ECONSTOR
Make Your Publications Visible.

A Service of

ZBW Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Bolinth, Lisa

Research Report
Entwurf des American Privacy Rights Acts: Ansätze des europäischen und US-amerikanischen Datenschutzes im Vergleich und die möglichen Auswirkungen an die datenschutzrechtlichen Anforderungen am Beispiel eines transnationalen Online-Vertriebs

Beiträge der Hochschule Pforzheim, No. 186

Provided in Cooperation with:
Hochschule Pforzheim

Suggested Citation: Bolinth, Lisa (2025) : Entwurf des American Privacy Rights Acts: Ansätze des europäischen und US-amerikanischen Datenschutzes im Vergleich und die möglichen Auswirkungen an die datenschutzrechtlichen Anforderungen am Beispiel eines transnationalen Online-Vertriebs, Beiträge der Hochschule Pforzheim, No. 186, ISBN 978-3-911165-08-2, Hochschule Pforzheim, Pforzheim

This Version is available at:
https://hdl.handle.net/10419/330327

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

WWW.ECONSTOR.EU

Mitglied der Leibniz-Gemeinschaft

HS PF

vunk

Lisa Bolinth LL.B.

Entwurf des American Privacy Rights Acts:

Ansätze des europäischen und US-amerikanischen Datenschutzes im Vergleich und die möglichen Auswirkungen an die datenschutzrechtlichen Anforderungen am Beispiel eines transnationalen Online-Vertriebs

Nachhaltigkeit | Digitalisierung und IT | Konsumentenforschung & Market Insights

Verbraucherrecht | Verbraucherstreitbeilegung | Lehre | Wettbewerb, Werte, Wohlfahrt

Nr. V008 der Ausgabe

Forschung für die Zukunftsgesellschaft

Schriftenreihe des vunk

Lisa Bolinth LL.B.

Entwurf des American Privacy Rights Acts:

Ansätze des europäischen und US-amerikanischen Datenschutzes im Vergleich und die möglichen Auswirkungen an die datenschutzrechtlichen Anforderungen am
Beispiel eines transnationalen Online-Vertriebs

Erschienen als Nr. V008 in der Schriftenreihe des vunk:
„Forschung für die Zukunftsgesellschaft“

Zugleich erschienen als Teil der Beiträge der Hochschule Pforzheim als Nr. 186

Pforzheim, Oktober 2025

ISSN: 0946-3755

ISBN: 978-3-911165-08-2

https://opus-hspf.bsz-bw.de

https://hs-pforzheim.de/vunk/schriftenreihe

Forschung für die Zukunftsgesellschaft. Schriftenreihe des vunk.

Beitrag Nr. V008

Herausgeberschaft

Prof. Dr. Hanno Beck (Hochschule Pforzheim)
Prof. Dr. Tobias Brönneke (Hochschule Pforzheim)
Prof. Dr. Peter Heidrich (Hochschule Pforzheim)
Prof. Dr. Ulrich Jautz (Hochschule Pforzheim)
Prof. Dr. Steffen Kroschwald LL.M. (Hochschule Pforzheim)
Dr. Patrik Schmidt LL.M.
Prof. Dr. Marina Tamm (Hochschule Neubrandenburg)

Hochschule Pforzheim
Institut für Verbraucherforschung
und nachhaltigen Konsum | vunk
Tiefenbronner Str. 65
75175 Pforzheim

Tel: +49 7231 / 28-6018
E-Mail: Sekretariat.vunk@hs-pforzheim.de

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

Diese Schriftenreihe *Forschung für die Zukunftsgesellschaft*. *Schriftenreihe des vunk* ist Teil der Beiträge der Hochschule Pforzheim.

Herausgeberschaft der Beiträge der Hochschule Pforzheim

Prof. Dr. Hanno Beck (geschäftsführend; hanno.beck@hs-pforzheim.de), Prof. Dr. Rebecca Bulander, Prof. Dr. Thomas Cleff, Prof. Dr. Thomas Hensel, Prof. Dr. Norbert Jost, Prof. Dr. Christa Wehner

Hochschule Pforzheim
Tiefenbronner Str. 65
75175 Pforzheim
E-Mail: beitraege.hochschule@hs-pforzheim.de

Ausgabe: Oktober 2025

ISSN: 0946-3755

Vorwort der Herausgeber

Forschung für die Zukunftsgesellschaft: nutzerorientierte Gestaltung von Technik, Wirtschaft und Recht am Maßstab von konsentierten Grundwerten unter Ausgleich widerstreitender legitimer Interessen.

Das Zentrum Verbraucherforschung und nachhaltiger Konsum | vunk bündelt die interdisziplinären Forschungsaktivitäten der Hochschule zu Fragen der Zukunftsgesellschaft. Es bietet eine Plattform für angewandte Forschung im Bereich der Verbraucher-, Nutzer- und Nachhaltigkeitsforschung. Es ermöglicht den Transfer sowie den Austausch und die Zusammenarbeit mit sowie auch in Bezug auf staatliche Stellen, Zivilgesellschaft, Wirtschaft, Medien und Politik.

Die Arbeit des vunk bezieht sich dabei auf die Erforschung, Mitgestaltung und Begleitung einer Gesellschaft der Zukunft, ihrer Technologie, Wirtschaft und rechtlichen Rahmenbedingungen, unter Ausgleich der vielfältigen Interessen. Maßstab dieses Interessensausgleichs bilden Grundwerte, auf deren Geltung sich eine Zukunftsgesellschaft übergreifend einigen kann; z.B. Grundrechte. In den Mittelpunkt seiner Forschung stellt das vunk den Nutzer und seine Beziehung zu Produkten, Geschäftsmodellen und (digitalen) Gütern.

Die Ergebnisse der Forschung im vunk fließen regelmäßig in die Lehre an der Hochschule zurück.

Die Herausgeber

Bisher erschienen

• Shirin Mayasilci, Inhalt und Bedeutung der neu ins bürgerliche Recht eingeführten

Update-Pflicht

(vunk Schriftenreihe Nr. 1)

• Vanessa Schweikert, Das Lieferkettensorgfaltspflichtengesetz

(vunk Schriftenreihe Nr. 2)

• Hans-Joachim Grupp, Weihnachtsgeschichten aus dem Schwarzwald

(vunk Schriftenreihe Nr. 3)

• Annalena Secci, Erstellen und Veröffentlichen von Fotos nach der DSGVO. Eine

kritische Auseinandersetzung am Beispiel von Kinderfotos

(vunk Schriftenreihe Nr. 4)

• Denise Flattich, Die CE-Kennzeichnungspflicht im Fokus des neuen Sachmangelbegriffs

(vunk Schriftenreihe Nr. 5)

• Melanie Mitschke, Einziehung von Gegenständen des rechtswidrigen Glücksspiels nach § 148c GewO

(vunk Schriftenreihe Nr. 6)

• Heiko Steffens: Von der Arbeitsgemeinschaft der Verbraucherverbände (AgV) zum Verbraucherzentrale Bundesverband. Strukturreform von 1995 – 2001

(vunk Schriftenreihe Nr. 7)

Inhaltsverzeichnis

1. Einleitung 1
1.1. Problemstellung 1
1.2. Zielsetzung und Forschungsfrage 2
1.3. Gang der Arbeit und Methodik 3
2. Der American Privacy Rights Act in der Landschaft des US-amerikanischen Datenschutzes 4
2.1. Der US-amerikanische Datenschutz auf Bundesebene 5
2.2. Der US-amerikanische Datenschutz auf bundesstaatlicher Ebene 8
2.2.1. California Consumer Privacy Act 9
2.2.2. Aktuelle Entwicklungen im staatlichen Datenschutzrecht der USA 11
2.3. Die Konzeption des APRA 14
2.3.1. Inhaltliche Zusammenfassung des APRA 14
2.3.2. Sachlich-persönlicher Anwendungsbereich 19
2.3.3. Durchsetzung und Rechtsweg 21
2.4. Die Bedeutung des Status „Entwurf“ für den APRA und die Chancen seiner Umsetzung 23
3. US-amerikanischer Datenschutz im Verhältnis zur Datenschutzgrundverordnung (DSGVO) 27
3.1. Übersicht zur Historie der Regelungen zum Datentransfer zwischen der EU und den USA 27
3.1.1. Safe Harbour 28
3.1.2. Schrems I 29
3.1.3. Privacy Shield 31
3.1.4. Schrems II 32
3.1.5. EU-US Data Privacy Framework 34
3.2. Überschneidungen und Unterschiede 36
3.2.1. Anwendungsbereich 36
3.2.2. Grundsätze der Verarbeitung 38
3.2.3. Rechtsgrundlagen und Einwilligung 41
3.2.4. Betroffenenrechte 42
3.2.5. Large Data Holder und Data Broker 43
3.3. Möglichkeit eines Angemessenheitsbeschlusses 44
3.4. Perspektivenwechsel: Europäisches Datenschutzrecht aus Sicht der USA 48

4. Use Case: Anforderungen an den Datenschutz im transnationalen Online-Vertrieb in der EU und den USA mit Fokus auf grenzüberschreitende Datenflüsse 51

4.1. Beschreibung des Szenarios sowie die Arten von Daten und deren Verarbeitungen 52

4.2. Anwendungsbereich und Rechtsgrundlagen 52

4.3. Datenschutzerklärung 54

5. Fazit 56

5.1. Wichtigste Erkenntnisse der Arbeit 57

5.2. Zukunftsausblick 59

Abkürzungsverzeichnis

%	Prozent
ABl.	Amtsblatt der Europäischen Union
ADPPA	American Data Privacy Protection Act
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
Alt.	Alternative
APRA	American Privacy Rights Act of 2024
Art.	Artikel
B2C	Business-to-Consumer
BeckOK	Beck’scher Online-Kommentar
BeckRS	Beck-Rechtsprechungssammlung
BfDI	Bundesbeauftragte für den Datenschutz und die Informationssicherheit
BGH	Bundesgerichtshof
bspw.	beispielsweise
BVerfG	Bundesverfassungsgericht
bzgl.	bezüglich
bzw.	beziehungsweise
CCPA	California Consumer Privacy Act
COPPA	Children’s Online Privacy Protection Act
COPPA 2.0	Children’s Online Privacy Protection Act 2.0
CPPA	California Privacy Protection Agency

CPRA	California Privacy Rights Act of 2020
d.h.	das heißt
Dr.	Doktor
DSGVO	EU-Datenschutz-Grundverordnung
DSK	Konferenz unabhängiger Datenschutzaufsichtsbehörden des Bundes und der Länder
EDSA	Europäischer Datenschutzausschuss
EDSB	Europäischer Datenschutzbeauftragter
EU	Europäische Union
EU DS-RL	Europäische Datenschutzrichtlinien 95/46/ EG
EU-Charta	Charta der Grundrechte der Europäischen Union
EuG	Gericht der Europäischen Union
EuGH	Europäischer Gerichtshof
EU-Kommission	Europäische Kommission
EU-Parlament	Europäisches Parlament
EU-US DPF	EU-US Data Privacy Framework
f.	folgende
FAQ	Frequently Asked Questions
FTC	Federal Trade Commission
FTC-Act	Federal Trade Commission Act
gem.	gemäß
GG	Grundgesetz

ggf.	gegebenenfalls
HIPAA	Health Insurance Portability and Accountability Act
Hrsg.	Herausgeber
i.V.m.	in Verbindung mit
IAPP	International Association of Privacy Professionals
IHK	Industrie- und Handelskammer
IP-Adresse	Internetprotokoll-Adresse
KI	Künstliche Intelligenz
lit.	litera
Mio.	Millionen
MMR	Multimedia und Recht Zeitschrift für IT-Recht und Recht der Digitalisierung
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NSA	National Security Agency
NVwZ	Neue Zeitschrift für Verwaltungsrecht
Opt-Out	Opting-Out
PCLOB	Privacy and Civil Liberties Oversight Board
Prof.	Professor
Rdnr.	Randnummer
S.	Satz
SDK	Standardvertragsklausel

Sec.	Section
sog.	sogenannte
SSRN	Social Science Research Network
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz
u.a.	und andere
u.a.	unter anderem
US	United States
USA	United States of America
usw.	und so weiter
v.a.	vor allem
vgl.	vergleiche
WPA	Washington State Privacy Act
WS	Wintersemester
z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZD-Aktuell	Newsdienst der Zeitschrift für Datenschutz

1. Einleitung

„The American Privacy Rights Act gives Americans fundamental, enforceable data privacy rights, puts people in control of their own data and eliminates the patchwork of state laws“, heißt es in einer Pressemitteilung des Ausschusses für Energie und Handel der Vereinigten Staaten von Amerika im April 2024. Darin wird ein als historisch erachteter neuer Entwurf für ein umfassendes US-Bundesdatenschutzgesetz angekündigt. Das Besondere daran: Ein solch umfassendes Gesetz wäre zwischen vielen einzelstaatlichen und sektoralen Datenschutzgesetzen das erste seiner Art, wenn auch keinesfalls der erste Versuch ein solches Gesetz zu etablieren.[1]

Wie dieser Entwurf in der Landschaft des US-amerikanischen Datenschutzrechtes einzuordnen und wie er außerdem im Vergleich zur EU-Datenschutz-Grundverordnung (DSGVO)[2] ausgestaltet ist, soll in dieser Studienarbeit untersucht werden.

1.1. Problemstellung

Das europäische Datenschutzrecht ist mit der am 25.5.2018 in Kraft getretenen DSGVO EU-weit zentral geregelt. Anders als ihr Vorgänger, der Europäischen Datenschutzrichtlinie 95/46/EG (EU DS-RL)[3], welche gem. Art. 288 S. 3 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)[4] die Wahl der Form und Mittel den Mitgliedsstaaten gewährt, hat die DSGVO als EU-Verordnung gem. Art. 288 S. 2 AEUV allgemeine Geltung. Sie ist in all ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedsstaat. Im Gegensatz dazu besteht das US-

---

[1] Committee on Energy and Commerce (Hrsg.), Committee Chairs Rodgers, Cantwell Unveil Historic Draft Comprehensive Data Privacy Legislation.
[2] VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119/1 vom 4.5.2016, 1-88.
[3] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, 31-50.
[4] Konsolidierte Fassungen des Vertrags über die Europäische Union und des Vertrags über die Arbeitsweise der Europäischen Union, ABl. C 202 vom 7.6.2016, 1-361.

amerikanische Datenschutzrecht aus einem Flickenteppich zahlreicher einzelstaatlicher Datenschutzgesetze, ohne eine existierende national einheitliche Lösung.[5] Der Mangel eines solchen einheitlichen und belastbaren Datenschutzrechts stellt nicht nur innerhalb der USA eine Herausforderung dar. Auch für europäische Staaten trägt dies zu Unsicherheiten bzgl. des sicheren Datentransfers in die USA bei. Wie die sog. „Schrems-Urteile“[6] des Europäischen Gerichtshofs (EuGH) zeigen, ist dies durchaus begründet, da das Gericht den Vereinigten Staaten ein angemessenes Datenschutzniveau, welches dem in der EU gleichwertig ist, bereits zwei Mal wieder abgesprochen hat. Mit dem neuen Entwurf des American Privacy Rights Act of 2024 (APRA)[7] könnte den Rechtsunsicherheiten bzgl. der fragmentierten Gesetzeslage im US-amerikanischen Datenschutzrecht ein Ende gesetzt werden. Damit einher geht auch die Hoffnung, dass ein neues, kohärentes, einheitliches Datenschutzrecht in den USA insgesamt auf einem höheren Datenschutzniveau ansetzt. Dies vermag auch Auswirkungen auf die Angemessenheitsbewertung seitens der Europäischen Union und folglich auf die Möglichkeiten für Datentransfers zwischen den USA und der EU für Unternehmen zu haben.

1.2. Zielsetzung und Forschungsfrage

Folgende Frage soll in dieser Arbeit untersucht werden:

Wie lässt sich der APRA in die aktuelle US-amerikanische Gesetzeslage zum Datenschutz einordnen und mit der DSGVO vergleichen und welche Bedeutung könnte das Inkrafttreten des APRA für den Datentransfer zwischen der EU und den USA, insbesondere im Hinblick auf die Gestaltung einer Vertriebswebsite, haben?

Dazu wird nach einer Analyse des APRA und dem Vergleich zur DSGVO der Use Case einer (fiktionalen) Vertriebswebsite betrachtet. Es soll sich um ein in Deutschland ansässiges Unternehmen handeln, welches sowohl in der EU als auch

---

[5] IAPP (Hrsg.), *Fazlioglu*, US Federal Privacy Legislation Tracker.
[6] EuGH, Urteil vom 6.10.2015 – C-362/14, NJW 2015, 3151 – 3158; EuGH, Urteil vom 16.7.2020 – C-311/18, NJW 2020, 2613-2622.
[7] U.S. Congress (Hrsg.), H.R.8818 – American Privacy Rights Act of 2024 118th Congress (2023-2024).

den USA aktiv ist. An verschiedenen Aspekten lassen sich die Anforderungen beider Gesetze an die Gestaltung einer solchen Seite, insbesondere an die Gestaltung der Datenschutzerklärung, gut aufzeigen und mögliche Veränderungen durch die Bestimmungen des APRA praktisch betrachten. Zudem sollen Prognosen zur Umsetzung des APRA und der Bewertung des Datensicherheitsniveaus aus EU-Perspektive aufgestellt werden.

1.3. Gang der Arbeit und Methodik

Es handelt sich um eine rechtswissenschaftliche Arbeit. Nach einer Gesetzesanalyse des APRA und dessen Vergleich mit der DSGVO sollen durch Anwendung der daraus gewonnenen Zwischenergebnisse Aussagen über eine mögliche Neubewertung des Schutzniveaus von personenbezogenen Daten in den USA getroffen werden. Zuletzt soll eine vergleichende Betrachtung der Gesetze auf den Anwendungsfall der Gestaltung einer Vertriebswebsite vorgenommen werden.

In Kapitel 2 wird hierzu zunächst die Ausgangssituation der US-amerikanischen Gesetzeslage zum Datenschutz dargestellt und schließlich der APRA inhaltlich zusammengefasst. Zudem wird erörtert, inwiefern der APRA tatsächliche Chancen zur Umsetzung hat. Für den Vergleich mit der DSGVO wird in Kapitel 3 zunächst eine Übersicht zur Historie der Bewertung der Angemessenheit des Schutzes von personenbezogenen Daten bei deren Übermittlung aus der EU in die USA gegeben. Schließlich werden die Überschneidungen und Unterschiede beider Gesetze analysiert, um anschließend die Bewertung im Rahmen eines Angemessenheitsbeschlusses gem. Art. 45 DSGVO erörtern zu können. Beim Vergleich der Gesetze werden grundsätzlich zuerst die Bestimmungen der DSGVO gelistet und schließlich analysiert, ob eine sinngemäß gleiche Regelung im APRA vorgesehen ist oder sogar zusätzliche Anforderungen an Unternehmen bestehen. Im selben Kapitel wird zudem die US-amerikanische Sicht auf die europäische Herangehensweise zum Datenschutzrecht erläutert, um ein tieferes Verständnis für die Entwicklung beider Gesetzgebungen zu schaffen. Im vierten Kapitel wird das erlangte Wissen schließlich auf die Gestaltung einer Vertriebswebsite angewendet, wobei die Transparenzanforderungen im Mittelpunkt stehen. Auch hier wird der Vergleich von DSGVO und APRA wie im dritten Kapitel aufgebaut.

Der Arbeit ist voranzustellen, dass sich verwendete Personenbezeichnungen auf alle Geschlechter beziehen, zur besseren Lesbarkeit jedoch das generische Maskulinum verwendet wird. Der Zitierstil amerikanischer Gesetze orientiert sich des Weiteren an dem im APRA verwendeten Stil. Fachbegriffe wie bspw. personenbezogene Daten, Betroffene, Verarbeitung, Dritte usw. haben in verschiedenen Gesetzen voneinander abweichende Definitionen. Sie sollten daher immer im Kontext des jeweiligen Gesetzes gelesen werden, wobei zur Übersetzung von Begriffen aus dem APRA oft die Begriffsbezeichnung des europäischen Pendants verwendet wird. Die Fundstelle der Definition wird ggf. zum besseren Verständnis in Fußnoten ergänzt oder der Originalbegriff in englischer Sprache aus dem APRA verwendet. Die in dieser Arbeit zitierte Version des APRA bezieht sich auf den Entwurf, wie er am 25. Juni 2024 vorgestellt und auf der Website des US-Kongresses[8] veröffentlicht wurde. Der Fokus der Arbeit liegt zudem auf den „American Privacy Rights“ gem. Titel I APRA und nicht auf dem „Children’s Online Privacy Protection Act 2.0“ (COPPA 2.0) gem. Titel II APRA.

2. Der American Privacy Rights Act in der Landschaft des US-amerikanischen Datenschutzes

Um zu verstehen, welche Rolle der APRA in Zukunft spielen könnte und um ihn inhaltlich einordnen zu können, liegt es nahe, sich zunächst einen Überblick zur aktuellen Gesetzeslage zum Thema Datenschutz in den USA zu verschaffen.

Dieser Aufgabe müssen sich auch Unternehmen stellen, die in den Vereinigten Staaten agieren. Dies gilt besonders dann, wenn sie große Mengen von personenbezogenen Daten verarbeiten, welche potenziell in den Anwendungsbereich eines der vielen US-Gesetze fallen könnten. In jüngerer Vergangenheit und aktuell waren bzw. sind in den USA zahlreiche Gesetze auf Bundes- und Bundesstaatenebene im Bereich des Datenschutzes zu verzeichnen. Diese vielen, zum Teil neuen Gesetze zum Datenschutz in den USA treten zu unterschiedlichen Zeiten in Kraft und ihre Anwendungsbereiche, Fristen und

[8] U.S. Congress (Hrsg.), H.R.8818 - American Privacy Rights Act of 2024 118th Congress (2023-2024).

Anforderungen für besondere Kategorien von Daten unterscheiden sich stark voneinander. Daher ist es für in der EU ansässige Unternehmen schwierig den Überblick zu behalten. Dies ist jedoch bei geschäftlicher Tätigkeit in den USA notwendig.[9] Dann stellt die Unkenntnis des gesetzlichen Rahmens besonders deshalb ein Risiko dar, da nicht nur Bußgelder und hohe Schadensersatzsummen aus Sammelklagen, sondern auch Imageschäden drohen.[10] Zunächst sollen deshalb gesetzliche Regelungen zum Datenschutz auf Bundes- und Bundesstaatenebene in den USA betrachtet werden, um anschließend den APRA einordnen und die Chancen seiner Umsetzung nachvollziehen zu können.

