blog/20170908-verschluesselung-von-dateien-stolperfallen-beim-datenschutz/, zuletzt abgerufen am 04.08.2023.

945 Haben verschlüsselte Daten einen Personenbezug? abrufbar: https://www.datenschutz-praxis.de/tom/haben-verschluesselte-daten-einen-personenbezug/, zuletzt abgerufen am 04.08.2023.

946 Haben verschlüsselte Daten einen Personenbezug? abrufbar: https://www.datenschutz-praxis.de/tom/haben-verschluesselte-daten-einen-personenbezug/, zuletzt abgerufen am 04.08.2023.

947 Diese Erläuterung über die Verschlüsselung und das Stand der Technik wird in dem folgenden Artikel beschrieben. S.: Haben verschlüsselte Daten einen Personenbezug? abrufbar: https://www.datenschutz-praxis.de/tom/haben-verschluesselte-daten-einen-personenbezug/, zuletzt abgerufen am 04.08.2023.

948 Verschlüsselung, abrufbar: https://ascon-datenschutz.de/datenschutz-abc/verschluesselung/, zuletzt abgerufen am 04.08.2023.

Die meisten **Homepages** verwenden eine SSL- (Secure Sockets Layer) oder TLS- (Transport Layer Security) Verschlüsselung, „die eine verschlüsselte Kommunikation und Authentifizierung zwischen Homepageanbieter und Nutzerbrowser ermöglicht".[949] Nach herrschender Meinung ist die Erhebung von Nutzerdaten (z. B. über Kontaktformulare) nur mit einer solchen Verschlüsselung zulässig.[950]

Bei der **E-Mail-Verschlüsselung** ist zwischen Transportverschlüsselung / „TLS-Encryption" und Inhaltsverschlüsselung bzw. Ende-zu-Ende-Verschlüsselung / „End-to-End-Encryption" zu unterscheiden. Bei der Transportverschlüsselung wird die E-Mail nur während des Transports verschlüsselt; vor und nach der Übertragung bleibt sie unverschlüsselt auf dem Server. Laut dem Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) ist die TLS-Verschlüsselung ein „notwendiger Baustein für die elektronische Kommunikation".[951]

Bei der Inhaltsverschlüsselung sind die Metadaten einer E-Mail (d. h. Absender, Empfänger sowie Betreff) weiterhin lesbar, der restliche Inhalt ist jedoch verschlüsselt.[952] Für eine solche Verschlüsselung werden vor allem die Standards S/MIME und OpenPGP verwendet.[953] Bei besonders sensiblen Daten (z. B. Gesundheitsdaten) kann nach Ansicht der Behörde auch eine Ende-zu-Ende-Verschlüsselung erforderlich sein.[954]

Bei der Nutzung von **öffentlichen WLAN-Netzen** kann eine Verschlüsselung über ein VPN eingerichtet werden.[955] Durch den Einsatz der Tunneltechnik werden die Sicherheitseigenschaften, die im privaten Netz gelten, auch im öffentlichen Netz beibehalten.[956] Die Anwendung des öffentlichen Netzes bleibt für die Nutzer transparent; die Kommunikationsverbindung erscheint als dedizierte private Verbindung.[957] Ein VPN bezweckt damit, die Nutzer des Netzwerks zu authentifizieren, die Vertraulichkeit der transferierenden Daten zu gewährleisten, die notwendigen Schlüssel zu generieren und stets zu erneuern.[958]

949 *Bommel*, Informationen zum Datenschutz.
950 *Bommel*, Informationen zum Datenschutz.
951 Diese Erläuterung über die E-Mail-Verschlüsselung wird in dem folgenden Artikel beschrieben. S.: Die DSGVO und die E-Mail-Verschlüsselung, abrufbar: https://www.e-recht24.de/artikel/datenschutz/11284-dsgvo-und-e-mail-verschluesselung.html, zuletzt abgerufen am 04.08.2023.
952 Die DSGVO und die E-Mail-Verschlüsselung, abrufbar: https://www.e-recht24.de/artikel/datenschutz/11284-dsgvo-und-e-mail-verschluesselung.html, zuletzt abgerufen am 04.08.2023.
953 *Bommel*, Informationen zum Datenschutz.
954 *Bommel*, Informationen zum Datenschutz.
955 *Bommel*, Informationen zum Datenschutz.
956 *Eckert*, IT-Sicherheit: Konzepte – Verfahren – Protokolle, S. 765.
957 *Eckert*, IT-Sicherheit: Konzepte – Verfahren – Protokolle, S. 765.
958 *Eckert*, IT-Sicherheit: Konzepte – Verfahren – Protokolle, S. 765.

Darüber hinaus besteht die Idee der Verwendung eines **VPN** darin, dass der Datenverkehr zentralisiert wird, so dass zur Vermeidung von Datenverlusten nachvollzogen werden kann, welche Daten zu diesem Zweck übertragen werden und dass der Unbefugte keinen Zugriff darauf hat.[959] VPN kann beispielsweise dazu verwendet werden, geografisch verteilte Organisationen (z. B. weltweit agierende Unternehmen) zu verbinden, die mehrere verschiedene Subnetze verwenden.[960]

Bei der Verschlüsselung von Daten besteht die berechtigte Sorge, dass bei Verlust des Schlüssels der Zugriff auf die Daten nicht mehr möglich ist.[961] Dies ist jedoch das Risiko, das im Rahmen einer Sicherheitsverwaltung in Kauf genommen werden sollte.[962] Die Sicherheit der Schlüssel muss gewährleistet werden.[963] Es gibt keinen primären Grund, Daten nicht zu verschlüsseln, es sei denn, es ist eine veraltete Software / „Legacy-Software" im Einsatz, die die Verschlüsselung nicht wahrnehmen kann.[964] In einem solchen Fall muss festgestellt werden, wie den Zugang so weit wie möglich einschränkt werden kann.[965]

Die Verschlüsselung hat eine ähnliche Wirkung wie die Pseudonymisierung.[966] In beiden Fällen ist ein Datensatz für Dritte grundsätzlich unlesbar, weil der Inhalt verändert wurde.[967] Bei der Verschlüsselung wird jedoch der gesamte Inhalt des Datensatzes mit Hilfe einer mathematischen Formel (Schlüssel) in einen Zeichentext (Geheimtext) umgewandelt, der ohne den Schlüssel nicht ohne weiteres gelesen werden kann.[968] Der Text kann jederzeit vom Besitzer des Schlüssels wieder lesbar gemacht werden.[969]

Zusammenfassend lässt sich sagen, dass die Daten verschlüsselt werden sollten.[970] Die Entschlüsselung erhält nur Hash-Werte.[971] Diese Hash-Werte sollten nicht auf eine Person verweisen können.[972] Sie müssen anonymisiert werden, so dass selbst wenn sie enthasht sind, die Person immer noch nicht betroffen ist.[973]

---

959 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 22.
960 *Eckert*, IT-Sicherheit: Konzepte – Verfahren – Protokolle, S. 765 ff.
961 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 29.
962 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 29.
963 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 29.
964 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 29.
965 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 29.
966 *Auernhammer -Kramer/Meinst*, DSGVO BDSG, Art. 32 Rn. 19.
967 *Auernhammer -Kramer/Meinst*, DSGVO BDSG, Art. 32 Rn. 19.
968 *Auernhammer -Kramer/Meinst*, DSGVO BDSG, Art. 32 Rn. 19; vgl.: *Kühling/Buchner -Jandt*, DSGVO/BDSG, Art. 32 Rn. 19.
969 *Auernhammer -Kramer/Meinst*, DSGVO BDSG, Art. 32 Rn. 19.
970 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 23.
971 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 23.
972 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 23.
973 Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 23.

4.4.4 Die PDCA-Methodik: Plan-Do-Check-Act

Um alle oben beschriebenen Maßnahmen in einer Organisation sorgfältig und zielgerichtet umsetzen zu können, ist die PDCA-Methodik anzuwenden. PDCA (Plan-Do-Check-Act) ist aus dem Bereich des Qualitätsmanagements als Deming-Zyklus bekannt.[974] Sie ist die bevorzugte Methode für die meisten Informationssicherheitsteams, die u. a. ISO/IEC 27001 zur kontinuierlichen Verbesserung erfordert.[975] Kontinuierliche Verbesserung spielt in ISO-Normen eine zentrale Rolle, wobei das Erkennen von Schwachstellen, Abweichungen, Bewertung sowie Priorisierung entsprechender Maßnahmen und Umsetzung sowie Überwachung lediglich in einem kontinuierlichen Kreislauf zum Ziel führen.[976]

PDCA ist dann anzuwenden, wenn eine Organisation eine Änderung vornehmen möchte. Wenn eine Organisation beispielsweise einen neuen Firewall installieren oder eine neue Richtlinie beschließen möchte, sind vier grundlegende Schritte zu unternehmen, nämlich: 1. Plan (planen), 2. do (umsetzen), 3. check (überprüfen) und 4. act (handeln / verbessern).[977]

Diese Phasen laufen zyklisch: „Was geplant wird, muss umgesetzt werden. Was umgesetzt wurde, muss überprüft und ggf. gemessen werden“.[978] Aus den Ergebnissen müssen Korrektur- oder Verbesserungsmaßnahmen abgeleitet werden, die wiederum neu geplant werden müssen.[979]

4.4.4.1 Plan / Planung

In der Planungsphase sind klare Ziele und Vorgaben wichtig.[980] Plant eine Organisation beispielsweise neue Maßnahmen, um die Informationssicherheit zu erhöhen, könnte das Ziel darin bestehen, die Eintrittswahrscheinlichkeit von Risiken zu reduzieren, wofür Ressourcen (z. B. Personal und Budget) und Zeitrahmen (z. B. Umsetzungstermine) bereitgestellt werden sollten.[981] Entscheidend ist hierbei die gedankliche Antizipation der zu ergreifenden Handlungsschritte in der Umsetzungsphase.[982]

974 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 29.
975 Information security and PDCA (Plan-Do-Check-Act), abrufbar: https://ictinstitute.nl/pdca-plan-do-check-act/, zuletzt abgerufen am 04.08.2023.
976 Datenschutz und Informationssicherheit: Zwillinge oder Verwandte – kurze Erläuterung zu den Familienverhältnissen. Datenschutz und Informationssicherheit - worin besteht der Unterschied? abrufbar: https://www.coc-ag.de/managed-it-service-stories/datenschutz-und-informationssicherheit, zuletzt abgerufen am 04.08.2023.
977 Information security and PDCA (Plan-Do-Check-Act), abrufbar: https://ictinstitute.nl/pdca-plan-do-check-act/, zuletzt abgerufen am 04.08.2023.
978 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 30.
979 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 30.
980 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 30.
981 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 30.
982 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 30.

4.4.4.2 Do / Umsetzung

In der Umsetzungsphase bzw. Implementierungsphase / Durchführungsphase müssen geplante Maßnahmen verwirklicht und kontrolliert werden; d. h., dass Pläne umgesetzt, Budgets bereitgestellt und Verantwortlichkeiten bestimmten Personen zugewiesen werden sollten.[983] Diese Personen sollten die Schritte durchführen und entsprechend protokollieren.[984] Alles, was in der Planungsphase geplant wird, muss in dieser Phase umgesetzt werden.

4.4.4.3 Check / Überprüfung

In der Check-Phase werden die Abweichungen aufgedeckt, deren Beseitigung im Plan vorgesehen und in der Do-Phase umgesetzt werden.[985] In dieser Phase sind drei Gesichtspunkte zu unterscheiden: Konformität, Effektivität und Effizienz.[986] Durch **Konformitätsprüfung** wird bewertet, ob ein Prozess, ein Verfahren bzw. eine Maßnahme wie geplant umgesetzt wurde oder von den Planungsvorgaben abweicht.[987] Die **Wirksamkeits- / Effektivitätsprüfung** bewertet, ob die geplanten Ziele durch einen Prozess bzw. eine Maßnahme tatsächlich erreicht wurden.[988] Nur weil ein Prozess konform ist, bedeutet das nicht, dass er effektiv ist.[989] **Effizienz / Wirkungsgrad** bewertet, ob ein Prozess bzw. eine Maßnahme im bestmöglichen Verhältnis zum Ergebnis steht.[990]
Die Überprüfungsphase ist nur dann erfolgreich, wenn im Rahmen der Planungsphase die mit den umgesetzten Neuerungen bzw. Änderungen verbundenen Ziele klar beschrieben werden.[991]

4.4.4.4 Act / Verbesserung

Die Informationen, die in der Überprüfungsphase gesammelt werden, liefern den wesentlichsten Input für die Verbesserungsphase, die in der Verbesserungsmaßnahmen ergriffen werden.[992]
In der überwiegenden Mehrheit der Abweichungen wird bestätigt, dass die Maßnahmen umgesetzt wurden.[993] Wenn etwas als kritisch eingestuft wird, zeigt dies, was zu erwarten ist[994] und wo Verbesserungspotentiale liegen. Daraus ergeben sich Anregungen, was bei dem neuen Projekt oder Prozess besser gemacht werden sollte.

983 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 31.
984 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 31.
985 Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 10.
986 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 31.
987 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 31.
988 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 32.
989 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 32.
990 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 32.
991 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 31.
992 *Brenner,* Praxisbuch, ISO/IEC 27001, S. 32.
993 Interwiew mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 11.
994 Interwiew mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 11.

4.5 Zusammenfassung der präventiven Maßnahmen

In den vorangegangenen Kapiteln (Kapitel 1 bis Kapitel 7) wurde deutlich, dass die Verarbeitung bzw. die Transfers von Daten bis hin zur Verletzung von Menschenrechten reicht. Daher ist es unerlässlich zu bestimmen, was bei dem internationalen Datentransfer beachten werden sollte, insbesondere wenn die Daten den Behörden offengelegt oder an die Behörden übermittelt werden. Die Anforderungen sowie Handlungsempfehlungen sind im Wesentlichen im Bereich des Datenschutzes und der Informationssicherheit zu finden.

Kapitel 9 hat deutlich gemacht, was Informationssicherheit gewährleistet und worin der Unterschied zwischen dem Datenschutz und der Informationssicherheit besteht. Es wurde auch deutlich gemacht, dass die Informationssicherheit für den Schutz aller Daten, einschließlich personenbezogener Daten, aber nicht die dahinterstehende Personen sorgt. Dies wird im Wesentlichen durch die Eigenschaften der Vertraulichkeit, Integrität und Verfügbarkeit gewährt. Als weitere Schutzziele werden Authentizität / Authentifizierung, Nichtabstreitbarkeit, Verbindlichkeit, Zuverlässigkeit und Zurechenbarkeit vorgestellt. Sie kollidieren miteinander und ermöglichen einen rechtskonformen und sicheren Datentransfer sowohl national als auch international.

Der bestmögliche internationale Standard für den Umgang mit Informationssicherheitsrisiken im Hinblick auf den Datentransfer findet sich in ISO/IEC 27001. Diese Norm enthält Schritte und Anforderungen, u. a. für die Risiko-Beurteilung. Durch die **Risiko-Beurteilung** werden Risiken identifiziert, analysiert und schließlich bewertet. Dies gibt der Organisation die Möglichkeit, Risiken, die bei dem Datentransfer entstehen können, vorherzusehen und zu beseitigen. Dieser Prozess ist sowohl in der EU als auch in den USA gesetzlich abgesichert.

In der EU regelt die DSGVO mittelbar die Risiko-Beurteilung. Sie bietet Bewertungskriterien sowie Faktoren zur Bestimmung der Schwere des Schadens an. Dies ermöglicht die Akzeptanz der Risiken oder die Durchführung von Abhilfemaßnahmen zur Minderung der Risiken. Anders als in der EU ist das Thema in den USA sektorspezifisch und nicht vollumfangreich festgehalten. Das bedeutet, dass eine Organisation, die in den spezifischen Sektoren tätig ist, verpflichtet werden kann, die Risiko-Beurteilung durchzuführen. Ansonsten kann eine Organisation diese freiwillig oder auf Anfrage einer anderen Organisation vornehmen.

In der EU finden sich **präventive rechtliche Maßnahmen** grundsätzlich im Privacy by Design und Privacy by Default sowie in technischen und organisatorischen Maßnahmen. Privacy by Design versucht, den Datenschutz in der EU zu stärken, Privacy by Default verbessert die Position des Betroffenen.[995] Als Anforderungen für EU-TOM sind Pseudonymisierung, Verschlüsselung, Verfügbarkeit / Backup, Verhaltensregeln, Zertifizierungen und Mitarbeiterunterweisungen zu erwähnen.

Präventive rechtliche Maßnahmen müssen ergriffen werden, um Daten und Systeme zu schützen und ein reibungsloses Funktionieren der Organisation zu ermöglichen. Es sollte jedoch betont werden, dass es sich bei EU-TOM nur um Mindestanforderungen und nicht um alle möglichen Maßnahmen handelt. Jede Organisation muss für sich selbst festlegen, welche Maßnahmen noch ergriffen werden sollten, um die Daten und damit die dahinter stehenden Menschen zu schützen.

Zur Darlegung der präventiven rechtlichen Maßnahmen in den USA wurden die nach der DSGVO erforderlichen Maßnahmen den USA-Maßnahmen gegenübergestellt. Als Ergebnis wurde festgestellt, dass all diese Themen in den USA bekannt, anerkannt und umgesetzt sind, allerdings nicht in dem Umfang wie in der EU. Die branchenspezifischen Anforderungen verursachen das Fehlen einer allumfassenden Regulierung. Entsprechend gibt es keine Möglichkeit, die präventive rechtliche Maßnahmen umfassend in jeder Organisation zu fordern und zu implementieren.

Zur Visualisierung der aktuellen Lage in den USA wurden die DSGVO-Anforderungen grundsätzlich mit den SCA / CLOUD Act und CCPA / CPRA verglichen. Es wurde festgestellt, dass die Themen in diesen Gesetzen grundsätzlich vorhanden sind. Allerdings ist zu beachten, dass sich ihre Anforderungen oft an andere Länder richten oder nicht ausreichend beschrieben sind.

Hierzu lässt sich festhalten, dass in der EU die Themen rund um den (internationalen) Datentransfer gesetzlich vollumfangreich vorgeschrieben sind und alle notwendigen Mindestanforderungen zur Orientierung gegeben sind. In den USA sind die Themen ebenfalls geregelt, jedoch nicht so tief wie in der EU. Wenn sie nicht unter die festgelegten Kriterien fallen, bleibt es bei der Freiwilligkeit oder der Verpflichtung einer anderen Organisation, präventive Maßnahmen durchzuführen. Dies kann keinen dauerhaften Schutz für alle Kategorien personenbezogener Daten bieten.

995 *Auernhammer -Brüggemann*, DSGVO BDSG, Art. 25 Rn. 1.

Sowohl in der EU als auch in den USA kann jede Organisation grundsätzlich freiwillig präventive normative Maßnahmen umsetzen. Die Norm ISO/IEC 27001 kann die rechtskonforme und zielgerichtete Umsetzung von Datenschutz- und Informationssicherheitsmaßnahmen ermöglichen. Sie stellt Mindestanforderungen bereit, die für jede Organisation entscheidend sind. In Bezug auf die Datenübertragung muss eine Organisation gemäß ISO/IEC 27001 zunächst die Bedrohungslage ermitteln, dann alle organisatorische Themen zum Schutz der Daten bei dem (internationalen) Datentransfer verschriftlichen, Beschäftigte entsprechend informieren und schlussendlich alles technisch umsetzen. All dies soll in Form der PDCA-Methodik erfolgen.

Bei der **PDCA-Methodik** besteht die Möglichkeit, die durchgeführten Maßnahmen bzw. Verfahren zunächst zu planen, dann umzusetzen, nach der Umsetzung zu überprüfen / zu kontrollieren und die geprüften Maßnahmen bzw. Verfahren zu verbessern. Nur so ist es möglich, (personenbezogene) Daten insbesondere bei deren Transfer zu schützen, den dahinterstehenden Personen die Ausübung ihrer (Persönlichkeits-) Rechte zu ermöglichen und das Informationssicherheitsniveau in der Organisation zu garantieren.

Trotz aller Bemühungen kann die Sicherheit bei der Datenübertragung beeinträchtigt werden: Die sensiblen Daten können verloren gehen, die Informationen können manipuliert werden, die Systeme können angegriffen werden. Aus diesem Grund müssen neben den präventiven Maßnahmen auch die nachgelagerte Maßnahmen betrachtet werden. Dies sind die Maßnahmen, die zum Einsatz kommen, wenn ein Schadensfall auftritt und trotz aller Anstrengungen die Präventivmaßnahmen nicht mehr helfen können. Was das genau bedeutet und wie dagegen vorzugehen ist, wird im Folgenden analysiert.