2.1. Der US-amerikanische Datenschutz auf Bundesebene

Datenschutz betrifft in den Vereinigten Staaten bundesweit unterschiedlichste US-Institutionen und deren Interessenvertreter. Dazu gehört auf Regierungsebene sowohl der exekutive als auch der judikative Arm.[11] Hinzu kommen außerdem unabhängige Behörden, die zwar vom Kongress als legislative Ebene beaufsichtigt werden, aber von der Exekutive, genauer dem amtierenden Präsidenten und dessen sog. Executive Office sowie vom Kabinett unabhängig sind.[12] Sofern einem Betroffenen oder einem Interessenvertreter ein Klagerecht eingeräumt wurde, entscheiden darüber die zuständigen Gerichte als judikativer Arm.[13]

Anders als in der EU gibt es für den US-amerikanischen Datenschutz bislang keine zentrale Regelung, die mit der DSGVO vergleichbar wäre. Allerdings gibt es seit einigen Jahren eine wachsende Anzahl an Gesetzen, die verschiedene Teilaspekte des Datenschutzes bundesweit regeln. Diese können in die Kategorien Verbraucherdatenschutz, Datenschutz am Arbeitsplatz und im Gesundheitswesen, Schutz von Finanzdaten, Kinder und Bildung sowie datenschutzrechtliche Verpflichtungen für den Staat aufgeteilt werden.[14]

---

[9] *Spies*, MMR 2023, 69, 69-72.
[10] *Hoeren/Pinelli*, MMR 2018, 711, 715; *Spies*, MMR 2023, 69, 70.
[11] IAPP (Hrsg.), *Zweifel-Keegan*, US Institutions Privacy Stakeholder Map, 1 f. und 4.
[12] IAPP (Hrsg.), *Zweifel-Keegan*, US Institutions Privacy Stakeholder Map, 2 f.
[13] IAPP (Hrsg.), *Zweifel-Keegan*, US Institutions Privacy Stakeholder Map, 5.
[14] IAPP (Hrsg.), *Fazlioglu*, US Federal Privacy Legislation Tracker Introduced in the 118th Congress (2023-2024), 1.

Der APRA, der in der Kategorie Verbraucherdatenschutz eingeordnet werden kann, wäre bei Inkrafttreten das erste Gesetz, welches drei wichtige Aspekte zugleich erfüllt. Der Entwurf wird nicht nur sowohl von Seiten der Republikaner als auch der Demokraten unterstützt, sondern hat zugleich auch Vorrang vor bundesstaatlichem Recht bzw. hebt dieses auf und bietet Privatpersonen im Falle einer Verletzung ihrer Rechte die Möglichkeit zur Klage vor Gericht.[15] Für den aktuellen Entwurf des APRA liegt die erste Entscheidung über das weitere Vorgehen beim Ausschuss für Energie und Handel[16]. Dieser ist thematisch für den zwischenstaatlichen und ausländischen Handel, elektronische Kommunikation, Internetpolitik, Cybersicherheit, Datenschutz und -sicherheit sowie Verbraucherschutz zuständig. Der Ausschuss beaufsichtigt zudem die Federal Trade Commission (FTC), eine der zuvor genannten unabhängigen Behörden. Die FTC setzt sich im Allgemeinen für die Verhinderung betrügerischer, irreführender und unlauterer Geschäftspraktiken ein und stellt diesbezüglich Informationen für Verbraucher bereit.[17] Sie ist außerdem für die Durchsetzung von Bundesgesetzen zum Verbraucherschutz und das Vorbringen derer Verletzungen vor Gericht zuständig. Auch kann sie, in begrenztem Umfang, verbindliche Regelungen erlassen. Die Durchsetzungsbefugnisse im Rahmen des APRA würden ebenfalls in die Verantwortung der FTC fallen. Der APRA wäre Teil des Aufgabenbereichs des Büros für Verbraucherschutz, unterstützt durch ein extra für den Zweck der Durchsetzung des APRA neu einzurichtendes Büro gem. Sec. 115 (a) (1) und (2) APRA.[18]

Bei der Durchsetzung im Bereich Datenschutz konzentriert sich die FTC besonders auf den Schutz sensibler Daten aus bestimmten Branchen, besonders schutzbedürftiger Personen oder auf spezifische Anwendungsfälle. Dazu gehören bspw. manipulative Muster zur Beeinflussung von Verbrauchern, sog. „Dark Patterns“. Die von der FTC durchgesetzten Maßnahmen können, ähnlich wie die verschiedenen Bundesgesetze, in Kategorien unterteilt werden: allgemeiner Datenschutz, Schutz der Daten von Kindern, Datenschutz im Gesundheitswesen,

---

[15] IAPP (Hrsg.), *Fazlioglu*, US Federal Privacy Legislation Tracker Introduced in the 118th Congress (2023-2024), 2-18.
[16] Im Original: House Committee on Energy and Commerce.
[17] USAGov (Hrsg.), Federal Trade Commission (FTC).
[18] IAPP (Hrsg.), *Fazlioglu*, US Federal Privacy Legislation Tracker Introduced in the 118th Congress (2023-2024), 3; Federal Trade Commission (Hrsg.), Bureaus & Offices.

Datenschutzverletzungen und Instrumente zur Datensicherheit sowie Regulierung von Künstlicher Intelligenz (KI) und der Zugriff auf Daten durch Dritte. Die Bestimmungen der Zuständigkeit und die durchgeführten Maßnahmen basieren auf unterschiedlichen sektoralen Bundesgesetzen. Dazu gehört der „Federal Trade Commission Act“ (FTC-Act), die „Health Breach Notification Rule“, der „Gramm-Leach-Bliley Act“ und der „Fair Credit Reporting Act“. Wurden in der Vergangenheit noch kaum genaue Richtlinien für Unternehmen erlassen, so hat sich dies in der Zwischenzeit durch zahlreiche von der FTC entwickelten Leitlinien geändert. Zusätzlich zu diesen Leitlinien ergibt sich auch aus den Durchsetzungsmaßnahmen der FTC eine Art Gewohnheitsrecht zum Datenschutz. Es lassen sich bspw. Handlungen definieren, welche die FTC als Verstöße gegen das US-Wettbewerbsrecht ahndet und unter dem FTC-Act vor Gericht bringt.[19]

Das IAPP Westin Research Center hat aus der Analyse von durch die FTC geführten Gerichtsverfahren aus den Jahren 2018 bis 2024 Richtlinien für Unternehmen zu den oben genannten Kategorien entwickelt. Bei der Verarbeitung der Daten von Kindern als besonders schutzbedürftige Personengruppe konzentriert die FTC sich verstärkt auf die Durchsetzung des Children’s Online Privacy Protection Act (COPPA)[20]. Unternehmen müssen bei der Erhebung von personenbezogenen Daten von Kindern unter dreizehn Jahren deren Eltern benachrichtigen und ihre Zustimmung überprüfbar einholen. Zudem sollte die Verarbeitung der Daten auf das notwendige Minimum reduziert und die Daten auf Wunsch der Eltern gelöscht werden. Des Weiteren sollten die Kauf- und Kommunikationsmöglichkeiten von Kindern online begrenzt werden. Werbung und die Weitergabe der Daten an Dritte sowie deren Verwendung zum Training von Algorithmen müssen kontrolliert werden. Datenschutzeinstellungen für Kinder müssen standardmäßig privat eingestellt sein und Dark Patterns, bspw. zur Manipulation zum Kauf, sind unzulässig. Fälle wie das Verfahren der FTC gegen „Epic Games“, den Hersteller des bekannten Computerspiels „Fortnite“, welcher

[19] IAPP (Hrsg.), Folks/Olivero, FTC enforcement trends: From straightforward actions to technical allegations; IAPP (Hrsg.), *Fazlioglu*, US Federal Privacy Legislation Tracker Introduced in the 118th Congress (2023-2024), 3.
[20] Amtlicher Titel: Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505.

im Rahmen eines Vergleichs zur Zahlung von 245 Mio. US-Dollar verpflichtet wurde, verdeutlichen die Härte des Vorgehens der FTC.[21]

Auch zu den anderen Kategorien lassen sich aus von der FTC geführten Verfahren Verhaltensgrundsätze dieser Art für Unternehmen ableiten. Bspw. achtet die FTC besonders stark auf den Umgang von Unternehmen mit großflächigen Datenlecks. Sie verlangt adäquate Sicherheitsmaßnahmen im Vorfeld sowie deren regelmäßige Überprüfung. In den USA hat ein Verfahren der FTC gegen Uber Technologies, eine Vermittlungs-App für Fahrten[22], medial große Aufmerksamkeit bekommen. Aufgrund unzureichender Schutzmechanismen waren Standort- und Kontaktdaten von sowohl Fahrern als auch Kunden offengelegt worden. Die FTC übte v.a. Kritik daran, wie Uber schließlich mit der Datenpanne umging, da trotz laufender Untersuchungen auch ein Jahr später die betroffenen Personen nicht vom Unternehmen informiert wurden.[23]

Es lässt sich folglich feststellen, dass es falsch wäre anzunehmen, in den USA gebe es trotz des Fehlens eines umfassenden Datenschutzgesetzes keinen bundesweit durchsetzbaren Datenschutz. Trotzdem stehen die begrenzten Befugnisse der FTC in der Kritik. So fordert bspw. Rebecca Slaughter, Commissioner der FTC, in einer Stellungnahme zum Fall Uber zusätzliche Mittel und Befugnisse der Behörde. Sie betont auch, dass die Befugnis Bußgelder zu verhängen Unternehmen dazu anspornen würde ihre Versprechen gegenüber Verbrauchern einzuhalten und angemessene Datensicherheitsmaßnahmen umzusetzen.[24]

2.2. Der US-amerikanische Datenschutz auf bundesstaatlicher Ebene

Obwohl es auf Bundesebene an umfassenden Gesetzen zur Regelung von Datenschutz fehlt, lässt sich dasselbe nicht auf bundesstaatlicher Ebene bemängeln.

---

[21] Federal Trade Commission (Hrsg.), FTC Sends Refund Payments to Consumers Impacted by Epic Games' Unlawful Billing Practices.
[22] Uber (Hrsg.), Was ist Uber – von A bis Z.
[23] IAPP (Hrsg.), Folks/Olivero, FTC enforcement trends: From straightforward actions to technical allegations; Federal Trade Commission (Hrsg.), Federal Trade Commission Gives Final Approval to Settlement with Uber.
[24] Federal Trade Commission (Hrsg.), Statement of Commissioner Rebecca Kelly Slaughter In the Matter of Uber Technologies, Inc..

Zusätzlich zu vielen sektorspezifischen Gesetzen existieren bislang in neunzehn verschiedenen Staaten Datenschutzgesetze,[25] die als umfassend und nicht nur sektoral bezeichnet werden können.[26] Unternehmen wird daher empfohlen, ihre Datenschutzerklärungen und internen Richtlinien an die im jeweiligen Bundesstaat geltenden Erfordernisse anzupassen. Als grundsätzlich strengstes und etabliertestes Datenschutzgesetz wird der California Consumer Privacy Act (CCPA)[27] eingestuft. Bei der Betrachtung der staatlichen Gesetzeslage soll dieser daher gesondert dargestellt werden, da der CCPA in den letzten Jahren als bedeutendstes staatliches Datenschutzgesetz in den USA galt.[28]

2.2.1. California Consumer Privacy Act

So soll zunächst also ein Blick auf das kalifornische Datenschutzgesetz geworfen werden. Der CCPA, etabliert im Jahr 2018, trat am 1. Januar 2020 in Kraft und schützt die personenbezogenen Daten der Einwohner des US-Bundesstaats Kalifornien. Der Anwendungsbereich des Gesetzes ist eröffnet, wenn Unternehmen mindestens einen Bruttojahresumsatz von 25 Mio. US-Dollar erwirtschaften, sie die persönlichen Daten von mindestens 50.000 Einwohnern Kaliforniens verarbeiten oder 50% oder mehr ihres Umsatzes aus dem Kauf oder Verkauf dieser persönlichen Daten stammt.[29] Gem. der Definition in Sec. 1798.140 (v) (1) CCPA, sind mit persönlichen Daten im Kontext dieses Gesetzes Informationen gemeint, die einen bestimmten Verbraucher oder Haushalt identifizieren, sich auf ihn beziehen, ihn beschreiben, vernünftigerweise mit ihm in Verbindung gebracht werden können oder vernünftigerweise direkt oder indirekt mit ihm in Verbindung gebracht werden könnten. Den Einwohnern Kaliforniens wird dabei das Recht auf Auskunft, Löschung und die Möglichkeit zum Opt-Out beim Verkauf ihrer persönlichen Daten eingeräumt sowie das Recht, beim Ausüben ihrer CCPA-

[25] Stand Ende des Jahres 2024.
[26] IAPP (Hrsg.), *Kibby*, US State Privacy Legislation Tracker.
[27] Amtlicher Titel: TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100].
[28] *Spies*, MMR 2022, 839, 839.
[29] *Spies*, MMR 2023, 69, 69.

Rechte nicht dafür diskriminiert zu werden.[30] Möglich sind zudem Sammelklagen gegen bestimmte Unternehmen, denen dann hohe Schadensersatzsummen drohen.[31]

Der CCPA wurde weiter durch den California Privacy Rights Act of 2020[32] (CPRA) ergänzt, welcher seit dem Jahr 2023 in Kraft ist. Durch den CPRA wurde die für die Implementierung und Durchsetzung kalifornischer Datenschutzgesetze zuständige Aufsichtsbehörde, die California Privacy Protection Agency (CPPA), etabliert. Zudem wurden so weitere Rechte für Betroffene eingeführt, darunter das Recht auf Berichtigung persönlicher Daten, der Limitierung von Vorratsspeicherung und der Verarbeitung sensibler persönlicher Daten.[33] Durch den „Delete-Act“[34], der Anfang des Jahres 2024 in Kraft trat, wurde das kalifornische Datenschutzrecht außerdem durch ein Gesetz erweitert, das ein zentrales Löschverfahren für sog. „Data Broker“ einführt. Damit sind Unternehmen gemeint, die persönliche Daten der Einwohner Kaliforniens nicht direkt vom Verbraucher, sondern z.B. von Dritten erhalten und weiterverkaufen. Betroffene Unternehmen müssen sich bei der CPPA registrieren lassen und bestimmte Informationen bereitstellen, die schließlich von der Behörde veröffentlicht werden. Die Behörde erstellt zudem ein Löschkonzept, durch das betroffene Verbraucher einen Antrag auf Löschung ihrer Daten stellen können. Unternehmen müssen dem Gesuch grundsätzlich innerhalb einer Frist von 45 Tagen nachkommen. Bei Nichteinhaltung sind Gebühren und Geldstrafen vorgesehen. Es handelt sich in den USA um das erste Gesetz dieser Art, findet sich in ähnlicher Form allerdings auch im überarbeiteten Entwurf des APRA in Sec. 112 (c) APRA wieder. Betroffenen Unternehmen wird daher die Erstellung eines Compliance-Programms zur Bearbeitung von Transparenzpflichten und Löschanfragen sowie interne Richtlinien zur Prozessüberprüfung empfohlen.[35]

Insgesamt wurden im Jahr 2024 sechs Änderungen zum CCPA auf den Weg gebracht, u.a. zum erweiterten Schutz Minderjähriger und im Kontext von KI-

---

[30] State of California Department of Justice – Attorney General Rob Bonta (Hrsg.), California Consumer Privacy Act (CCPA).
[31] *Spies*, MMR 2023, 69, 70.
[32] Kein eigenes Gesetz mit amtlichem Titel, sondern Änderung am bestehenden CCPA, im Gesetz als „Amended by initiative Proposition 24“ gekennzeichnet.
[33] State of California Department of Justice – Attorney General Rob Bonta (Hrsg.), California Consumer Privacy Act (CCPA).
[34] Amtlicher Titel: Data Broker Registry / Delete Act [1798.99.80 - 1798.99.89].
[35] *Spies*, ZD-Aktuell 2024, 01505, 01505.

Modellen, die dazu in der Lage sind, persönliche Daten auszugeben.[36] Bislang bleibt Kalifornien zudem der einzige US-Bundesstaat mit eigener dedizierter Datenschutzbehörde.[37]

2.2.2. Aktuelle Entwicklungen im staatlichen Datenschutzrecht der USA

Im Jahr 2024 setzten sich sieben neue staatliche Datenschutzgesetze durch, die zukünftig nach und nach in Kraft treten. Somit steigt die Gesamtanzahl nun auf zwanzig. Dabei ist allerdings der „Florida Digital Bill of Rights“[38] insoweit kritisch zu betrachten, als die Definition des Begriffs „Controller“, d.h. des Verantwortlichen, so eng gefasst ist, dass die meisten Unternehmen gar nicht erst in den Anwendungsbereich des Gesetzes fallen. Das Gesetz fällt deshalb in der Gesamtbetrachtung umfassender einzelstaatlicher US-Datenschutzgesetze heraus.[39]

Grundsätzlich ist festzustellen, dass die neuen einzelstaatlichen Datenschutzgesetze inhaltlich variierter sind als früher. Viele der Gesetze aus den Jahren 2021-2023 orientierten sich am nie in Kraft getretenen „Washington State Privacy Act“ (WPA) aus dem Jahr 2019. Dieser legt z.B. den Begriff der „covered entity“ anhand bestimmter Schwellenwerte zugrunde und bildet die Konkurrenz zum verbraucherfreundlicheren CCPA.[40] Mittlerweile setzen sich aber auch andere Modelle durch.[41] Zusätzlich zu den neuen Gesetzen wurden im Jahr 2024 aber auch viele Änderungen an bereits bestehenden staatlichen Datenschutzgesetzen umgesetzt, v.a. zum erweiterten Schutz bestimmter Datenkategorien. So fallen bspw. neuronale Daten nun auch in die Definition sensibler Daten unter dem „Colorado Privacy Act“. Immer verbreiteter sind zudem Änderungen zum erweiterten Schutz der Daten von Kindern und Jugendlichen wie bspw. im bereits

---

[36] IAPP (Hrsg.), *Lamont/Stauss*, Retrospective: 2024 in comprehensive state data privacy law.
[37] IAPP (Hrsg.), *Fazlioglu*, US State Comprehensive Privacy Laws Report – Overview.
[38] Amtlicher Titel: Florida 382 Digital Bill of Rights.
[39] IAPP (Hrsg.), *Folks*, Defining 'comprehensive': Florida, Washington and the scope of state tracking.
[40] IAPP (Hrsg.), *Duball*, State privacy prospects bring new paradigm in 2023.
[41] IAPP (Hrsg.), *Lamont/Stauss*, Retrospective: 2024 in comprehensive state data privacy law.

angerissenen Fall des CCPA oder im Rahmen des „Virginia Consumer Data Protection Act“.[42]

Zu den umfassenden staatlichen Datenschutzgesetzen gesellen sich außerdem auch neue Gesetze, die nur bestimmte Fälle, Branchen oder Datenkategorien regeln sollen, wie es sie auch auf Bundesebene gibt. Neben der umstrittenen „Florida Digital Bill of Rights“ ist hier z.B. der „My Health My Data Act“[43] aus dem Staat Washington zu nennen. Auch 2025 ist ein datenschutzrechtlich ereignisreiches Jahr, da einige der neuen Gesetze in Kraft treten. Die umfassenden staatlichen Datenschutzgesetze von Delaware, Iowa, Nebraska, New Hampshire und New Jersey traten bereits im Januar in Kraft, im zweiten Halbjahr folgen schließlich Oregon, Tennessee, Minnesota und Maryland.[44] Das Jahr 2024 war bisher eines der aktivsten Jahre für US-amerikanische Datenschutzgesetze mit wichtigen Auswirkungen auf die gesamte Datenschutzlandschaft. Es soll deshalb ein kurzer Blick in einige der staatlichen Gesetze geworfen werden, von denen sich Elemente im APRA wiederfinden und in denen sich die aktuellen Datenschutz-Trends in den USA spiegeln.[45]

Das Datenschutzgesetz von Maryland wird als bisher verbraucherfreundlichstes Datenschutzgesetz betrachtet und steht bereits seit 2020 in Diskussion. Es weicht stark vom – vergleichsweise handelsfreundlicheren – WPA-Ansatz ab. Das gilt v.a. bei der strengen Regelung zur Datenminimierung. Die Verarbeitung personenbezogener Daten muss verhältnismäßig und erforderlich zur Bereitstellung eines Produkts oder einer Dienstleistung sein und bei sensiblen Daten auf das notwendige Minimum beschränkt werden. Der Verkauf der Daten ist dabei ganz verboten. Auch Maine und Vermont haben versucht, Gesetze mit ähnlichen Vorschriften zur Datenminimierung einzuführen, allerdings erfolglos. Trotzdem ist ein klarer Wandel zu mehr Orientierung am Konsumenten statt an der Industrie erkennbar. Dies stößt allerdings auf starkes Lobbying und große Gegenkampagnen, wie das Veto gegen ein privates Klagerecht in Vermont zeigt - eine verbreitete

---

[42] IAPP (Hrsg.), US State Comprehensive Privacy Laws Report 2024 LEGISLATIVE SESSION, 5.
[43] Amtlicher Titel: Washington My Health My Data Act, 2023 Wash. Laws 191.
[44] IAPP (Hrsg.), *Kibby*, US State Privacy Legislation Tracker.
[45] IAPP (Hrsg.), US State Comprehensive Privacy Laws Report 2024 LEGISLATIVE SESSION, 5.

Hürde, der sich auch der APRA stellen muss.[46] Andere Staaten wie New Jersey, Rhode Island und Minnesota orientieren sich weiterhin am alten WPA-Modell, aber mit einigen neuen Definitionen und Anforderungen. So führt New Jersey z.B. eine allgemeine Benachrichtigungspflicht bei Tracking-Technologien ein. Rhode Island verpflichtet zur Offenlegung von Dritten und potentiellen Käufern, denen personenbezogene Daten weitergegeben werden. Zudem führt Minnesota das Verbraucherrecht ein, eine belastende Entscheidung durch Profiling anzufechten.[47] Andere Staaten orientieren sich an bereits existierenden Datenschutzgesetzen wie dem „Texas Data Privacy and Security Act" oder dem „Virginia Consumer Data Protection Act", welcher allerdings Arbeitnehmerdaten ausschließt.[48] Viele andere Staaten orientieren sich auch am CCPA, wie auch der „Kentucky Consumer Data Protection Act", der im Jahr 2026 in Kraft treten wird, wobei auch hier kein privates Klagerecht vorgesehen ist.[49]

Trotz der vielen neuen Gesetze sind nur wenige aktive Durchsetzungsmaßnahmen der Staaten zu beobachten. Auch hier gilt Kalifornien als Vorreiter. Immer mehr dieser Durchsetzungsmaßnahmen auf staatlicher Ebene stützen sich zudem auf den FTC-Act, d.h. auf die Basis unlauterer und betrügerischer Handlungen aus dem US-Wettbewerbsrecht. So hat der Generalstaatsanwalt von Texas unter dieser Definition bspw. einen US-amerikanischen Automobilhersteller verklagt, weil dieser, ohne die Verbraucher zu informieren oder gar ihre Einwilligung einzuholen, Daten aus Autos sammelte und an Versicherungsgesellschaften verkaufte.[50] Ein einheitliches Datenschutzgesetz auf Bundesebene würde daher die Rechtssicherheit und Durchsetzung des Datenschutzes bedeutend vereinfachen, weshalb der Druck auf den Kongress steigt.