5 Nachgelagerte Maßnahmen

5.1 Cyber-Bedrohungen – gefährlicher denn je

5.1.1 Einführung und Relevanz

„The healthy functioning of Cyberspace is essential to our economy and our national security."
George W. Bush [996]

Der Cyberspace hat eine lange Geschichte.[997] Er wurde in den 1960er Jahren als Projekt der Advanced Research Project's Agency ins Leben gerufen, um die aus dem amerikanisch-sowjetischen Rüstungswettlauf resultierenden Kommando- und Kontrollprobleme zu lösen.[998]
Wirtschaftliche und soziale Abhängigkeiten wurden in den letzten 30 Jahren durch technologische Entwicklungen beeinflusst, die die Globalisierung von Wirtschaft und Information erleichtern.[999] Die zunehmende Unabhängigkeit hat zu Schwachstellen sowie absoluten Gewinnen geführt.[1000] Die Verwundbarkeit des Cyberspace als Ergebnis komplexer Interdependenz ist eine Funktion der zunehmenden Abhängigkeit von vernetzten Systemen, die sich über souveräne Räume erstrecken und interoperable Informationsarchitekturen nutzen.[1001]
Cyber ist wichtig, weil er eine moderne Infrastruktur bildet, die die Säulen der nationalen Sicherheit stützt.[1002] Die nationale Sicherheit hängt vom Cyberspace ab.[1003] Die Staaten befinden sich in einer zunehmend vernetzten Welt mit einem vielfältigen Bedrohungsspektrum und wissen nur wenig darüber, wie Entscheidungen in diesem amorphen Bereich getroffen werden.[1004]
Neben der nationalen Sicherheit sind auch Bereiche, wie die Wirtschaft und das tägliche Leben, betroffen. IDC (International Data Corporation) fand heraus, dass 80 % der Verbraucher ihre Geschäfte durch andere Unternehmen laufen lassen würden, wenn sie von einer Datenschutz-verletzung betroffen wären.[1005]

996 *Brantly*, The decision of Attack: Military and Intelligence Cyber Decision-Making, S. 31.
997 *Brantly*, The decision of Attack: Military and Intelligence Cyber Decision-Making, S. 2.
998 *Brantly*, The decision of Attack: Military and Intelligence Cyber Decision-Making, S. 2.
999 *Brantly*, The decision of Attack: Military and Intelligence Cyber Decision-Making, S. 10.
1000 *Brantly*, The decision of Attack: Military and Intelligence Cyber Decision-Making, S. 10.
1001 *Brantly*, The decision of Attack: Military and Intelligence Cyber Decision-Making, S. 10
1002 *Brantly*, The decision of Attack: Military and Intelligence Cyber Decision-Making, S. 26.
1003 *Brantly*, The decision of Attack: Military and Intelligence Cyber Decision-Making, S. 12.
1004 *Brantly*, The decision of Attack: Military and Intelligence Cyber Decision-Making, S. 1.
1005 Incident Response Plan 101: The 6 Phases, Templates, and Examples, abrufbar: https://www.exabeam.com/incident-response/incident-response-plan/, zuletzt abgerufen am 05.08.2023.

Der Wert des Cyberspace spiegelt die Verbindungen zu den Systemen der Logik wider und liegt mit seiner Fähigkeit zum speichern, interagieren, verbinden und kontrollieren.[1006] Die Macht und die Gefahr des Cyberspace liegt in der Beziehung zwischen Informationen und der sie umgebenden Welt sowie in der Art und Weise, wie Nutzer in einem sozialen Umfeld auf diese Informationen zugreifen und sie manipulieren oder verstehen.[1007]

Der grenzübergreifende Datentransfer schafft den internationalen Cyber-Raum, der eine internationale Angelegenheit ist und dementsprechend internationale Hindernisse mit sich bringt. Die Cyber-Domäne ist ein modernes Schlachtfeld und erfordert ein ganzheitliches Verständnis.[1008]

Sehr oft zielen Cyber-Angriffe darauf ab, die Arbeitsprozesse oder die Hardware sowie die Software einer Organisation zu beeinträchtigen. Wenn das ,,Nervensystem" einer Organisation, wie die für informationstechnologische und digitale Lösungen, betroffen ist, ist die gesamte Organisation bedroht.[1009] Hierbei kann es zu Datenschutzverletzungen, Informationssicherheitsvorfällen oder Cyber-Angriffen kommen, die sowohl geschäftskritische Daten bzw. Informationen als auch personenbezogene Daten und damit die Rechte jedes Einzelnen schädigen bzw. gefährden können. Sie erfordern daher einen hochprofessionellen Umgang mit dem Thema und den Schutz dieser Daten. Vor diesem Hintergrund sollten nach der Konkretisierung der cyberspezifischen Risiken das Verhalten zur Risiko-Prävention / ,,Preparedness" und beim Ernstfall / ,,Response" definiert werden.[1010]

Das Thema ,,Prävention" wurde bereits beschrieben (s. → S. 122-156). Grundlegend ging es hierbei darum, welche rechtlichen und normativen Maßnahmen ergriffen werden sollten, um einen Vorfall gar nicht erst entstehen zu lassen. Allerdings ist zu beachten, dass „Preparedness" keine 100-prozentige Sicherheit garantiert.[1011] Aus verschiedenen Gründen kann eine Organisation dennoch mit einem Sicherheitsvorfall konfrontiert werden. Jede Organisation muss wissen, was im Notfall bzw. im ,,Ernstfall" zu tun ist.[1012]

1006*Brantly*, The decision of Attack: Military and Intelligence Cyber Decision-Making, S. 3.
1007*Brantly*, The decision of Attack: Military and Intelligence Cyber Decision-Making, S. 3.
1008*Brantly*, The decision of Attack: Military and Intelligence Cyber Decision-Making, S. 108.
1009*Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 17.
1010*Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 18.
1011*Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 12.
1012*Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 12.

Um festzulegen, wie im Falle eines Vorfalls zu reagieren ist, sollten Maßnahmen bzw. Schritte implementiert werden, die klarstellen, wie damit umgegangen wird. Da Cybersicherheit kein rein technisches Thema ist, sollte neben dem IT-Bereich auch eine umfassende organisatorische / unternehmenische Sichtweise implementiert werden, die aufzeigt, welche Bereiche sowie Assets besonders bedeutsam oder schützenswert sind.[1013] Cyber und Recht lassen sich nicht trennen.[1014] Technisch-organisatorische Maßnahmen basieren am besten auf gesetzlichen Anforderungen, da diese jeden Verantwortlichen und Auftragsverarbeiter gleichermaßen verpflichten. Dies schafft einen einheitlichen Rahmen für jede Person oder Organisation, die an dem internationalen Datentransfer beteiligt ist.

Bedrohungen gegen den Schutz der Daten bzw. Informationen einer Organisation werden im Folgenden definiert (B. Gefährdungen der Informationssicherheit und C. Cyber-Attacken). Um diesen Gefahren oder Angriffen vorzubeugen und die Geschäftsprozesse am Laufen zu halten, muss sich eine Organisation dafür vorher vorbereiten (Kapitel 15 – Incident Response) und bei einem Sicherheitsvorfall entsprechende Schritte vornehmen (Kapitel 16 – Incident Response Steps).

5.1.2 Gefährdungen der Informationssicherheit

„**Gefahr**“ wird als übergeordneter Begriff betrachtet; unter **Gefährdung** / „Applied Threat“ wird eine räumlich und zeitlich nach Art, Ausmaß und Richtung genau beschriebene Gefahr gesehen.[1015] Sie ist eine Bedrohung, die sich durch eine Schwachstelle auf ein Objekt auswirkt.[1016] Zum Beispiel können defekte oder gestohlene Datenträger zu Datenverlusten[1017] führen.[1018] Defekte Datenträger sowie Diebstahl von Datenträgern sind Gefährdungen, Datenverlust ist eine Gefahr.[1019]

1013 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 7.

1014 Diese Meinung wurde auf der Global GRC, Data Privacy & Cyber Security ConfEx am 31.05.2023 in NY/USA geäußert.

1015 BSI, IT-Grundschutz-Kompendium, Glossar – S. 3.

1016 BSI, IT-Grundschutz-Kompendium, Glossar – S. 3.

1017 Ein Datenverlust ist ein Ereignis, das zu einem Verlust der Verfügbarkeit führt, so dass ein Datensatz nicht mehr wie gewünscht verwendet werden kann. Ein Beispiel für einen Datenverlust ist das unbeabsichtigte oder unbefugte Löschen von Daten, u.a. aufgrund von Fehlbedienung, Stromausfällen, Verunreinigungen oder Malware. S.: BSI, Elementare Gefährdungen, S. 48; BSI, IT-Grundschutz-Kompendium, Elementare Gefährdungen – S. 45.

1018 BSI, IT-Grundschutz-Kompendium, Glossar – S. 3.

1019 BSI, IT-Grundschutz-Kompendium, Glossar – S. 3.

Zu den Gefahren der Informationssicherheit, die Sicherheit von Informationen oder Geschäftsprozessen gefährden, gehören laut BSI (Bundesamt für Sicherheit in der Informationstechnik)[1020] u. a. die folgenden Ereignisse: 1. Verletzung von Gesetzen oder Vorschriften,[1021] 2. Ausfall oder Störung von Versorgungsnetzen (z. B. Strom, Wasser oder Telefon),[1022] 3. Entmagnetisierung von Magnetdatenträgern durch hohe Temperatur,[1023] 4. Unbefugte Verwendung von Geräten und Systemen,[1024] 5. Nötigung, Erpressung oder Korruption.[1025]

6. Großveranstaltungen: Straßenfeste, Sportveranstaltungen oder Demonstrationen können den ordnungsgemäßen Betrieb einer Organisation beeinträchtigen.[1026] Solche Veranstaltungen können zur Einschüchterung von Mitarbeitern, zu Gewalt gegen das Personal und das Gebäude führen.[1027]

7. Elektromagnetische Störstrahlung: Es gibt viele verschiedene Quellen von elektromagnetischen Feldern bzw. Strahlungen (z. B. WLAN, Bluetooth oder GSM), deren ausreichend starke elektromagnetische Störstrahlung elektronische Geräte beeinträchtigen oder beschädigen kann.[1028] In der Folge kann es u. a. zu Ausfällen oder Störungen kommen.[1029] Auf bestimmten Datenträgern gespeicherte Informationen können durch solche Strahlungen gelöscht oder verfälscht werden.[1030]

8. Abfangen kompromittierender Strahlung: Elektrische Geräte (z. B. Computer oder Drucker), die elektromagnetische Wellen abstrahlen, können die zu verarbeitenden Informationen mit sich führen.[1031] Ein Angreifer, der sich in der Nähe befindet, kann diese Aussendung empfangen und daraus die verarbeiteten Daten rekonstruieren.[1032]

9. Fehlfunktion von Geräten oder Systemen: Geräte und Systeme, die zur Informationsverarbeitung eingesetzt werden, haben grundsätzlich viele Funktionen, und dementsprechend komplex sind sowohl ihre Hardware- als auch ihre Softwarekomponenten aufgebaut.[1033] Diese Komplexität bedeutet, dass es in solchen Komponenten viele verschiedene Fehlerquellen gibt.[1034] Infolgedessen funktionieren Geräte und Systeme nicht wie vorgesehen, was zu Sicherheitsproblemen führt.[1035]

1020Das BSI ist in Deutschland tätig, aber die von ihm aufgelisteten Bedrohungen sind Ereignisse, die weltweit existieren und allen betroffenen Organisationen oder Einrichtungen schaden u.a. in der EU sowie in den USA.
1021BSI, Elementare Gefährdungen, S. 32.
1022BSI, Elementare Gefährdungen, S. 13.
1023BSI, Elementare Gefährdungen, S. 5.
1024BSI, Elementare Gefährdungen, S. 33.
1025BSI, Elementare Gefährdungen, S. 38.
1026BSI, Elementare Gefährdungen, S. 10.
1027BSI, Elementare Gefährdungen, S. 10.
1028BSI, Elementare Gefährdungen, S. 15.
1029BSI, Elementare Gefährdungen, S. 15.
1030BSI, Elementare Gefährdungen, S. 15.
1031BSI, Elementare Gefährdungen, S. 16.
1032BSI, Elementare Gefährdungen, S. 16.
1033BSI, Elementare Gefährdungen, S. 29.
1034BSI, Elementare Gefährdungen, S. 29.
1035BSI, Elementare Gefährdungen, S. 29.

10. Ressourcenmangel: Werden für bestimmte Aufgaben nur unzureichende personelle, zeitliche und finanzielle Ressourcen zur Verfügung gestellt, kann das vielfältige negative Auswirkungen haben.[1036] Wenn z. B. notwendige Rollen in Projekten nicht mit geeigneten Personen besetzt werden oder Hard- oder Software nicht mehr ausreichen, können Fachaufgaben nicht erfolgreich bearbeitet werden.[1037]

5.1.3 Cyber-Attacken

„We are Anonymous. We are Legion.
We do not forgive. We do not forget. Expect us."
Zitiert in Scott S., „We are Anonymous."[1038]

Cyber-Kriminalität ist eine sehr ernsthafte Bedrohung für jede Organisation. Das Bundeskartellamt (BKA) sieht in der Cyberkriminalität nach dem islamischen Terrorismus derzeit die größte Herausforderung für seine Arbeit.[1039] Cyber-Angriffe sind das größte Risiko in Märkten, die 50 % des weltweiten Bruttoinlandsprodukt ausmachen.[1040]

Die Qualität von Cyber-Angriffe steigt stetig.[1041] Cyber-Kriminelle sind technisch versiert und mit immensen Ressourcen ausgestattet.[1042] Außerdem sind sie kreativ und finden immer neue Wege, Organisationen zu gefährden.[1043] Sie versuchen, anonym zu bleiben und geplante Ziele, wie Reputationsschäden einer Organisation durch unterschiedliche Wege zu erreichen, z. B. durch Verschlüsselung von Daten oder durch illegale Veröffentlichung von Informationen.

Die **Anonymität** im Cyberspace hat viele Gesichter.[1044] Die Ebenen der Anonymität werden durch die drei folgenden Merkmale bestimmt: 1. Die Unmöglichkeit der Identifizierung, 2. die Unmöglichkeit zu erkennen, dass ein Angriff stattfindet und 3. die Unmöglichkeit, das Objekt eines Angriffs zu isolieren.[1045] Die Anonymität von Cyber-Angriffen ist von Natur aus gefährlich, da diese Bedrohungen jedem Akteur zugeschrieben werden können, der eine ungünstige Beziehung zum Opfer des Angriffs hat.[1046]

1036 BSI, Elementare Gefährdungen, S. 30.
1037 BSI, Elementare Gefährdungen, S. 30.
1038 *Brantly,* The decision of Attack: Military and Intelligence Cyber Decision-Making, S. 79.
1039 Tagung des BKA: Cyberkriminalität – eine der größten Herausforderungen, abrufbar: https://www.deutschlandfunk.de/tagung-des-bka-cyberkriminalitaet-eine-der-groessten-100.html, zuletzt abgerufen am 05.08.2023.
1040 From unemployment to growing cyber-risk: business executives in different regions have different worries, abrufbar: https://www.weforum.org/press/2018/11/from-unemployment-to-growing-cyber-risk-business-executives-in-different-regions-have-different-worries/, zuletzt abgerufen am 05.08.2023.
1041 *Gabel u.a.,* Rechtshandbuch Cyber-Security, S. 3.
1042 *Gabel u.a.,* Rechtshandbuch Cyber-Security, S. 4.
1043 *Gabel u.a.,* Rechtshandbuch Cyber-Security, S. 4.
1044 *Brantly,* The decision of Attack: Military and Intelligence Cyber Decision-Making, S. 80.
1045 *Brantly,* The decision of Attack: Military and Intelligence Cyber Decision-Making, S. 80.
1046 *Schünemann/Baumann,* Privacy, Data Protection and Cybersecurity in Europe, S. 102.

Alle Arten von kriminellen Aktivitäten profitieren von der Nutzung weit verbreiteter, oft unzureichend geschützter Computernetzwerke für den Umgang mit vertrauenswürdigen Informationen oder sogar für wirtschaftliche Transaktionen.[1047] Es gibt also tatsächlich Kriminelle im Internet.[1048] Es ist aber nicht alles, was die Bedrohungswahrnehmung ausmacht.[1049] Darüber hinaus gibt es Cyber-Krieger und Terroristen, die die kritische Infrastruktur der Gesellschaft angreifen und sogar aus der Ferne materiellen Schaden anrichten könnten.[1050] Aus dieser Perspektive sind Cyber-Bedrohungen nicht nur ein Thema der Polizeiarbeit und der Heimatpolitik, sondern können auch gravierende Herausforderungen für die internationale Politik, Sicherheit und Ordnung darstellen.[1051] Zu häufigsten Formen der Cyber-Angriffe gehören u. a. die folgenden Angriffe:

1. Ransomware:[1052] Im Allgemeinen gibt es zwei Arten davon: Blockierung bzw. Sperrung des Zugriffs zu dem System und Verschlüsselung der Daten der infizierten Systeme.[1053] In beiden Fällen ist Arbeit mit den Computern nicht mehr möglich, da der Zugriff auf Daten sowie Anwendungen verweigert werden.[1054] Um frei zu kommen, soll eine Organisation ein „Lösegeld" zahlen, meist in Form von digitalen Bitcoins.[1055]

2. Malware: Hierbei geht es um die Vernichtung von Daten oder die Sabotage betrieblicher Abläufe.[1056] Das Opfer wird mittels Schadsoftware / „Malicious Software" bzw. „Malware" angegriffen, um seine Wettbewerbsfähigkeit zu schwächen und seinen Ruf zu schädigen.[1057]

3. Man-in-the-Middle-Attacke: Bei diesem Angriff nimmt der Hacker unbemerkt eine Vermittlerposition zwischen den Kommunikationsteilnehmern ein und gibt zu diesem Zweck für den Absender einer Nachricht an den tatsächlichen Empfänger und für den Empfänger an den tatsächlichen Absender vor.[1058] Gelingt dies, ist der Hacker in der Lage, Nachrichten zwischen Empfänger und Absender entgegenzunehmen und zu manipulieren.[1059]

1047*Schünemann/Baumann*, Privacy, Data Protection and Cybersecurity in Europe, S. 101 ff.
1048*Schünemann/Baumann*, Privacy, Data Protection and Cybersecurity in Europe, S. 102.
1049*Schünemann/Baumann*, Privacy, Data Protection and Cybersecurity in Europe, S. 102.
1050*Schünemann/Baumann*, Privacy, Data Protection and Cybersecurity in Europe, S. 102.
1051*Schünemann/Baumann*, Privacy, Data Protection and Cybersecurity in Europe, S. 102.
1052Die Ransomware „WannaCry" griff im Mai 2017 mehr als 230 000 Systeme in über 150 Ländern an, darunter Unternehmen, Institutionen und Privatpersonen. S.: Bundeskartellamt, Cybercrime: Bundeslagebild S. 12.
1053*Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 4.
1054*Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 4.
1055*Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 4.
1056*Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 4.
1057*Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 4.
1058BSI, Elementare Gefährdungen, S. 46.
1059BSI, Elementare Gefährdungen, S. 46.

4. CEO-Fraud: Bei diesem Angriff gibt sich der Täter als Geschäftsführer oder eine andere Führungskraft aus und versucht, sogar ohne gefragt zu werden, relevante Mitarbeiter einer Organisation unter Druck zu setzen, damit sie das Geld überweisen.[1060] Sie informieren sich im Voraus über Projekte oder geplante Investitionen und versuchen mittels verschiedener Quellen wie Wirtschaftsnachrichten, Publikationen oder Social-Media-Plattformen, eine glaubwürdige „Story" zurechtzulegen.[1061]

5. Spionage: Sie beinhaltet das Sammeln, Auswerten und Verarbeiten von Informationen über eine Organisation, Personen, Produkte oder andere Gegenstände.[1062] Diese Informationen können zum Verschaffen von Wettbewerbsvorteilen gegenüber anderer Organisation, zur Erpressung der Personen oder zum Replizieren eines Produktes eingesetzt werden.[1063]

6. APT-Angriff (Advanced Persistent Threat): Bei diesem Angriff bleibt der Angreifer häufig lange Zeit im Netzwerk unentdeckt, um eine Organisation auszuspionieren und so viele Informationen wie möglich zu beschaffen.[1064] Die Spionage-Software wird über eine Spear-Phishing-E-Mail in die gezielte Organisation eingeschleust, d. h. sie wird personalisiert und an ausgewählte Mitarbeiter gesendet.[1065] Die Adressaten werden dazu verleitet, eine bestimmte Website aufzurufen oder einen Anhang herunterzuladen.[1066] Geschieht dies, wird die Schadsoftware auf dem betroffenen Computer installiert, die sich im Hintergrund in der gesamten Organisation verbreitet.[1067]

7. DoS-Attacke (Verhinderung von Diensten / „Denial of Service"): Bei dieser Art von Angriffen geht es häufig um verteilte Ressourcen, die von einem Angreifer so weit verbraucht werden, dass sie für die tatsächlichen Benutzer nicht mehr verfügbar sind.[1068] Er nutzt bereits bekannte Sicherheitslücken oder Fehler in der Maschinenkonfiguration aus, um auf das Zielsystem zuzugreifen, das „über ungeschützte Ports, unsichere Dienste oder andere Schwachstellen" erreichbar ist.[1069] Solche Angriffe zielen auf geschäftsrelevante Werte aller Art ab.[1070] Typische Erscheinungsformen von DoS-Angriffen sind die Unterbrechung von Geschäftsprozessen, die Beeinträchtigung der Infrastruktur und die Verursachung von IT-Ausfällen.[1071]

1060 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 6.
1061 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 6.
1062 BSI, Elementare Gefährdungen, S. 17.
1063 BSI, Elementare Gefährdungen, S. 17.
1064 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 5; Bundeskartellamt, Bundeslagebild: Cybercrime, S. 27 ff.
1065 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 5.
1066 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 5 Rn. 12.
1067 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 5 Rn. 12.
1068 BSI, Elementare Gefährdungen, S. 43.
1069 *Eckert*, IT-Sicherheit: Konzepte – Verfahren – Protokolle, S. 122.
1070 BSI, Elementare Gefährdungen, S. 43.
1071 BSI, Elementare Gefährdungen, S. 43.

8. DDoS-Attacke (Verteilte Diensteverweigerung / „Distributed Denial of Service“): Dieser Angriff ist ein DoS-Angriff wobei mehrere Computer oder Maschinen verwendet werden, um eine Zielressource zu überfluten.[1072] Der Angreifer sendet massive Anfragen an den Server des Opfers und überlastet dessen Systeme.[1073] Die Fernsteuerung von Tausenden von manipulierten Computern verschafft dem Angreifer eine Bandbreite für einen Angriff, die die meisten Internetzugänge um Größenordnungen übersteigt.[1074] Solche Angriffe können für den Wettbewerb äußerst schädlich sein, weil sie z. B. IT-gestützte Arbeitsprozesse zur Folge haben.[1075]

Sowohl DoS- als auch DDoS-Angriffen überlasten einen Server oder eine Webanwendung mit dem Ziel, Dienste zu unterbrechen. Hierbei sind sie u. a. durch die folgenden Merkmale zu unterscheiden: 1. Bei einem DoS-Angriff handelt es sich um einen Angriff auf ein einzelnes System, während bei einem DDoS-Angriff mehrere Systeme ein einzelnes System angreifen. 2. Da ein DoS-Angriff von einer einzigen Stelle ausgeht, ist es einfacher, seinen Ursprung zu erkennen und die Verbindung zu unterbrechen; ein gut funktionierender Firewall kann dies tun. Ein DDoS-Angriff hingegen geht von mehreren entfernten Standorten aus und verschleiert seinen Ursprung. 3. Da ein DDoS-Angriff von mehreren Standorten ausgeht, kann er viel schneller ausgeführt werden als ein DoS-Angriff, der von einem einzigen Standort ausgeht. Die höhere Angriffsgeschwindigkeit erschwert die Erkennung des Angriffs, was zu größeren Schäden oder sogar zu einer Katastrophe führen kann.[1076]

1072 DoS Attack vs. DDoS Attacks, abrufbar: https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos, zuletzt abgerufen am 05.08.2023.

1073 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 5.

1074 *Eckert*, IT-Sicherheit: Konzepte – Verfahren – Protokolle, S. 78.

1075 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 5.

1076 Der Unterschied zwischen DoS- und DDoS-Angriffe wird in dem folgenden Artikel beschrieben. S.: DoS Attack vs. DDoS Attacks, abrufbar: https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos, zuletzt abgerufen am 05.08.2023.

5.2 Incident Response

„We do not second-guess good faith exercises of judgement about cyber-incident disclosure. But we have also cautioned that a company's response to such an event could be so lacking that an enforcement action would be warranted."
Steven Peikin, (Co-Director of the U.S. Securities and Exchange Commission, Enforcement Division)[1077]

Laut einer Bericht von IBM (International Business Machines Corporation) betrugen die durchschnittlichen Kosten einer Datenschutzverletzung im Jahr 2023 weltweit 4,45 Mio. USD, was einem Anstieg um 15% innerhalb von drei Jahren entspricht.[1078] Ein effektiver Reaktionsprozess kann diese Kosten erheblich senken und den Ruf einer Organisation schützen.[1079] Ein solcher Prozess kann allerdings nur durch eine angemessene Vorbereitung erreicht werden, die eine schnelle Beseitigung des Vorfalls sowie Rückkehr zum Normalbetrieb gewährleistet.

Cyber Incident Response ist die Bezeichnung für die Reaktion auf einen IT-Sicherheitsvorfall und die damit verbundenen Maßnahmen.[1080] Es müssen Vorkehrungen für den Fall getroffen werden, dass es trotz der getroffenen Sicherheitsmaßnahmen zu einem Cyber-Vorfall kommt.[1081] Kernstück der Notfallplanung sind ein Notfallteam / „**Incident Response Team**" und ein Maßnahmenplan / „**Incident Response Plan**".[1082]

Die Vorbereitungsphase gehört zu dem Cyber-Security Governance.[1083] Ziel dieser Phase ist es, durch Zuständigkeiten, Kommunikations- sowie Entscheidungsprozesse die Voraussetzungen für entsprechende Maßnahmen und Entscheidungen zu schaffen, die auch unter Zeitdruck umgesetzt werden können.[1084] In diesem Zusammenhang ist es wichtig, die negativen Auswirkungen eines Sicherheitsvorfalls abzumildern und die Kontinuität sowie Widerstandsfähigkeit der wirtschaftlichen und sozialen Aktivitäten zu unterstützen.[1085]

1077 U.S. Securities and Exchange Commission, Altaba, Formerly known as Yahoo! Charged with Failing to Disclosure Massive Cybersecurity Breach; Agrees to Pay $35 Million, Press Release 2018-71.
1078 Cost of a Data Breach Report 2023: A million-dollar race to detect and respond, abrufbar: https://www.ibm.com/reports/data-breach, zuletzt abgerufen am 05.08.2023.
1079 Incident Response Plan 101: The 6 Phases, Templates, and Examples, abrufbar: https://www.exabeam.com/incident-response/incident-response-plan/, zuletzt abgerufen am 05.08.2023.
1080 Warum Incident Response wichtiger denn je ist, abrufbar: https://www.pwc.de/de/im-fokus/cyber-security/cyber-incident-response.html?utm_source=google&utm_medium=cpc&utm_campaign=XM_thenewequation_CS&utm_id=suche&utm_content=text&utm_term=cyber%20incident%20response, zuletzt abgerufen am 05.08.2023.
1081 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 43.
1082 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 43.
1083 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 43.
1084 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 43.
1085 OECD, Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, 3, 11.

Bei der Responsephase sind die mittelbaren und unmittelbaren Reaktionen zu unterscheiden. Die **unmittelbare Reaktion** erfolgt ab dem Zeitpunkt, zu dem die Organisation von dem Vorfall erfährt, und konzentriert sich auf die Schadensbegrenzung.[1086] Die **mittelbare Reaktion** erfolgt nach der unmittelbaren Reaktion auf den Cybervorfall und erreicht die Normalisierung der Unternehmensprozesse durch die Aufarbeitung von Lerneffekten.[1087]

5.2.1 Incident Response Team

Gemäß ISO/IEC 27001: A.5.24 sollen Prozesse sowie Rollen und Verantwortlichkeiten definiert, implementiert und kommuniziert werden, um Informationssicherheitsvorfälle zu handhaben. Klare Festlegungen, die den betroffenen Personengruppen vermittelt werden, sind wichtig, um den Aspekt der Kohärenz zu berücksichtigen.[1088]

Entsprechend dem prozessorientierten Ansatz eines Managementsystems muss vor allem festgelegt werden, wer bei einem Informationssicherheitsvorfall involviert wird und was genau zu tun ist.[1089] Verantwortlichkeiten werden grundsätzlich durch die Rollendefinition und Zuweisung der Personen bzw. Gruppen festgelegt.[1090] Dies wird am besten in einer Richtlinie und einer Matrix klar definiert und aufgeführt.

Das **Ziel** des Reaktionsteams / „Incident Response Teams“ ist es, die wichtigsten Ressourcen sowie Teammitglieder während eines Vorfalls zu koordinieren und aufeinander abzustimmen, um die Auswirkungen zu minimieren und den Betrieb so schnell wie möglich wiederherzustellen.[1091] Dazu gehören Untersuchung und Analyse, Kommunikation, Schulung und Sensibilisierung, Dokumentation und Erstellung eines Zeitplans,[1092] Entwicklung eines Reaktionsplans, das Testen auf und die Behebung von Systemschwachstellen, die Aufrechterhaltung strenger Best Practices für die Sicherheit und die Unterstützung bei allen Maßnahmen zur Behandlung von Vorfällen.[1093]

1086 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 43.
1087 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 43.
1088 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 90.
1089 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 89.
1090 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 90.
1091 Incident Response Team: What are the Roles and Responsibilities? abrufbar: https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response/arming-your-incident-response-team, zuletzt abgerufen am 05.08.2023.
1092 Incident Response Team: What are the Roles and Responsibilities? abrufbar: https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response/arming-your-incident-response-team, zuletzt abgerufen am 05.08.2023.
1093 incident response team, abrufbar: https://www.techtarget.com/searchsecurity/definition/incident-response-team, zuletzt abgerufen am 05.08.2023.

Die Mitglieder eines Incident Response Teams verfügen in der Regel über verschiedene technische **Fähigkeiten**, Hintergründe und Rollen, um auf unvorhergesehene Sicherheitsvorfälle vorbereitet zu sein. Darüber hinaus weisen sie Problemlösungskompetenzen, gute Teamarbeit und Kommunikationsfähigkeiten, intellektuelle Neugier sowie eine scharfe Beobachtungsgabe auf. Rede- und Schreibfähigkeiten sind dazu unerlässlich, denn Kooperation und Koordination sind der Schlüssel zu einer effektiven Reaktion auf Vorfälle.[1094]

Die **Standorte** der Reaktionsteams können variieren. Wenn eine Organisation einige Standorte hat, ist es unter Umständen nicht möglich, an jedem Standort ein komplettes Team bereitzuhalten. In einem solchen Fall soll eine Organisation versuchen, an jedem Standort einen vertrauenswürdigen Vertreter für jede Incident-Response-Funktion zu haben, um die Vorfälle persönlich zu untersuchen und zu analysieren.[1095]

Wenn es um die Reaktion auf einen Vorfall geht, sollte das **Krisenmanagement** unter Einbeziehung der IT-Abteilung eingeschaltet werden, wobei alle wichtigen Geschäftsbereiche zu vertreten sind. Im Allgemeinen lassen sie sich in die folgenden Bereiche unterteilen: 1. Technik (die IT-Forensiker und IT-Instandsetzung), 2. Organisation (die Betriebsorganisation und Betriebsunterbrechung), 3. Kommunikation (die interne und externe Kommunikation, einschließlich der Erpresser-Kommunikation) und 4. Legal (einschließlich Datenschutz und Versicherung).[1096]

Bei einem Vorfall sind insbesondere die folgenden **Rollen** zu berücksichtigen: Teamleiter (auch als ein Prozessverantwortlicher, ein Manager, oder Security Incident Coordinator bezeichnet[1097]): Er leitet und koordiniert alle Aktivitäten des Teams und sorgt dafür, dass man sich auf die Schadensminimierung sowie die schnelle Wiederherstellung konzentriert. Leitender Ermittler: Er sammelt und analysiert u. a. alle Beweise, ermittelt die Grundursache und führt eine schnelle System- und Dienstwiederherstellung durch. Kommunikationsleiter: Er leitet die Bemühungen um Kommunikation für alle Zielgruppen, sowohl innerhalb als auch außerhalb der Organisation. Leiter der Dokumentation und des Zeitplans: Er dokumentiert alle Aktivitäten und entwickelt einen zuverlässigen Zeitplan für jede Phase des Vorfalls.[1098]

1094 Die Fähigkeiten der Mitglieder eines Incident Responce Teams wird in dem folgenden Artikel beschrieben. S.: Incident Response Team: What are the Roles and Responsibilities? abrufbar: https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response/arming-your-incident-response-team, zuletzt abgerufen am 05.08. 2023.

1095 Über die Standorte des Reaktionsteams wird in dem folgenden Artikel beschrieben. S.: incident response team, abrufbar: https://www.techtarget.com/searchsecurity/definition/incident-response-team, zuletzt abgerufen am 05.08. 2023.

1096 Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 17 ff.

1097 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 90.

1098 Die Rollen, die in dem Abschnitt beschrieben worden sind, finden sich in dem folgenden Artikel. S.: Incident Response Team: What are the Roles and Responsibilities? abrufbar: https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response/arming-your-incident-response-team, zuletzt abgerufen am 05.08.2023.

Darüber hinaus muss bei einer Datenschutzverletzung / Datenpanne der Datenschutzbeauftragte (DSB) bzw. der für den Datenschutz Verantwortliche unverzüglich eingeschaltet werden. Bei einem Informationssicherheitsvorfall muss der Informationssicherheitsbeauftragter / „Chief Information Security Officer“ (CISO)[1099] bzw. die für die Informationssicherheit zuständige Person unverzüglich involviert werden.

Hierbei sind einige Beispiele für **Formen** des Incident Response Teams aufgeführt: Computer Security Incident Response Team (CSIRT)[1100] / Security Incident Response Team (SIR-Team):[1101] Hierbei handelt es sich um ein Team von Fachleuten, das für die Prävention und Reaktion auf Sicherheitsvorfälle zuständig ist.[1102] Zu seinen Aufgaben gehören das Sammeln der Informationen, die Durchführung der Analyse und die Beantwortung von Anfragen der Antragsteller.[1103] Ein CSIRT kann dauerhaft oder für bestimmten Fällen eingerichtet werden.[1104] Es kann auch Aspekte der Reaktion auf Vorfälle in anderen Abteilungen übernehmen, z. B. den Umgang mit rechtlichen Fragen oder die Kommunikation mit der Presse.[1105]

Es gibt eine breite Palette von CSIRTs. Beispielsweise ist ein internes CRIST Teil der Regierungen, Konzerne oder Universitäten, das u. a. Disaster-Recovery-Pläne sicherstellt. Das nationale CSIRT ist für die Reaktion auf Sicherheitsvorfälle zuständig, die sich auf ein ganzes Land auswirken.[1106]

1099 Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 12.

1100 Alternative Begriffe des CSIRT sind u.a.: „CIRC (Computer Incident Response Capability), CIRT (Computer Incident Response Team), IRC (Incident Response Center or Incident Response Capability), IRT (Incident Response Team), SERT (Security Emergency Response Team) und SIRT (Security Incident Response Team)“. S.: Computer Security Incident Response Team (CSIRT), abrufbar: https://www.computerweekly.com/de/definition/Computer-Security-Incident-Response-Team-CSIRT, zuletzt abgerufen am 05.08.2023.

1101 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 90.

1102 incident response team, abrufbar: https://www.techtarget.com/searchsecurity/definition/incident-response-team, zuletzt abgerufen am 05.08.2023.

1103 Computer Security Incident Response Team (CSIRT), abrufbar: https://www.computerweekly.com/de/definition/Computer-Security-Incident-Response-Team-CSIRT, zuletzt abgerufen am 05.08.2023.

1104 Computer Security Incident Response Team (CSIRT), abrufbar: https://www.computerweekly.com/de/definition/Computer-Security-Incident-Response-Team-CSIRT, zuletzt abgerufen am 05.08.2023.

1105 incident response team, abrufbar: https://www.techtarget.com/searchsecurity/definition/incident-response-team, zuletzt abgerufen am 05.08.2023.

1106 Die in diesem Abschnitt dargestellte Beschreibung findet sich in dem folgenden Artikel. S.: Computer Security Incident Response Team (CSIRT), abrufbar: https://www.computerweekly.com/de/definition/Computer-Security-Incident-Response-Team-CSIRT, zuletzt abgerufen am 05.08.2023.

Computer Emergency Response Team (CERT): Hierbei geht es grundsätzlich um ein CSIRT,[1107] d. h. um ein Team von Fachleuten, das für den Umgang mit Cyber-Bedrohungen und Schwachstellen innerhalb einer Organisation zuständig ist.[1108] Darüber hinaus veröffentlicht es seine Erkenntnisse, um anderen bei der Stärkung ihrer Sicherheitsinfrastruktur zu helfen.[1109]

Sicherheitsoperationszentrum / „Security Operations Center" (SOC): Es handelt sich um eine Art Kommandozentrale, die sich der Überwachung, der Analyse und dem Schutz einer Organisation vor Cyberangriffen widmet. Ein SOC besteht in der Regel aus Bedrohungsjägern und Analysten, die sich ausschließlich auf die Reaktion auf Sicherheitsvorfälle konzentrieren.[1110]

5.2.2 Incident Response Plan

Bei einem Vorfall benötigt das Reaktionsteam einen Notfallplan / „Incident Response Plan", um entsprechend agieren zu können. Keine Organisation kann eine wirksame Reaktion auf einen Zwischenfall von jetzt auf gleich auf die Beine stellen.[1111] Diejenigen, die erst während eines Angriffs einen Plan entwickeln, geraten unter Druck.[1112] Es muss ein Plan zur Vorbeugung und Reaktion auf Ereignisse vorhanden sein.[1113]

Ein Plan zur Reaktion auf Vorfälle ist ein Dokument, das die Verfahren, Schritte sowie Verantwortlichkeiten im Rahmen des Programms zur Reaktion auf Vorfälle beschreibt. Da es hierbei nicht nur um eine technische Angelegenheit geht, muss der Plan auf die Prioritäten einer Organisation und das akzeptable Risikoniveau abgestimmt werden. Der Wert dieses Plans endet nicht, wenn ein Vorfall vorbei ist; er bietet weiterhin Unterstützung bei erfolgreichen Rechtsstreitigkeiten, Dokumentation für Auditoren sowie historisches Wissen, das in den Risikobewertungsprozess einfließt und den Reaktionsprozess auf Vorfälle verbessert.[1114]

1107 Computer Security Incident Response Team (CSIRT), abrufbar: https://www.computerweekly.com/de/definition/Computer-Security-Incident-Response-Team-CSIRT, zuletzt abgerufen am 05.08.2023.

1108 incident response team, abrufbar: https://www.techtarget.com/searchsecurity/definition/incident-response-team, zuletzt abgerufen am 05.08.2023.

1109 incident response team, abrufbar: https://www.techtarget.com/searchsecurity/definition/incident-response-team, zuletzt abgerufen am 05.08.2023.

1110 Diese Beschreibung des SOC findet sich in dem folgenden Artikel. S.: incident response team, abrufbar: https://www.techtarget.com/searchsecurity/definition/incident-response-team, zuletzt abgerufen am 05.08.2023.

1111 Incident Response (IR): Plan & Process, abrufbar: https://www.crowdstrike.com/cybersecurity-101/incident-response/, zuletzt abgerufen am 05.08.2023.

1112 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 12.

1113 Incident Response (IR): Plan & Process, abrufbar: https://www.crowdstrike.com/cybersecurity-101/incident-response/, zuletzt abgerufen am 05.08.2023.

1114 Diese Erläuterung des Notfallplans wird in dem folgenden Artikel beschrieben. S.: Incident Response (IR): Plan & Process, abrufbar: https://www.crowdstrike.com/cybersecurity-101/incident-response/, zuletzt abgerufen am 05.08.2023.