---

[46] IAPP (Hrsg.), *Hartzog/Richards*, The Vermont veto is a step backward for privacy.
[47] IAPP (Hrsg.), *Lamont/Stauss*, Retrospective: 2024 in comprehensive state data privacy law; IAPP (Hrsg.), US State Comprehensive Privacy Laws Report 2024 LEGISLATIVE SESSION, 4.
[48] IAPP (Hrsg.), *Lamont/Stauss*, Retrospective: 2024 in comprehensive state data privacy law; The National Law Review (Hrsg.), *Vanderzanden/Seigner*, omprehensive Data Privacy Law Brings Big Changes to Virginia, but Excludes Employee Personal Data.
[49] *Spies*, ZD-Aktuell 2024, 01626, 01626.
[50] IAPP (Hrsg.), *Lamont/Stauss*, Retrospective: 2024 in comprehensive state data privacy law; Texas Office of the Attorney General (Hrsg.), Attorney General Ken Paxton Sues General Motors for Unlawfully Collecting Drivers' Private Data and Selling It To Several Companies, Including Insurance Companies.

2.3. Die Konzeption des APRA

Die Arbeit am APRA stagniert, nicht zuletzt auch wegen des Widerstandes der bundesstaatlichen Interessenvertreter. Der APRA hätte Vorrang vor staatlichem Recht, ein Einschnitt einzelstaatlicher Befugnisse, der erwartungsgemäß auf Proteste stößt. Einigen der Vertreter ist der APRA dabei zu umfassend ausgestaltet, da sie das darin eingeräumte private Klagerecht für eine Verschwendung von Zeit und Geld halten.[51] Andere wiederum, bspw. die CPPA, befürchten durch den APRA eine Schwächung der Rechte ihres staatlichen Datenschutzes[52]. Es ist folglich notwendig, den Inhalt und Anwendungsbereich des Entwurfs näher zu untersuchen.[53]

2.3.1. Inhaltliche Zusammenfassung des APRA

Folgende inhaltliche Übersicht zum APRA soll die wichtigsten Punkte des Entwurfs zusammenfassen. Dieser teilt sich nach einer Überarbeitung des erstmals am 7. April 2024 vorgestellten Entwurfs in zwei Titel – den ursprünglich vorgestellten „American Privacy Rights Act“, nun Titel I, und den „Children’s Online Privacy Protection Act 2.0“, der neu angehängte Titel II. Beide zusammen ergeben schließlich den American Privacy Rights Act of 2024.

Der erste Titel ist in 34 sog. Sections (Sec.) unterteilt. In vielen Artikeln ist zudem eine Befugnis der FTC vorgesehen, zusätzliche Leitlinien zur Umsetzung wie bspw. Templates zu erlassen.

Sec. 101 APRA enthält 60 verschiedene alphabetisch sortierte Begriffsdefinitionen, die ausschließlich im Kontext des Entwurfs Anwendung finden. Sie enthalten zahlreiche Unterdefinitionen, bspw. definiert Sec. 101 (36) (D) APRA den Bruttojahresumsatz im Kontext der Definition eines Large Data Holders. Auch finden sich in den Definitionen zahlreiche dem Gesetz vorweggenommene

---

[51] IAPP (Hrsg.), *Saniuk-Heinig*, Private Rights of Action in US Privacy Legislation.
[52] California Privacy Protection Agency (Hrsg.), Re: H.R. 8818, The American Privacy Rights Act of 2024—Opposed.
[53] IAPP (Hrsg.), Lamont/Stauss, Retrospective: 2024 in comprehensive state data privacy law; IAPP (Hrsg.), US State Comprehensive Privacy Laws Report 2024 LEGISLATIVE SESSION, 5.

Regelungen. So wird z.B. in Sec. 101 (1) APRA nicht nur der Begriff „Affirmative Express Consent“, also die ausdrückliche Einwilligung definiert (vgl. Sec. 101 (1) (A) APRA), sondern sogleich auch die Anforderungen an die Gestaltung für die Anfrage an die Einwilligung und deren Widerruf festgelegt (vgl. Sec. 101 (1) (B) und (D) APRA). Neben der reinen Definition werden in einigen Fällen außerdem auch Besonderheiten, Ausnahmen und Auslegungsregeln mitaufgenommen. Bspw. wird in Sec. 101 (35) (B) APRA erläutert, wann von Wissen über die Nutzung von Produkten oder Dienstleistungen durch Kinder auszugehen ist. Zudem klären die Definitionen von Begriffen wie „covered data“[54] gem. Sec. 101 (12) APRA oder „covered entity“[55], d.h. der vom Gesetz abgedeckten Unternehmen gem. Sec. 101 (13) APRA, über den Anwendungsbereich des APRA auf. Dieser ist auch nachfolgend in keinem anderen Abschnitt ausdrücklich genannt.

Sec. 102 APRA beschreibt die Anforderungen des Gesetzes an die Datenminimierung. Generell darf ein Unternehmen gem. Sec. 102 (a) APRA personenbezogene Daten nicht sammeln, verarbeiten, aufbewahren oder übertragen[56], wenn dies nicht notwendig, verhältnismäßig und begrenzt auf bestimmte Zwecke ist. Dazu zählt die Bereitstellung oder Instandhaltung eines Produkts oder Services, eine auf diesen Kontext bezogene Kommunikation mit der Person[57], die keine Werbung ist, oder ein in Sec. 102 (d) APRA definierter anderer zulässiger Zweck. Sec. 102 (b) APRA begrenzt die Übertragung von sensiblen personenbezogenen Daten[58] an Dritte zudem auf die vorherige Einholung einer ausdrücklichen Genehmigung[59] der betroffenen Person, es sei denn, diese dient einem vom Gesetz ausdrücklich genehmigten Zweck. Diese Anforderung gilt gem. Sec. 102 (c) APRA grundsätzlich auch für das Sammeln, Verarbeiten, Speichern und Übermitteln von biometrischen und genetischen Daten.

Sec. 103 (a) und (b) APRA verpflichtet Unternehmen im Rahmen des Prinzips „Privacy by Design“ zur Einführung von Richtlinien und anderen Verfahren zur Identifikation, Bewertung und Mitigation bestimmter Risiken bei der Verarbeitung

---

[54] Im Folgenden als personenbezogene Daten übersetzt.
[55] Im Folgenden auch Unternehmen genannt.
[56] Gem. der Definitionen von „collect“, „process“, „retain“ und „transfer“ nach Sec. 101 (6), (46), (48) und (58) APRA.
[57] Gem. der Definition von „Individual“ nach Sec. 101 (34) APRA.
[58] Gem. der Definition von „Sensitive Covered Data“ nach Sec. 101 (49) APRA.
[59] Gem. der Definition von „Affirmative Express Consent“ nach Sec. 101 (1) APRA.

von personenbezogenen Daten. Dabei soll auf die Rolle des Unternehmens bei der Verarbeitung der Daten Bezug genommen werden, sowie speziell auf Risiken bezüglich der Daten Minderjähriger[60], Personen mit Behinderung und Personen über 65 Jahren und der Produkte und Dienstleistungen selbst eingegangen werden. Zu den Verfahren gehören auch interne Schulungen und Sicherheitsvorkehrungen. Gem. Sec. 103 (c) APRA sollen dabei verschiedene Faktoren wie Art und Menge der Daten berücksichtigt werden.

Sec. 104 APRA beschäftigt sich mit dem Thema Transparenz und führt die Pflicht zur Veröffentlichung einer Datenschutzerklärung ein (vgl. Sec. 104 (a) APRA). Zudem wird deren Inhalt und Gestaltung präzisiert (vgl. Sec. 104 (b) – (d) APRA). Sec. 104 (e) APRA sieht bei grundlegenden Änderungen[61] zudem einen Hinweis und eine entsprechende Möglichkeit für Betroffene zum Opt-Out vor. Des Weiteren ergänzt Sec. 104 (e) APRA zusätzliche Anforderungen für „Large Data Holder".

Die Betroffenenrechte auf Zugang zu und Berichtigung und Löschung von ihren personenbezogenen Daten sowie das Recht auf Datenübertragbarkeit sind in Sec. 105 APRA geregelt. Während Sec. 105 (a) APRA die einzelnen Rechte präzisiert, regelt Sec. 105 (b) APRA die Häufigkeit und Kosten der Betroffenenanfragen. Die ersten drei Anfragen innerhalb von zwölf Monaten sollen dabei kostenfrei sein. Gem. Sec. 105 (c) APRA hat ein Unternehmen nach Eingang der Anfrage 45 Tage Zeit, diese zu bearbeiten, für „Large Data Holder" verkürzt sich die Frist auf 30 Tage. Falls notwendig ist eine Verlängerung möglich, dann ist der Betroffene allerdings über die Verlängerung und ihren Grund zu informieren. Sec. 105 (d) APRA schreibt eine Verifizierung des Anfragenstellers vor. In bestimmten Fällen darf ein Unternehmen gem. Sec. 105 (e) APRA die Anfrage nicht genehmigen oder hat die Wahl, dem Gesuch nicht nachzukommen. Dies ist z.B. bei der Entstehung unverhältnismäßig hoher Kosten oder wenn das öffentliche Interesse betroffen ist der Fall.

In Sec. 106 (a) APRA sind Opt-Out-Rechte für den Datentransfer an Dritte und für die Nutzung personenbezogener Daten für gezielte Werbung[62] vorgesehen. Gem.

---

[60] Gem. der Definition von „Covered Minor" nach Sec. 101 (15).
[61] Gem. der Definition von „Material Change" nach Sec. 101 (38) APRA.
[62] Gem. der Definition von „Targeted Advertising" nach Sec. 101 (54) APRA.

Sec. 106 (b) APRA soll die FTC dafür zudem allgemeine Anforderungen und technische Spezifikationen für Opt-Out-Mechanismen schaffen.

Sec. 107 und 108 APRA schützen den Betroffenen zusätzlich. Sec. 107 APRA verbietet die Beeinträchtigung von Verbraucherrechten, v.a. durch manipulative „Dark Patterns“[63]. Sec. 108 (a) APRA verbietet es Unternehmen darüber hinaus, Repressalien durch bspw. Preisdiskriminierung gegen Verbraucher zu üben, die ihre Rechte geltend machen. Sog. „Bona Fide Loyalty Programs“[64], d.h. das Anbieten von Rabatten, Prämien oder Mitgliedschaften, ist mit ausdrücklicher Einwilligung und unter bestimmten Umständen aber erlaubt. Ebenso erlaubt sind Anreize zur Teilnahme der Kunden an Marktforschung.

Sec. 109 (a) APRA verpflichtet Unternehmen zur Einführung von angemessenen Konzepten für die Datensicherheit, um die Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten zu gewährleisten und diese vor unbefugtem Zugriff zu schützen. Dazu gehören gem. Sec. 109 (b) APRA auch präventive Risikobewertung und deren Mitigation, ein Löschkonzept, die Schulung von Mitarbeitern und ein Prozess zur Bearbeitung von Betroffenenanfragen.

Gem. Sec. 110 APRA sind Unternehmen zur Benennung eines qualifizierten Datenschutz- und Datensicherheitsbeauftragten verpflichtet. Sec. 110 (b) APRA stellt zusätzliche Anforderungen an „Large Data Holder“, bei denen je ein Datenschutz- und ein Datensicherheitsbeauftragter gefordert wird. Sie müssen interne Kontrollen und Berichtsstrukturen durch die FTC zertifizieren lassen und haben zudem die Pflicht, Datenschutzfolgeabschätzungen durchzuführen. Dabei werden die Vorteile der Verarbeitung personenbezogener Daten gegen mögliche Beeinträchtigungen der Privatsphäre der Betroffenen abgewogen und die zur Gewährleistung der Datensicherheit verwendeten Technologien überprüft.

Pflichten bei der Übermittlung personenbezogener Daten an Auftragsverarbeiter und Dritte werden in Sec. 111 APRA bestimmt. Ein Auftragsverarbeiter[65], der Daten im Auftrag oder auf die Anweisung eines Unternehmens sammelt, verarbeitet, speichert oder übermittelt, ist gem. Sec. 111 (a) APRA verpflichtet, sich

---

[63] Gem. der Definition von „Dark Patterns“ nach Sec. 101 (16) APRA.
[64] Gem. der Definition von „Bona Finde Loyalty Program“ nach Sec. 108 (b) (1) (B) APRA.
[65] Gem. der Definition von „Service Provider“ nach Sec. 101 (50) APRA.

an dessen Anweisungen zu halten und bei der Beantwortung von Verbraucherrechtsanfragen zu assistieren (vgl. Sec. 111 (a) (1) APRA). Überdies ist zuvor ein Vertrag zwischen dem Auftragsverarbeiter und dem verantwortlichen Unternehmen notwendig. Der Vertrag muss die Mittel der Verarbeitung und die sonstigen Pflichten des Auftragsverarbeiters regeln (vgl. Sec. 111 (a) (2) APRA). Für die Übertragung personenbezogener Daten an Dritte sieht Sec. 111 (b) APRA eigene Rechtsgrundlagen vor. Diese Datenübertragung ist dem Unternehmen nur dann gestattet, wenn es den Transparenzanforderungen aus Sec. 104 APRA nachgekommen ist. Für sensible personenbezogene Daten muss zudem eine ausdrückliche Einwilligung des Betroffenen vorliegen. Zwischen dem übermittelnden Unternehmen oder Auftragsverarbeiter und dem Dritten ist vorab zudem ein Vertrag nötig, der u.a. den Zweck der Übertragung regelt.

Die Pflichten von „Data Brokern“[66], also Unternehmen, die den Großteil ihres Umsatzes aus dem Kauf und Verkauf von Daten erzielen, sind in Sec. 112 APRA aufgeführt. Gem. Sec. 112 (a) APRA müssen sich „Data Broker“ öffentlich als solche ausweisen und gem. Sec. 112 (c) APRA bei der FTC registrieren. Dort sollen anschließend alle „Data Broker“ öffentlich einsehbar sein und Personen sollen über einen zentralen Mechanismus die Möglichkeit haben, sog. „Do Not Collect“- und „Delete My Data“-Anfragen zu stellen, denen diese grundsätzlich nachkommen müssen.

Sec. 113 APRA ermöglicht es Unternehmen, ihre internen Richtlinien auf Antrag von der FTC genehmigen zu lassen, um sich anschließend selbst zertifizieren zu dürfen. Sie haben zudem die Option, sich für die Teilnahme an einem in Sec. 114 APRA vorgesehenen Pilotprogramm für die Erprobung von Technologien zur Verbesserung des Datenschutzes zu bewerben.

Weiter wird die Durchsetzung des APRA durch die FTC mit Hilfe eines neu einzurichtenden Büros in Sec. 115 APRA geregelt. Gem. Sec. 116 APRA können außerdem auch Bundesstaaten unter bestimmten Umständen Durchsetzungsmaßnahmen ergreifen. Sec. 118 APRA schafft und konkretisiert den

---

[66] Gem. der Definition von „Data Broker“ nach Sec. 101 (17) APRA.

Anspruch von betroffenen Einzelpersonen, bei der Verletzung bestimmter Rechte aus dem APRA vor Gericht zu klagen.

Wie bereits umrissen, wird dem APRA in Sec. 118 (a) (2) APRA grundsätzlich Vorrang vor staatlichem Recht eingeräumt. Zwei der zahlreichen Ausnahmen dieser Regel sind gem. Sec. 118 (3) APRA z.B. staatliches Strafrecht oder staatliche Regelungen zur elektronischen Überwachung. Darüber hinaus kann der APRA grundsätzlich auch kein anderes gültiges Bundesgesetz einschränken (vgl. Sec. 118 (b) APRA). In Sec. 119 APRA wird dabei speziell auf den COPPA eingegangen und Sec. 120 APRA untersagt sowohl gezielte Werbung als auch Erstanbieterwerbung[67], die an Minderjährige gerichtet ist.

Im „Children's Online Privacy Protection Act 2.0", dem zweiten Titel des APRA, sind ergänzende Definitionen und Bestimmungen für das bestehende Gesetz enthalten. Dabei verweisen einige der Definitionen schlicht auf den ersten Titel des Entwurfs, andere weichen hiervon ab. Statt „covered data" wird hier bspw. „personal information" definiert, womit der Anwendungsbereich des COPPA von Titel I des APRA abweicht.

2.3.2. Sachlich-persönlicher Anwendungsbereich

Weiter soll der Geltungsbereich des ersten Titels des APRA genauer betrachtet werden. Sachlich umfasst der APRA solche Daten, die unter die Definition der sog. „covered data", d.h. personenbezogene Daten im Rahmen des ersten Titels im APRA gem. Sec. 101 (12) APRA, fallen. Diese Definition der Daten lehnt an bereits existierende staatliche Datenschutzgesetze an, weicht aber in der Benennung vom Begriff „personal data", wie er im CCPA (vgl. Sec. 1798.140. (v) CCPA) oder in Sec. 201 (a) (3) APRA für den COPPA 2.0 beschrieben wird, ab. Gem. Sec. 101 (12) (A) APRA sind „covered data" Informationen, die eine Person oder ein Gerät identifizieren oder die allein oder in Kombination mit anderen Informationen mit einer Person oder einem Gerät in Verbindung stehen oder vernünftigerweise in Verbindung gebracht werden können. In anderen Worten fallen darunter also auch

[67] Gem. der Definition von „First Party Advertising" nach Sec. 101 (30) APRA.

Daten, die sich auf mehrere bestimmbare Personen beziehen oder zukünftig beziehen könnten. Auch Daten dieser Art, die von anderen Informationen abgeleitet werden können, z.B. durch Werbung oder KI-Modelle, sind von der Definition erfasst. Gem. Sec. 101 (12) (B) APRA sind zudem bestimmte Datenkategorien vom Begriff der personenbezogenen Daten ausgeschlossen. Darunter gehören z.B. öffentlich zugängliche Daten (vgl. Sec. 101 (12) (B) (iii) APRA). Wie in Kapitel 3.4 näher ausgeführt, soll so die Meinungsfreiheit aus dem ersten Zusatzartikel der US-Verfassung geschützt werden. In Sec. 101 (12) (B) (ii) APRA werden außerdem Personaldaten[68] ausgeschlossen, was auch für staatliche Datenschutzgesetze typisch ist. Eine weitere Einschränkung der Definition personenbezogener Daten besteht zudem im Ausschluss von sog. „on-device data", also Daten, die ausschließlich auf dem Gerät einer Person gesammelt und verarbeitet werden (vgl. Sec. 101 (12) (B) (vi) i.V.m. Sec. 101 (40) APRA).[69]

Zu den personenbezogenen Daten mit besonderem Schutz gehören die in Sec. 101 (49) APRA definierten sensiblen personenbezogenen Daten. Diese sind abschließend aufgezählt und umfassen u.a. Gesundheits- und biometrische Daten, genaue Standortdaten und Finanzdaten. Hinzu kommen zudem bspw. auch Informationen über die Religion oder Ethnie einer Person.

Der persönliche Anwendungsbereich muss genauer betrachtet werden, um zu bestimmen, wer genau als Person im Sinne des APRA gilt. Von den Rechten aus dem APRA profitieren betroffene Personen, wovon gem. Sec. 101 (34) APRA natürliche Personen mit Wohnsitz in den USA umfasst sind. Dies weicht auffällig von den meisten staatlichen Gesetzen ab[70], die nicht von Personen, sondern von Konsumenten bzw. Verbrauchern reden und den Anwendungsbereich damit auf einen B2C-Kontext beschränken.[71] Von den Pflichten, die der APRA auferlegt, sind grundsätzlich Unternehmen betroffen, die als „covered entity" gem. Sec. 101 (13) APRA definiert werden können. Dies sind Unternehmen, die allein oder gemeinsam mit anderen den Zweck und die Mittel der Verarbeitung bestimmen, äquivalent zum Verantwortlichen gem. Art. 4 Nr. 7 DSGVO. Sie müssen zudem in den Zuständigkeitsbereich der FTC gem. Section 5 (a) (2) FTC-Act fallen, wozu die

---

[68] Gem. der Definition von „Employee Information" nach Sec. 101 (25) APRA.
[69] IAPP (Hrsg.), *Fisher/Folks*, The American Privacy Rights Act's definition of covered data.
[70] Darunter Kalifornien, Maryland und Texas.
[71] IAPP (Hrsg.), *Fisher/Folks*, The American Privacy Rights Act's definition of covered data.

meisten Unternehmen wie Banken und Versicherungsgesellschaften gehören[72]. Der APRA inkludiert aber auch gemeinnützige Organisationen und öffentliche Verkehrsunternehmen[73]. Von den Pflichten des APRA unberührt bleiben z.B. Kleinunternehmen gem. Sec. 101 (51) APRA. Dazu gehören Unternehmen, die einen Jahresumsatz von unter 40 Millionen US-Dollar erwirtschaften und die personenbezogenen Daten von weniger als 200.000 Personen verarbeiten. Sie dürfen darüber hinaus grundsätzlich keine Einnahmen durch die Weitergabe von personenbezogenen Daten an Dritte erzielen. Auch Auftragsverarbeiter und Dritte sind, z.B. durch vertragliche Verpflichtungen aus Sec. 104 APRA, von den Pflichten aus dem APRA betroffen.[74]

Ein räumlicher Anwendungsbereich ist weniger ausdrücklich bestimmt. Ohne genauere Bestimmungen zu dem Sitz des Unternehmens, dem Ort der Verarbeitung oder speziellen Regelungen zum Auslandstransfer findet der APRA also immer dann Anwendung, wenn die Daten von Personen mit Wohnsitz in den USA verarbeitet werden. Zeitlich tritt das Gesetz gem. Sec. 124 APRA bei Veröffentlichung des Gesetzes nach 180 Tagen in Kraft, sofern nichts anderes bestimmt ist. Sonderregelungen lassen sich z.B. für die Aufgaben der FTC identifizieren. Exemplarisch ist dabei das Zeitlimit von einem Jahr, um gem. Sec. 103 (d) APRA-Leitlinien betreffend den Grundsatz „Privacy by Design“ zu erlassen.

2.3.3. Durchsetzung und Rechtsweg

Der APRA soll in erster Linie durch die FTC durchgesetzt werden. Eine Durchsetzung durch die Generalstaatsanwälte, den obersten Verbraucherschutzbeauftragen oder andere bevollmächtigte Stellen oder Beamten der Bundesstaaten sowie ein umstrittenes privates Klagerecht sind aber ebenfalls vorgesehen.[75]

---

[72] Federal Trade Commission (Hrsg.), What the FTC Does.
[73] Im Original „Common Carriers“.
[74] IAPP (Hrsg.), AMERICAN PRIVACY RIGHTS ACT cheat sheet.
[75] IAPP (Hrsg.), AMERICAN PRIVACY RIGHTS ACT cheat sheet; IAPP (Hrsg.) *Saniuk-Heinig*, Private Rights of Action in US Privacy Legislation.

Die Durchsetzungsbefugnisse der FTC sehen gem. Sec 115 (a) APRA die Unterstützung eines neu dafür einzurichtenden Büros vor. Dieses soll in Struktur und Größe an den bereits existierenden Büros der Behörde, wie dem Büro für Verbraucherschutz oder Wettbewerb[76], orientiert sein. Zudem soll es mit qualifizierten Mitarbeitern aus unterschiedlichsten Berufsfeldern, wie Anwälten und Psychologen, besetzt werden. Dabei sollen Verletzungen des Gesetzes nach Sec. 115 (b) (1) und (3) APRA als unlautere oder betrügerische Handlung wie in Sec. 18 (a) (1) (B) FTC-Act definiert betrachtet und geahndet werden, wie es der Aufgabenbereich der FTC bereits verlangt[77]. Gem. Sec. 115 (b) (5) APRA sollen alle dabei erlangten Geldstrafen in einen Hilfsfond für die Opfer der Verstöße fließen. Er dient dazu Betroffene finanziell entschädigen zu können. Sollte dies nicht möglich sein, soll das Geld für die Schulung von Verbrauchern und Unternehmen, sowie die Erforschung von Technologien für Datenschutz und -sicherheit verwendet werden. Des Weiteren verpflichtet Sec. 115 (c) APRA die FTC dem Kongress über ihre Durchsetzungsmaßnahmen Bericht zu erstatten.

Sec. 116 (a) (1) APRA gestattet es ermächtigten staatlichen Vertretern, zivilrechtliche Klagen vor einem zuständigen Gericht vorzubringen. Sie dürfen dies dann, wenn Einwohner des jeweiligen Bundesstaates von Verletzungen ihrer Rechte aus dem APRA betroffen sind. Die Klage kann darauf abzielen, die Einhaltung des APRA einzufordern und Bußgelder, Schadensersatz und Prozesskosten sowie andere angemessene Entschädigungen zu erlangen. Gem. Sec. 116 (b) und (c) APRA behält trotz allem die FTC die Hoheit und muss möglichst vor Einleitung eines staatlichen Verfahrens informiert werden. Es ist ihr sodann vorbehalten einzuschreiten. Zudem ist das Einreichen einer Klage auf staatlicher Ebene verboten, wenn die FTC in derselben Angelegenheit bereits einen Prozess führt.

Zuletzt regelt Sec. 116 APRA das private Klagerecht für einzelne betroffene Personen. Dieses ist auf abschließend aufgelistete Bestimmungen des APRA begrenzt und kann die Erlangung von Schadensersatz, Unterlassungsansprüchen, Feststellungsklagen und angemessenen Anwalts- und Prozesskosten umfassen.[78]

---

[76] Federal Trade Commission (Hrsg.), Bureaus & Offices.
[77] Federal Trade Commission (Hrsg.), What the FTC Does.
[78] IAPP (Hrsg.), AMERICAN PRIVACY RIGHTS ACT cheat sheet.

Vor der Erhebung einer Unterlassungsklage oder einer Klage auf Schadensersatz muss die verletzte Person allerdings das betroffene Unternehmen informieren und gem. Sec. 116 (b) und (c) APRA eine Frist zur Heilung von 60 Tagen setzen. Sec. 116 (d) APRA erklärt zudem vorab getroffene Schiedsgerichtsvereinbarungen für Personen unter 18 Jahren oder bei erheblicher Beeinträchtigung der Privatsphäre[79] für unwirksam.

2.4. Die Bedeutung des Status „Entwurf“ für den APRA und die Chancen seiner Umsetzung

Bis der APRA tatsächlich in Kraft treten kann, hat der viel kritisierte Entwurf noch einen weiten Weg vor sich. Doch bevor genauer auf die am häufigsten diskutierten Streitpunkte eingegangen werden kann, soll zunächst grob der US-amerikanische Gesetzgebungsprozess umrissen werden.

Art. 1 der US-Verfassung sieht zur Entstehung von neuen Gesetzen einen Kongress aus zwei Kammern vor: dem Repräsentantenhaus und dem Senat. Durch dieses System soll ein Ausgleich zwischen absoluten Mehrheitsverhältnissen und den Interessen der einzelnen Bundesstaaten geschaffen werden. Um ein Gesetz verabschieden zu können, müssen immer beide Kammern dem Gesetzesentwurf zustimmen. Dieser wird anschließend dem Präsidenten vorgelegt. Der genaue Prozess ist dabei aber von Gesetz zu Gesetz verschieden.[80] Der Entwurf des APRA wurde dem Repräsentantenhaus vorgelegt und dieser hat ihn zur weiteren Bearbeitung dem Ausschuss für Energie und Handel zugewiesen. Nach der Einigung auf eine finale Version des Textes kommt der Entwurf anschließend vor den Senat.[81]

Die nächsten Schritte des Repräsentantenhauses bleiben nach erster Vorstellung und Änderung des Entwurfs aber ungewiss. Aufgrund der anhaltenden Debatten über Änderungen sind weitere Schritte im Kongress bislang ausgeblieben. Eine erneute Sitzung wurde zuletzt am 27. Juni 2024 in letzter Minute abgesagt. Neben

---

[79] Gem. der Definition von „Substantial Privacy Harm“ nach Sec. 101 (53) APRA.
[80] U.S. Congress (Hrsg.), Overview of the Legislative Process.
[81] U.S. Congress (Hrsg.), All Actions: H.R.8818 — 118th Congress (2023-2024).

Streitigkeiten um den Inhalt spielten dabei auch der Zeitdruck wegen der nahenden US-Wahlen und die im August anstehenden Kongressferien eine Rolle. Ein neuer Termin ist bislang nicht absehbar.[82]

Auch der nie in Kraft getretene American Data Privacy Protection Act (ADPPA)[83] aus dem Jahr 2022, der als Vorgänger des APRA gilt, hatte diese Phase bereits durchlaufen.[84] Nach Jahren der Verhandlung sollte auch der ADPPA eine bundesweite Regelung des Datenschutzes bieten und orientierte sich ebenfalls an existierenden staatlichen Datenschutzgesetzen. Trotz Billigung des Entwurfs durch den Energie- und Handelsausschuss am 20. Juli 2022 stimmte das Repräsentantenhaus nie ganzheitlich über den ADPPA ab. Einerseits spielten dabei verschiedene politische Erwägungen im Entwurf eine Rolle, wie z.B. die vorgesehene Offenlegung, ob Daten an bestimmte von den USA als kritisch eingestufte Länder wie China oder Russland übertragen werden. Auf der anderen Seite wurde der Vorrang des Gesetzes vor bundesstaatlichem Recht stark kritisiert[85]. Dazu gehörten vor allem kalifornische Vertreter, die im Vergleich zum bestehenden staatlichen Recht eine Schwächung des Verbraucherschutzes befürchteten.[86] Zentrale Bestandteile des ADPPA wurden im APRA übernommen, aber auch bedeutende Unterschiede, wie das private Klagerecht und der Ausschluss von Kleinunternehmen aus dem Anwendungsbereich des Gesetzes, sind zu verzeichnen.[87]

Der Weg zur Umsetzung des APRA lässt allerdings ähnliche Hürden befürchten. Trotz der allgemeinen Einigung bezüglich der Notwendigkeit eines bundesweit einheitlichen Datenschutzgesetzes ist v.a. die Debatte über das Vorrangverhältnis zum Staatsrecht groß. Auf der einen Seite argumentiert die CPPA erneut, dass staatliches Recht besseren Verbraucherschutz zulässt. Auch andere Bundesgesetze zum Datenschutz, wie etwa der „Health Insurance Portability and Accountability

---

[82] IAPP (Hrsg.), *Duball*, American Privacy Rights Act markup canceled, next US House steps uncertain.
[83] U.S. Congress (Hrsg.), H.R.8152 - American Data Privacy and Protection Act - 117th Congress (2021-2022).
[84] U.S. Congress (Hrsg.), All Actions: H.R.8152 — 117th Congress (2021-2022).
[85] *Spies*, MMR 2023, 69, 69.
[86] IAPP (Hrsg.), *Duball*, Pelosi opposes proposed American Data Privacy and Protection Act, seeks new preemption compromise; State of California Department of Justice – Office oft the Attorney General (Hrsg.), Attorney General Bonta, Governor Newsom and CPPA File Letter Opposing Federal Privacy Preemption.
[87] Congressional Research Service (Hrsg.), The American Privacy Rights Act.

Act“ (HIPAA), der „Gramm-Leach-Bliley Act“ und der „Fair Credit Reporting Act“ würden den Staaten einen solchen stärkeren Schutz ermöglichen.[88] Andere Interessenvertreter fordern hingegen, den Vorrang des APRA weiter auszubauen. Die vielen Ausnahmen würden lediglich Kosten erhöhen, Verwirrung stiften und keinen einheitlichen Datenschutz gewährleisten.[89]

Beanstandet wird zudem das private Klagerecht für Betroffene, ein Punkt, der historisch häufig zu Debatten in der US-amerikanischen Gesetzgebung führt.[90] Die Durchsetzung des APRA sei bereits zur Genüge durch die FTC und die Bundesstaaten gewährleistet und die Kosten eines privates Klagerechts überträfen daher den Nutzen.[91] Eine andere Ansicht vertritt, dass das Recht auf Schutz der Privatsphäre aufgrund seines zutiefst persönlichen Charakters auch die Möglichkeit umfassen müsse, eine Verletzung individuell durchzusetzen.[92] Dem Betroffenen würde eine Verletzung zudem auch am ehesten auffallen und daher die Effektivität des Gesetzes erhöhen.[93]

Auch die Restriktionen gezielter Werbung und die erhöhten Anforderungen an die Datenminimierung werden sowohl von gewerblichen als auch staatlichen Vertretern kritisch gesehen.[94] Die pauschale Reduzierung der Datenverarbeitung allein auf den ursprünglichen Zweck würde Innovation beschränken, stattdessen müsse der Fokus auf die Rechte der Verbraucher zur Kontrolle über ihre Daten gesetzt werden.[95]

Missbilligt werden darüber hinaus die bereits vorgenommenen Änderungen am Entwurf. Dazu gehören bspw. der COPPA 2.0, der ans Ende des APRA gehängt wurde, statt direkt im Text des vorhandenen COPPA inkludiert zu werden.[96]

---

[88] California Privacy Protection Agency (Hrsg.), Re: H.R. 8818, The American Privacy Rights Act of 2024—Opposed.
[89] Information Technology & Innovation Foundation (Hrsg.), *Johnson*, How to Improve the American Privacy Rights Act.
[90] IAPP (Hrsg.), *Saniuk-Heinig*, Private Rights of Action in US Privacy Legislation.
[91] Information Technology & Innovation Foundation (Hrsg.), *Johnson*, How to Improve the American Privacy Rights Act.
[92] *Scholz*, William & Mary Law Review William & Mary Law Review (2021-2022), 1639, 1663-1667.
[93] IAPP (Hrsg.), *Saniuk-Heinig*, Private Rights of Action in US Privacy Legislation.
[94] IAPP (Hrsg.), *Duball*, Stakeholders consider impacts of latest APRA draft text; IAPP (Hrsg.), *Duball*, American Privacy Rights Act markup canceled, next US House steps uncertain.
[95] Information Technology & Innovation Foundation (Hrsg.), *Johnson*, How to Improve the American Privacy Rights Act.
[96] IAPP (Hrsg.), *Duball*, Proposed American Privacy Rights Act clears US House subcommittee.

Unternehmen würden durch die Haftungsrisiken sogar eher dazu angehalten, mehr personenbezogene Daten zu sammeln, um das Alter ihrer Kunden zu überwachen.[97]

Trotz der Unterstützung des Entwurfs vonseiten beider großen Parteien wird bemängelt, dass die neueste Version des APRA v.a. den Interessen der Republikaner entgegen kommt.[98] Die Demokraten würden zu viele Eingeständnissen an die wirtschaftlichen Interessen der Republikaner tolerieren und damit den Schutz von Bürgerrechten einschränken. Auch die Abschaffung einer Klausel gegen Diskriminierung durch KI führt zu Protesten.[99] Der Hauptzweck des Datenschutzes sei, dass die eigenen personenbezogenen Daten nicht gegen den Betroffenen verwendet werden können und seine Einwilligung für die Verarbeitung eingeholt werden muss. Diesem Zweck komme der APRA nicht mehr nach. Zudem gäbe es bei Weitem zu viele Ausnahmen und Schlupflöcher zu jeder Vorschrift, bspw. die Exklusion von „on-device data" bei der Definition personenbezogener Daten.[100]

Zusammenfassend lässt sich also festhalten, dass der Werdegang des APRA weiter ungewiss bleibt, da es äußerst heikel ist, alle Interessenvertreter zufriedenzustellen, weshalb durchaus die Möglichkeit besteht, dass er in der aktuellen Fassung nie Gültigkeit erlangt. Trotzdem zeigt sich die dem Ausschuss für Energie und Handel vorsitzende Republikanerin Cathy McMorris Rodgers weiterhin zuversichtlich. Sie verspricht sich auch weiterhin für die Online-Privatsphäre von Amerikanern einzusetzen, da ein solches Gesetz von grundlegender Bedeutung für die Zukunft und die nächste Generation sei. [101]

---

[97] Information Technology & Innovation Foundation (Hrsg.), Johnson, How to Improve the American Privacy Rights Act.
[98] IAPP (Hrsg.), *Duball*, American Privacy Rights Act markup canceled, next US House steps uncertain.
[99] Wired (Hrsg.), *Cameron*, Surprise! The Latest 'Comprehensive' US Privacy Bill Is Doomed; Leadership Conference on Civil and Human Rights (Hrsg.), Civil Rights Advocates Decry Removal of Civil Rights Protections in APRA.
[100] Lawyers' Committee for Civil Rights Under Law (Hrsg.), Lawyers' Committee Opposes New Draft of American Privacy Rights Act, Urges Representatives to Vote No.
[101] Committee on Energy and Commerce (Hrsg.), Chair Rodgers Statement on the American Privacy Rights Act.

3. US-amerikanischer Datenschutz im Verhältnis zur Datenschutzgrundverordnung (DSGVO)

Auf Basis der Analyseergebnisse des zweiten Kapitels zum US-amerikanischen Datenschutz im Allgemeinen und dem APRA im Speziellen sollen in diesem Kapitel APRA und DSGVO einander gegenübergestellt werden, um im vierten Kapitel schließlich die Anforderungen beider Gesetze auf den Use Case anwenden zu können. Dazu wird zunächst auf die bisherigen Rahmen zur Datenübermittlung aus der EU in die USA eingegangen und schließlich die DSGVO mit dem APRA verglichen. Dies dient dazu, später bestimmen zu können, ob der APRA die Kriterien eines Angemessenheitsbeschlusses aus Sicht der EU theoretisch erfüllen könnte. So soll eine Aussage zur potenziellen Entwicklung der Anforderungen an den Datentransfer zwischen den Vereinigten Staaten und der EU getroffen werden. Anschließend soll zudem das europäische Datenschutzrecht aus US-amerikanischer Sicht betrachtet werden, um die Chancen, die der APRA bietet, zu verstehen und Prognosen zur Rechtsentwicklung anstellen zu können.

3.1. Übersicht zur Historie der Regelungen zum Datentransfer zwischen der EU und den USA

Nachfolgend soll die Entwicklung von Angemessenheitsbeschlüssen der EU-Kommission bezüglich der Vereinigten Staaten gem. Art. 45 DSGVO sowie deren Entwicklung erläutert werden. Dazu gehört die Entscheidung zur Safe-Harbour-Vereinbarung aus dem Jahr 2000[102] und das sog. Schrems I-Urteil aus dem Jahr 2015[103]. Schließlich folgt die darauffolgende Antwort in Form des EU-US Privacy Shields im Jahr 2017[104] und das sog. Schrems II-Urteil aus dem Jahr 2020 [105], durch

---

[102] Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. L 215 vom 25.8.2000, 7-47.
[103] EuGH, Urteil vom 6.10.2015 – C-362/14, NJW 2015, 3151 – 3158.
[104] Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes, ABl. L 207/1 vom 1.8.2016, 1-112.
[105] EuGH, Urteil vom 16.7.2020 – C-311/18, NJW 2020, 2613-2622.

das das Privacy Shield vom EuGH ebenso für ungültig erklärt wurde.[106] Zuletzt wird der aktuelle Angemessenheitsbeschluss der EU-Kommission, namentlich der EU-US Data Privacy Framework (EU-US DPF)[107] und dessen erste jährliche Überprüfung vom Oktober 2024 betrachtet.[108]

3.1.1. Safe Harbour

Die Safe-Harbour-Entscheidung vom 26. Juni 2000 war ein auf vom amerikanischen Handelsministerium veröffentlichten Grundsätzen und „Frequently Asked Questions“[109] (FAQ) basierender Beschluss der EU-Kommission. Dabei handelt es sich um einen sektoralen Angemessenheitsbeschluss für bestimmte Unternehmen. Unter diese Entscheidung fallende Übermittlungen personenbezogener Daten aus der EU in die USA waren demnach ohne zusätzliche Garantien möglich, da die Kommission entschied, dass das in Art. 25 der EU DS-RL[110] vorgesehene angemessene Schutzniveau gewährleistet sei. Das zugrunde liegende System umfasst die Selbstzertifizierung von Unternehmen, die sich zu den Grundsätzen und FAQ bekennen. Die zertifizierten Unternehmen werden in einer Liste aufgenommen, die im Verantwortungsbereich des US-Handelsministeriums liegt.

Die Grundsätze werden in Anhang I aufgeführt. Der Beitritt für Unternehmen ist vollkommen freiwillig. Er basiert auf selbst entwickelten Maßnahmen zur Umsetzung der Grundsätze und FAQ. Die Nichtbeachtung könnte einen Verstoß gegen Abschnitt 5 des FTC-Act zur Verhinderung unlauterer und irreführender

---

[106] *Wolff/Brink/v. Ungern-Sternberg*, in: BeckOK Datenschutzrecht (01.05.2023), Art. 45 DSGVO Rdnr. 59-61.
[107] DURCHFÜHRUNGSBESCHLUSS (EU) 2023/1795 DER KOMMISSION vom 10.7.2023 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA, ABl. L 231/118, 118-229.
[108] EU-Kommission (Hrsg.), BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT über die erste regelmäßige Überprüfung der Funktionsweise des Angemessenheitsbeschlusses zum Datenschutzrahmen EU-USA, Bericht – COM(2024)451.
[109] Zu übersetzen mit „häufig gestellte Fragen“.
[110] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, 31-50.

Praktiken darstellen. Dies wird bei den Durchsetzungsmöglichkeiten in Anhang III näher beschrieben.

Für die Grundsätze sind in Bezug auf einzuhaltende Datenschutzanforderungen zudem Ausnahmen vorgesehen. Diese gelten für Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses und zur Durchführung von US-Recht. Weitere Ausnahmen gelten für Personaldaten, welche grundsätzlich nicht Teil der Zertifizierung sind. Zudem werden grundlegende Prinzipien des Datenschutzrechtes wie Datenintegrität, begrenzte Auskunftsrechte oder Durchsetzungs- und Rechtsbehelfsmechanismen aus heutiger Sicht nur vage umrissen. Anhang II enthält die FAQ, wobei z.B. FAQ Nr. 7 und 8 herausstechen, die auch die Kontrolle der Umsetzung den Unternehmen selbst überlassen und zahlreiche Einschränkungen für das Auskunftsrecht Betroffener[111] vorsehen.[112]

3.1.2. Schrems I

Mit dem Urteil des EuGH vom 6. Oktober 2015, welches als Schrems I-Entscheidung bekannt geworden ist,[113] wird der Angemessenheitsbeschluss der EU-Kommission, der auf Grundlage des Safe-Harbour-Systems getroffen wurde, offiziell für ungültig erklärt. Das Gericht klärt aufgeworfene Fragen aus einem Verfahren gegen den irischen Datenschutzbeauftragen vom 17. Juli 2014. Darin hatte Herr Schrems eine Beschwerde zur Prüfung beim irischen Datenschutzbeauftragen eingelegt. Er wollte damit erreichen, dass die Übermittlung und Speicherung seiner personenbezogenen Daten von Facebook Ireland auf US-amerikanischen Servern geprüft und untersagt wird. Diese würden nicht ausreichend geschützt, was er vorwiegend auf die Enthüllungen von Edward Snowden zu den Überwachungstätigkeiten der US-Behörden stützte.[114] Der Datenschutzbeauftragte weigerte sich, die Beschwerde zu überprüfen. Er wies sie wegen Mangel an Beweisen und der – seiner Ansicht nach – rechtmäßigen

---

[111] Laut Legaldefinition Art. 4 Nr. 1 DS-GVO: „betroffene Personen“.
[112] Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. L 215 vom 25.8.2000, 7-47.
[113] EuGH, Urteil vom 6.10.2015 – C-362/14, NJW 2015, 3151–3158.
[114] Amnesty International (Hrsg.), Der Fall Edward Snowden.

Datenübermittlung als unbegründet zurück. Die Rechtmäßigkeit des Datentransfers in die USA begründete er mit dem Safe-Harbour-Angemessenheitsbeschluss der EU-Kommission. Herr Schrems klagte gegen die Entscheidung des irischen Datenschutzbeauftragten. Das irische oberste Gericht vertrat schließlich die Auffassung, dass Snowdens Enthüllungen zu undifferenzierten Massenüberwachungen der NSA und weiteren amerikanischen Bundesbehörden jedenfalls nicht mit irischem Recht vereinbar und daher die Beschwerde zu prüfen wäre. Fragen das Unionsrecht betreffend verwies das Gericht jedoch in Form eines Vorabentscheidungsersuchens nach Art. 267 AEUV an den EuGH, welcher über die Gültigkeit des Angemessenheitsbeschlusses auf Grundlage des Safe-Harbour-Systems entscheiden sollte.[115] Dieser entschied hierzu, dass, wenn eine Angemessenheitsentscheidung der EU-Kommission nach Art. 25 VI EU DS-RL vorliegt, die nationalen Datenschutzbehörden keine diesem Beschluss entgegenstehenden Maßnahmen treffen, aber entgegenstehende Beschwerden dennoch prüfen können.[116] Der EuGH stellt weiter fest, dass Art. 1 des Safe-Harbour-Beschlusses mit den Anforderungen aus Art. 25 VI EU DS-RL im Licht der EU-Grundrechtecharta nicht vereinbar ist.[117] So sei eine Selbstzertifizierung zwar für sich genommen nicht ungeeignet ein angemessenes Datenschutzniveau zu schaffen, aber es waren keine hinreichenden Überwachungs- und Kontrollmechanismen vorgesehen.[118] Zudem bewertete der EuGH die Einschränkungen der Datenschutzanforderungen für Zwecke der nationalen Sicherheit und des öffentlichen Interesses als zu weitgehend.[119] Ein möglicher Eingriff in das Grundrecht auf die Achtung des Privatlebens erfordere klare objektive Kriterien, Beschränkungen und Garantien für den Betroffenen, welche hier nicht gegeben sind. Zudem reichen die Befugnisse der FTC nicht weit genug, um über Grundrechtsstreitigkeiten zu entscheiden. Nach Bewertung des EuGH fehlte es zudem an administrativen oder gerichtlichen Rechtsbehelfen für Betroffene.[120] Auch Art. 3 des Safe-Harbour-Beschlusses sei ungültig, da europäischen nationalen Kontrollstellen die Möglichkeit genommen wurde

---

[115] EuGH, Urteil vom 6.10.2015 – C-362/14, NJW 2015, 3151, 3151 f..
[116] EuGH, Urteil vom 6.10.2015 – C-362/14, NJW 2015, 3151, 3153 f., Rdnr. 52-57.
[117] EuGH, Urteil vom 6.10.2015 – C-362/14, NJW 2015, 3151, 3157, Rdnr. 98.
[118] EuGH, Urteil vom 6.10.2015 – C-362/14, NJW 2015, 3151, 3156, Rdnr.81 f..
[119] EuGH, Urteil vom 6.10.2015 – C-362/14, NJW 2015, 3151, 3156 f., Rdnr. 86-90.
[120] EuGH, Urteil vom 6.10.2015 – C-362/14, NJW 2015, 3151, 3157, Rdnr. 91-95.