NIST schreibt in SP 800-61: 2.3.2, Absätze 1 und 2 ausdrücklich vor, dass jede Organisation einen Plan benötigt, der ihren individuellen Anforderungen entspricht, basierend auf dem Auftrag, der Größe, der Struktur und den Funktionen der Organisation, und stellt die erforderlichen **Komponenten sowie Anforderungen** an diesen Plan bereit. Der Notfallplan sollte die folgenden Elemente enthalten: 1. Auftrag, 2. Strategien und Ziele, 3. Genehmigung durch das Senior Management, 4. Organisatorischer Ansatz zur Reaktion auf Vorfälle, 5. Kommunikationswege auf Vorfälle mit der eigenen sowie mit anderen Organisationen, 6. Metriken zur Messung der Reaktionsfähigkeit auf Zwischenfälle und ihrer Wirksamkeit, 7. Fahrplan für die Entwicklung der Reaktionsfähigkeit auf Vorfälle, 8. Sicherstellung, wie sich das Programm in die Gesamtorganisation einfügt. Der Auftrag, die Strategien und die Ziele der Organisation in Bezug auf die Reaktion auf Zwischenfälle sollten bei der Festlegung der Struktur der Reaktionsfähigkeit auf Zwischenfälle helfen. Die Struktur des Programms zur Reaktion auf Zwischenfälle sollte ebenfalls im Plan erörtert werden.

Gemäß SP 800-61: 2.3.2, Abs. 3 muss eine Organisation, sobald sie einen Incident Response Plan entwickelt und die Genehmigung der Geschäftsleitung erhalten hat, diesen umsetzen und mindestens einmal jährlich überprüfen. Dadurch kann sie sicherstellen, dass die Organisation den Notfallplan für die Entwicklung der Fähigkeit und die Erfüllung ihrer Ziele für die Reaktion auf Zwischenfälle einhält.

Der Notfallplan sollte immer verfügbar sein und gut kommuniziert werden.[1115] Es wird vorzugsweise sowohl in elektronischer als auch in Papierform zur Verfügung gestellt, so dass er für alle, die ihn benötigen, immer sofort erreichbar ist. Außerdem muss der Plan in Krisenübungen getestet werden, um festzustellen, ob er im Ernstfall funktioniert oder ob etwas angepasst werden muss. Diese Übungen gewährleisten auch, dass die beteiligten Personen im Vorfall richtig handeln.

1115 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 12.

5.3 Incident Response Steps

Ist niedergeschrieben, wie es mit einem Vorfall umzugehen ist, steht fest, wer in einem Incident Response Team beteiligt sein dürfte, und ist ein Incident Response Plan erstellt worden, bleibt nur die richtige Handlung während des Vorfalls.

Um den Angriff rasch verhindern und Geschäftsprozesse schnell wiederherstellen zu können, müssen folgende Schritte unternommen werden, nämlich: 1. Erfassung und Bewertung des Angriffs / ,,Identification“, 2. Schadensbegrenzung / ,,Minimization“ und Beseitigung, 3. Dokumentation aller relevanten Informationen / ,,Documentation“, 4. Benachrichtigung bzw. Meldung / ,,Notification“, 5. Beweissicherung, 6. Analyse der Ursachen und möglicher Maßnahmen / ,,Lessons Learned“ und 7. Rückkehr zum Normalbetrieb / ,,Remediation“. All dies wird in den kommenden Abschnitten betrachtet und analysiert.

5.3.1 Erfassung und Bewertung des Angriffs / „Identification“

Zunächst muss der Sachverhalt ermittelt werden.[1116] Dazu muss ein klares Bild über das Ausmaß und die Auswirkungen des Cyberangriffs vermittelt werden, d. h. welche Form der Angriff hat, wer wahrscheinlich der Täter ist, welche Systeme, Netzwerke und Daten[1117] oder welche natürlichen bzw. juristischen Personen betroffen sind.[1118] Außerdem muss festgestellt werden, ob der Angriff andauert, welche Schwachstellen ausgenutzt wurden und welche Mittel zur Durchführung des Angriffs verwendet wurden.[1119] Bei einem IT- und Cyber-Vorfall ist es, solange verwertbare Spuren vorhanden sind, immer notwendig, einen IT-Forensiker einzuschalten.[1120]

Die IT-Forensiker sind mit ihren Analysen in der Lage zu rekonstruieren, was passiert ist und wie es zu dem Vorfall kam.[1121] Dadurch wird der Sachverhalt nachgebildet.[1122] Es ist hierbei zu erwähnen, dass je länger der Vorfall zurückliegt, desto wahrscheinlicher es ist, dass es keine forensisch verwertbaren Daten mehr gibt.[1123] In einem solchen Fall sind meistens die Daten nicht mehr da, bzw. es gibt keine Protokolldateien mehr.[1124]

1116 Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 14.
1117 Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 14; Gabel u.a., Rechtshandbuch Cyber-Security, S. 12.
1118 Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 14.
1119 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 44 und 47.
1120 Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 14.
1121 Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 15.
1122 Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 15.
1123 Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 15.
1124 Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 15.

Grundsätzlich werden Informationssicherheitsereignisse durch die technische Überwachung der IT- und Kommunikationsinfrastruktur identifiziert und dokumentiert.[1125] Es sollte jedoch betont werden, dass einige Hinweise auf potenzielle Verletzungen der Informationssicherheit aus dem Wissen bzw. der Erfahrung von Einzelpersonen in Verbindung mit Aufmerksamkeit im Tagesgeschäft resultieren.[1126] Mitarbeiter sollten aufgefordert werden, jede verdächtige Aktivität im Zusammenhang mit Hardware, Software oder physischer Sicherheit der zuständigen Stelle zu melden und alle erforderlichen Schritte einzuleiten. Hierfür sind geeignete Meldewege und Dokumentationsmöglichkeiten vorzusehen.[1127] All dies wird in der Regel am besten durch entsprechende Richtlinien und Arbeitsanweisungen geregelt.

Nach der Identifizierung des Vorfalls ist dieser zu bewerten.[1128] Es ist immer notwendig, zuerst vollumfangreich zu erfassen, was passiert ist (analysieren), dann zu bewerten, wie es passiert ist (nachdenken) und schließlich zu bestimmen, was dagegen zu tun ist (handeln).[1129] Dazu gehört auch die Feststellung, ob es sich um eine Datenschutzverletzung oder einen Vorfall im Bereich der Informationssicherheit handelt.

5.3.1.1 Datenschutzverletzung

Beim Umgang mit einem Vorfall ist es wichtig zu bestimmen, um welche Art bzw. Kategorie es sich handelt. Hierbei ist grundsätzlich zwischen Datenschutzverletzungen und Informationssicherheitsvorfällen zu unterscheiden.

Ein **Sicherheitsvorfall** ist ein Ereignis, das gegen die Prozesse, Richtlinien oder Verfahren einer Organisation verstößt.[1130] Sicherheitsverletzungen können das Ergebnis eines vorsätzlichen Angriffs sein, bei dem eine Person oder eine Gruppe von Personen absichtlich in ein Netzwerk eindringt, um Daten während der Übertragung zu erfassen oder in eine Datenbank einzudringen, um Daten im Ruhezustand zu erfassen und einzusehen, zu zerstören oder zu entwenden.[1131] Es kann aber auch durch Fahrlässigkeit oder Versehen geschehen, z. B. wenn ein Angestellter eines Unternehmens einen Laptop auf dem Weg zu einer Besprechung in einem Taxi zurücklässt.[1132]

1125 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 90.
1126 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 90.
1127 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 90.
1128 Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 14.
1129 Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 14.
1130 The difference between a security incident and a data breach, abrufbar: https://www.empowerit.com.au/blog/difference-between-security-incident-and-data-breach/, zuletzt abgerufen am 05.08.2023.
1131 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 146.
1132 *Kirtley/Shally-Jensen*, Privacy Rights in the Digital Age, S. 146.

Datenschutzverletzungen fallen unter den Sicherheitsvorfall, bei dem ein unbefugter Nutzer Zugang zu vertrauliche Informationen bekommt. Diese Informationen sind in der Regel personenbezogene Daten. Eine Datenschutzverletzung wird durch böswillige Bedrohungen verursacht (z. B. Phishing, Account-Hijacking oder Malware-Angriff), kann aber auch durch Mitarbeiter verursacht werden (z. B. Missbrauch von Zugangsrechten, Diebstahl vertraulicher Informationen oder versehentliche Offenlegung vertraulicher Daten). Daher sind alle Datenschutzverletzungen Sicherheitsvorfälle, aber nicht alle Sicherheitsvorfälle sind Datenschutzverletzungen. [1133]

Eine Datenpanne bzw. Datenschutzverletzung **auf EU-Ebene** liegt vor, wenn gegen die Datenschutzvorschriften verstoßen wird, weil z. B. unbefugte Dritte sich Zugang zu den Daten verschafft haben und der Umgang damit unsicher ist.[1134]

Artikel 4 Nr. 12 DSGVO definiert die Datenschutzverletzung als eine „Verletzung des Schutzes personenbezogener Daten“, die die folgenden Situationen umfasst: 1. Vernichtung (jegliche unwiderrufliche Löschung / Entfernung der Daten), 2. Verlust (unvorhersehbarer temporärer oder dauerhafter Datenverlust), 3. Veränderung (inhaltliche Neugestaltung der Daten, die den Daten einen neuen Inhalt gibt), 4. unbefugte Offenlegung bzw. Weitergabe (Offenlegung oder Weitergabe der Daten an Dritte ohne Einwilligung oder Rechtsvorschrift) sowie 5. unbefugter Zugang[1135] (unautorisierte bzw. unerlaubte Einsicht zu Daten).

In den USA ist die Definition einer Datenschutzverletzung vom jeweiligen Landesgesetz abhängig, beinhaltet jedoch in der Regel den unbefugten Zugriff auf oder die Aneignung von Computerdaten, die die Sicherheit, Vertraulichkeit oder Integrität personenbezogener Daten beeinträchtigen.[1136]

Gemäß Cal. Civ. Code bedeutet „Verletzung der Systemsicherheit“ die unbefugte Aneignung von Computerdaten, die die Sicherheit, Vertraulichkeit oder Integrität personenbezogener Daten gefährdet, die von der Behörde (nach 1798.29 (f) Cal. Civ. Code), einer Person oder einem Unternehmen (nach 1798.82 (g) Cal. Civ. Code) verwaltet werden. Die gutgläubige Erlangung personenbezogener Daten für die Zwecke der Behörde, der Person oder des Unternehmens stellt keine Verletzung der Systemsicherheit dar, sofern diese Daten nicht verwendet oder einer weiteren unbefugten Offenlegung unterzogen werden.

1133 The difference between a security incident and a data breach, abrufbar: https://www.empowerit.com.au/blog/difference-between-security-incident-and-data-breach/, zuletzt abgerufen am 05.08.2023.

1134 *Solmecke/Kocatepe*, DSGVO für Website-Betreiber: Ihr Leitfaden für die sichere Umsetzung der EU-Datenschutz-Grundverordnung, S. 76.

1135 DSGVO: So gehen Sie mit Datenpannen richtig um, abrufbar: https://www.datenschutz-praxis.de/pleiten-pech-pannen/dsgvo-datenpannen/, zuletzt abgerufen am 05.08.2023.

1136 Data Protection Laws and Regulations USA 2023, abrufbar: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa, zuletzt abgerufen am 05.08.2023.

5.3.1.2 Informationssicherheitsvorfall

Das Erkennen von Informationssicherheitsvorfällen erfolgt durch Informationssicherheitsereignisse.[1137] Einzeln betrachtet, müssen sie nicht unbedingt Anlass zur Sorge geben.[1138] Der Verdacht auf einen Verstoß gegen Informationssicherheitsregeln oder -maßnahmen (z. B. ein fehlgeschlagener Versuch zur Authentifizierung wegen eines falschen Passworts) entsteht oft nur in einem bestimmten Zusammenhang.[1139]

ISO/IEC 27000: 3.31 definiert den Begriff des **Informationssicherheitsvorfall** / „Information Security Incident". Demnach handelt es sich um ein einzelnes oder eine Reihe unbeabsichtigter oder unerwarteter Informationssicherheitsereignisse, bei denen die Wahrscheinlichkeit groß ist, dass sie die Geschäftsaktivitäten gefährden und die Informationssicherheit bedrohen.

Ein Informationssicherheitsvorfall unterscheidet sich von einem **IT-Vorfall**. Bei einem IT-Vorfall handelt es sich um eine Fehlfunktion von Software, Hardware oder IT-Infrastruktur. Dabei handelt es sich nicht um eine unbefugte Partei wie einen Hacker. Wenn die Fehlermeldung oder Störung durch eine Person oder eine Aktion verursacht wird, die die Funktionalität der Software, Hardware oder IT-Infrastruktur beeinträchtigt oder unmöglich macht, ist die Rede von einem Informationssicherheitsvorfall. Zum Beispiel meldet ein Mitarbeiter, dass sein Computer nicht mehr funktioniert oder das Netzteil durchgebrannt ist.[1140] Solche Fälle sind typische IT-Vorfälle, die von der IT-Abteilung zu bearbeiten sind.[1141] Wenn der Computer aber nicht mehr funktioniert, weil er mit Schadsoftware infiziert ist, dann ist die Rede von einem Informationssicherheitsvorfall.[1142]

5.3.2 Schadensbegrenzung / „Minimization" und -beseitigung

Wird der Sachverhalt erfasst und bewertet, muss weiterer Schaden verhindert und beseitigt werden. Zunächst ist das laufende Ereignis aktiv zu bekämpfen (z. B. im Falle eines Ransomware-Angriffs, wenn die Daten verschlüsselt sind, die Internetverbindung mit allen Endgeräten zu trennen), und es sind die negativen Einfluss zu stoppen, damit das Schadenereignis nicht mehr weitergeht.[1143] Hierbei werden u. a. die Passwörter geändert, Systeme gehärtet und weitere Verbreitung der Schadsoftware verhindert.[1144]

1137*Brenner*, Praxisbuch, ISO/IEC 27001, S. 90.
1138*Brenner*, Praxisbuch, ISO/IEC 27001, S. 90.
1139*Brenner*, Praxisbuch, ISO/IEC 27001, S. 90.
1140Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 11.
1141Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 11.
1142Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 11.
1143Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 16.
1144Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 16.

Werden Schäden verhindert, muss sichergestellt werden, dass das Problem dauerhaft beseitigt wird.[1145] Dafür ist eine von diesen Handlungen zu übernehmen: 1. Es muss eine Entschlüsselungssoftware bzw. der Schlüssel dafür eingeholt werden, die verschlüsselte Daten zu entschlüsseln, oder 2. die Daten sollen durch Backups wiederhergestellt werden. Bevor die Systeme wieder in Betrieb genommen werden, muss sichergestellt werden, dass das Netz gereinigt wird und ein erneuter Angriff durch Angreifer ausgeschlossen ist. Darüber hinaus ist es wichtig dem Management beratend zur Verfügung zu stehen,[1146] um die bestmögliche Entscheidungen zum Schutz der Daten und die gesamte Organisation treffen zu können.

Aus technischer Sicht besteht die zentrale Herausforderung darin, die festgestellten Sicherheitslücken zu schließen.[1147] Weil jede Cyber-Attack individuell ist, kann kein exakter Ablauf zur Schließung der Sicherheitslücken beschrieben werden, aber Szenarien können vorhersehen und eine Einstufung möglicher Angriffsarten festgelegt werden.[1148] Basierend auf den Erstinformationen nach einem Cybervorfall sind erste Entscheidungen zu treffen, z. B. welche Experten beteiligt werden sollten und welche Reaktionen in Betracht gezogen werden können, um Schäden möglichst effizient zu reduzieren.[1149]

5.3.3 Dokumentation

ISO/IEC 27001: A.5.26 schreibt vor, dass auf Vorfälle im Bereich der Informationssicherheit durch dokumentierte Verfahren reagiert wird. Dies ist natürlich auch im Falle einer Datenschutzverletzung wichtig.

Für die spätere Rechtsverfolgung und Rechenschaftslegung ist es wichtig, alle relevanten Informationen über den Angriff festzuhalten.[1150] Die Dokumentation sollte die Art des Angriffs, die ergriffenen Gegenmaßnahmen, alle relevanten Protokolldaten und weitere technische Details sowie alle anderen Aktivitäten des Angreifers enthalten.[1151] Wenn z. B. ein Mitarbeiter eine verdächtige Aktivität bemerkt hat, muss dokumentiert werden, wann, wo, was passiert ist und wer daran beteiligt war.

1145Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 16.
1146*Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 12 ff.
1147*Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 44.
1148*Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 44.
1149*Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 44.
1150*Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 13.
1151*Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 13.

5.3.4 Benachrichtigung bzw. Meldung / „Notification“

Cyber-Angriffe und ihre Folgen sind für Organisationen oft keine „Privatsache“; sie müssen klären, welchen Informationspflichten sie rechtlich unterworfen sind.[1152] Außerdem ist im Einzelfall zu prüfen, ob weitere Dritte (z. B. Behörden, Versicherungen oder Geschäftspartner) zu benachrichtigen sind.[1153]

Im Bereich „Notification“ bei einer Datenschutzverletzung unterscheiden sich die gesetzlichen Anforderungen auf europäischer und US-amerikanischer Ebene. Deshalb werden sie einzeln dargestellt und in der Zusammenfassung miteinander verglichen.

In dem Bereich der Notification bei einem Informationssicherheitsvorfall gibt es keine europaweite oder amerikaweite Verpflichtungen. Meldewesen existieren derzeit in Europa nur landesweit. In Deutschland wird beispielsweise nur von KRITIS-Unternehmen[1154] erwartet, dass sie der Meldepflicht im Falle eines Informationssicherheitsvorfalls nachkommen.[1155]

Dies ändert sich durch die **NIS-2-Richtlinie** (EU-Richtlinie zur Netzwerk- und Informationssicherheit),[1156] die für Unternehmen, die zu den wesentlichen oder wichtigen Sektoren gehören (z. B. Strom und öffentlicher Nahverkehr), mehr als 50 Mitarbeiter beschäftigen und einen Jahresumsatz / Jahresbilanz von mehr als 10 Millionen Euro haben, gelten.[1157] Gemäß ErwGr. 102 NIS-2-Richtlinie sollten die Einrichtungen dieser Sektoren unverzüglich, spätestens jedoch innerhalb von 24 Stunden, eine Frühwarnung und innerhalb von 72 Stunden eine Meldung vorlegen. Spätestens einen Monat nach der Meldung des Sicherheitsvorfalls sollte ein Abschlussbericht vorgelegt werden. Diese Richtlinie muss bis spätestens 2024 in nationales Recht umgesetzt werden.[1158]

In den USA verlangt CIRCIA (Cyber Incident Reporting for Critical Infrastructure Act of 2022) von der CISA (Cybersecurity and Infrastructure Security Agency), Vorschriften zu entwickeln und zu erlassen, die die betroffenen Unternehmen dazu verpflichten, der CISA alle erfassten Cyber-Vorfälle innerhalb von 72 Stunden nach dem Zeitpunkt zu melden, an dem das Unternehmen vernünftigerweise glaubt, dass der Vorfall eingetreten ist.[1159]

1152 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 13.

1153 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 13.

1154 „Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“ (z.B. Energie und Wasserversorgung). S.: Kritische Infrastrukturen, abrufbar: https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html, zuletzt abgerufen am 05.08.2023.

1155 Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 13.

1156 Interview mit Dr. Florian Wrobel, im elektronischen Zusatzmaterial, Anlage 2, S. 12.

1157 NIS-2-Richtlinie: neue Cybersecurity-Pflichten verabschiedet, abrufbar: https://www.reuschlaw.de/news/nis-2-richtlinie-neue-cybersecurity-pflichten-verabschiedet/, zuletzt abgerufen am 05.08.2023.

1158 NIS-2-Richtlinie: neue Cybersecurity-Pflichten verabschiedet, abrufbar: https://www.reuschlaw.de/news/nis-2-richtlinie-neue-cybersecurity-pflichten-verabschiedet/, zuletzt abgerufen am 05.08.2023.