Maßnahmen zur Einhaltung von Art. 25 EU DS-RL zu ergreifen.[121] Da Art. 1 und 3 der Entscheidung untrennbar mit anderen Artikeln verbunden waren, erklärte der EuGH den gesamten Beschluss zu den Safe-Harbour-Grundsätzen für ungültig.[122]

3.1.3. Privacy Shield

Als Antwort auf das Urteil des EuGH folgte am 12. Juli 2016 ein neuer Rahmen für Datenübermittlungen von der EU in die USA, der vor allem für kleine Unternehmen mehr Rechtssicherheit schaffen sollte. Dieser sah striktere Anforderungen an US-Unternehmen und mehr Kontroll- und Durchsetzungsmechanismen der FTC vor. Darüber hinaus war vorgesehen, den Austausch mit europäischen Datenschutzbehörden zu intensivieren und deren Entscheidungen in Bezug auf Personaldaten verbindlich zu beachten. Auch der zuvor so stark kritisierte Zugriff von US-Behörden auf personenbezogene Daten sollte nur noch in gesetzlich geregelten Fällen und in begrenztem Umfang möglich sein. Durch höhere Transparenz sollte jetzt die Notwendigkeit und Verhältnismäßigkeit der Zugriffe gewährleistet sein. Auch waren neue Behelfe für EU-Bürger durch die Benennung einer Ombudsstelle für Beschwerden und neue Fristen für Auskunftsanfragen vorgesehen.[123]

Doch schon nach der ersten jährlichen Überprüfung im September 2017 wurde die EU-Kommission zu Nachjustierung des Privacy Shields aufgefordert. Dabei wurde v.a. Kritik an dem weiterhin als schwach eingestuften Rechtsweg für betroffene EU-Bürger über den Ombudsmann geübt.[124] Allen voran in Fällen, in denen Strafverfolgungsbehörden auf die personenbezogenen Daten von Unternehmen Zugriff haben, seien keine wirksamen Rechtsbehelfe für Einzelpersonen vorgesehen. Die Prüfungskommission beanstandete auch die fehlenden Umsetzungshilfen für Unternehmen und Betroffenenrechte sowie unzureichende Kontrollen der selbstzertifizierten Unternehmen durch das amerikanische

---

[121] EuGH, Urteil vom 6.10.2015 – C-362/14, NJW 2015, 3151, 3157 f., Rdnr. 99-102.
[122] EuGH, Urteil vom 6.10.2015 – C-362/14, NJW 2015, 3151, 3158, Rdnr. 105 f..
[123] EU-Kommission (Hrsg.), Kommission und Vereinigte Staaten einigen sich auf neuen Rahmen für die transatlantische Datenübermittlung: den EU-US-Datenschutzschild.
[124] BfDI (Hrsg.), Privacy Shield: Die Datenschutzbehörden fordern Nachverhandlungen.

Handelsministerium und die FTC.[125] Die zweite jährliche Überprüfung lobte zwar, dass viele Kritikpunkte umgesetzt wurden, wie bspw. die Anpassung des Zertifizierungsprozesses für US-Unternehmen und die Veröffentlichung von Umsetzungshilfen, kam aber zu dem Schluss, dass weiterhin Defizite bestanden. Die Kritik an mangelnden Kontrollmechanismen für zertifizierte Unternehmen und mangelnden Berichte zu den verschiedenen behördlichen Überwachungsprogrammen blieb bestehen.[126] Auch in der dritten Überprüfung im Jahr 2019 wurde weiterhin die Kontrolle der zertifizierten Unternehmen bemängelt, wobei aber die Besetzung der Ombudsstelle und eines Aufsichtsgremiums positiv hervorgehoben wurde. Angemerkt wurde zudem das nachstehend beschriebene laufende Schrems II-Verfahren, dessen Urteil zu diesem Zeitpunkt noch erwartet wurde.[127]

3.1.4. Schrems II

Das Urteil des EuGH vom 16. Juli 2020 entschied über die Gültigkeit des sog. SDK-Beschlusses[128] vom 5. Februar 2010 über Standardvertragsklauseln bei der Übermittlung personenbezogener Daten in ein unsicheres Drittland und erklärte den Angemessenheitsbeschluss zum EU-US Privacy Shield für ungültig.

Dem vorausgegangen war ein erneuter Rechtsstreit auf Betreiben von Max Schrems in Bezug auf Facebook. In dessen Rahmen hatte Facebook Ireland erklärt, dass sie, nach den für ungültig erklärten Safe-Harbour-Grundsätzen, den Großteil der in die USA transferierten personenbezogenen Daten auf Grundlage der im SDK-Beschluss enthaltenen Standardvertragsklauseln übermittelten. Daraufhin hatte Herr Schrems auf Aufforderung eine umformulierte Beschwerde beim irischen Datenschutzbeauftragten eingereicht. Darin kritisierte er, dass diese Vertragsklauseln keine hinreichende Rechtfertigung für die Übermittlung personenbezogener Daten in die USA seien, wenn diese dort im Rahmen von

---

[125] EU-Kommission (Hrsg.), Erste jährliche Überprüfung der Funktionsweise des EU-US-Datenschutzschilds.
[126] EDSA (Hrsg.), EU – U.S. Privacy Shield – Second annual Joint Review.
[127] EDSA (Hrsg.), EU – U.S. Privacy Shield – Third annual Joint Review.
[128] Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, ABl. L 39/5, 5-18.

Überwachungsprogrammen der US-Behörden in unvereinbarer Weise mit Art. 7, 8 und 47 der EU-Charta verarbeitet werden. Nach dem Verweis an das Oberste Gericht in Irland entschied schließlich erneut der EuGH über die Gültigkeit des SDK-Beschlusses und der Vollständigkeit der Antwort halber auch über die Gültigkeit des Angemessenheitsbeschlusses zum Privacy Shield. Das Gericht entschied, dass die Standardvertragsklauseln nach SDK-Beschluss geeignet sind, um das erforderliche, dem der EU gleichwertige Schutzniveau zu garantieren, sofern kein gültiger Angemessenheitsbeschluss vorliegt. Allerdings ist dies nicht der Fall, wenn ersichtlich ist, dass die Klauseln nicht eingehalten werden können, da somit kein angemessener Schutz nach Art. 45 und 46 DSGVO gesichert ist. Hinsichtlich des Angemessenheitsbeschlusses zum Privacy Shield entschied das Gericht, dass die Beschränkungen der Grundsätze zu Zwecken der nationalen Sicherheit, des öffentlichen Interesses oder zur Durchführung von US-Gesetzen den Datenempfänger in den USA verpflichten, die Grundsätze zu missachten. Dies könnte einen Eingriff in die Grundrechte der betroffenen Person darstellen, wenn hier keine Verhältnismäßigkeit gewahrt und der Eingriff auf ein erforderliches Maß reduziert wird. Der EuGH kam zu dem Schluss, dass auch die gesetzlichen Grundlagen, auf denen behördliche Zugriffe in den Staaten erfolgen, diese Voraussetzungen nicht angemessen würdigen und auch keine Garantien oder durchsetzbaren Rechtsbehelfe für die betroffene Person vorsahen. Insgesamt konnte das Schutzniveau für personenbezogene Daten deshalb nicht als gleichwertig zu dem der EU betrachtet werden. Auch der Ombudsmann konnte hier keine Abhilfe schaffen. Folglich erklärte das Gericht den Angemessenheitsbeschluss für unvereinbar mit Art. 45 I DSGVO sowie der Auslegung nach Art. 7, 8 und 47 EU-Charta und damit in seiner Gesamtheit für ungültig und verwies auf Datentransfer auf Grundlage von Art. 49 DSGVO.

Auch der Europäische Datenschutzausschuss (EDSA), welcher die jährlichen Überprüfungen veröffentlicht, verwies in seiner Erklärung vom 17. Juli 2020 auf die Leitlinien zu den Ausnahmen nach Art. 49 DSGVO und erkannte die vom

EuGH betonte Notwendigkeit an, nicht nur Standardvertragsklauseln zu nutzen, sondern auch ihre Einhaltung in der Praxis zu überprüfen.[129]

3.1.5. EU-US Data Privacy Framework

Der aktuell gültige Angemessenheitsbeschluss der EU-Kommission vom 10. Juli 2023 zum EU-US DPF ist unmittelbar in Kraft getreten. Er hat erneut das Ziel, ein angemessenes Schutzniveau für Übermittlungen an nach den Vorgaben des Frameworks handelnden Unternehmen sicherzustellen. Auch basiert dieser Beschluss wieder auf einer Liste selbstzertifizierter US-Unternehmen und Organisationen. Für diese kann der Angemessenheitsbeschluss zum Framework als Rechtsgrundlage für Datentransfers in die USA ohne zusätzliche Maßnahmen nach Art. 46 DSGVO genutzt werden. Anwendungshinweise wurden von der deutschen Konferenz unabhängiger Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) bereits veröffentlicht.[130] Für Unternehmen, die nicht zertifiziert sind, sind weiterhin die Auswirkungen der Schrems II-Entscheidung des EuGH relevant. Voraussetzung für die Zertifizierung eines Unternehmens ist, dass es entweder unter die Durchsetzungsbefugnis der FTC oder des Verkehrsministeriums fällt und vom Handelsministerium überprüft wurde, ob das Unternehmen alle Anforderungen des EU-US DPF erfüllt. Auch eine Neuzertifizierung ist erneut erforderlich, welche jährlich stattfindet. Die Betroffenenrechte wurden erweitert, z.B. um ein Zugriffs- und Berichtigungsrecht sowie um ein Recht auf Löschung der personenbezogenen Daten des Betroffenen bei Nichteinhaltung der Prinzipien des Beschlusses. Auch neue Opt-Out-Mechanismen und Beschwerdemöglichkeiten für EU-Bürger sowie ein neu etabliertes Gericht, vor dem die Betroffenen Rechte durchsetzen können, unterscheiden das EU-US DPF von seinen Vorgängern. Erneut gibt es zudem überarbeitete verbindliche Vorschriften und Aufsichtsstellen,

---

[129] EDSA (Hrsg.), Erklärung zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 – Data Protection Commissioner gegen Facebook Ireland und Maximilian Schrems.

[130] DSK (Hrsg.), Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023.

um den behördlichen Zugriff auf personenbezogene Daten auf das absolut notwendige und verhältnismäßige Maß zu beschränken.[131]

Wie in den Erwägungsgründen vorgesehen, lag der Fokus der ersten jährlichen Untersuchung von Oktober 2024 auf der Prüfung der Umsetzung und Funktion aller im EU-US DPF vorgesehenen Instrumente und auch neuere Entwicklungen des US-Datenschutzrechts seit Inkrafttreten des Datenschutzrahmens wurden dabei berücksichtigt. Positiv hervorgehoben wurden u.a. die neuen unabhängigen Beschwerdestellen, die nun auch Stichprobenkontrollen bei gelisteten Unternehmen durchführen. Auch die FTC führt nach eigener Aussage mehrere Untersuchungen auf Grundlage von Beschwerden durch, kann aber bislang noch keine erlassenen Beschlüsse zur Durchsetzung vorweisen. Da generell nur wenige Beschwerden bei Unternehmen und unabhängigen Stellen eingegangen seien, stellt die Prüfgruppe fest, dass Privatpersonen mehr sensibilisiert werden müssen. Viele Entwicklungen im US-Datenschutzrecht wurden lobend erwähnt, darunter die Executive Order 14117 vom Februar 2024, der den Transfer sensibler Daten mit einigen Ländern beschränkt, aber auch Regelungen zur Sicherung der Privatsphäre im Kontext von Künstlicher Intelligenz. Zudem wurden Richter für den neuen Gerichtsstand des sog. „Data Privacy Review Courts“ ernannt, bisher gibt es aber mangels Beschwerden bei den europäischen Aufsichtsbehörden keine laufenden Verfahren. Auch die enge Zusammenarbeit der EU-Kommission mit den US-Behörden wurde positiv hervorgehoben. Zuletzt hält die Prüfgruppe die nächste regelmäßige Überprüfung in drei Jahren für angemessen, wie auch in Erwägungsgrund 211 vorgesehen, da Leitlinien der FTC in Zusammenarbeit mit EU-Datenschutzbehörden erst entwickelt werden müssen sowie die Überprüfung von der Einhaltung der Grundsätze bei Überwachungstätigkeiten sowie Untersuchungen und Durchsetzungsmechanismen bei den zertifizierten Unternehmen dann beurteilt werden können.[132]

---

[131] DURCHFÜHRUNGSBESCHLUSS (EU) 2023/1795 DER KOMMISSION vom 10.7.2023 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA, ABl. L 231/118, 118-229.

[132] EU-Kommission (Hrsg.), BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT über die erste regelmäßige Überprüfung der Funktionsweise des Angemessenheitsbeschlusses zum Datenschutzrahmen EU-USA, Bericht – COM(2024)451.

3.2. Überschneidungen und Unterschiede

Im vierten Kapitel der Arbeit soll die Gestaltung einer Website auf Basis der Anforderungen des APRA und der DSGVO untersucht werden. Dazu müssen die beiden Gesetze zunächst miteinander verglichen und Unterschiede aufgezeigt werden, um schließlich Möglichkeiten der Umsetzung diskutieren zu können. Hierfür werden allgemeine Aspekte der DSGVO erläutert und schließlich festgestellt, ob ein Äquivalent im APRA vorhanden ist.

3.2.1. Anwendungsbereich

Der Anwendungsbereich der DSGVO ist in Art. 2 und 3 DSGVO ausdrücklich definiert. Der sachliche Anwendungsbereich gem. Art. 2 DSGVO umfasst die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder werden sollen. Personenbezogene Daten sind dabei gem. Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, insbesondere wenn dies mittels einer Zuordnung oder besonderen Kennung möglich ist. Gem. Art. 4 Nr. 2 ist eine Verarbeitung jeder Vorgang im Zusammenhang mit personenbezogenen Daten. Der räumliche Anwendungsbereich der DSGVO erstreckt sich auf die Verarbeitung personenbezogener Daten durch eine Stelle mit Niederlassung in der EU (Art. 3 Abs. 1) sowie auf die Verarbeitung von Daten von Personen, die sich in der EU befinden, durch eine Stelle außerhalb der EU, sofern die Datenverarbeitung im Zusammenhang mit dem Angebot von Waren oder Dienstleistungen oder der Beobachtung ihres Verhaltens steht (Art. 3 Abs. 2). Dem gegenüber stehen die in Kapitel 2.3.2 erläuterten Definitionen der Begriffe „covered data“, „covered entity“ und „Individual“ gem. Sec. 101 (12), (13) und (34) APRA.

Beide Definitionen von personenbezogenen Daten nach DSGVO und APRA beziehen sich dabei auf eine identifizierte oder identifizierbare Person. Erwägungsgrund 36 der DSGVO stellt an die Identifizierbarkeit die Anforderung, dass alle Mittel berücksichtigt werden müssen, die vom Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden,

um die natürliche Person zu identifizieren. Die Anforderung der wahrscheinlichen Nutzung stellt der APRA hingegen nicht. Für eine Identifizierbarkeit nach APRA ist es ausreichend, wenn die Daten zumindest vernünftigerweise mit einer Person in Verbindung gebracht werden können.[133] Allerdings schließt der APRA auch verschiedene Datenkategorien ganz aus. Dazu gehören z.B. öffentlich zugängliche Daten (vgl. Sec. 101 (12) (B) (iii) i.V.m. Sec. 101 (47) APRA) sowie Personaldaten (vgl. Sec. 101 (12) (B) (ii) i.V.m. Sec. 101 (25) APRA). Diese können aber unter die Definition personenbezogener Daten nach DSGVO fallen, was ihren Anwendungsbereich größer macht.

Wie bereits in Kapitel 2.3.2 festgestellt, definiert der APRA den Begriff des „individual“, d.h. der Person. Der Begriff wird ähnlich wie der Begriff der betroffenen Person gem. Art. 4 Nr. 1 DSGVO verwendet. Dies unterscheidet sich vom Begriff des Verbrauchers, eine Definition, die in vielen staatlichen US-Datenschutzgesetzen üblich ist. Der im APRA gewählte Ansatz kann deshalb als Annäherung an die DSGVO gewertet werden. Die Person muss gem. Sec. 101 (34) APRA aber ihren Wohnsitz in den USA haben, eine Anforderung die in der Definition der betroffenen Person gem. Art. 4 I DSGVO nicht gestellt wird.[134] Auch Art. 3 Abs. 2 DSGVO gilt nicht für Personen mit Wohnsitz in der EU, sondern es kommt auf den tatsächlichen Aufenthaltsort der betroffenen Person an.[135]

Schließlich finden sich in Sec. 101 (13) (C) APRA auch Unternehmenstypen, die nicht als „covered entity“ definiert werden dürfen. So exkludiert der APRA gem. Sec. 101 (13) (C) (iii) i.V.m. Sec. 101 (51) APRA Kleinunternehmen ganz vom Anwendungsbereich des Gesetzes. In der DSGVO sind Erleichterungen, wie in Art. 37 DSGVO zur Pflicht zur Benennung eines Datenschutzbeauftragten oder in Art. 30 V DSGVO zu den Dokumentationspflichten, vorgesehen.[136] In der Definition eines Unternehmens gem. Art. 4 Nr. 18 DSGVO wird eine solche Differenzierung aber nicht vorgenommen.[137]

---

[133] IAPP (Hrsg.), *Fischer/Folks*, The American Privacy Rights Act's definition of covered data.
[134] IAPP (Hrsg.), *Fischer/Folks*, The American Privacy Rights Act's definition of covered data.
[135] *Hanloser*, in: BeckOK Datenschutzrecht (01.05.2023), Art. 3 DSGVO Rdnr. 43 f..
[136] EU-Kommission (Hrsg.), Gelten die Vorschriften für KMU?.
[137] IAPP (Hrsg.), *Fischer/Folks*, The American Privacy Rights Act's definition of covered data.

3.2.2. Grundsätze der Verarbeitung

Die in Art. 5 DSGVO aufgeführten Grundsätze bestimmen, wie personenbezogene Daten verarbeitet werden dürfen.[138] Der erste Grundsatz, die Rechtmäßigkeit der Verarbeitung gem. Art. 5 I lit. a i.V.m. Art. 6 DSGVO, regelt zudem genau, ob und wann Daten verarbeitet werden dürfen. Auf sie soll deshalb im anschließenden Unterkapitel gesondert eingegangen werden. Die Anforderungen an den Grundsatz der Transparenz, ebenfalls aus Art. 5 I lit. a DSGVO, werden in weiteren Artikeln des Gesetzes genauer definiert. Art. 12 DSGVO verweist dabei auf die in Art. 13 und 14 DSGVO im Detail beschriebene Informationspflicht bei Erhebung von personenbezogenen Daten. Diese Hinweise werden gemeinhin als Datenschutzerklärung bezeichnet.[139] Zu den Transparenzpflichten gehören auch die Mitteilungen gem. Art. 15-33 DSGVO, als Antwort auf eingetroffene Verlangen der dort geregelten Rechte der Betroffenen. Mitteilungen dieser Art sind in Sec. 105 APRA geregelt. Auffallend ist allerdings, dass die in Art. 34 DSGVO ausdrücklich verlangte Benachrichtigung betroffener Personen im Falle einer Verletzung des Schutzes ihrer personenbezogenen Daten ein Äquivalent im APRA vermissen lässt, zumal die FTC dies verstärkt bei Unternehmen kritisiert.[140] In Sec. 109 (b) (6) APRA ist lediglich die Implementierung von Verfahren zur Erkennung, Reaktion auf und Wiederherstellung nach Sicherheitsvorfällen, einschließlich Datenschutzverletzungen vorgesehen. Gem. Art. 12 V 1 DSGVO müssen die erwähnten verpflichtenden Informationen und Mitteilung zudem unentgeltlich zur Verfügung gestellt werden. Im APRA hingegen gilt dies gemäß Sec. 105 (c) APRA nur für die ersten drei Betroffenenrechtsanfragen einer Person innerhalb eines Jahres.

Art. 5 I lit. b DSGVO enthält außerdem den Grundsatz der Zweckbindung. Die Erhebung und Verarbeitung personenbezogener Daten darf demnach nur für festgelegte, eindeutige und rechtmäßige Zwecke erfolgen. Die Verarbeitung ist nur zulässig, wenn sie für den Zweck erforderlich ist und der Zweck klar, konkret und

---

[138] *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, Art. 5 DSGVO, Rdnr. 7-9.
[139] Datenschutzstelle Fürstentum Liechtenstein (Hrsg.), Informationspflicht (Art. 13 und 14 DSGVO).
[140] IAPP (Hrsg.), *Folks/Olivero*, FTC enforcement trends: From straightforward actions to technical allegations.

nicht zu vage ist. Eine Zweckänderung ist zudem von den Ausnahmen nach Art. 6 IV DSGVO abgesehen grundsätzlich unzulässig.[141] Die Zweckbindung ist im APRA über die Erforderlichkeit im Rahmen der Datenminimierung gem. Sec. 102 APRA abgedeckt und enthält klar vorgegebene Zwecke, für die Daten verarbeitet werden dürfen, welche sich mit den Rechtsgrundlagen aus Art. 6 I DSGVO überschneiden. Davon abgesehen muss in Anfragen, welche auf eine Einwilligung abzielen, der Zweck der Verarbeitung gem. Sec. 101 (1) (B) (iii) APRA angegeben sein.

Weiter gilt gem. Art. 5 I lit. c der Grundsatz der Datenminimierung, der drei Anforderungen an die Verarbeitung personenbezogener Daten enthält. Zum einen muss die Verarbeitung für den verfolgten Zweck erheblich sein, d.h. im Rahmen einer Verhältnismäßigkeitsprüfung geeignet sein, um ein legitimes Ziel zu erreichen. Zudem muss die Verarbeitung für den Zweck erforderlich, also auf das notwendige Maß reduziert sein. Zuletzt muss die Verarbeitung dem Zweck angemessen sein. Es muss daher eine Verhältnismäßigkeit im engeren Sinne vorliegen. Eine Verarbeitung für einen rein hypothetischen Zweck wäre daher unzulässig.[142] Die Verhältnismäßigkeit schreibt auch der APRA in Sec. 102 (a) APRA ausdrücklich vor. Im Allgemeinen dürfen personenbezogene Daten nach APRA nur erhoben, verarbeitet, aufbewahrt oder übertragen werden, wenn dies notwendig, verhältnismäßig und begrenzt auf einen erlaubten Zweck geschieht. Grundsätzlich ist daher auch hier eine Verhältnismäßigkeitsprüfung vorgesehen. Eine Angabe dazu, wie diese zu bestimmen ist, gibt es jedoch nicht.

Gem. Art. 5 I lit. d DSGVO müssen personenbezogene Daten sachlich richtig und auf dem neuesten Stand sein. Mit Blick auf den Zweck der Verarbeitung müssen sie andernfalls gelöscht oder berichtigt werden. Konkretisiert wird dies durch den Anspruch des Betroffenen auf Berichtigung der Daten gem. Art. 16 DSGVO.[143] Erwägungsgrund 39 S. 11 führt aber aus, dass der Verantwortliche verpflichtet ist, die Daten unabhängig von einem solchen Verlangen zu überprüfen. Zudem muss er alle vertretbaren Schritte unternehmen, damit unrichtige Daten unverzüglich gelöscht oder berichtigt werden. Eine solche Verpflichtung ist im APRA nicht

---

[141] *Pötters*, in: Gola/Heckmann, DS-GVO BDSG, Art. 5 DSGVO, Rdnr. 15 und 19.
[142] *Schantz*, in: BeckOK Datenschutzrecht (1.5.2023), Art. 5 DSGVO, Rdnr. 24-26.
[143] *Heberlein*, in: Ehmann/Selmayr, DSGVO, Art. 5, Rdnr. 33.

explizit genannt, aber auch hier hat der Betroffene gem. Sec. 105 (a) (3) APRA das Recht, die Berichtigung oder gem. Sec. 105 (a) (5) APRA die Löschung seiner Daten zu verlangen.

Ein weiterer Grundsatz für die Verarbeitung ist gem. Art. 5 I lit. e DSGVO die Speicherbegrenzung, die grundsätzlich vorsieht, dass die Daten nach Zweckerreichung gelöscht werden müssen.[144] Die Speicherung von personenbezogenen Daten unterliegt gem. Sec. 102 (a) 3. Alt. APRA dem Prinzip der Datenminimierung, da eine Speicherung nach Erreichung des Zwecks wohl nicht notwendig wäre. Ausdrücklich ist dies zudem in Sec. 109 (b) (3) und (4) APRA vorgesehen. Demnach ist die Löschung nach Zweckerreichung und das Einführen eines Löschkonzepts verpflichtend. Eine grundsätzliche Höchstfrist für die Speicherung von drei Jahren ist nur für biometrische und genetische Daten gem. Sec. 102 (c) (3) APRA vorgesehen.

Der Grundsatz der Integrität und Vertraulichkeit gem. Art. 5 I lit. f DSGVO besagt, dass personenbezogene Daten nur in einer Weise verarbeitet werden dürfen, die eine angemessene Sicherheit, Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und unabsichtlichem Verlust, unabsichtlicher Zerstörung oder Schädigung gewährleistet. Ausgestaltet wird dieser Grundsatz durch die Anforderungen des Art. 25 DSGVO an den Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen und die technischen und organisatorischen Anforderungen an die Sicherheit der Verarbeitung in Art. 32 DSGVO.[145] Sec. 103 APRA stellt Anforderungen an „Privacy by Design“. Verlangt wird die Etablierung von Verfahren zur Wahrung der Datensicherheit, um die Vertraulichkeit, Integrität und Verfügbarkeit der erfassten Daten sowie Schutz vor unautorisiertem Zugriff zu gewährleisten.

Zuletzt sieht Art. 5 II DSGVO eine Rechenschaftspflicht vor. Nach dieser ist der Verantwortliche für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten verantwortlich und muss dies auch nachweisen können. Für Art und Umfang der Maßnahmen ist dabei ein risikobasierter Ansatz ausschlaggebend.[146] Gem. Erwägungsgrund 76 muss eine objektive

---

[144] *Pötters*, in: Gola/Heckmann, DS-GVO BDSG, Art. 5 DSGVO, Rdnr. 18.
[145] *Heberlein*, in: Ehmann/Selmayr, DSGVO, Art. 5, Rdnr. 37 f..
[146] *Heberlein*, in: Ehmann/Selmayr, DSGVO, Art. 5, Rdnr. 40.

Risikobewertung erfolgen. Eine identische Entsprechung zur Rechenschaftspflicht gibt es im APRA nicht, doch da die in diesem Unterkapitel genannten Pflichten direkt dem Unternehmen oder Auftragsverarbeiter auferlegt werden, ist davon auszugehen, dass diese auch für die Einhaltung verantwortlich sind. Auch schreibt Sec. 109 (b) (1) APRA als Anforderung an Datenschutzverfahren eine routinemäßige Risikoeinschätzung vor. Verstärkte Verpflichtungen für „High-Impact Social Media" Unternehmen[147], „Large Data Holder" und „Data Broker", die die Daten von besonders vielen Personen verarbeiten, lassen auch auf eine Annäherung an den risikobasierten Ansatz der DSGVO schließen.[148]

3.2.3. Rechtsgrundlagen und Einwilligung

Für die rechtmäßige Verarbeitung personenbezogener Daten gilt in der DSGVO das Verbotsprinzip mit Erlaubnisvorbehalt. Die Verarbeitung ist demnach grundsätzlich verboten, es sei denn die Voraussetzungen mindestens einer Erlaubnisnorm gem. Art. 6 I DSGVO sind erfüllt.[149] Auch im APRA gilt das Verbotsprinzip, wie sich aus der Formulierung von Sec. 102 (a) APRA schließen lässt. In Sec. 102 APRA sind unter dem Grundsatz der Datenminimierung insgesamt siebzehn ausdrücklich erlaubte Tatbestände definiert. Einige davon könnten unter die Rechtsgrundlage des berechtigten Interesses gem. Art. 6 I lit. F DSGVO fallen, wie bspw. nicht personalisierte Werbung gem. Sec. 102 (d) (14) APRA.[150] Zudem werden, ähnlich wie für die Verarbeitung besonderer Datenkategorien gem. Art. 9 DSGVO, auch in Sec. 102 (b) und (c) APRA spezielle Anforderungen an die Verarbeitung besonders sensibler Datenkategorien gestellt. Bei biometrischen und genetischen Daten wird dabei im Gegensatz zur DSGVO aber auch zwischen den einzelnen Arten der Verarbeitung unterschieden.

Nähere Bestimmungen zur Einwilligung der betroffenen Person als Rechtsgrundlage der Verarbeitung personenbezogener Daten sind in Art. 6 I lit. a

---

[147] Gem. der Definition von „Covered High-Impact Social Media Company" nach Sec. 101 (14) APRA.
[148] IAPP (Hrsg.), Maldoff, The Risk-Based Approach in the GDPR: Interpretation and Implications, 3.
[149] *Schantz*, in: BeckOK Datenschutzrecht (1.11.2021), Art. 5 DSGVO, Rdnr. 5 f.; BfDI (Hrsg.), Die Grundlagen des Datenschutzrechts.
[150] Siehe Erwägungsgrund 47 S. 7 DSGVO.

i.V.m. Art. 7 DSGVO beschrieben. Gem. Art. 4 Nr. 11 DSGVO muss die Einwilligung aus einer freiwilligen, für einen bestimmten Fall, in informierter Weise und unmissverständlich abgegebenen Willensbekundung in Form einer Erklärung oder einer sonstigen bestätigenden Handlung bestehen. Damit muss die betroffene Person zu verstehen geben, dass sie mit der Verarbeitung einverstanden ist. Die Anforderungen des APRA an eine Einwilligung gem. Sec. 101 (1) APRA sind im Wesentlichen gleich. Nichtstun kann genau wie im Rahmen der DSGVO hier nicht als Zustimmung gewertet werden.[151] Im Gegensatz zur DSGVO erlaubt es der APRA aber in besonderen Fällen, bestimmt in Sec. 106 (a) (1) und (2) APRA, beim Transfer von Daten an Dritte und bei gezielter Werbung Opt-Out-Konstruktionen zu verwenden.[152] Der Widerruf der Einwilligung muss sowohl gem. Art. 7 III 4 als auch gem. Sec. 101 (1) (A) APRA so einfach wie die Erteilung der Einwilligung sein. Keines der beiden Gesetze enthält außerdem bestimmte Formvorschriften.

3.2.4. Betroffenenrechte

Bedeutende Unterschiede zwischen DSGVO und APRA lassen sich jedenfalls bei den Betroffenenrechten feststellen. So ist ein ausdrückliches Auskunftsrecht der betroffenen Person gem. Art. 15 DSGVO, in Sec. 105 APRA, der die Rechte der Betroffenen regelt, nicht vorgesehen. Man könnte wohl aber argumentieren, dass dies durch das Recht auf Zugriff des Betroffenen auf seine Daten gem. Sec. 105 (a) (1) APRA erfasst ist. Zum Recht aus Berichtigung der Daten gem. Art. 16 DSGVO gibt es hingegen, wie bereits erwähnt, ein Äquivalent in Sec. 105 (a) (2) APRA. Auch das Recht der betroffenen Person auf Löschung ihrer personenbezogenen Daten gem. Art. 17 DSGVO ist in Sec. 105 (a) (3) APRA ausdrücklich genannt. Weiter überschneidet sich das europäische sog. „Recht auf Vergessenwerden“, wonach bei einem Löschverlangen alle vertretbaren Schritte unternommen werden müssen, um veröffentlichte Daten vollständig zu löschen[153], mit der Anforderung aus Sec. 105 (a) (3) APRA. Auftragsverarbeiter und Dritte

---

[151] EDSA (Hrsg.), Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, 20.
[152] EDSA (Hrsg.), Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, 21 f..
[153] BfDI (Hrsg.), Datenschutz-Grundverordnung – Bundesdatenschutzgesetz – Texte und Erläuterungen, 59.

müssen demnach über das Löschgesuch informiert werden und dabei assistieren, dieses auszuführen. Ein Recht auf Einschränkung der Verarbeitung gem. Art. 18 DSGVO hat wiederum kein passendes Pendant im APRA, genauso wie das Widerspruchsrecht aus Art. 21 DSGVO. In beiden Gesetzen ist jedoch ein Recht auf Datenübertragbarkeit vorgesehen (vgl. Art. 20 DSGVO und Sec. 105 (a) (4) APRA). Zudem können, wie im vorherigen Unterkapitel beschrieben, Betroffene auf Grundlage beider Gesetze ihre Einwilligung zur Verarbeitung widerrufen. In der aktuellen Version des APRA wurden allerdings Formulierungen gegen datengestützte Diskriminierung im Rahmen von Risikofolgenabschätzungen und KI herausgenommen. Diese hätten voraussichtlich ähnliche Ansprüche etabliert, wie sie in Art. 22 DSGVO vorgesehen sind.[154] Darin erhalten betroffene Personen das Recht, nicht einer ausschließlich automatisierten Verarbeitung unterworfen zu werden, wenn diese ihr gegenüber eine rechtliche Wirkung entfaltet oder sie in ähnlicher Weise beeinträchtigt. Zu einer derartigen automatisierten Verarbeitung gehört insbesondere das Profiling. Zuletzt ist festzustellen, dass das in Art. 77 DSGVO ausgeführte Beschwerderecht gegenüber der Aufsichtsbehörde kein explizit genanntes Pendant im APRA hat.

3.2.5. Large Data Holder und Data Broker

Eigens erwähnt werden sollen zuletzt noch die Vorschriften für „Large Data Holder“ und „Data Broker“. Dabei handelt es sich um Begriffe, die im Rahmen des APRA definiert werden, aber kein gleichgestelltes Konzept in der DSGVO haben.

„Large Data Holder“ ist ein Unternehmen gem. Sec. 101 (36) (A) APRA im Allgemeinen dann, wenn es im letzten Kalenderjahr Bruttoeinnahmen von zumindest 250 Mio. US-Dollar erwirtschaftet hat und bei der Verarbeitung personenbezogener Daten bestimmte Schwellenwerte an Personen oder Geräten überschreitet. Sobald dies der Fall ist, werden die entsprechenden Unternehmen vom APRA mit zusätzlichen Anforderungen belastet. Dazu gehört bspw. eine

[154] Lawyers’ Committee for Civil Rights Under Law (Hrsg.), Lawyers’ Committee Opposes New Draft of American Privacy Rights Act, Urges Representatives to Vote No.

kürzere Frist zur Bearbeitung von Betroffenenrechtsanfragen oder erhöhte Transparenzanforderungen (vgl. Sec. 105 (c) (1) (B) und Sec. 104 (f) APRA).

„Data Broker“ sind gem. Sec. 101 (17) (A) APRA Unternehmen, deren Haupteinnahmen aus der Verarbeitung und Übertragung personenbezogener Daten stammen, welche das Unternehmen nicht direkt bei der betroffenen Person erhoben hat. Auch sie unterliegen zusätzlichen Anforderungen. Dazu gehört insbesondere die Registrierung in einem dafür vorgesehenen Register der FTC gemäß Sec. 112 APRA.

Der risikobasierte Ansatz der DSGVO berücksichtigt an einigen Stellen ebenfalls die Art und den Umfang der Verarbeitung, v.a. gestützt auf den risikobasierten Ansatz für technische und organisatorische Maßnahmen gem. Art. 24 I DSGVO[155] und bei den bereits erwähnten Erleichterungen für Kleinunternehmen. Äquivalente zu den Konzepten „Large Data Holder“ und „Data Broker“ nach APRA gibt es aber nicht, was in den USA insofern innovativer ist.

3.3. Möglichkeit eines Angemessenheitsbeschlusses

Wie bereits umrissen, ist die EU-Kommission dazu ermächtigt, sog. Angemessenheitsbeschlüsse gem. Art. 45 DSGVO zu erlassen. Ein solcher betrifft gem. Art. 45 I 1 DSGVO die Entscheidung, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Die Rechtsfolge eines solchen Beschlusses ist es gem. Art. 45 I 2 DSGVO, dass entsprechend abgedeckte Datenübermittlungen keiner besonderen Genehmigungen mehr bedürfen. D.h., es dürfen ohne weitere Anforderungen Daten ins Drittland übermittelt werden.[156] Folglich sind Datentransfers auf Basis eines Angemessenheitsbeschlusses klar zu bevorzugen, weil sie solchen innerhalb der EU gleichgestellt sind[157] und Unternehmen nicht erst geeignete Garantien gem. Art 46

---

[155] *Heberlein*, in: Ehmann/Selmayr, DSGVO, Art. 5, Rdnr. 40.
[156] EDSB (Hrsg.), Glossar – Angemessenheitsbeschluss.
[157] Der Hessische Beauftragte für Datenschutz und Informationsfreiheit (Hrsg.), Überblick – Angemessenheitsbeschlüsse der Europäischen Kommission.

DSGVO bereitstellen müssen.[158] Wie in Kapitel 3.1.5 ausgeführt, liegt ein solcher Angemessenheitsbeschluss in Form des EU-US DPF aktuell in einem begrenzten Rahmen für bestimmte zertifizierte Unternehmen vor. Die Historie der Rahmen für Datentransfers aus der EU in die USA wirft jedoch die Frage auf, inwieweit auf das Bestehen des Beschlusses Verlass ist. Es gilt zu bewerten, wie ein mögliches Inkrafttreten des APRA sich auf den Angemessenheitsbeschluss auswirken könnte. Dazu muss analysiert werden, ob und in welchem Maße die Vorschriften des APRA die hierfür festgelegten Kriterien erfüllen.

Es gilt zunächst zu verstehen, wie ein Angemessenheitsbeschluss erlassen wird. Das EU-Parlament und der Europarat können die EU-Kommission ersuchen, einen Angemessenheitsbeschluss zu beschließen, zu ändern oder aufzuheben (vgl. Art. 45 III 1 und V 1 DSGVO). Mit Umsetzung des APRA wäre z.B. eine Änderung des Rahmens des aktuellen Beschlusses denkbar, welcher auf die vom Anwendungsbereich des APRA abgedeckten Unternehmen ausgeweitet werden könnte. Zum Stand des Jahres 2024 sind insgesamt vierzehn Angemessenheitsbeschlüsse in Kraft. Zudem fand am 4. März 2024 das erste Treffen verschiedener Länder zum Thema sicherer internationaler Datenflüsse statt, für die ein Angemessenheitsbeschluss vorliegt. Sie erörterten, wie man sicheren Datentransfer stärken und bei der Durchsetzung enger zusammenarbeiten könnte.[159] Bei der Prüfung eines angemessenen Schutzniveaus werden gem. Art. 45 II die innerstaatlichen Rechtsvorschriften, Datenschutzaufsichtsbehörden und die eingegangenen internationalen Verpflichtungen des betreffenden Drittlandes von der EU-Kommission betrachtet. Die Entscheidung wird dann über ein sog. „Ausschussverfahren“ getroffen. Sie beinhaltet neben dem Vorschlag der EU-Kommission eine Stellungnahme der ehemaligen Artikel-29-Datenschutzgruppe, mittlerweile ersetzt durch den Europäischen Datenschutzausschuss (EDSA). Hinzu kommt eine Stellungnahme von Vertretern der Mitgliedsstaaten und die Annahme der Entscheidung durch die Kommission, sofern EU-Parlament und Rat keine Einwände vorbringen.[160]

---

[158] EU-Kommission (Hrsg.), Welche Vorschriften gelten, wenn meine Organisation Daten nach außerhalb der EU übermittelt?.
[159] EU-Kommission (Hrsg.), Adequacy decisions – How the EU determines if a non-EU country has an adequate level of data protection..
[160] EDSB (Hrsg.), Glossar – Angemessenheitsbeschluss.

Die Vorschriften des APRA sollen nun mit der offiziellen Referenzgrundlage für Angemessenheit abgeglichen werden. Diese dient als Orientierung für die EU-Kommission und der ehemaligen Artikel-29-Datenschutzgruppe bei der Beurteilung des Datenschutzniveaus von Drittländern.[161] Die Referenzgrundlage wurde schließlich auch vom EDSA gebilligt und durch Empfehlungen zum Datenschutz bei der Strafverfolgung ergänzt.[162] Bei der Definition eines angemessenen Schutzniveaus greift die Referenzgrundlage auf die im Schrems I-Urteil verfassten Ausführungen zurück. Danach ist das Ziel nicht etwa die exakte Reproduktion des europäischen Datenschutzes, sondern es reicht aus, diesem „der Sache nach gleichwertig" zu sein.[163] Zunächst sollen dafür die Vorschriften des APRA mit den aufgelisteten obligatorischen Datenschutzgrundsätzen abgeglichen werden.

Der erste Unterpunkt betrifft Datenschutzbegriffe oder -grundsätze, die mit den im europäischen Datenschutzrecht verwurzelten, zentralen Begriffen im Einklang stehen sollen. Dazu gehören z.B. „personenbezogene Daten", „Verarbeitung personenbezogener Daten", „Verantwortlicher", „Auftragsverarbeiter", „Empfänger" und „sensible Daten".[164] Sowohl die Verarbeitung von Daten, der Begriff des Auftragsverarbeiters als auch sensible Daten sind in der APRA definiert (vgl. Sec. 101 (46), (50) und (49) APRA), wenn auch nicht wortgleich zu ihren Äquivalenten in der DSGVO. Die Abweichung der zentralen Begriffe „covered data" und „covered entity" gem. Sec. 101 (12) und (13) APRA mit den Begriffsbestimmungen von „personenbezogenen Daten" und „Verantwortlicher" aus Art. 4 Nr. 1 und 7 DSGVO wurde bereits in Kapitel 3.2.1 erläutert, da die APRA so ihren Anwendungsbereich verglichen mit der DSGVO einschränkt und kontextualisiert. Ein auf bestimmte Unternehmen eingeschränkter Anwendungsbereich steht jedoch dem Erlass eines Angemessenheitsbeschlusses nicht im Weg, da über das aktuelle EU-US DPF auch nur bestimmte zertifizierte Unternehmen abgedeckt sind. Auch der Angemessenheitsbeschluss für Kanada deckt nur diejenigen Unternehmen ab, die in den Anwendungsbereich des

---

[161] EU-Kommission (Hrsg.), Referenzgrundlage für Angemessenheit, 2.
[162] EDSB (Hrsg.), Empfehlungen 01/2021 zu der Referenzgrundlage für den Begriff „Angemessenheit" in der Richtlinie zum Datenschutz bei der Strafverfolgung.
[163] EU-Kommission (Hrsg.), Referenzgrundlage für Angemessenheit, 3; EuGH, Urteil vom 6.10.2015 – C-362/14, NJW 2015, 3155, Rdnr. 73f..
[164] EU-Kommission (Hrsg.), Referenzgrundlage für Angemessenheit, 5.

kanadischen „Personal Information Protection and Electronic Documents Act“ fallen.[165] Bedenklich könnten aber grundlegende Abweichungen wie der Ausschluss von Personaldaten gem. Sec. 101 (12) (ii) APRA sein, deren Schutz gegenwärtig vom EU-US DPF abgedeckt ist.[166]

An zweiter Stelle steht die Datenverarbeitung auf rechtmäßige, faire und legitime Weise, die ausreichend klar dargelegt werden muss. Das Vorhandensein von Rechtsgrundlagen für die Verarbeitung von Daten sowie die Anforderungen an Einwilligungen der Betroffenen wurde im Kapitel 3.2.3 erörtert und sind zu bejahen. Auch die Grundsätze der Zweckbindung, der Datenqualität und Verhältnismäßigkeit, der Speicherbegrenzung, der Integrität und Vertraulichkeit und der Transparenz wurden bereits in Kapitel 3.2.1 mit der DSGVO verglichen und haben alle ein entsprechendes Äquivalent in der APRA.[167]

Der in Kapitel 3.2.4 festgestellte Mangel eines Rechts auf Widerspruch gegen die Verarbeitung sowie auf deren Einschränkung entspricht jedoch nicht den Vorgaben der Referenzgrundlage. Die Gewährleistung eines angemessenen Schutzniveaus bei der Übermittlung von Daten ist hingegen durch die in Kapitel 2.3.1 beschriebenen Bestimmungen für Auftragsverarbeiter und Dritte gem. Sec. 111 APRA abgedeckt. Besondere Anforderungen an internationale Übermittlungen aus den USA heraus werden aber nicht gestellt.

Die zudem verlangten anspruchsvolleren Anforderungen für besondere Datenkategorien sowie die Möglichkeit des Widerspruchs gegen Direktwerbung durch Opt-Out sind jedoch im APRA verankert, wie bereits in Kapitel 2.3.1 beschrieben. Verschärfte Diskussionen um die Änderungen des APRA bezüglich der Diskriminierung durch automatisierte Entscheidungen und Profiling, wie in

---

[165] Amtlicher Titel: Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5); Entscheidung der Kommission vom 20. Dezember 2001 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet, ABl. L 002, 13-16.