1159 Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), abrufbar:

5.3.4.1 Notification nach dem europäischen Recht

Im Falle einer Datenschutzverletzung ist festzulegen, ob, wann und wie diese den zuständigen Aufsichtsbehörden gemeldet und die betroffenen Personen benachrichtigt werden müssen.[1160] Von der Meldepflicht umfasst sind alle Verantwortlichen sowie öffentliche Stellen.[1161] Auf diese Weise erhalten die Betroffenen die Möglichkeit, auch selbst die geeigneten und notwendigen Maßnahmen zu ergreifen, um weiteren Schaden abzuwenden.[1162]

Solche Verletzungen stehen im Zusammenhang mit den IT-Sicherheitszielen der Vertraulichkeit, Verfügbarkeit und Integrität. Ihre Meldepflicht besteht, wenn die Schutzmaßnahmen nicht wirksam waren und dadurch gegen die DSGVO-Anforderungen verstoßen wurde, unabhängig davon, ob dies durch Verschulden, unbeabsichtigt oder unrechtmäßig geschehen ist. Eine bloße Softwarepanne ohne Personenbezug ist damit nicht erfasst. Entscheidend ist dabei, wie viele Informationen über Art, Umfang sowie sonstige Umstände der Verletzung vorgelegt sind; lediglich ein Verdacht oder die vage Identifizierung des Vorfalls reicht nicht aus.[1163]

Die Meldung an die Aufsichtsbehörde muss nach Art. 33 Abs. 3 DSGVO folgende Angaben enthalten: 1. Beschreibung der Art der Verletzung, 2. Kategorien und Anzahl der betroffenen Personen, 3. Kategorien und Anzahl der betroffenen Datensätze, 4. Name und Kontakt-informationen des Datenschutzbeauftragten oder der Kontaktstelle, 5. Beschreibung der voraussichtlichen Folgen der Verletzung und 6. Beschreibung der eingeleitete sowie vorgeschlagenen Maßnahmen.

Die Meldung muss nach Art. 33 Abs. 1 S. 1 DSGVO unverzüglich und möglichst innerhalb von 72 Stunden erfolgen. Kann diese Frist nicht eingehalten werden, muss nach Art. 33 Abs. 1 S. 2 DSGVO die Meldung einen Grund für die Verzögerung enthalten.

---

https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia, zuletzt abgerufen am 05.08.2023.

1160 DSGVO: So gehen Sie mit Datenpannen richtig um, abrufbar: https://www.datenschutz-praxis.de/pleiten-pech-pannen/dsgvo-datenpannen/, zuletzt abgerufen am 05.08.2023.

1161 DSGVO: So gehen Sie mit Datenpannen richtig um, abrufbar: https://www.datenschutz-praxis.de/pleiten-pech-pannen/dsgvo-datenpannen/, zuletzt abgerufen am 05.08.2023.

1162 *Solmecke/Kocatepe*, DSGVO für Website-Betreiber: Ihr Leitfaden für die sichere Umsetzung der EU-Datenschutz-Grundverordnung S. 33.

1163 Die in diesem Abschnitt dargestellte Aussage findet sich in dem folgenden Artikel. S.: DSGVO: So gehen Sie mit Datenpannen richtig um, abrufbar: https://www.datenschutz-praxis.de/pleiten-pech-pannen/dsgvo-datenpannen/, zuletzt abgerufen am 05.08.2023.

Die Meldung muss nicht unbedingt in ihrer Gesamtheit auf einmal erfolgen. Da nur in seltenen Fällen alle relevanten Informationen über die Verletzung von Anfang an vorgelegt sein können, erlaubt Art. 33 Abs. 4 DSGVO ein schrittweises Vorgehen. Sobald neue Informationen verfügbar sind, werden diese in einer Folgemeldung mit einem Verweis auf frühere Meldungen mitgeteilt. Die kumulative Meldung beinhaltet eine „Ermittlungspflicht“ des Verantwortlichen, bis alle Informationen vorliegen, die die Aufsichtsbehörde zur Prüfung des Vorfalls benötigt.[1164]

Ein „normales“ Risiko, das keine speziellen Qualifikation erfordert, reicht für die Meldepflicht an die Aufsichtsbehörde aus.[1165] Der Betroffene ist nach Art. 34 Abs. 1 DSGVO nur dann zu benachrichtigen, wenn die Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten des Betroffenen darstellt.

Die Benachrichtigung muss nach Art. 34 Abs. 2 DSGVO in klarer und einfacher Sprache verfasst werden und die folgenden Angaben enthalten: 1. Die Art des Datenschutzverletzung, 2. die voraussichtlichen Folgen, 3. die eingeleiteten oder vorgeschlagenen Maßnahmen und 4. den Namen sowie die Kontaktdaten des Datenschutzbeauftragten oder der Kontaktstelle.

Gemäß Art. 34 Abs. 3 DSGVO entfällt die Benachrichtigungspflicht, wenn: 1. Der Verantwortliche geeignete technische und organisatorische Maßnahmen getroffen hat. Dies bezieht sich insbesondere auf die Vorkehrungen, durch die personenbezogene Daten für Unbefugte unzugänglich gemacht werden (z. B. Verschlüsselung), 2. der Verantwortliche sichergestellt hat, dass durch die nachfolgende Maßnahmen das hohe Risiko für die Rechte und Freiheiten des Betroffenen mit hoher Wahrscheinlichkeit nicht mehr besteht oder 3. die Benachrichtigung mit unverhältnismäßigem Aufwand verbunden ist. In einem solchen Fall ist stattdessen eine öffentliche Bekanntmachung bzw. eine ähnliche Maßnahme zu ergreifen, die den Betroffenen in vergleichbar wirksamer Weise informiert.

1164Die in diesem Abschnitt dargestellte Aussage findet sich in dem folgenden Artikel. S.: DSGVO: So gehen Sie mit Datenpannen richtig um, abrufbar: https://www.datenschutz-praxis.de/pleiten-pech-pannen/dsgvo-datenpannen/, zuletzt abgerufen am 05.08.2023.

1165DSGVO: So gehen Sie mit Datenpannen richtig um, abrufbar: https://www.datenschutz-praxis.de/pleiten-pech-pannen/dsgvo-datenpannen/, zuletzt abgerufen am 05.08.2023.

5.3.4.2 Notification nach dem amerikanischen Recht

In den USA gibt es kein nationales Bundesgesetz zur Meldung von Datenschutzverletzungen; stattdessen haben **alle Bundesstaaten** (einschließlich der US-Territorien und des District of Columbia) ihre eigenen Gesetze erlassen.[1166]

Ein Unternehmen mit oder ohne physische Präsenz in einem bestimmten Staat muss in der Regel die Gesetze dieses Staates einhalten, wenn es mit unbefugtem Zugriff auf persönliche Informationen konfrontiert wird, die es über Einwohner dieses Staates sammelt, speichert, überträgt bzw. verarbeitet.[1167]

Die Gesetze gelten für bestimmte Arten von persönlichen Informationen bzw. personenbezogenen Daten der Einwohner des jeweiligen Bundesstaates. Die Arten dieser Informationen variieren, wobei die meisten Staaten personenbezogene Daten so definieren, dass sie den Vor- und Nachnamen einer Person mit der Führerschein- oder Personalausweisnummer sowie Zahlungskarten-Informationen umfassen. In einigen Staaten gibt es weitere zusätzliche auslösende Datenpunkte, wie z. B. das Geburtsdatum oder biometrische Daten.[1168]

Meldepflichten bei Datenschutzverletzungen werden ausgelöst, wenn die Vertraulichkeit, Sicherheit oder Integrität der personenbezogenen Daten durch Verlust oder unbefugten Zugriff beeinträchtigt wurde.[1169] Zur Feststellung dieser Verpflichtung enthalten die staatlichen Gesetze in der Regel einen Schwellenwert für das Risiko eines Schadens.[1170] Beispielsweise verlangen einige Staaten, dass ein wesentliches oder erhebliches Risiko / „a material or substantial risk“ besteht, bevor eine Meldung erforderlich ist.[1171] Eine Minderheit von Staaten, u. a. Kalifornien und New York, legt keinen Schwellenwert für einen Schaden fest und verlangt nur eine tatsächliche oder begründete Annahme, dass ein Verstoß stattgefunden hat.[1172] Die kalifornischen Gesetze zu diesem Thema gelten als die strengsten.[1173] [1174]

1166 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 357; vgl.: California Data Security Breach Reporting Requirements, abrufbar: https://www.termsfeed.com/blog/data-security-breach-reporting-requirements-california/, zuletzt abgerufen am 05.08.2023.

1167 Data Protection Laws and Regulations USA 2023, abrufbar: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa, zuletzt abgerufen am 05.08.2023.

1168 Die in diesem Abschnitt dargestellte Aussage findet sich in dem folgenden Artikel. S.: Data Protection Laws and Regulations USA 2023, abrufbar: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa, zuletzt abgerufen am 05.08.2023.

1169 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 357.

1170 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 357.

1171 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 357.

1172 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 357.

1173 California Data Security Breach Reporting Requirements, abrufbar: https://www.termsfeed.com/blog/data-security-breach-reporting-requirements-california/, zuletzt abgerufen am 05.08.2023.

1174 Das Security Magazine berichtet unter Berufung auf eine Studie von Omnisend, dass Kalifornien, Heimat einiger der größten Unternehmen der Welt, mit über 5 750 000 000 Datenschutzverletzungen von 2005 bis 2019 56 % aller Fälle in Amerika ausmachte. S.: California Data Security Breach Reporting Requirements, abrufbar: https://www.termsfeed.com/blog/data-security-breach-reporting-requirements-california/, zuletzt abgerufen am 05. 08.2023.

Das kalifornische Zivilgesetzbuch / California Civil Code (Cal. Cic. Code) schreibt vor, nach welche Anforderungen Mitteilungen bei der Aufsichtsbehörde bzw. dem Generalstaatsanwalt zu erfolgen haben und die Verbraucher zu benachrichtigen sind.

Nach 1798.29 (e) Cal. Civ. Code ist jede Behörde oder nach 1798.82 (f) Cal. Civ. Code ist eine natürliche oder juristische Person (d. h. eine in Kalifornien geschäftlich tätige natürliche oder juristische Person, die Eigentümer oder Lizenznehmer von computergestützten Daten ist und die persönliche Informationen beinhalten), die aufgrund einer Verletzung des Sicherheitssystems eine Benachrichtigung über eine Sicherheitsverletzung an mehr als 500 in Kalifornien ansässige Personen herausgeben muss, verpflichtet, dem Generalstaatsanwalt elektronisch eine Musterkopie dieser Benachrichtigung über die Sicherheitsverletzung zu übermitteln. Alle persönliche Informationen sind von der Mitteilung ausgeschlossen.

Gemäß 1798.29 (d) (2) und 1798.82 (d) (2) Cal. Civ. Code muss die Benachrichtigung über eine Sicherheitsverletzung mindestens die folgenden Informationen enthalten: 1. Den Namen und die Kontaktinformationen der Benachrichtigungsstelle, 2. die Art der betroffenen oder potenziell betroffenen personenbezogenen Daten, 3. das (geschätzte) Datum der Sicherheitsverletzung oder den Zeitraum, in dem die Sicherheitsverletzung aufgetreten ist, falls bereits bekannt, sowie das Datum der Benachrichtigung, 4. ggf. die Angabe über die Verzögerung der Benachrichtigung aufgrund von Ermittlungen der Strafverfolgungsbehörden, falls bereits vorhanden, 5. eine Beschreibung der Sicherheitsverletzung, falls bereits vorhanden, sowie 6. die gebührenfreien Telefonnummern und Adressen der wichtigsten Kreditauskunfteien, wenn durch die Sicherheitsverletzung eine Sozialversicherungsnummer, ein Führerschein oder eine kalifornische Personalausweisnummer offengelegt wurde, 7. die Information über ein Angebot zur kostenlosen Bereitstellung geeigneter Dienste zur Verhinderung und Eindämmung von Identitätsdiebstahl für mindestens 12 Monate – diese Information wird gem. 1798. 82 (d) (2) Cal. Civ. Code nur von einer natürlichen oder juristischen Person an die Person zur Verfügung gestellt, nicht von der Behörde.

Nach 1798.29 (a) muss jede Behörde und nach 1798.82. (a) Cal. Civ. Code jede natürliche oder juristische Person, die personenbezogene Daten verarbeiten, jede Verletzung der Sicherheit des Systems den Einwohnern Kaliforniens benachrichtigen, wenn einer der beiden folgenden Punkte erfüllt ist. Erstens verlangt 1798.29 (a) (1) Cal. Civ. Code die Benachrichtigung der in Kalifornien ansässigen Person, wenn unverschlüsselte personenbezogene Daten von einer unbefugten Person erlangt wurden oder der Verdacht besteht, dass sie erlangt wurden.

Zweitens muss gemäß 1798.29 (a) (2) Cal. Civ. Code für eine Benachrichtigung folgendes erfüllt sein, nämlich: 1. Verschlüsselte personenbezogene Daten wurden von einem Unbefugten erlangt oder es besteht der Verdacht, dass sie erlangt wurden, 2. der Verschlüsselungsschlüssel oder der Sicherheitsnachweis wurde von einem Unbefugten erlangt, oder es besteht der Verdacht, dass er erlangt wurde, 3. es gibt die Möglichkeit, dass der Verschlüsselungsschlüssel oder die Sicherheitsberechtigung diese Informationen lesbar oder nutzbar machen könnte.
Nach 1798.29 (d) (1) und 1798.82 (d) (1) Cal. Civ. Code muss die Benachrichtigung über die Sicherheitsverletzung in einfacher Sprache verfasst sein, den Titel „Notice of Data Breach" tragen und die folgenden Informationen enthalten: 1. Beschreibung der Verletzung, 2. betroffene Informationen, 3. ergriffene Maßnahmen und 4. Handlungsempfehlungen an Betroffenen. Zusätzliche Informationen können als Ergänzung zu der Bekanntmachung bereitgestellt werden.
Gemäß 1798.29 (b) und 1798.82 (b) Cal. Civ. Code muss eine Benachrichtigung unverzüglich nach der Entdeckung einer Verletzung der Datensicherheit erfolgen, wenn die personenbezogene Daten von einer unbefugten Person erlangt wurden oder ein begründeter Zweifel besteht, dass sie erlangt wurden.
Nach 1798.29 (c) und 1798.82 (c) Cal. Civ. Code kann die Benachrichtigung aufgeschoben werden, wenn eine Strafverfolgungsbehörde feststellt, dass eine solche Benachrichtigung die strafrechtlichen Ermittlungen beeinträchtigen würde. Die Benachrichtigung darf erst dann erfolgen, wenn die Strafverfolgungsbehörde festgestellt hat, dass sie die Ermittlungen nicht beeinträchtigt.

5.3.5 Beweissicherung

Neben einer sofortigen Reaktion und einer Ursachenanalyse ist manchmal auch eine juristische Aufarbeitung erforderlich, wobei die Sicherung belastbarer Beweise unerlässlich ist.[1175] Laut ISO/IEC 27001: A.5.28 muss eine Organisation Verfahren zur Identifizierung, Sammlung, Aufzeichnung sowie Aufbewahrung von Beweisen in der Verbindung mit Informationssicherheitsvorfällen festlegen und implementieren. Vor allem sollten Maßnahmen eingeleitet werden, um zu verhindern, dass potenzielle Beweismittel absichtlich bzw. unabsichtlich zerstört oder unbrauchbar gemacht werden (z. B. durch Löschen oder Überschreiben von Daten).[1176]

1175*Brenner*, Praxisbuch, ISO/IEC 27001, S. 93.
1176*Brenner*, Praxisbuch, ISO/IEC 27001, S. 94.

Darüber hinaus muss festgelegt werden, wie Beweise für die Verwendung vor Gericht gesichert und ggf. den Strafverfolgungsbehörden oder Dritten zur Verfügung gestellt werden.[1177] Die IT-Forensik dient der Beweissicherung für die Strafverfolgung der Angreifer und der Geltendmachung von Haftungsansprüchen, die sich nicht nur gegen die Angreifer (z. B. auch gegen Lieferanten) richten können.[1178] Im Falle eines Vorfalls müssen die Daten forensisch gesichert werden.[1179] Das bedeutet, dass von den betroffenen Daten mit geeigneten forensischen Werkzeugen Bilder angefertigt werden.[1180] Damit sind sie gerichtsfest.[1181] Die Festplatten müssen nicht aufbewahrt werden.[1182] Aufgrund der rechtlichen Relevanz forensischer Themen sollten sie in enger Abstimmung mit der Rechtsberatung durchgeführt werden.[1183]

5.3.6 Analyse der Ursachen und möglicher Maßnahmen / „Lessons learned“

ISO/IEC 27001: A.5.27 schreibt vor, dass die Erkenntnisse aus Informationssicherheitsvorfällen genutzt werden sollten, um Maßnahmen zur Informationssicherheit zu stärken und zu verbessern. Nach jedem Vorfall ist eine abschließende Überprüfung obligatorisch, um aus dem Vorfall zu lernen und ähnliche Vorfälle in Zukunft zu verhindern.[1184]

Zunächst muss geklärt werden, ob es sich um eine einfache Störung oder um eine Datenverletzung bzw. einen Informationssicherheitsvorfall handelte. Nachher muss das Ausmaß des Vorfalls festgelegt werden. Darüber hinaus ist die Bestimmung des Charakters des Vorfalls wichtig, um entsprechende Schlussfolgerungen zu ziehen und die richtige Ursachenanalyse durchzuführen.

Nach einem Vorfall ist es wichtig, alles ehrlich und offen zu analysieren und die Sicherheitslücken sowohl technisch als auch organisatorisch zu schließen.[1185] Es muss dafür gesorgt werden, dass es sich nicht wiederholt.[1186] Dazu kann es u. a. notwendig werden, Personaländerungen vorzunehmen oder einen neuen Dienstleister zu beauftragen.[1187] Außerdem ist festzustellen, ob der Notfallplan bzw. Incident-Management-Plan angepasst und verbessert werden sollte.[1188] Ergänzend lassen sich Maßnahmen ableiten, die eine noch schnellere, bessere und gezieltere Reaktion ermöglichen, falls sich ein ähnlicher Vorfall wiederholt.[1189]

1177 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 94.
1178 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 47.
1179 Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 16.
1180 Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 15 ff.
1181 Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 15 ff.
1182 Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 16.
1183 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 47.
1184 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 93.
1185 Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 19.
1186 Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 19.
1187 Interview mit Jan-Henning Evers, im elektronischen Zusatzmaterial, Anlage 3, S. 19.
1188 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 93.
1189 *Brenner*, Praxisbuch, ISO/IEC 27001, S. 93.

Laut ErwGr. 8 S. 1 Rechtsakt zur Cybersicherheit ist Cybersicherheit nicht nur eine Frage der Technik, sondern auch des menschlichen Verhaltens. Das bedeutet, dass jede Organisation nach dem Vorfall darüber nachdenken sollte, was im Bereich der Schulung der Mitarbeiter getan werden sollte. Es ist festzulegen, ob sie geändert oder noch proaktiver angeboten werden sollte. Sie sollen unbedingt eingeführt werden, wenn sie in der Organisation noch nicht stattfinden.

Eine Lessons-Learned-Sitzung mit allen betroffenen Parteien sollte nach einem schwerwiegenden Vorfall obligatorisch und nach einem weniger schwerwiegenden Vorfall wünschenswert sein, um die Behandlung von Vorfällen und die Sicherheit insgesamt zu verbessern.[1190] Dies schafft eine Möglichkeit für jeden Beteiligten, gemeinsam mit allen relevanten Abteilungen / Einheiten zu überlegen, was, wann und wie verschärft und / oder verbessert werden sollte. So ist es auch einfach, Verantwortlichkeiten zuzuweisen und sich gegenseitig zu kontrollieren bzw. zu unterstützen, um ein besseres Ergebnis zu erzielen.

5.3.7 Rückkehr zum Normalbetrieb / „Remediation“

Wurden die wichtigsten Schritte unternommen, geht es nun darum, den laufenden Betrieb abzusichern.[1191] Ziel dieser Phase ist es, die Rückkehr zum normalen Betrieb zu ermöglichen.[1192] Hierbei muss sichergestellt werden, dass alle Mittel für einen dauerhaften Zugang zum Netzwerk berücksichtigt wurden, dass die Aktivitäten des Angreifers ausreichend eingedämmt sind und dass alle Beweise gesammelt worden sind.[1193] Wenn die Ursache des Eindringens und / oder der ursprüngliche Zugangsvektor bekannt sind, kann er auch die Härtung oder Änderung der Umgebung zum Schutz der Zielsysteme beinhalten.[1194] Selbst nach dem Unterbinden eines Angriffs sollen alle Systeme zur sofortige Erkennung neuer Aktivitäten weiter überwachen werden.[1195]

Das gesamte Netzwerk sollte so gereinigt und auf den solchen Stand gebracht worden sein, dass kein Verdacht mehr besteht, dass die bekannte Schwachstellen noch existieren oder dass der Angreifer wieder im Netz ist bzw. wiederkommen könnte. Hardware, Software, physische Orte (z. B. Büros, Räume oder Eingänge) und Beschäftigte sollten reibungslos arbeiten und Daten auf rechtskonforme Weise übertragen können.

1190 Incident Response (IR): Plan & Process, abrufbar: https://www.crowdstrike.com/cybersecurity-101/incident-response/, zuletzt abgerufen am 05.08.2023.

1191 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 13.

1192 CISA, Cybersecurity Incident & Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems S. 15.

1193 CISA, Cybersecurity Incident & Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems S. 15.

1194 CISA, Cybersecurity Incident & Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems S. 15.

1195 *Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 13.

Um die Aktivitäten böswilliger Akteure hinreichend einzuschränken und die Rückkehr zum Normalbetrieb zu ermöglichen, sind u. a. die folgenden Schritte zu unternehmen: 1. Identifizierung und Überprüfung der Integrität der korrekten Datensicherung vor der Wiederherstellung, 2. Installation von Patches, 3. Zurücksetzen der Kontopasswörter, 4. Abrufen der Sicherungskopie, 5. Verschärfung der Perimetersicherheit, 6. Anschließen der wiederhergestellten Systeme wieder an das Netzwerk, 7. Testen der Systeme gründlich, einschließlich der Sicherheitskontrollen, 8. Wiederherstellung des normalen Betriebs der Systeme und Bestätigung, dass sie ordnungsgemäß funktionieren, 9. Überwachen des Betriebs auf abnormales Verhalten, 10. Sicherung der neuen Konfiguration auf einem sicheren Medium, 11. Durchführung einer unabhängigen Überprüfung der Kompromittierung und der damit verbundenen Aktivitäten.[1196]

1196*Powell u.a.,* RESPONDING TO AND RECOVERING FROM A CYBER ATTACK: Cybersecurity for the Manufacturing Sector, 2, 9.

5.4 Zusammenfassung der nachgelagerten Maßnahmen

Prävention bzw. Umsetzung präventiver Maßnahmen ist unerlässlich, wenn eine Organisation (personenbezogene) Daten verarbeitet und sich vornimmt, die Rechte jedes Einzelnen zu gewährleisten. Bei ,,Nowadays Reality" geht es jedoch nicht darum, ob eine Organisation jemals angegriffen wird, sondern wann dies geschieht. Wie Gabel erwähnte, kann ,,Preparedness" keine 100-prozentige Garantie anbieten, dass bei der genauen Umsetzung von Präventivmaßnahmen eine Organisation nicht angegriffen wird. (Personenbezogene) Daten sollten immer geschützt werden. Die Cybersicherheit trägt dazu bei, dies zu erreichen. Sie dient Datenschutzzielen.[1197]

Wenn ein Angriff auftritt, bestehen viele Komponenten, die eine Organisation verwenden kann, um ihn zu verhindern und den damit verbundenen Schaden zu minimieren. Es ist entscheidend, zunächst genau zu definieren und zu wissen, was diese Gefahren sind, welche Charakter sie aufweisen und durch welche Wege sie in der Organisation gelandet sind (z. B. durch ein DoS-Angriff oder eine Phishing-E-Mail). Darüber hinaus muss festgestellt werden, in welche Kategorie der Vorfall fällt: Handelt es sich um eine Datenschutzverletzung oder einen Informationssicherheitsvorfall. Jeder Angriff verdient unterschiedliche Response-Methode.

Um eine Datenschutzverletzung oder einen Informationssicherheitsvorfall schnell zu bewältigen, ist es wichtig, ein **Incident Response Team** und einen **Incident Response Plan** vorzubereiten. Diese sind zwei wichtige Bestandteile für den Schutz vor Cyber-Angriffen bzw. einem Informationssicherheitsvorfall. Alle materiellen, zeitlichen, monetären oder personellen Ressourcen müssen stets zur Verfügung gestellt werden.

Neben dem Team und Plan gibt es Schritte zur Reaktion auf Vorfälle, die genau befolgt werden müssen, wenn ein Vorfall aufgetreten ist. Diese Schritte wurden oben ausführlich betrachtet, wobei klargestellt wurde, dass vor allem eine **Identifizierung bzw. Bewertung** des Angriffs, **Schadensminimierung und Dokumentation** aller relevanten Informationen vorzunehmen sind. Danach folgt der Schritt der Notification, nämlich Meldung an die Behörden und / oder Benachrichtigung der Betroffenen.

1197*Schünemann/Baumann*, Privacy, Data Protection and Cybersecurity in Europe, S. 109.

Die **Notification** ist sowohl in der EU als auch in den USA obligatorisch. Grundsätzlich sind diesbezügliche Anforderungen in Europa sowie in Amerika sehr ähnlich. In der EU ist die Verpflichtung zur Notification im Falle einer Datenschutzverletzung in der DSGVO und im Falle eines Informationssicherheitsvorfalls in der NIS-2-Richtlinie geregelt. Hervorzuheben ist, dass dieses Thema in den USA noch ernster genommen wird als präventive Maßnahmen. Diese Pflicht ist in allen Staaten Amerikas in den jeweiligen staatlich anerkannten Gesetzen geregelt.
Da diese Gesetze jedoch nur für bestimmte Arten der Daten gelten, betreffen sie nicht so viele Daten und damit nicht so viele Personen wie die DSGVO.
Als nächste Schritte sind die **Beweissicherung** sowie die **Analyse der Ursachen** und mögliche Maßnahmen vorzunehmen. Die Beweissicherung ist sehr wichtig für die juristische Aufarbeitung des Falles. Die Ursachenanalyse bzw. „Lessons Learned" ermöglicht es, aus dem Ereignis zu lernen und denselben Fehler nicht zu wiederholen.
Ganz am Ende steht die **Rückkehr zum Normalbetrieb**, wobei gewährleistet sein soll, dass die betroffene Organisation alle Schwachstellen beseitigt hat und in der Lage ist, (personenbezogene) Daten weiter zu verarbeiten und die Rechte und Freiheiten jedes Einzelnen, einschließlich Datenschutz- sowie Persönlichkeitsrechte zu gewährleisten.

6 Das Ergebnis

„I hope our wisdom will grow with our power, and teach us that the less we use our power the greater it will be."

Thomas Jefferson[1198]

Tesla hat das Software-Update so schnell und professionell durchgeführt, dass der Besitzer das Gefühl hatte, magische Elfen hätten sein Auto repariert; mit anderen Worten: Tesla hat seinen Kunden durch richtig umgesetzte technische und organisatorische Maßnahmen glücklich gemacht. Genauso wichtig ist es, diese Maßnahmen und die sich daraus ergebenden rechtlichen sowie normativen Anforderungen umzusetzen, um das Wohl des Menschen und damit seine Persönlichkeitsrechte wahrnehmen zu können.

Das Recht auf die eigene Persönlichkeit war schon immer ein Thema für jede Generation. Was die letzten Jahrhunderte mit sich brachten, sind die technologischen Entwicklungen, die heute insbesondere im internationalen Datentransfer zu finden sind. Weltweit sind die EU und die USA die führenden Akteure und die wichtigsten Partner füreinander. Hinzu kommt, dass die meisten Anbieter von Computer-Dienstleistungen Amerikaner sind,[1199] was die Bedeutung dieses Landes weiter stärkt. Deshalb ist es wichtig, die Anforderungen auf europäischer und amerikanischer Ebene sinnvoll zu regeln und zu implementieren. Dies ist das **Hauptthema** dieser Dissertation.

Das **Hauptproblem** ist der Zugang zu (personenbezogenen) Daten von US-Behörden und Geheimdiensten, die diese manchmal sogar „over a few beers"[1200] erhalten. Dies beeinträchtigt die Persönlichkeitsrechte und schafft einen Schwebezustand. Wie Metin Hakverdi (Deutscher Bundestag 2015) sagte: *„Today one is able to launch an attack from afar at any point, from any place in the world (…) Today it's about professional criminal structures or even intelligence agencies who have even more resources."*[1201]

Europäische Unternehmen und die Datenspeicherung in Europa sind nicht immun gegen außereuropäische Gesetzgebung, wie z. B. den CLOUD Act. (Personenbezogene) Daten, die in Europa verarbeitet werden, d. h. im Prinzip in der EU sind und bleiben, fallen unter den CLOUD Act und damit unter US-Recht und können von der US-Regierung angefordert werden. Es ist sogar bei europäischen Unternehmen möglich, dass sie die Verarbeitung und Speicherung komplett in Europa vornehmen.[1202]

1198 *Brantly*, The decision of Attack: Military and Intelligence Cyber Decision-Making, S. 63.

1199 *Christakis/Terpan*, IDPL, Vol. 11, Nr. 2, 2021, 81, 89.

1200 How an app to decrypt criminal messages was born 'over a few beers' with the FBI, abrufbar: https://theconversation.com/how-an-app-to-decrypt-criminal-messages-was-born-over-a-few-beers-with-the-fbi-162343, zuletzt abgerufen am 05.08.2023.

1201 *Schünemann/Baumann*, Privacy, Data Protection and Cybersecurity in Europe, S. 101.

1202 Das in diesem Abschnitt beschriebene Problem findet sich in dem folgenden Artikel. S.: How the CLOUD-Act

Das Beispiel des CLOUD Act zeigt, welche Folgen eine Gesetzgebung hat, wenn sie extraterritoriale Wirkung hat. Die Gesetzgebung im digitalen Bereich hat zunehmend eine solche Wirkung. Dies erschwert die Sicherheit von Informationen in der EU und die Einhaltung von EU- sowie nationalen Gesetzen bzw. Vorschriften im Bereich des Datenschutzes und der Informationssicherheit.[1203]

Laut NIST SP 800-53, Rev. 5: Abs. 2 Introduction ergeben sich die Anforderungen an die Informationssicherheit und den Datenschutz aus den geltenden Gesetzen, Verordnungen, Richtlinien, Vorschriften, Normen und den Erfordernissen des Auftrags, um die Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten, gespeicherten oder übermittelten Informationen zu gewährleisten und die Risiken für den Datenschutz zu beherrschen. Organisationen müssen sich stets die Frage stellen, gegen welche extraterritorialen Rechtsordnungen und damit Länder sie sich wappnen wollen bzw. können und was das für die Auswahl der Lieferanten und den Einsatz zusätzlicher Kontrollmaßnahmen bedeutet.[1204]

Um das oben genannte Hauptproblem zu verstehen und zu untersuchen, wurden die rechtlichen Anforderungen, das MLAT-Abkommen und der neue EU-US Data Protection Framework analysiert. Die **rechtlichen Anforderungen** regeln, wann und ob der internationale Datentransfer zulässig ist, welche Rechtsgrundlagen vorgelegt werden sollten und wer dafür überhaupt verantwortlich ist. Diese Anforderungen haben deutlich gezeigt, dass sie in der EU breiter gefasst sind und tiefer gehende und komplexere Anforderungen enthalten als in den USA. Dies wurde insbesondere durch die Darstellung der Anforderungen im Rahmen der DSGVO und des CLOUD Acts deutlich.

MLAT-Abkommen bzw. **MLAT-Verfahren**, die in der EU unter den Sonderfall der DSGVO und in den USA unter die alternativen Wege des CLOUD Acts fallen, sind zwar grundsätzlich positiv zu bewerten, gewährleisten aber leider bisher kein schnelles Verfahren und verlangsamen oft die Strafverfolgung. Daher wird dieses Verfahren nicht intensiv genutzt. Als Alternative wird von den USA der CLOUD Act angeboten. Verfahren, die nach diesem Gesetz durchgeführt werden können, können den Ablauf von Strafverfahren beschleunigen, würden aber die Persönlichkeitsrechte beeinträchtigen und sind in der EU nicht anerkannt.

works in data storage in Europe, abrufbar: https://english.ncsc.nl/latest/weblog/weblog/2022/how-the-cloud-act-works-in-data-storage-in-europe, zuletzt abgerufen am 05.08.2023.

1203Die in diesem Abschnitt dargestellte Aussage findet sich in dem folgenden Artikel. S.: How the CLOUD-Act works in data storage in Europe, abrufbar: https://english.ncsc.nl/latest/weblog/weblog/2022/how-the-cloud-act-works-in-data-storage-in-europe, zuletzt abgerufen am 05.08.2023.

1204How the CLOUD-Act works in data storage in Europe, abrufbar: https://english.ncsc.nl/latest/weblog/weblog/2022/how-the-cloud-act-works-in-data-storage-in-europe, zuletzt abgerufen am 05.08.2023.

Der neue **EU-US Data Protection Framework** sieht ein Verfahren vor, das den internationalen Datentransfer primär im Wirtschaftsbereich vereinfacht und den Datenverkehr ohne weitere Schutzmaßnahmen ermöglicht. Dieser enthält jedoch bereits Schwachstellen, und es bleibt abzuwarten, wie er bei seiner Umsetzung die betroffenen Personen schützen wird und was der EUGH dazu äußern wird.

Nach diesen Überlegungen wurden einige **Lösungen** präsentiert und untersucht, um sicherzustellen, ob es bereits den einen Mechanismus gibt, der die Lage vereinfachen kann oder ob ein neuer Mechanismus für den rechtskonformen internationalen Datentransfer geschaffen werden soll.

Es wurde festgestellt, dass es möglich ist, die derzeitige Situation sowohl durch die bestehenden Anforderungen bzw. Maßnahmen zu verbessern als auch durch die neuen Methoden zu vereinfachen. Diese Lösungen sind **rechtlich** durch 1. die Vereinfachung des MLAT-Verfahrens, durch 2. die „Verhandlung ähnlicher Beschränkungen" und / oder durch 3. die Melde- und Konsultationspflicht zu gewährleisten. Die richtige **organisatorische** Gestaltung kann dazu beitragen, dass die Daten so verarbeitet werden, dass gegen kein Gesetz auf EU- sowie US-Ebene verstoßen wird. Alles, was organisatorisch geregelt ist, muss unbedingt auch technisch im Berufsalltag umgesetzt werden. Die **technische** Gestaltung der Organisation ermöglicht die korrekte Umsetzung der rechtlichen und technischen Anforderungen und schafft die Möglichkeit, die Daten vor bzw. während des Transfers sowie vor unberechtigtem Zugriff (einschließlich Zugriff von Behörden) zu schützen. **Praktische Schritte** (z. B. Schulung der Mitarbeiter oder ausreichende Ressourcen), wie ebenfalls oben beschrieben, sind unerlässlich, um bei der internationalen Datentransfer datenschutzkonform handeln zu können.

Der **rechtliche Schritt**, wie das Vereinheitlichen des MLAT-Abkommens und das Vereinfachen des MLAT-Verfahren bietet die Möglichkeit, alle ein- und ausgehende Anfragen an einer Stelle zeitgerecht zu bearbeiten. Darüber hinaus sollte genügend professionelles Personal eingestellt werden, das über alle Ressourcen verfügt, um die Anfragen schnell und bestmöglich zu bearbeiten.

Wenn die relevanten Einheiten in einer Organisation **organisatorisch** so getrennt sind, dass sie keinen Zugriff auf EU- oder US-Daten erhalten, kann die gleichzeitige Einhaltung der DSGVO und des CLOUD Acts gewährleistet werden. Dabei sind nicht nur die Rollen und Verantwortlichkeiten der Beschäftigten zu trennen, sondern auch die IT-Systeme und die IT-Infrastruktur. All dies muss natürlich ggf. vertraglich oder schriftlich festgehalten werden.

Alles, was organisatorisch geregelt ist, muss **technisch** umgesetzt werden. Das bedeutet, dass alle organisatorischen Maßnahmen gelebt werden müssen. Außerdem müssen technische Maßnahmen wie die Verschlüsselung umgesetzt werden, um einen rechtskonformen, internationalen Datentransfer bei gleichzeitigem Zusammenspiel von DSGVO und CLOUD Act zu ermöglichen.

Wenn **praktische Schritte** unternommen werden, bedeutet dies, dass alle notwendigen zeitlichen, personellen und finanziellen Ressourcen zur Verfügung gestellt werden. Auf diese Weise werden behördliche Anträge schnell und bestmöglich bearbeitet.

Die oben vorgeschlagenen Lösungen können in der Praxis nur umgesetzt werden, wenn eine Organisation geeignete **rechtliche und normative Maßnahmen** ergreift. Diese Maßnahmen müssen getroffen werden, damit alles im Berufsalltag umgesetzt werden kann. Es hat sich gezeigt, dass eine Organisation auf der sicheren Seite ist, wenn sie alle erforderlichen Mindestanforderungen gemäß den gesetzlichen Bestimmungen erfüllt und alle wichtigen internationalen Standards (z. B. ISMS nach ISO/IEC 27001) implementiert. Das bedeutet jedoch nicht, dass eine solche Organisation niemals angegriffen werden kann.

Jede Organisation muss auf einen **Cyber-Angriff** gut vorbereitet sein. Dies ist durch richtig angewandte nachgelagerte Maßnahmen möglich. Die Cybersicherheit unterliegt „starken internationalen Einflüssen, insbesondere aus den USA", wo sie seit langem rechtlich verankert ist.[1205] Diejenigen, die nicht umfassend vorbereitet und rechtlich nicht handlungsfähig sind, „spielen mit ihrem guten Ruf und setzen sich massiven finanziellen Risiken aus".[1206]

Die Reaktion auf einen Vorfall umfasst sowohl rechtliche als auch technisch-organisatorische Schritte, die zur schnellen Beseitigung des Vorfalls unternommen werden sollten. **Incident Response Team** und **Incident Response Plan** sind die wichtigsten Komponenten. Präzise geplante Schritte / **Incident Response Steps** zur Bewältigung eines Cybervorfalls ermöglichen den Erfolg. Wenn der Vorfall schnell behoben ist und die Organisation weiter funktionieren kann, bedeutet dies, dass die (personenbezogene) Daten auf der sicheren Seite sind und die Ausübung der Persönlichkeitsrechte jederzeit möglich ist.

Zusammenfassend lässt sich feststellen, dass Persönlichkeitsrechte sehr eng mit der digitalen Welt verknüpft sind. Menschen bestehen aus Daten und, wenn Daten nicht geschützt werden, sind Menschen nicht geschützt.[1207] Aus diesem Grund ist das Thema „Internationaler Datentransfer" sowohl im rechtlichen als auch im technisch-organisatorischen Bereich stark ausgeprägt. Es ist daher unabdingbar, sich mit dem Thema auseinanderzusetzen und die oben beschriebenen Lösungen bzw. Handlungsempfehlungen gesetzlich niederzuschreiben und in jeder Organisation umzusetzen. Dies ermöglicht ein besseres Verständnis der Materie und gewährleistet einen besseren Schutz des Einzelnen durch Schutz der Persönlichkeitsrechte.

1205*Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 14.
1206*Gabel u.a.*, Rechtshandbuch Cyber-Security, S. 14.
1207Interview mit Kyle Duncan, im elektronischen Zusatzmaterial, Anlage 4, S. 31.

Sind Persönlichkeitsrechte geschützt, sind Menschenrechte geschützt – ein Wert, bei dem nichts und niemand Vorrang hat. Menschen und ihre Rechte werden immer höher eingestuft als jegliche Organisation oder Regierungen auf der Welt. Daher darf nicht vergessen werden, dass, wenn es Menschen gut geht, es auch Organisationen und Regierungen gut geht. Dies soll Kernpunkt und Motivation für diejenigen sein, die sich auf rechtlicher, technischer oder organisatorischer Ebene mit dem Thema „Internationaler Datentransfer" auseinandersetzen: Das gilt für diejenigen, die die rechtlichen oder technischen Anforderungen niederschreiben, sowie für diejenigen, die sie umsetzen. Und wann geht es Menschen gut? Wenn sie nicht überwacht bzw. kontrolliert werden.

„Doch was ist Kontrolle?" – fragte sich Ferdinand Lundberg in seinem Buch „Die Mächtigen und die Supermächtigen". Dort heißt es: *„Bei den Hearings hatte es den Anschein, als verstünden viele unter dem Begriff „Kontrolle" eine Art Würgegriff. Dies ist eine verbreitete Fehlereinschätzung. Die Kontrolle über ein Großunternehmen sieht ganz anders aus – sie wird leise und vornehm praktiziert–, bis sie herausgefordert wird. Wenn Gefahr droht, kann es zu handfesten Auseinandersetzungen kommen. Wer das Establishment eines Unternehmens herausfordert, muß sich darauf gefaßt machen, dass Steine fliegen und häßliche Worte fallen."*[1208] In jeder Art und Weise wird die Kontrolle nirgendwo gerne akzeptiert, verursacht viele Unannehmlichkeiten bis hin zur Verletzung der Rechte. Wenn sie als Würgegriff, stillschweigend oder anderweitig geschieht, ist sie nie willkommen, und wenn sie auf jeden Fall gesetzlich gemacht werden sollte, sollte auch ein ganz bestimmter Grund bzw. eine Rechtfertigung vorgelegt werden, um die Persönlichkeitsrechte auf bestmögliche Weise zu schützen.