[166] DURCHFÜHRUNGSBESCHLUSS (EU) 2023/1795 DER KOMMISSION vom 10.7.2023 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA, ABl. L 231/118, 118-229, III. 9..

[167] EU-Kommission (Hrsg.), Referenzgrundlage für Angemessenheit, 5 f..

Kapitel 2.4 beschrieben, könnten aber dem Erlass eines Angemessenheitsbeschlusses weiter im Weg stehen.

Im Gegensatz hierzu dürfte das in der bisherigen Version des Entwurfs durchgesetzte private Klagerecht, sowie die Befugnisse zur Durchsetzung der FTC als unabhängige Aufsichtsbehörde, in der Bewertung positiv ausfallen. Dieses wurde in Kapitel 2.3.3 näher ausgeführt.

Da die Zugangsmöglichkeiten nationaler Sicherheitsbehörden von anderen Bundesgesetzen der USA bestimmt werden, ist hier auf die gleichen Erwägungen wie im derzeitigen Beschluss zum EU-US DPF zu verweisen.[168]

Insgesamt kann der APRA den Großteil der Anforderungen an einen Angemessenheitsbeschluss abdecken. Der Ausschluss bestimmter Datenkategorien von der Begriffsbestimmung personenbezogener Daten, das Fehlen eines Rechts auf Widerspruch und Einschränkung von Verarbeitungen und der Ausschluss der Rechte gegen Diskriminierung durch Profiling und automatisierte Entscheidungen lassen aber eine abschließende Prognose nicht zu.

3.4. Perspektivenwechsel: Europäisches Datenschutzrecht aus Sicht der USA

Nach Erläuterung der europäischen Sicht auf die Angemessenheit des US-Datenschutzes liegt es nahe, auch die umgekehrte Sichtweise zu betrachten. So soll ein besseres Verständnis für die Entwicklung des APRA vermittelt und Prognosen erleichtert werden. Sowohl das europäische als auch das US-amerikanische Datenschutzrecht gehen dabei von einer immer stärker vernetzten Welt aus und evaluieren dabei die Stellung des Individuums. Die verschiedenen Ansätze werden dabei von unterschiedlichen rechtlichen Traditionen und kulturellen Perspektiven geprägt.[169]

---

[168] DURCHFÜHRUNGSBESCHLUSS (EU) 2023/1795 DER KOMMISSION vom 10.7.2023 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA, ABl. L 231/118, 118-229, 3..

[169] Bundeszentrale für politische Bildung (Hrsg.), *Lewinski*, Was Europa und die USA in Sachen Datenschutz unterscheidet.

Historisch stehen sich das auf Grundrechten basierende Datenschutz-System Europas und der vergleichsweise unternehmensfreundlichere Ansatz der Vereinigten Staaten gegenüber. Galt die USA in den sechziger Jahren noch als Vorreiter in der Debatte um die digitale Privatsphäre von Menschen, so änderte sich dies spätestens mit dem sog. Volkszählungsurteil, welches einen Meilenstein des deutschen Datenschutzes darstellt. Das BVerfG stützt den Schutz personenbezogener Daten auf Art. 2 I i.V.m. Art. 1 I GG und arbeitet im Urteil das Recht auf informationelle Selbstbestimmung heraus.[170] Auch auf europäischer Ebene basiert Datenschutz auf dem Schutz von Grundrechten. Art. 8 EU-Charta bestimmt dabei explizit den Schutz personenbezogener Daten.[171] Während also der Datenschutz in Europa stets von der Perspektive des Betroffenen ausgeht, verfolgen die USA einen freiheitsbasierten Ansatz.[172] Dabei wird der Schutz personenbezogener Daten grundsätzlich mit wirtschaftlichen Interessen abgewogen. Der vierte Zusatzartikel der US-Verfassung garantiert im Gegensatz zu Art. 8 EU-Charta keinen umfassenden Schutz personenbezogener Daten. Er schützt US-Bürger nur gegen unzumutbare Durchsuchungen und Beschlagnahmen durch die Regierung. Daher gilt es aus US-amerikanischer Sicht zu hinterfragen, ob ein umfassendes Datenschutzgesetz äquivalent zur DSGVO nicht mit Grundrechten kollidieren könnte. In Betracht dafür käme bspw. das Recht auf freie Meinungsäußerung aus dem ersten Zusatzartikel der US-Verfassung. Zudem erfolgt stets eine Abwägung mit wirtschaftlichen und bundesbehördlichen Interessen.[173]

Der US-Datenschutz wird dabei von Big-Tech-Unternehmen und Lobbyarbeit beeinflusst, wie das Beispiel Vermont aus Kapitel 2.2.2 zeigt. Zudem wird bei der Einführung von zu strikten Datenschutzgesetzen ein Wettbewerbsnachteil befürchtet. Der sektorale und einzelstaatliche Datenschutz bietet außerdem auch Vorteile. Einer Meinung nach sind „US-Datenschutzgesetze […] spezifischer, differenzierter und aktueller; sie belegen automatische Datenverarbeitung nicht mit

---

[170] Bundeszentrale für politische Bildung (Hrsg.), *Lewinski*, Was Europa und die USA in Sachen Datenschutz unterscheidet; BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83 u. a., NJW 1984, 419, 419.
[171] BfDI (Hrsg.), Die Grundlagen des Datenschutzrechts.
[172] *Whitman*, The Yale Law Yournal 2004, 1151, 1160-1164.
[173] *Bakare*, Computer Science & IT Research Journal 2024, 528, 537-539; *Pernot-Leplay*, SSRN 2020, 101, 111.

allgemeinen Verboten, sondern reagieren auf konkrete Gefährdungen mit abgewogenen Regelungen, die der Meinungs- und Informationsfreiheit sowie Technologieinnovation Raum geben."[174]

Doch auch US-Bürger sorgen sich um die durch Snowden enthüllte Bedrohung der Massenüberwachung und empfehlen teils sogar die Nutzung von EU-Technologien für besser geschützte Daten.[175] Die unternehmensfreundliche Sichtweise auf den Datenschutz durch diffuse dezentrale und sektorale Ansätze stößt auf immer mehr Gegenstimmen. Die DSGVO wird teils auch als erstrebenswerter Standard gesehen, dem sich einzelne staatliche Datenschutzgesetze wie der CCPA nähern wollen.[176] „U.S. legislation isn't even close to providing adequate protection of consumer privacy interests", wird in einem Artikel der US-Magazins Forbes kritisiert.[177] Dennoch sehen viele Amerikaner die Überwachung ihres Online-Verhaltens insgesamt locker, sofern diese in ihrem eigenen Interesse geschieht oder ein Preis ist, der für den Erhalt von Vergünstigungen gezahlt wird.[178]

Der APRA zeigt aber deutlich, dass eine Orientierung am europäischen Modell und damit einem ganzheitlichen Datenschutzgesetz mit starken Rechten für die Betroffenen immer beliebter wird. Staatliche Datenschutzrechte wie der „Connecticut Data Privacy Act", die 2022 noch als fortschrittlich und konsumentenfreundlich angesehen wurden[179], werden mittlerweile als rückschrittlich und schwach kritisiert[180]. Dies zeigt einen starken Wandel in der Sicht auf den Bedarf von umfassendem Datenschutz der USA.[181]

Aus US-amerikanischer Sicht ist der starke Einfluss der DSGVO dem First Mover Advantage geschuldet.[182] Dies wurde durch das aus Sicht der USA mangelnde Vorhandensein eines starken konkurrierenden Modells verstärkt. Dies intensiviere zudem den sog. „Brussels Effect". Damit ist das Verbreiten europäischer Werte und

---

[174] *Determann*, NVwZ 2016, 561, 567.
[175] Forbes (Hrsg.), *Beens*, The Privacy Mindset Of The EU Vs. The US.
[176] IAPP (Hrsg.), *Neil*, The Vermont veto is a step backward for privacy.
[177] Forbes (Hrsg.), *Beens*, The Privacy Mindset Of The EU Vs. The US.
[178] Pew Research Center (Hrsg.), *Duggan/Rainie*, Privacy and Information Sharing – Many Americans say they might provide personal information, depending on the deal being offered and how much risk they face.
[179] IAPP (Hrsg), *Stauss*, State data privacy legislation: Takeaways from 2022 and what to expect in 2023.
[180] IAPP (Hrsg.), *Neil*, The Vermont veto is a step backward for privacy.
[181] IAPP (Hrsg.), *Lamont/Stauss*, Retrospective: 2024 in comprehensive state data privacy law.
[182] *Pernot-Leplay*, SSRN 2020, 101, 105.

Normen gemeint, wenn sich Unternehmen im internationalen Handel an die in Europa rechtsverbindlichen Normen anpassen müssen.[183] Mit der Einführung des privaten Klagerechts nähert sich auch der APRA weiter an das europäische Datenschutzrecht an. Trotzdem enthält er aber, wie auch schon der CCPA, bewusste Abweichungen im Anwendungsbereich und geht nicht von den Grundrechten der Betroffenen aus.[184] Trotzdem ist insgesamt eine zunehmende Annäherung der US-amerikanischen und europäischen Datenschutzansätze zu beobachten.[185] Ein bundesweites amerikanisches Datenschutzrecht mit Prinzipien des US-Verbraucherrechts und Ansätzen aus der DSGVO könnte einen neuen Standard setzen und soll mit der DSGVO in ihrem internationalen Einfluss konkurrieren.[186]

4. Use Case: Anforderungen an den Datenschutz im transnationalen Online-Vertrieb in der EU und den USA mit Fokus auf grenzüberschreitende Datenflüsse

Auf Grundlage der bisher gewonnen Erkenntnisse sollen schließlich die Anforderungen der DSGVO und des APRA an die Gestaltung einer Vertriebswebsite untersucht werden. Es sollen ausschließlich Anforderungen des APRA und der DSGVO betrachtet werden. Andere einschlägige Gesetze wie das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) oder der „Gramm-Leach-Bliley Act“ bleiben außen vor. Dabei sollen bei der Betrachtung der häufig auf Websites dieser Art gesammelten personenbezogenen Daten die möglichen Rechtsgrundlagen der Verarbeitung sowie Anforderungen an die Transparenz und die Einwilligung berücksichtigt werden. Schließlich sollen daraus Schlüsse für mögliche datenschutzkonforme Gestaltungen gem. DSGVO und APRA gezogen werden.

---

[183] *Pernot-Leplay*, SSRN 2020, 101, 101-108.
[184] *Pernot-Leplay*, SSRN 2020, 101, 116-123.
[185] EU-Kommission (Hrsg.), BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT über die erste regelmäßige Überprüfung der Funktionsweise des Angemessenheitsbeschlusses zum Datenschutzrahmen EU-USA, Bericht – COM(2024)451, 10.
[186] *Pernot-Leplay*, SSRN 2020, 101, 123 f..

4.1. Beschreibung des Szenarios sowie die Arten von Daten und deren Verarbeitungen

Zur Veranschaulichung soll vom fiktiven Szenario der Vertriebswebsite eines Unternehmens ausgegangen werden. Diese soll vom Standort in Deutschland aus betrieben werden. Über die Website sollen digitale Dienste an Kunden in Europa und den USA angeboten werden.

Dabei werden für eine solche Seite typische Daten gesammelt. Dazu gehören technisch notwendige Cookies zur Sicherheit der Seite und Anpassung der Benutzeroberfläche, aber auch solche zur Analyse des Nutzerverhaltens zu Marketingzwecken und Reichweitenmessung. Darüber hinaus werden Log-Dateien wie der Zeitpunkt der Zugriffe und IP-Adressen zur Protokollierung sowie Fehlererkennung und -behebung gesammelt. Zudem werden in einem Kontaktformular Namen und Kontaktdaten abgefragt. Des Weiteren sollen eine Tracking- und Analysesoftware sowie Social Media Plugins zum Teilen der Seite verwendet werden.[187]

4.2. Anwendungsbereich und Rechtsgrundlagen

Zur Betrachtung der Rechtsgrundlagen soll die Einordnung von Cookies und IP-Adressen in die Definitionen von personenbezogenen Daten vorangestellt werden. Im Rahmen der DSGVO ist beides eindeutig zu bejahen. In seiner Rechtsprechung aus dem Jahr 2017 entschied der BGH, dass die IP-Adresse ein personenbezogenes Datum darstellt.[188] Einem anderen Urteil des EuGH kann außerdem entnommen werden, dass auch Cookies personenbezogene Daten darstellen.[189] Mangels einschlägiger Rechtsprechung, Richtlinien oder der Möglichkeit Vorgehen von Unternehmen zu beurteilen, lässt sich dies für den APRA nicht mit Gewissheit beantworten, da die Begriffe nicht ausdrücklich in Sec. 101 (12) APRA als personenbezogene Daten definiert sind. Im zweiten Titel des APRA sind beide allerdings explizit als „personal information“ gem. Sec. 202 (a) (2) (A) APRA im

---

[187] IHK Regensburg für Oberpfalz / Kelheim (Hrsg.), Anforderungen an Websites nach der DSGVO.
[188] BGH, Urteil vom 16.5.2017 – VI ZR 135/13, ZD 2017, 424, 424.
[189] EuGH, Urteil vom 1.10.2019 – C-673/17, MMR 2019, 732-740; *Klabunde/Horváth*, in: Ehmann/Selmayr, DSGVO, Art. 4, Rdnr. 15.

Anwendungsbereich des COPPA ergänzt. Dies könnte dafür sprechen, dass Cookies und IP-Adressen in den Anwendungsbereich beider Gesetze fallen.

Dem Prinzip der Datenminimierung und Zweckbindung beider Gesetze (vgl. Kapitel 3.2.2) ist zudem zu entnehmen, dass bspw. im Kontaktformular nur notwendige Daten abgefragt werden sollten.[190]

Für die Rechtmäßigkeit der Verarbeitung ist zudem auf das Verbotsprinzip beider Gesetze (vgl. Kapitel 3.2.3) abzustellen. Es muss also zumindest eine Bedingung gem. Art. 6 I DSGVO erfüllt sein und mindestens eine ausdrückliche Einwilligung oder ein genehmigter Zweck gem. Sec. 102 APRA vorliegen. Bei der Verarbeitung durch nichtöffentliche Verantwortliche bei der Erbringung von Telemediendiensten, wie es in diesem Szenario der Fall ist, sind im Rahmen der DSGVO grundsätzlich die Einwilligung gem. Art. 6 I lit. a DSGVO, die vertragliche Verpflichtung nach Art. 6 I lit. b DSGVO oder überwiegende berechtigte Interessen gem. Art. 6 I lit. f DSGVO einschlägig.[191] Ein Vergleich dieser Rechtsgrundlagen mit denen des APRA kann Kapitel 3.2.3 entnommen werden. Zu den vertraglichen Verpflichtungen nach Art. 6 Abs. 1 lit. b DSGVO ist hinzuzufügen, dass die Verarbeitung im Rahmen eines gültigen Vertrags mit der betroffenen Person erfolgen muss. Die Verarbeitung muss zudem zur Erfüllung des Vertrags erforderlich sein.[192] Sec. 102 (d) (3) APRA ist vager und verlangt lediglich erkennbare Ansprüche des Unternehmens oder Auftragsverarbeiters. Für die Rechtsgrundlage des berechtigten Interesses gem. Art. 6 I lit. f DSGVO muss für einen Vergleich mit den erlaubten Zwecken gem. Sec. 102 (d) APRA eine abgleichende Prüfung durchgeführt werden. Zuerst müsste ein berechtigtes Interesse des Verantwortlichen oder des Dritten vorliegen. Außerdem müsste die Verarbeitung der personenbezogenen Daten zur Wahrung des Interesses auch erforderlich sein. Zuletzt muss dieses mit den Interessen und Rechten der betroffenen Person im Einzelfall abgeglichen werden.

---

[190] IHK Regensburg für Oberpfalz / Kelheim (Hrsg.), Anforderungen an Websites nach der DSGVO.
[191] DSK (Hrsg.), Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021, 27-31.
[192] EDSA (Hrsg.), Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, 9, Rdnr. 23-25.

Aus dem Verbotsprinzip beider Gesetze, welches in Kapitel 3.2.3 erläutert wird, ergibt sich zudem, dass eine Einwilligung, sofern sie die alleinige Rechtsgrundlage darstellt, bereits vor der Verarbeitung vorliegen muss. Technisch dürfen z.B. Tracking-Verfahren also auch erst dann zum Einsatz kommen.[193]

4.3. Datenschutzerklärung

Die wohl wichtigste Transparenzanforderung im Kontext einer Website ist die Datenschutzerklärung. Um die Bestimmungen der DSGVO diesbezüglich mit denen der APRA abgleichen zu können, sollen, konform mit der Vergleichsmethodik aus Kapitel 3.2, die Vorschriften der DSGVO aufgezeigt und sodann Äquivalente im APRA gegenübergestellt werden.

Gem. Art. 12 I 1 i.V.m. Art. 13 DSGVO muss die Datenschutzerklärung in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache gehalten sein. Art. 12 I 2 DSGVO schließt dabei die Informationsbereitstellung in elektronischer Form mit ein. Sec. 104 (a) APRA schreibt im Wesentlichen das Gleiche vor. Die Datenschutzerklärung muss demnach in klarer und auffälliger, nicht irreführender und leicht zu lesender Weise veröffentlicht werden. Sec. 104 (c) APRA präzisiert die sprachlichen Anforderungen zudem ausdrücklich. Demnach muss die Datenschutzerklärung in den Sprachen veröffentlicht werden, in denen auch das Produkt oder die Dienstleistung angeboten wird. Sec. 104 (d) APRA schreibt darüber hinaus die Bereitstellung in für Menschen mit Behinderung angemessener Art und Weise vor. Art. 12 V 1 DSGVO schreibt außerdem Unentgeltlichkeit vor, was im APRA in diesem Kontext keine Erwähnung findet.

Inhaltlich müssen gem. Art. 13 I lit. a DSGVO der Name und die Kontaktdaten des Verantwortlichen und seines Vertreters genannt werden. Sec. 104 (b) (1) (A) APRA fügt diesen Anforderungen in Art. 104 (b) (1) (A) außerdem die Nennung bestimmter verbundener Unternehmen innerhalb der Unternehmensstruktur des Verantwortlichen hinzu, an welche das Unternehmen oder der Auftragsverarbeiter

---

[193] DSK (Hrsg.), Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021, 30.

Daten übertragen kann. Weiter müssen gem. Art. 13 I lit. b DSGVO die Kontaktdaten des Datenschutzbeauftragen genannt werden. Der APRA nennt diese Anforderung nicht. Die obligatorische Aufführung der Zwecke und Rechtsgrundlagen der Verarbeitung in der Datenschutzerklärung findet sowohl in Art. 13 I lit. c DSGVO als auch in Sec. 104 (b) (2) APRA Erwähnung. Sollte Art. 6 I f DSGVO die Rechtsgrundlage einer Verarbeitung darstellen, müssen zudem die Interessen der Verantwortlichen genannt werden. Hier könnten die in Sec. 102 (d) APRA erlaubten Zwecke enthalten sein. Den zu nennenden Empfängern oder Empfängerkategorien gem. Art. 13 I lit. e DSGVO fügt der APRA in Sec. 104 (3) APRA außerdem hinzu, dass zusätzlich jeder Data Broker zu benennen ist. Für die Nennung der Umstände, unter denen gem. Art. 13 I lit. f DSGVO der Drittlandtransfer unternommen wird, gibt es im APRA keine Entsprechung. In Art. 13 II lit. a DSGVO ist die Dauer oder Kriterien für Festlegung der Dauer der Speicherung der erhobenen Daten vorgesehen. Sec. 104 (b) (4) APRA entspricht dem fast wörtlich. Des Weiteren sind Verweise auf die Rechte der Betroffenen in Art. 13 II lit. a und b DSGVO vorgegeben. Diese stimmen, wie in Kapitel 3.2.4 beschrieben, nicht mit den Betroffenenrechten aus dem APRA überein. Die im APRA gewährten Betroffenenrechte müssen gem. Sec. 104 (b) (5) APRA zudem nicht nur genannt werden, sondern es muss in der Datenschutzerklärung auch eine deutliche Beschreibung darüber enthalten sein, wie eine Person diese Rechte ausüben kann. Sollten personenbezogene Daten vertraglich oder gesetzlich bereitgestellt werden müssen, muss gem. Art. 13 II lit. e DSGVO über die Konsequenzen informiert werden, die bei Nichtbereitstellung folgen können. Gem. Art. 13 II lit. f DSGVO müssen zudem Informationen zu etwaigem Profiling in der Datenschutzerklärung aufgenommen werden. Beides hat kein Äquivalent in Sec. 104 APRA.[194]

Gemäß Sec. 104 (b) (6) APRA muss in der Datenschutzerklärung darlegt werden, inwiefern das Unternehmen personenbezogene Daten von Minderjährigen anders behandelt als die von anderen Personen. Vorausgesetzt ist dabei das Wissen oder Wissenmüssen, dass solche Daten gesammelt werden. Sec. 104 (e) APRA enthält eine weitere Anforderung, die in den Bestimmungen zur Datenschutzerklärung gemäß den Vorgaben der DSGVO nicht ausdrücklich festgelegt ist. Bei

[194] *Daum*, MMR 2020, 643, 645-647.

grundlegenden Änderungen der Datenschutzerklärung sieht Sec. 101 (38) APRA vor, dass die Betroffenen informiert werden und die Möglichkeit erhalten, Verarbeitungen aufgrund dieser Änderungen per Opt-Out abzulehnen.

Bei der Einholung von Einwilligungen durch sog. „Consent Banner“ können diese wie bereits erwähnt nur dann wirksam sein, wenn sie vor der Verarbeitung eingeholt wurden. Der Betroffene muss klar informiert werden und seine Einwilligung muss auf Basis einer freien Entscheidung durch aktives Handeln erfolgen.[195] Dabei inkludieren die Vorschriften der DSGVO auch das Verbot der unzulässigen Einflussnahme auf diese Entscheidung, sog. „Nudging“.[196] Diese Anforderung an die Gestaltung werden auch durch das Verbot von „Dark Patterns“ gem. Sec. 107 (a) APRA gestellt. Zudem fordern sowohl Art. 25 II DSGVO als auch die Regeln zum „Privacy by Design“ gem. Sec. 103 APRA datenschutzfreundliche Voreinstellungen. Bewusst verwirrende Gestaltungen zur Abgabe oder zum Widerruf einer Einwilligung sind daher unzulässig. Häufig genutzte Beispiele hierfür sind das In-den-Fokus-Rücken des Buttons, um Cookies zu akzeptieren oder einen Newsletter zu abonnieren.[197]

5. Fazit

Abschließend ist festzuhalten, dass der APRA zwar eine Chance zur Vereinheitlichung des amerikanischen Datenschutzes und damit zur Verringerung der herrschenden Rechtsunsicherheit darstellen könnte, aber seine Zukunft ungewiss bleibt. In diesem Kapitel sollen die wichtigsten Erkenntnisse der Arbeit zusammenfassend rekapituliert und auf diese Weise die Forschungsfrage beantwortet werden. Dabei soll zuerst auf die Einordnung des APRA, dann auf den Vergleich mit der DSGVO und die mögliche Bedeutung für den Datentransfer von der EU in die USA eingegangen werden. Zuletzt werden die Erkenntnisse zu den

---

[195] DSK (Hrsg.), Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021, 30.
[196] Der Landesbeauftragte für den Datenschutz Niedersachsen (Hrsg.)
Handreichung: Datenschutzkonforme Einwilligungen auf Webseiten – Anforderungen an Consent-Layer (September 2022), 5-7.
[197] Verbraucherzentrale (Hrsg.), Dark Patterns: So wollen Websites und Apps Sie manipulieren.