Sollte dies nicht geschehen, muss jeder ein **David Rockefeller** werden, der als einziger des Rockefeller-Syndikats auf Jahreshauptversammlungen zur Abstimmung der Tagesordnung seine Stimme erhob, als alle anderen im Hintergrund blieben.[1209]

1208*Lundberg*, Die Mächtigen und die Supermächtigen: Das Rockefeller-Syndrom, S. 48.
1209*Lundberg*, Die Mächtigen und die Supermächtigen: Das Rockefeller-Syndrom, S. 48 ff.

Literaturverzeichnis

Ann, Christoph / Loschelder, Michael / Grosch, Marcus (Hrsg.)	Praxishandbuch: Know-how-Schutz, Köln 2010
Asendorpf, Jens B.	Persönlichkeit: Was uns ausmacht und warum, Deutschland 2018
Auernhammer / Eßer, Martin (Hrsg.) / Kramer, Philipp (Hrsg.) / von Lewinski, Kai (Hrsg.)	DSGVO, BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze: Kommentar, 6. Aufl. Köln 2018 (zit.: *Auernhammer u. a. -Bearbeiter,* DSGVO, BDSG, Art. XY, Rn. XY.)
Bagauri, Tatia	Betroffenenrechte im Vergleich: DSGVO – CCPA in: Bonner Rechtsjournal 01/2022, S. 43-48 (zit.: *Bagauri*, BRJ 01/2022, S. 1, S. XY.)
Balser, Jimmy	Overview of Governmental Action Under the Stored Communications Act (SCA), USA 03.08.2022, 1-4
Baumann, Bastian	Datenschutzkonflikte zwischen der EU und den USA: Angemessenheit des Datenschutzniveaus am Beispiel der PNR-Abkommen, Bd. 37, Berlin 2016 (zit.: *Baumann*, Datenschutzkonflikte zwischen der EU und den USA, S. XY.)
Beater, Axel	Medienrecht, 2. Aufl. Tübingen 2016
Beverley-Smith, Huw / Ohly, Ansgar / Lucas-Schloetter, Agnes	Privacy, Property and Personality: Civil Law Perspectives on Commercial Appropriation, New York 2005 (zit.: *Beverley-Smith u.a.*, Privacy, Property and Personality, S. XY.)
Bommel, Robert	Verschlüsselung unter der DSGVO in: Informationen zum Datenschutz, 10.2019 (zit.: *Bommel*, Informationen zum Datenschutz.)
Bossong, Raphael	SWP-Studie: Intelligente Grenzen und interoperable Datenbanken für die innere Sicherheit der EU: Umsetzungsrisiken und rechtsstaatliche Anforderungen, Berlin 04.2018, S. 5-34
Boyne, Shawn Marie	Data Protection in the United States, in: The American Journal of Comparative Law, Bd. 66, 2018, S. 299-343 (zit.: *Boyne*, Data Protection in the United States, S. 299, S. XY.)
Brantly, Aaron Franklin	The decision of Attack: Military and Intelligence Cyber Decision-Making, Georgia 2016

Brenner, Michael / Felde, Nils gentschen / Hommel, Wolfgang / Metzger, Stefan / Reiser, Helmut / Schaaf, Thomas	Praxisbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung, 4. Aufl. München 2022 (zit.: *Brenner u. a.,* Praxisbuch ISO/IEC 27001, S. XY.)
Brüggemeier, Gert / Colombi Ciacchi, Aurelia / O'Callaghan, Patrick	The common core of europian private law: Personality Rights in European Tort Law, Cambridge 2010 (zit.: *Brüggemeier u.a.*, Personality Rights in European Tort Law, S. XY.)
Bundesamt für Sicherheit in der Informationstechnik (BSI)	Elementare Gefährdungen, 07.12.2020, S. 2-50
Bundesamt für Sicherheit in der Informationstechnik (BSI)	IT-Grundschutz- Kompendium, Bonn 2022
Bundeskartellamt	Big Data und Wettbewerb: Schriftenreihe „Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft" Bonn, 10.2017, S. 1-14
Bundeskartellamt	Cybercrime: Bundeslagebild 2017, Wiesbaden, 07.2018, S. 1-37
Bundesministerium für Wirtschaft und Energie (BMWi)	Sicherer Datenaustausch: Themenheft Mittelstand-Digital, Berlin 04.2021, S. 1-37
Christakis, Theodore / Terpan, Fabien	EU-US negotiations on law enforcement access to data: Divergences, challenges and EU law procedures and options, in: International Data Privacy Law, Bd. 11, Nr. 2, 2021, S. 81-106 (zit.: *Christakis/Terpan*, IDPL, Vol. 11, Nr. 2, 2021, S. 81, S. XY.).
Defense Privacy and Civil Liberties Office	Introduction to the Privacy Act, Virginia, S. 1-22
Dworkin, Gerald	Reports of Committees: The Younger Committee Report on Privacy, in: The Modern Law Review, Bd. 36, Nr. 4, 04.1973, S. 399-406 (zit.: *Dworkin,* The Younger Committee Report on Privacy, S. 399, S. XY.)
Däubler, Wolfgang / Wedde, Peter / Weichert, Thilo / Sommer, Imke	EU-DSGVO und DBSG: Kompaktkommentar: EU-Datenschutzgrundverordnung (EU-DSGVO), neues Bundesdatenschutzgesetz (BDSG), weitere datenschutzrechtliche Vorschriften, 2. Aufl. Frankfurt am Main 2020, (zit.: *Däubler u. a. - Bearbeiter,* EU-DSGVO und BDSG, Art. XY Rn. XY oder S. XY.)
Eckert, Claudia	IT-Sicherheit: Konzepte – Verfahren – Protokolle, 8. Aufl. München 2013

Ehmann, Horst	Der Begriff des Allgemeinen Persönlichkeitsrechts als Grundrecht und als absolut-subjektives Recht, in: Festschrift für Apostolos Georgiades, Athen / München 2005, S. 1-28 (zit.: *Ehmann*, Der Begriff des Allgemeinen Persönlichkeitsrechts, S. 1, S. XY.)
Europäische Kommission	Pressemitteilung: Datenschutz: Kommission leitet Verfahren zur Annahme eines Angemessenheitsbeschlusses für einen sicheren Datenverkehr mit den USA ein, 13.12.2022
Europäische Kommission	Fact Sheet, Questions and Answers on the EU-US data protection "Umbrella agreement", 08.09.2015
Farivar, Cyrus	habeas data: Privacy vs. The Rise of Surveillance Tech, New York und London 2018 (zit.: *Farivar*, habeas data, S. XY.)
Federrath, Hannes	Informattionssicherheit und technischer Datenschutz durch verteilte Systeme in: Mitteilungen der Mathematischen Gesellschaft in Hamburg, Bd. 34, Hamburg 2014, S. 21-32 (zit.: *Federrath*, Mitt. Math. Ges. Hamburg 34/2014, S. 21, S. XY.)
Franzen, Martin / Galler, Inken / Oetker, Hartmut (Hrsg.)	Kommentar zum europäischen Arbeitsrecht, 4. Aufl. München 2022
Fuster, Gloria González / Hijmans, Hielke	Discussion paper: The EU rights to privacy and personal data protection: 20 years in 10 questions, Version 1 – 13.05.2019, S. 1-13
Gabel, Detlev (Hrsg.) / Heinrich, Tobias A. / Kiefner, Alexander	Rechtshandbuch Cyber-Security: IT-Sicherheit, Gesellschaftsrecht, Compliance, M&A, Versicherungen, Aufsichtsrecht, Arbeitsrecht, Litigation, Frankfurt am Main 2019 (zit.: *Gabel*, Rechtshandbuch Cyber-Security, S. XY.)
Gandenberger, Gertrud / Krennerich	Politik & Unterricht: Menschenrechte, unveräußerlich – universell – unteilbar, Heft 3/4-2014
Gellers, Joshua C.	Rights for Robots: Artificial Intelligence, Animal and Environmental Law, New York 2021
Greve, Holger	Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, Bd. 30, Berlin 2012
Gola, Peter / Heckmann, Dirk	Datenschutz-Grundverordnung / VO (EU) 2016/679 / Bundesdatenschutzgesetz: Kommentar, 3. Aufl. 2022 (zit.: *Gola/Heckmann -Bearbeiter*, DSGVO/DBSG, Art. XY, Rn. XY.)
G2012 Mexiko	Requesting Mutual Legal Assistance in Criminal Matters from G20 Countries: A Step-by-step Guide, 2012, S. 3-121
Götting, Horst-Peter	Persönlichkeitsrechte als Vermögensrechte, Tübingen 1995

Götting, Horst-Peter / Schertz, Christian / Seitz, Walter (Hrsg.)	Handbuch Persönlichkeitsrecht: Presse und Medienrecht, 2. Aufl. München 2019
Hildebrand, Knut / Gebauer, Marcus / Mielke, Michael (Hrsg.)	Daten- und Informationsqualität: Die Grundlage der Digitalisierung, 5. Aufl. Wiesbaden 2021
Hollywood, John S. / Winkelman, Zev	Improving Information-Sharing Across Law Enforcement: Why can't we know? A project of the RAND corporation, the police executive research forum, RTI international and the university of Denver, 2015, S. 2-31 (zit.: *Hollywood/Winkelman*, Improving Information-Sharing Across Law Enforcement, S. 2, S. XY.)
Hubbard, Michael T.	Personal Data of U.S. Citizens Transferred Abroad Needs Protection in: The National Law Review, Bd. 9, Nr. 211, 25.06.2019, S. 1-3 (zit.: *Hubbard*, The National Law Review, S. 1, S. XY.)
Information Commisioner's Office	Encryption, 03.03.2016, S. 2-35
IONOS	White Paper: Aktuelle Rechtslage zum US-Datentransfer unter besonderer Berücksichtigung des US CLOUD Act, 2021, S. 4-18
Kirtley, Jane E. /Shally-Jensen, Michael	Privacy Rights in the Digital Age, 2. Aufl. New York 2019
Koenig, Matthias / Bonacker, Thorsten (Hrsg.) / Lohmann, Hans-Martin (Hrsg.)	Menschenrechte, Frankfurt / New York 2005
Kuner, Christopher	Transborder Data Flows and Data Privacy Law, Oxford 2013
Kühling, Jürgen / Buchner, Benedikt (Hrsg.)	DSGVO / BDSG: Datenschutz-Grundverordnung / Bundesdatenschutzgesetz: Kommentar, 3. Aufl. München 2020 (zit.: *Kühling/Büchner -Bearbeiter*, DSGVO/BDSG, Art. XY, Rn. XY.)
Linebaugh, Chris D. / Liu, Edward C.	EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield, Congressional Research Service R46724, USA 17.03.2021, S. 1-14
Lipner, Steven B. / Lampson, Butler W.	Risk Management and the Cybersecurity of the U.S.: Government Input to the Commission on Enhancing National Cybersecurity, S. 1-7
Lundberg, Ferdinand	Die Mächtigen und die Supermächtigen: Das Rockefeller-Syndrom, München 1975

McGeveran, William	Friending the Privacy Regulators in: Arizona Law Review, Bd. 58:959, 2016, S. 959-1025 (zit.: *McGeveran*, Arizona Law Review, S. 959, S. XY.)
Organisation for Economic Co-operation and Development (OEDC)	Digital Security Risk Management for Economic and Social Prosperity: Recommendation and Companion Document, 2015, S. 3-69
Paal, Boris P. / Pauly Daniel A (Hrsg.)	Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 3. Aufl. München 2021
Pell, Owen C. / GraCe, SuSan L.	In the Supreme Court of the United States: United States of America v. Microsoft Corporation, on Writ of Certiorari to the United States Court of Appeals for the Second Circuit, Brief of Amicus Curiae Gesellschaft für Freiheitsrechte e.V. in Support of respondent Microsoft Corporation, New York 18.01.2018, S. 1-24
Powell, Michael	RESPONDING TO AND RECOVERING FROM A CYBER ATTACK: Cybersecurity for the Manufacturing Sector, Virginia 11.2022
Ramirez, Edith	Remarks of Commissioner Edith Ramirez Privacy by Design Conference: Privacy By Design and the New Privacy Framework of the U.S. Federal Trade Commission, Hong Kong 13.06.2012, S. 1-11
Randall, Karen Painter / Kroll, Steven A.	Protecting Data Security Risk Assessments from Disclosure in Subsequent Breach Litigation in: US LAW, Fall / Winter 2017 (zit.: *Randall/Kroll*, US Law, Fall/Winter 2017.)
Rehm, Gebhard Marc	Just Judicial Activism? Privacy and Informational Self-Determination in U.S. and German Constitutional Law, SSRN Electronic Journal 01.2000 (zit.: *Rehm*, SSRN Electronic Journal 01.2000.)
Ruppel, Karl-Ludwig	Persönlichkeitsrechte an Daten? Deliktsrechtlicher Datenschutz nach § 823 Abs. 1 BGB zwischen informationeller Selbstbestimmung, Rechtsgüterschutz und Eingriffstypisierung, Frankfurt am Main 2001
Rush, Mark A. / Kephart, Jared A.	Lifting the Veil on the MLAT Process: A Guide to Understanding and Responding to MLA Requests in: Legal Insight, 20.01.2017, S. 1-9 (zit.: *Rush/Kephart*, Legal Insight, S. 1, S. XY.)
Schantz, Peter / Wolff, Heinrich Amadeus	Das neue Datenschutzrecht: Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, München 2017

Schünemann, Wolf J. / Baumann, Max-Otto	Privacy, Data Protection and Cybersecurity in Europe, Bonn 2017
Sharpson, Eleanor	Schlussanträge der Generalanwältin Eleanor Sharpson vom 27. September 2018 Rechtssache C-345/17 (ECLI:EU:C:2018:780)
Solmecke, Christian / Kocatepe, Sibel	DSGVO für Website-Betreiber: Ihr Leitfaden für die sichere Umsetzung der EU-Datenschutz-Grundverordnung, 2. Aufl. Bonn 2018
Specht, Louisa	Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen, in: CR, 32 Aufl. Köln 2016, S. 288-296 (zit.: *Specht*, CR 2016, S. 288, S. XY.)
Specht, Louisa	Konsequenzen der Ökonomisierung informationeller Selbstbestimmung: Die zivilrechtliche Erfassung des Datenhandels, Köln 2012
Specht, Louisa / Mantz, Reto (Hrsg.)	Handbuch europäisches und deutsches Datenschutzrecht: Bereichsspezifischer Datenschutz in Privatwirtschaft und öffentlichem Sektor, München 2019 (zit.: *Specht/Mantz*, Handbuch europäisches und deutsches Datenschutzrecht, S. XY.)
Stucke, Maurice E.	Breaking Away: How to Regain Control Over Our Data, Privacy, and Autonomy, New York 2022
The United States Department of Justice	Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 04.2019, S. 2-18
U.S. Securities and Exchange Commission	Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million, Press Release 2018-71
Vance, Ashlee	Elon Musk: Tesla, PayPal, SpaceX: Wie Elon Musk die Welt verändert – Die Biografie, 24. Aufl. München 2021
Voigt, Paul / von dem Bussche, Axel	EU-Datenschutz-Grundverordnung (DSGVO): Praktikerhandbuch unter vollständiger Berücksichtigung des deutschen Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU (DSAnpUG-EU), Deutschland 2018 (zit.: *Voigt/Axel*, EU-DSGVO, S. XY.)
Voßkuhle, Andreas / Eifert, Martin / Möllers, Christoph (Hrsg.)	Grundlagen des Verwaltungsrechts, 3. Aufl. Bd. 1, München 2022
Wandtke, Artur-Axel / Ohst, Claudia (Hrsg.)	Medienrecht Praxishandbuch: Persönlichkeitsrecht und Medienstrafrecht, 3. Aufl. Bd. 4, Berlin / Boston 2014 (zit.: *Wandtke/Ohst -Bearbeiter*, Medienrecht Praxishandbuch, S. XY.)

Wissenschaftliche Dienste des Deutschen Bundestages — Persönlichkeitsrechte im Internet: Aufbau und Entscheidungsfindung bei der Enzyklopädie Wikipedia, WD 10 - 3000 – 110/08, S. 5-23

Wissenschaftliche Dienste des Deutschen Bundestages — US-Datenrecht: Zugriff US-amerikanischer Behörden auf Daten, WD 3 - 3000 – 181/20, S. 2-10

Wood, Georgia / Lewis, James A. — The CLOUD Act and Transatlantic Trust, CSIS, resrep48724, 03.2023, 1-8 (zit.: *Wood/Lewis*, CSIS, 03.2023, S. 1, S. XY.)

Quellen aus Internetseiten

ACM Digital Library — Empowering Resignation: There's an App for That, abrufbar: https://dl.acm.org/doi/fullHtml/10.1145/3411764.3445293, zuletzt abgerufen am 30.07.2023.

ascon-Datenschutz — Pseudonymisierung, abrufbar: https://ascon-datenschutz.de/datenschutz-abc/pseudonymisierung/, zuletzt abgerufen am 04.08.2023.

ascon-Datenschutz — Verschlüsselung, abrufbar: https://ascon-datenschutz.de/datenschutz-abc/verschluesselung/, zuletzt abgerufen am 04.08.2023.

Bischoff, Paul — A breakdown of the Patriot Act, Freedom Act, and FISA, https://www.comparitech.com/blog/vpn-privacy/a-breakdown-of-the-patriot-act-freedom-act-and-fisa/, zuletzt abgerufen am 01.08.2023.

Blesch, William — California Data Security Breach Reporting Requirements, abrufbar: https://www.termsfeed.com/blog/data-security-breach-reporting-requirements-california/, zuletzt abgerufen am 05.08.2023.

Bloomberg Law — Data Privacy Laws by State: Comparison Charts, abrufbar: https://pro.bloomberglaw.com/brief/data-privacy-laws-in-the-u-s/, zuletzt abgerufen am 01.08.2023.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BKA) Kritische Infrastrukturen, abrufbar: https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html, zuletzt abgerufen am 05.08.2023.

Bundesamt für Justiz — Internationale Rechtshilfe in Strafsachen, abrufbar: https://www.bundesjustizamt.de/DE/Themen/InternationaleZusammenarbeit/Strafsachen/Rechtshilfe/Rechtshilfe_node.htm, zuletzt abgerufen am 02.08.2023.

Bundeszentrale für politische Bildung (BPB)	Das Recht auf informationelle Selbstbestimmung, abrufbar: https://www.bpb.de/themen/recht-justiz/persoenlichkeitsrechte/244837/das-recht-auf-informationelle-selbstbestimmung/, zuletzt abgerufen am 30.07.2023.
Bureau of Justice Assistance / U.S. Department of Justice (BJA)	Privacy Act of 1974, 5 U.S.C. § 552a, abrufbar: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1279, zuletzt abgerufen am 30.07.2023
Bureau of Justice Assistance / U.S. Department of Justice (BJA)	The Foreign Intelligence Surveillance Act of 1978 (FISA), abrufbar: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286, zuletzt abgerufen am 01.08.2023.
Bureau of Justice Assistance / U.S. Department of Justice (BJA)	What Is Risk Assessment, abrufbar: https://bja.ojp.gov/program/psrac/basics/what-is-risk-assessment, zuletzt abgerufen am 04.08.2023.
Chai, Wesley / Lewis, Sarah	incident response team, abrufbar: https://www.techtarget.com/searchsecurity/definition/incident-response-team, zuletzt abgerufen am 05.08.2023.
clarip	CCPA training requirement – Section 1798.130(a)(6) compliance, abrufbar: https://www.clarip.com/data-privacy/ccpa-training/, zuletzt abgerufen am 04.08.2023.
COC AG	Datenschutz und Informationssicherheit: Zwillinge oder Verwandte – kurze Erläuterung zu den Familienverhältnissen. Datenschutz und Informationssicherheit - worin besteht der Unterschied? abrufbar: https://www.coc-ag.de/managed-it-service-stories/datenschutz-und-informationssicherheit, zuletzt abgerufen am 04.08.2023.
ComputerWeekly.de	Computer Security Incident Response Team (CSIRT), abrufbar: https://www.computerweekly.com/de/definition/Computer-Security-Incident-Response-Team-CSIRT, zuletzt abgerufen am 05.08.2023.
Corbe, Marian / Olbring, Markus / Struck, Matthias	Grundlegende Begriffe und Schutzziele der Informationssicherheit, abrufbar: https://www.rst-beratung.de/themen/informationssicherheit, zuletzt abgerufen am abgerufen am 04.08.2023.
Cornell Law School / Legal Information Institute (LII)	Privacy, abrufbar: https://www.law.cornell.edu/wex/Privacy, zuletzt abgerufen am 30.07.2023.
Cornell Law School / Legal Information Institute (LII)	Publicity, abrufbar: https://www.law.cornell.edu/wex/publicity, zuletzt abgerufen am 30.07.2023.

Council of European Union	Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses, aburfbar: https://www.consilium.europa.eu/en/documents-publications/treaties-agreements/ratification/?id=2016043&partyid=UE&doclanguage=en, zuletzt abgerufen am 02.08.2023.
Crowdstrike	Incident Response (IR): Plan & Process, abrufbar: https://www.crowdstrike.com/cybersecurity-101/incident-response/, zuletzt abgerufen am 05.08.2023.
Cybersecurity and Infrastructure Security Agency	Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), abrufbar: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia, zuletzt abgerufen am 05.08.2023
datenschutzexperte.de	Risikoanalyse im Datenschutz, abrufbar: https://www.datenschutzexperte.de/datenschutz-risikoanalyse/, zuletzt abgerufen am 04.08.2023
datenschutzexperte.de	Technisch organisatorische Maßnahmen (TOM), abrufbar: https://www.datenschutzexperte.de/technisch-organisatorische-massnahmen/, zuletzt abgerufen am 06.08.2023.
Delacruz, Walter / Artzt, Matthias	How to comply with both the GDPR and the CLOUD Act, abrufbar: https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/, zuletzt abgerufen am 03.08.2023.
Der Landesbeauftragter für den Datenschutz und Datensicherheit, Rheinland-Pfalz	Standarddatenschutzklauseln der EU-Kommission oder einer Aufsichtsbehörde, abrufbar: https://www.datenschutz.rlp.de/de/themenfelder-themen/standarddatenschutzklauseln-der-eu-kommission-oder-einer-aufsichtsbehoerde/, zuletzt abgerufen am 02.08.2023.
DiGiacomo, John	MLAT Subpoenas: What EU Service Providers Need to Know, abrufbar: https://revisionlegal.com/internet-law/privacy/mlat-subpoenas/, zuletzt abgerufen am 02.08.2023.
DLA PIPER	Data Protection Laws of the World: United States, abrufbar: https://www.dlapiperdataprotection.com/index.html?t=transfer&c=US, zuletze abgerufen am 02.08.2023.
Dracoon	Datentransfer: So versenden Sie große Dateien sicher & einfach, abrufbar: https://www.dracoon.com/de/datentransfer, zuletzt abgerufen am 01.08.2023.

Dr. Datenschutz	Was sind Technisch und organisatorische Maßnahmen (TOM)? abrufbar: https://www.dr-datenschutz.de/was-sind-technisch-und-organisatorische-massnahmen-tom/, zuletzt abgerufen am 04.08.2023.
Dr. Datenschutz	Datenschutzkonformer Einsatz von Office 365 nach Cloud Act, abrufbar: https://www.dr-datenschutz.de/datenschutzkonformer-einsatz-von-office-365-nach-cloud-act/, zuletzt abgerufen am 03.08.2023.
DSGVO-Vorlagen / DeinData GmbH	Muster für eine Risikoanalyse nach DSGVO, abrufbar: https://dsgvo-vorlagen.de/muster-fuer-eine-datenschutz-folgenabschaetzung-dsfs-nach-dsgvo, zuletzt abgerufen am 04.08.2023.
EmpowerIT	The difference between a security incident and a data breach, abrufbar: https://www.empowerit.com.au/blog/difference-between-security-incident-and-data-breach/, zuletzt abgerufen am 05.08.2023.
encyclopedia.com	Judicial Assistance, abrufbar: https://www.encyclopedia.com/law/encyclopedias-almanacs-transcripts-and-maps/judicial-assistance, zuletzt abgerufen am 02.08.2023.
European Commission	Mutual legal assistance and extradition, abrufbar: https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en, zuletzt abgerufen am 02.08.2023.
European Data Protection Board	Der EDSA begrüßt Verbesserungen durch EU-US-Datenschutzrahmen, auch wenn nicht alle Bedenken ausgeräumt wurden, abrufbar: https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_de, zuletzt abgerufen am 03.08.2023.
European Data Protection Supervisor (EDPS)	Datenschutz, abrufbar: https://edps.europa.eu/data-protection/data-protection_de, zuletzt abgerufen am 04.08.2023.
European Union Agency for fundamental Rights (DRA)	Erläuterungen zur Charta der Grundrechte: Artikel 7 - Achtung des Privat- und Familienlebens, abrufbar: https://fra.europa.eu/de/eu-charter/article/7-achtung-des-privat-und-familienlebens#explanations, zuletzt abgerufen am 30.07.2023.
Europäische Kommission	Fragen und Antworten: Datenschutzrahmen EU-USA, abrufbar: https://ec.europa.eu/commission/presscorner/detail/de/qanda_23_3752, zuletzt abgerufen am 03.08.2023.

Europäische Menschenkonvention / Praetor Verlagsgesellschaft mbH	Privatsphäre und Familienleben, abrufbar: https://www.menschenrechtskonvention.eu/privatsphaere-und-familienleben-9292/, zuletzt abgerufen am 30.07.2023.
Exabeam	Incident Response Plan 101: The 6 Phases, Templates, and Examples, abrufbar: https://www.exabeam.com/incident-response/incident-response-plan/, zuletzt abgerufen am 05.08.2023.
Foitzick, Klaus	Rechenschaftspflichten bei der Datenverarbeitung, abrufbar: https://www.activemind.de/magazin/rechenschaftspflicht-dsgvo/, zuletzt abgerufen am 04.08.2023.
Foitzick, Klaus	U.S. CLOUD Act vs. GDPR, abrufbar: https://www.activemind.legal/guides/us-cloud-act/, zuletzt abgerufen am 03.08.2023.
Fortinet	DoS Attack vs DDoS Attack, abrufbar: https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos, zuletzt abgerufen am 05.08.2023
Herold, Philipp	Verschlüsselung von Dateien: Stolperfallen beim Datenschutz, abrufbar: https://www.mein-datenschutzbeauftragter.de/blog/20170908-verschluesselung-von-dateien-stolperfallen-beim-datenschutz/, zuletzt abgerufen am 04.08.2023.
Hessel, Stefan / Callewaert, Christoph	NIS-2-Richtlinie: neue Cybersecurity-Pflichten verabschiedet, abrufbar: https://www.reuschlaw.de/news/nis-2-richtlinie-neue-cybersecurity-pflichten-verabschiedet/, zuletzt abgerufen am 05.08.2023.
Hery-Moßmann, Nicole	Was ist Digital? Einfach erklärt, abrufbar: https://praxistipps.chip.de/was-ist-digital-einfach-erklaert_41596, zuletzt abgerufen am 31.07.2023.
iapp	The latest on the EU-US Data Privacy Framework, abrufbar: https://iapp.org/news/a/the-latest-on-the-eu-us-data-privacy-framework/, zuletzt abgerufen am 03.08.2023.
Industrie- und Handelskammer (IHK)	Dokumentationspflichten und Rechenschaftspflicht, abrufbar: https://www.frankfurt-main.ihk.de/recht/uebersicht-alle-rechtsthemen/datenschutzrecht/dokumentationspflichten-und-rechenschaftspflicht-5192962, zuletzt abgerufen am 04.08.2023.
Informationstechnologie Technische Universität München	Definition: vertrauliche Daten, abrufbar: https://www.it.tum.de/it/vertrauliche-daten/definition-vertrauliche-daten/#c2421, zuletzt abgerufen am 01.08.2023.

International Business Machines Corporation (IBM) — Cost of a data breach 2022: A million-dollar race to detect and respond, abrufbar: https://www.ibm.com/reports/data-breach, zuletzt abgerufen am 05.08.2023.

intersoft Consulting — Verschlüsselung, abrufbar: https://dsgvo-gesetz.de/themen/verschluesselung/, zuletzt abgerufen am 04.08.2023.

It Governance — Cybersecurity Risk Assessments, abrufbar: https://www.itgovernanceusa.com/cyber-security-risk-assessments, zuletzt abgerufen am 04.08.2023.

It Governance — Guide to the NIST CSF (Cybersecurity Framework), abrufbar: https://www.itgovernanceusa.com/nist-cybersecurity-framework, zuletzt abgerufen am 04.08.2023.

It Governance — National Institute of Standards and Technology (NIST), abrufbar: https://www.itgovernanceusa.com/nist, zuletzt abgerufen am 04.08.2023.

Kryptowissen.de — Schutzziele der Informationssicherheit, abrufbar: https://www.kryptowissen.de/schutzziele.php, zuletzt abgerufen am 04.08.2023.

Kulbeth, Marie — The CPRA & Third Parties, abrufbar: https://www.sixfifty.com/blog/the-cpra-third-parties/, zuletzt abgerufen am 04.08.2023.

Lambertz, Peer — Risiko-Beurteilung nach DSGVO in der Praxis, abrufbar: https://www.datenschutz-praxis.de/grundlagen/risikobeurteilung-nach-dsgvo-in-der-praxis/, zuletzt abgerufen am 04.08.2023.

Lanowitz, Theresa — Incident Response Team: What are the Roles and Responsibilities? abrufbar: https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response/arming-your-incident-response-team, zuletzt abgerufen am 05.08.2023.

Longley, Robert — What Are Individual Rights? Definition and Examples, abrufbar: https://www.thoughtco.com/individual-rights-definition-and-examples-5115456, zuletzt abgerufen am 30.07.2023.

Looß, Alina — Wie sicher sind Ihre Daten vor dem US CLOUD Act? abrufbar: https://www.plusserver.com/blog/cloud-act, zuletzt abgerufen am 02.08.2023.

Marschall, Kevin — DSGVO: So gehen Sie mit Datenpannen richtig um, abrufbar: https://www.datenschutz-praxis.de/pleiten-pech-pannen/dsgvo-datenpannen/, zuletzt abgerufen am 05.08.2023.

Matthäus, Alexander	Legal rift between the EU and USA: Data handling & data transfer and the implications for enterprises, abrufbar: https://blog.cryptshare.com/en/legal-rift-eu-usa-data-handling-data-transfer-implications-for-enterprises?hs_amp=true, zuletzt abgerufen am 02.08.2023.
Meckler, Inessa	Transatlantische Datentransfers: aktueller Stand zwischen EU und USA, abrufbar: https://www.dataguard.de/blog/update-transatlantische-datentransfer-bedeutung-fuer-eu-unternehmen, zuletzt abgerufen am 03.08.2023.
Mendoza, Miguel Ángel	Das Recht auf Privatsphäre im digitalen Zeitalter, abrufbar: https://www.welivesecurity.com/deutsch/2017/04/06/recht-privatsphaere-digitales-zeitalter/, zuletzt abgerufen am 30.07.2023.
Minority Rights Group International (MRG)	Self-determination, abrufbar: https://minorityrights.org/law/self-determination/, zuletzt abgerufen am 30.07.2023.
National Cyber Security Center / Ministry of Justice and Security	How the CLOUD-Act works in data storage in Europe, abrufbar: https://english.ncsc.nl/latest/weblog/weblog/2022/how-the-cloud-act-works-in-data-storage-in-europe, zuletzt abgerufen am 05.08.2023.
O- keyed	Datenschutz Zertifizierung, abrufbar: https://keyed.de/blog/datenschutz-zertifizierung/, zuletzt abgerufen am 04.08.2023.
Pittman, F. Paul / Levenberg, Kyle / Shamir, Shira	Data Protection Laws and Regulations USA 2023, abrufbar: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa, zuletzt abgerufen am 05.08.2023.
Privacy Europe / intersoft consulting services AG	European Privacy Framework, abrufbar: https://www.privacy-europe.com/european-privacy-framework.html, zuletzt abgerufen am 03.08.2023.
Public Domain sherpa	The rights of publicity and privacy, abrufbar: http://www.publicdomainsherpa.com/rights-of-publicity-and-privacy.html, zuletzt abgerufen am 30.07.2023.
Publications Office of the European Union	EU-US agreement on personal data protection, abrufbar: https://eur-lex.europa.eu/EN/legal-content/summary/eu-us-agreement-on-personal-data-protection.html, zuletzt abgerufen am 02.08.2023.

PwC Deutschland	Warum Incident Response wichtiger denn je ist, abrufbar: https://www.pwc.de/de/im-fokus/cyber-security/cyber-incident-response.html?utm_source=google&utm_medium=cpc&utm_campaign=XM_thenewequation_CS&utm_id=suche&utm_content=text&utm_term=cyber%20incident%20response, zuletzt abgerufen am 05.08.2023.
Rat der Euripäischen Kommission	Besserer Zugang zu elektronischen Beweismitteln für die Bekämpfung der Kriminalität, abrufbar: https://www.consilium.europa.eu/de/policies/e-evidence/, zuletzt abgerufen am 03.08.2023.
Rat der Europäischen Union	Zugang zu elektronischen Beweismitteln: Rat ermächtigt Mitgliedstaaten, internationales Übereinkommen zu ratifizieren, abrufbar: https://www.consilium.europa.eu/de/press/press-releases/2023/02/14/access-to-e-evidence-council-authorises-member-states-to-ratify-international-agreement/, zuletzt abgerufen am 03.08.2023.
Raveling, Jann	Digitalisierung? Teil I: Eine Reise in die Geschichte des Computers und der Digitalisierung, abrufbar: https://www.wfb-bremen.de/de/page/stories/digitalisierung-industrie40/seit-wann-gibt-es-die-digitalisierung-geschichte-teil-eins, zuletzt abgerufen am 31.07.2023.
Red hat	What are cloud services? abrufbar: https://www.redhat.com/en/topics/cloud-computing/what-are-cloud-services, zuletzt abgerufen am 01.08.2023.
Rehm, Stefan-Marc	Was unterscheidet Datenschutz von Informationssicherheit? abrufbar: https://www.haufe.de/compliance/management-praxis/was-unterscheidet-datenschutz-von-informationssicherheit_230130_482568.html, zuletzt abgerufen am 04.08.2023.
Rosenthal, David	Transfer Impact Assessment Templates: Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities, abrufbar: https://iapp.org/resources/article/transfer-impact-assessment-templates/, zuletzt abgerufen am 04.08.2023.
Rush, Mark A. / Kephart, Jared A.	Lifting the veil on the MLAT process: A guide to understanding and responding to MLA requests, abrufbar: https://www.klgates.com/Lifting-the-Veil-on-the-MLAT-Process-A-Guide-to-Understanding-and-Responding-to-MLA-Requests-01-20-2017, zuletzt abgerufen am 03.08.2023.

Schastlivtseva, Yuliia	Informational Self-Determination of Europe and Its Importance, abrufbar: https://legal-dialogue.org/informational-self-determination-of-europe-and-its-importance, zuletzt abgerufen am 30.07.2023.
Schmidt, Caroline	Die DSGVO und die E-Mail-Verschlüsselung, abrufbar: https://www.e-recht24.de/artikel/datenschutz/11284-dsgvo-und-e-mail-verschluesselung.html, zuletzt abgerufen am 04.08.2023.
Schneider, Maxie	Privacy Shield 2.0: Datentransfer in die USA, abrufbar: https://www.e-recht24.de/datenschutz/13085-eu-us-data-privacy-framework.html, zuletzt abgerufen am 03.08.2023.
Schonschek, Oliver	Haben verschlüsselte Daten einen Personenbezug? abrufbar: https://www.datenschutz-praxis.de/tom/haben-verschluesselte-daten-einen-personenbezug/, zuletzt abgerufen am 04.08.2023.
Schürmann, Rosenthal, Dreyer Partnerschaft von Rechtsanwälten	EuGH kippt Privacy Shield: US-Dienste weiterhin nutzen – FAQ zu Schrems II, abrufbar: https://www.srd-rechtsanwaelte.de/blog/privacy-shield-schrems-ii/, zuletzt abgerufen am 01.08.2023.
Steiner, Falk	Tagung des BKA: Cyberkriminalität – eine der größten Herausforderungen, abrufbar: https://www.deutschlandfunk.de/tagung-des-bka-cyberkriminalitaet-eine-der-groessten-100.html, zuletzt abgerufen am 05.08.2023.
Strömmer, Gunnar	Electronic evidence: Council confirms agreement with the European Parliament on new rules to improve cross-border access to e-evidence, abrufbar: https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/, zuletzt abgerufen am 03.08.2023.
Siriu, Stefanie	Was ist Informationssicherheit - eine Definition, abrufbar: https://www.haufe.de/compliance/management-praxis/informationssicherheit/was-ist-informationssicherheit-eine-defintion_230130_483132.html, zuletze abgerufen am 04.08.2023.
TeamDrive	Sicherer Datenaustausch: Definition, Entwicklung und Formate, abrufbar: https://teamdrive.com/blog-de/sicherer-datenaustausch-definition-entwicklung-und-formate, zuletzt abgerufen am 01.08.2023.
TeamDrive	The Cloud Act – Attention to US Cloud Services, abrufbar: https://teamdrive.com/en/blog-en/the-cloud-act-attention-to-us-cloud-services, zuletzt abgerufen am 29.07.2023.

The United States Department of Justice	276. Treaty requests, abrufbar: https://www.justice.gov/archives/jm/criminal-resource-manual-276-treaty-requests, zuletzt abgerufen am 02.08.2023.
The White House	FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework, abrufbar: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/, zuletzt abgerufen am 02.08.2023.
Thomson Reuters Practical Law	Technical and organisational measures, abrufbar: https://content.next.westlaw.com/practical-law/document/I8d24008059ec11e89bf199c0ee06c731/Technical-and-organisational-measures?originationContext=document&transitionType=DocumentItem&ppcid=45562d1e38a344b2b385a1f4739a475b&contextData=(sc.Category)&firstPage=true&viewType=FullText, zuletzt abgerufen am 04.08.2023.
Tuffley, David	How an app to decrypt criminal messages was born ‘over a few beers’ with the FBI, abrufbar: https://theconversation.com/how-an-app-to-decrypt-criminal-messages-was-born-over-a-few-beers-with-the-fbi-162343, zuletzt abgerufen am 05.08.2023.
United Nations (UN)	Peace, dignity and equality on a healthy planet, abrufbar: https://www.un.org/en/global-issues/human-rights, zuletzt abgerufen am 30.07.2023.
U.S. Department of Commerce	Statement from U.S. Secretary of Commerce Gina Raimondo on the European Union-U.S. Data Privacy Framework, abrufbar: https://www.commerce.gov/news/press-releases/2023/07/statement-us-secretary-commerce-gina-raimondo-european-union-us-data, zuletzt abgerufen am 03.08.2023.
van Otterloo, Sieuwert	Information security and PDCA (Plan-Do-Check-Act), abrufbar: https://ictinstitute.nl/pdca-plan-do-check-act/, zuletzt abgerufen am 04.08.2023.
Vialevo	Was ist der Unterschied zwischen Datenschutz und Informationssicherheit? abrufbar: https://www.vialevo.de/unterschied-zwischen-datenschutz-und-informationssicherheit/, zuletzt abgerufen am 04.08.2023.
Webhelm	Persönlichkeitsrechte, abrufbar: https://webhelm.de/persoenlichkeitsrechte/, zuletzt abgerufen am 30.07.2023.

Weise, Detlev — IT-Sicherheit und Datenschutz: Die Gesetzeslage in den USA und Deutschland im Vergleich, abrufbar: https://digitaleweltmagazin.de/it-sicherheit-und-datenschutz-die-gesetzeslage-in-den-usa-und-deutschland-im-vergleich/, zuletzt abgerufen am 04.08.2023.

Welekwe, Amakiri — A Guide to the Federal and State Data Privacy Laws in the U.S., abrufbar: https://www.comparitech.com/data-privacy-management/federal-state-data-privacy-laws/, zuletzt abgerufen am 30.07.2023.

Will, Michael — Aufgabe und Herausforderung des Datenschutzes, abrufbar: https://www.euroforum.de/datenschutz-kongress/aufgabe-und-herausforderung-des-datenschutzes/, zuletzt abgerufen am 04.08.2023.

Zopf, Yann — From unemployment to growing cyber-risk: business executives in different regions have different worries, abrufbar: https://www.weforum.org/press/2018/11/from-unemployment-to-growing-cyber-risk-business-executives-in-different-regions-have-different-worries/, zuletzt abgerufen am 05.08.2023.