Anforderungen an die Gestaltung einer Website zusammengefasst. Abschließend soll zudem ein kurzer Ausblick in die Zukunft gegeben werden.

5.1. Wichtigste Erkenntnisse der Arbeit

Im Hinblick auf die aktuelle Gesetzeslage zum Datenschutz in den USA setzt der APRA insgesamt auf einem hohen Datenschutzniveau an. Dieses soll umfassende Aspekte des Datenschutzes regulieren. Bundesweite Regelungen von Teilaspekten würden aber gem. Sec. 118 (b) (1) (C) APRA gleichwertig neben dem APRA bestehen bleiben. Die FTC wäre dabei als Hauptaufsichtsbehörde vorgesehen. Dabei würde die Durchsetzung weiterhin im Rahmen ihrer Befugnisse durch den FTC-Act umgesetzt. Zudem soll die FTC Richtlinien und Templates bzgl. der Regelungen im APRA erlassen. Das Gewohnheitsrecht, das sich aus den bisherigen Maßnahmen der FTC ableiten lässt, findet sich teils auch im APRA kodiert wieder. Dazu gehört bspw. das Verbot von „Dark Patterns“ oder die Einwilligung des gesetzlichen Vormunds für die Verarbeitung der personenbezogenen Daten von Kindern. Dabei kann die FTC Fälle von Verletzungen des APRA vor Gericht bringen, soll aber weiterhin keine zusätzlichen Befugnisse, wie das Verhängen von Bußgeldern, erhalten. Die Durchsetzung vor Gericht kann zudem durch staatliche Vertreter, aber auch über das private Klagerecht angestrengt werden. Im APRA finden sich zudem Konzepte und Trends verschiedener staatlicher Datenschutzgesetze wieder. Dies reicht von einem zentralen Löschmechanismus für „Data Broker“, ähnlich zum kalifornischen „Delete-Act“, bis hin zum speziellen Schutz der Daten von Kindern. Im Vergleich zu vor einigen Jahren lässt sich im US-Datenschutz insgesamt ein klarer Wandel zu verbraucherfreundlicheren Datenschutzgesetzen beobachten.

Im Vergleich mit der DSGVO stellen sich jedoch einige zentrale Unterschiede heraus. Dies beginnt bereits beim Anwendungsbereich. Anders als bei der DSGVO sind kleine Unternehmen grundsätzlich vom Geltungsbereich des APRA ausgeschlossen, genauso wie bestimmte Datenkategorien wie bspw. Personaldaten. Personenbezogene Daten können sich, anders als in der DSGVO-Definition, dabei auch auf Gruppen von Personen mit Wohnsitz in den USA beziehen. Die Grundsätze der Verarbeitung überschneiden sich aber weitgehend. In beiden

Gesetzen findet sich das Verbotsprinzip mit Erlaubnisvorbehalt wieder. Sec. 102 des APRA definiert allerdings deutlich mehr erlaubte Zwecke der Verarbeitung als die in Art. 6 I DSGVO gelisteten Rechtsgrundlagen. Zudem erlaubt der APRA in bestimmten Fällen die Nutzung von Opt-Out-Mechanismen. Insgesamt fehlen im APRA auch einige der in der DSGVO vorgesehenen Betroffenenrechte und auch besondere Regeln für den Auslandstransfer sind nicht vorgesehen. Allerdings sind die Konzepte des „Large Data Holder“ und „Data Broker“ mit zusätzlichen Anforderungen vorgesehen. Insgesamt lässt sich eine Annäherung an den risikobasierten Ansatz der DSGVO feststellen.

In Bezug auf den Transfer personenbezogener Daten aus der EU in die USA ist eine Ausweitung des aktuellen Angemessenheitsbeschlusses auf die vom APRA erfassten Unternehmen bei dessen Umsetzung denkbar. Trotz der Erfüllung vieler Anforderungen für einen solchen Beschluss könnten aber verschiedene Faktoren der Entscheidung im Weg stehen. Dazu gehört der Ausschluss bestimmter Datenkategorien aus dem Anwendungsbereich des Gesetzesentwurfs, der Mangel an bestimmten Betroffenenrechten und der fehlende Schutz vor Diskriminierung durch automatisierte Entscheidungen. Zur Bewertung des Zugangs zu personenbezogenen Daten durch US-Bundesbehörden, die in der Vergangenheit im Hinblick auf das Schutzniveau problematisch waren, enthält der APRA zudem keine umfassende Regelung. Hier wäre deshalb auf die bisherige Bewertung anderer diesbezüglicher US-Gesetze abzustellen.

Zu den Erkenntnissen zur Gestaltung einer Vertriebswebsite ist anzumerken, dass, wie auch in der Arbeit insgesamt, nur eine Analyse des Textes des APRA möglich ist, es aber offensichtlich an einschlägiger Rechtsprechung und Richtlinien fehlt. Trotzdem gilt es bei einer solchen Website sowohl nach der DSGVO als auch nach dem APRA bei der Verarbeitung personenbezogener Daten das Prinzip der Datenminimierung zu beachten. Zu den möglichen Rechtsgrundlagen ist zudem festzuhalten, dass berechtigte Interessen nach der DSGVO im Einzelfall geprüft und mit den siebzehn erlaubten Zwecken nach dem APRA abgeglichen werden müssen. Gem. beider Gesetze sollte zudem bei der Einholung von Einwilligungen der Betroffenen von manipulativen Gestaltungen abgesehen werden. In der Datenschutzerklärung müssten zusätzlich zu den Anforderungen aus der DSGVO einige Anforderungen des APRA beachtet werden. Dazu gehört die mehrsprachige

und behindertengerechte Veröffentlichung, aber auch das Hinzufügen von verbundenen Unternehmen zu den Angaben der Verantwortlichen. In den Empfängerkategorien ist zudem jeder „Data Broker“ zu nennen. Auch müssten die Unterschiede bei den Betroffenenrechten beachtet werden und die im APRA vorgesehene Beschreibung hinzugefügt werden, wie diese ausgeübt werden können. Insgesamt lassen sich die Anforderungen beider Gesetze in einer Datenschutzerklärung verbinden, denkbar ist aber auch eine separate Datenschutzerklärung für Einwohner der USA anzufügen.

5.2. Zukunftsausblick

Im Rahmen einer Prognose ist allerdings festzuhalten, dass eine erfolgreiche Umsetzung des APRA im Rahmen des US-amerikanischen Gesetzgebungsprozesses alles andere als gesichert ist. Viele Diskussionen und Streitpunkte bleiben aktuell noch offen und eine Zufriedenstellung aller Interessenvertreter scheint schwer umsetzbar. Die Interessen der Verbraucher werden mit wirtschaftlich liberaleren Positionen verglichen, wobei sowohl Republikaner und Demokraten als auch staatliche und sektorale Interessenvertreter miteinander in Konflikt stehen.

Auch der aktuelle Angemessenheitsbeschluss zum EU-US DPF wird stark kritisiert. Die Organisation „Noyb“ bezeichnet das Framework als Kopie des fehlgeschlagenen Privacy Shields und wirft den USA weiterhin vor, die Grundrechte von Europäern in Bezug auf Privatsphäre nicht ernst zu nehmen. Trotz neuer Regelungen im US-Recht gäbe es in Bezug auf die Massenüberwachung von Nicht-US-Bürgern noch immer keine echte Verhältnismäßigkeit und auch keine Möglichkeit für diese, in den USA Beschwerde einzureichen. Es gäbe daher keine substantiellen Änderungen zu den in den Schrems I und II-Urteilen angeprangerten Zugriffs- und Überwachungsmöglichkeiten der US-Regierung. Die Organisation kündigte deshalb bereits rechtliche Schritte an, weshalb wohl ein Schrems III-Urteil nicht ganz auszuschließen ist.[198] Ein aktuelles Urteil des Gerichts der Europäischen Union (EuG) vom 3. September 2025 bestätigt allerdings vorläufig die Gültigkeit

[198] Noyb (Hrsg.), Europäische Kommission gibt EU-US-Datentransfers 3. Runde beim EuGH.

des EU-US DPF.[199] Geklagt hatte der französische Abgeordnete Philippe Latombe. Er zweifelte dabei u.a. die Unabhängigkeit des US Data Protection Review Courts an und kritisierte den unzureichenden Schutz Betroffener bei der Massendatenerfassung durch US-Geheimdienste. Das Gericht wies dies auf Basis der Sach- und Rechtslage zurück, aufgrund derer die EU-Kommission die Angemessenheitsentscheidung im Jahr 2023 erlassen hatte. Weiter betonte das Gericht in seinem Urteil, dass die Kommission weiterhin verpflichtet bliebe die Situation zu überwachen und bei Bedarf einzugreifen. Das Urteil ist noch anfechtbar.[200] Obwohl das Urteil sich nur auf den ursprünglichen Zeitpunkt der Kommissionsentscheidung zum EU-US DPF bezieht, gibt es auch in der aktuellen politischen Lage in den USA Entwicklungen, die die Unabhängigkeit der zuständigen Aufsichtsbehörden in Frage stellen. Seit dem Regierungswechsel am 20. Januar 2025 hatte der amtierende Präsident Trump viel Kritik geerntet, u.a. für die Entlassung des Vorsitzenden und zwei weiterer Mitglieder des Privacy and Civil Liberties Oversight Boards (PCLOB) nur neun Tage nach Regierungswechsel und dieses damit handlungsunfähig gemacht. Das Organ ist für die Überwachung der Grundrechte bei Aktivitäten des US-Geheimdienstes zuständig und bildet damit auch eine wichtige Grundlage für die Anforderungen des EU-US DPF.[201] Dies entlassenen Mitglieder klagten bereits mit der Begründung, dass der Präsident nicht die gesetzliche Befugnis habe, Mitglieder des PCLOB nach Belieben zu entlassen.[202] Die Organisation „Noyb“ sieht die fehlende Unabhängigkeit der US-Datenschutzkontrollmechanismen damit erst recht bestätigt.[203]

Der Datenschutz in den USA bleibt also weiter im Wandel. Der Druck und die Notwendigkeit ein nationales umfassendes Datenschutzgesetz zu etablieren steigt. Der Entwurf des APRA gewährt folglich einen Blick in die zukünftige Entwicklung des US-Datenschutzes und könnte auch für europäische Unternehmen die Chance

---

[199] EuG, Urteil vom 3.9.2025 – T-553/23, BeckRS 2025, 22446 (aktuell nur original französische Fassung vorhanden).
[200] IAPP (Hrsg.), *Duball*, European General Court dismisses Latombe challenge, upholds EU-US Data Privacy Framework.
[201] Bloomberg Law (Hrsg.), *Riley*, Trump Fires Democrats from Privacy Oversight Board (Correct); EU-Parlament (Hrsg.), Aussetzung der Untersuchungen der US-amerikanischen Stelle zur Überwachung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten und deren Auswirkungen auf die Datenübermittlung zwischen der EU und den USA.
[202] Brennan Center for Justice (Hrsg.), LeBlanc v. U.S. Privacy and Civil Liberties Oversight Board.
[203] Noyb (Hrsg.), US-Cloud bald illegal? Trump schlägt erstes Loch in EU-US-Datenabkommen.

auf mehr Rechtssicherheit und Stabilität für den Transfer personenbezogener Daten in die USA darstellen.

Literaturverzeichnis

Amnesty International (Hrsg.)

Der Fall Edward Snowden, online abrufbar unter: https://www.amnesty.de/2013/9/9/der-fall-snowden, zuletzt besucht am 11.1.2025.

Amtsblatt der Europäischen Union C 202 vom 7.6.2016

Konsolidierte Fassungen des Vertrags über die Europäische Union und des Vertrags über die Arbeitsweise der Europäischen Union, 1-361.

Amtsblatt der Europäischen Union L 002 vom 4.1.2002

Entscheidung der Kommission vom 20. Dezember 2001 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet, 13–16.

Amtsblatt der Europäischen Union L 119/1 vom 4.5.2016

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), 1-88.

Amtsblatt der Europäischen Union L 207/1 vom 1.8.2016

Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes, 1-112.

Amtsblatt der Europäischen Union L 215 vom 25.8.2000

Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, 7-47.

Amtsblatt der Europäischen Union L 231/118 vom 20.9.2023

DURCHFÜHRUNGSBESCHLUSS (EU) 2023/1795 DER KOMMISSION vom 10.7.2023 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA, 118-229.

Amtsblatt der Europäischen Union L 281 vom 23.11.1995

Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, 31-50.

Amtsblatt der Europäischen Union L 39/5 vom 12.2.2010

Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, 5-18.

Bakare, Seun Solomin u.a.

DATA PRIVACY LAWS AND COMPLIANCE: A COMPARATIVE REVIEW OF THE EU GDPR AND USA REGULATIONS, Computer Science & IT Research Journal Volume 5 Nr. 3 2024, 528-543,

zitiert als: *Bakare*, Computer Science & IT Research Journal 2024.

Beck’sche Kompakt-Kommentare Datenschutzgrundverordnung Bundesdatenschutzgesetz

Paal, Boris P./Pauly, Daniel A. (Hrsg.), 3. Auflage 2021,

zitiert als: *Bearbeiter*, in: Paal/Pauly DS-GVO BDSG.

Beck’scher Online-Kommentar Datenschutzrecht

Brink, Stefan/Ungern-Sternberg, Antje/Wolff, Heinrich Amadeus (Hrsg.), 50. Edition, Stand: 01.05.2023 und 01.11.2021, München,
zitiert als: *Bearbeiter*, in: BeckOK Datenschutzrecht.

BfDI (Hrsg.)

Datenschutz-Grundverordnung – Bundesdatenschutzgesetz - Texte und Erläuterungen, online abrufbar unter:
https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/INFO1.pdf?__blob=publicationFile,
zuletzt besucht am 11.1.2025.

Die Grundlagen des Datenschutzrechts, online abrufbar unter: https://www.bfdi.bund.de/DE/Buerger/Inhalte/Allgemein/Datenschutz/GrundlagenDatenschutzrecht.html,
zuletzt besucht am 11.1.2025.

Privacy Shield: Die Datenschutzbehörden fordern Nachverhandlungen, online abrufbar unter:
https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2017/23_Privacy%20Shield.html;
zuletzt besucht am 11.1.2025.

Bloomberg Law (Hrsg.)

Riley, Tonya

Trump Fires Democrats from Privacy Oversight Board (Correct), abrufbar unter: https://news.bloomberglaw.com/privacy-and-data-security/trump-terminates-trio-of-democrats-from-privacy-oversight-board,
zuletzt besucht am 25.09.2025.

Brennen Center for Justice (Hrsg.)

LeBlanc v. U.S. Privacy and Civil Liberties Oversight Board, online abrufbar unter: https://www.brennancenter.org/our-work/research-reports/leblanc-v-us-privacy-and-civil-liberties-oversight-board,
zuletzt besucht am 25.09.2025.

Bundeszentrale für politische Bildung (Hrsg.)

Lewinksi, Kai

Was Europa und die USA in Sachen Datenschutz unterscheidet, online abrufbar unter: https://www.bpb.de/themen/daten/democracy/254254/was-europa-und-die-usa-in-sachen-datenschutz-unterscheidet/,
zuletzt besucht am 11.1.2025

Committee on Energy and Commerce (Hrsg.)

Chair Rodgers Statement on the American Privacy Rights Act, online abrufbar unter: https://energycommerce.house.gov/posts/chair-rodgers-statement-on-the-american-privacy-rights-act,
zuletzt besucht am 11.1.2025.

Congressional Research Service (Hrsg.)

The American Privacy Rights Act, online abrufbar unter: https://crsreports.congress.gov/product/pdf/LSB/LSB11161,
zuletzt besucht am 11.1.2025.

Datenschutzstelle Fürstentum Liechtenstein (Hrsg.)

Informationspflicht (Art. 13 und 14 DSGVO), online abrufbar unter: https://www.datenschutzstelle.li/datenschutz/themen-z/informationspflicht-art-13-und-14-dsgvo,
zuletzt besucht am 11.1.2025.

Daum, Oliver

Pflichtangaben auf Webseiten -Das Problem mit Impressums- und Datenschutz-Generatoren, MMR 2020, 643-647,
zitiert als: *Daum*, MMR 2020.

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit (Hrsg.)

Überblick – Angemessenheitsbeschlüsse der Europäischen Kommission, online abrufbar unter: https://datenschutz.hessen.de/datenschutz/internationaler-datentransfer/angemessenheitsbeschluesse-der-europaeischen-kommission, zuletzt besucht am 11.1.2025.

Der Landesbeauftragte für den Datenschutz Niedersachsen (Hrsg.)

Handreichung: Datenschutzkonforme Einwilligungen auf Webseiten – Anforderungen an Consent-Layer (September 2022), online abrufbar unter: https://www.lfd.niedersachsen.de/startseite/themen/internet/handreichung-datenschutzkonforme-einwilligungen-auf-webseiten-anforderungen-an-consent-layer-194906.html, zuletzt besucht am 1.11.2025.

Determann, Lothar

Datenschutz in den USA – Dichtung und Wahrheit, NVwZ 2016, 561-567, zitiert als: *Determann*, NVwZ 2016.

DSK (Hrsg.)

Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EUUS Data Privacy Framework) vom 10. Juli 2023, online abrufbar unter: https://datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf, zuletzt besucht am 11.1.2025.

Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021, online abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf, zuletzt besucht am 11.1.2025.

EDSA (Hrsg.)

Empfehlungen 01/2021 zu der Referenzgrundlage für den Begriff „Angemessenheit“ in der Richtlinie zum Datenschutz bei der Strafverfolgung, online abrufbar unter: https://www.edpb.europa.eu/system/files/2021-06/recommendations012021onart.36led.pdf_de.pdf, zuletzt besucht am 11.1.2025.

Erklärung zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 – Data Protection Commissioner gegen Facebook Ireland und Maximilian Schrems, online abrufbar unter: https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/statement-court-justice-european-union-judgment-case-c_de, zuletzt besucht am 11.1.2025.

EU – U.S. Privacy Shield – Second Annual Joint Review, online abrufbar unter: https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-privacy-shield-second-annual-joint-review-report_de, zuletzt besucht am 11.1.2025**.**

EU – U.S. Privacy Shield – Third annual Joint Review, online abrufbar unter: https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-privacy-shield-third-annual-joint-review-report_de, zuletzt besucht am 11.1.2025.

Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, online abrufbar unter: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_de_0.pdf, zuletzt besucht am 11.1.2025.

Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, online abrufbar unter: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf, zuletzt besucht am 11.1.2025.

EDSB (Hrgb.)

Glossar – Angemessenheitsbeschluss, online abrufbar unter: https://www.edps.europa.eu/data-protection/data-protection/glossary/a_de, zuletzt besucht am 11.1.2025.

Ehmann, Eugen/Selmayr, Martin

Kommentar Datenschutz-Grundverordnung, 3. Auflage, München 2024, zitiert als: *Bearbeiter*, in: Ehmann/Selmayr, DSGVO.

EU-Kommission (Hrsg.)

Adequacy decisions – How the EU determines if a non-EU country has an adequate level of data protection., online abrufbar unter: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?etrans=de&prefLang=de, zuletzt besucht am 11.1.2025.

BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT über die erste regelmäßige Überprüfung der Funktionsweise des Angemessenheitsbeschlusses zum Datenschutzrahmen EU-USA, Bericht - COM(2024)451, online abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52024DC0451&qid=1737306859047, zuletzt besucht am 11.1.2025.

Erste jährliche Überprüfung der Funktionsweise des EU-US-Datenschutzschilds, online abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/en/ip_17_3966, zuletzt besucht am 11.1.2025.

Gelten die Vorschriften für KMU?, online abrufbar unter: https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/application-regulation/do-rules-apply-smes_de, zuletzt besucht am 11.1.2025.

Kommission und Vereinigte Staaten einigen sich auf neuen Rahmen für die transatlantische Datenübermittlung: den EU-US-Datenschutzschild, online abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/de/ip_16_216, zuletzt besucht am 11.1.2025.

Referenzgrundlage für Angemessenheit, online abrufbar unter: https://ec.europa.eu/newsroom/article29/items/614108, zuletzt besucht am 11.1.2025.

Welche Vorschriften gelten, wenn meine Organisation Daten nach außerhalb der EU übermittelt?, online abrufbar unter: https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_de, zuletzt besucht am 11.1.2025.

EU-Parlament

Aussetzung der Untersuchungen der US-amerikanischen Stelle zur Überwachung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten und deren Auswirkungen auf die Datenübermittlung zwischen der EU und den USA,

online abrufbar unter: https://www.europarl.europa.eu/doceo/document/P-10-2025-000941_DE.html,
zuletzt besucht am 25.09.2025.

Federal Trade Commission (Hrsg.)

Bureaus & Offices, online abrufbar unter:
https://www.ftc.gov/about-ftc/bureaus-offices,
zuletzt besucht am 11.1.2025.

Federal Trade Commission Gives Final Approval to Settlement with Uber, online abrufbar unter: https://www.ftc.gov/news-events/news/press-releases/2018/10/federal-trade-commission-gives-final-approval-settlement-uber,
zuletzt besucht am 11.1.2025.

FTC Sends Refund Payments to Consumers Impacted by Epic Games' Unlawful Billing Practices, online abrufbar unter:
https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-sends-refund-payments-consumers-impacted-epic-games-unlawful-billing-practices,
zuletzt besucht am 11.1.2025.

Statement of Commissioner Rebecca Kelly Slaughter In the Matter of Uber Technologies, Inc., online abrufbar unter: https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-commissioner-rebecca-kelly-slaughter-matter-uber-technologies-inc,
zuletzt besucht am 11.1.2025.

What the FTC Does, online abrufbar unter:
https://www.ftc.gov/news-events/media-resources/what-ftc-does,
zuletzt besucht am 11.1.2025.

Forbes (Hrsg.)

Beens, Robert E.G.

The Privacy Mindset Of The EU Vs. The US, online abrufbar unter: https://www.forbes.com/councils/forbestechcouncil/2020/07/29/the-privacy-mindset-of-the-eu-vs-the-us/,
zuletzt besucht am 11.1.2025.

Gola, Peter/Heckmann, Dirk

Kommentar Datenschutzgrundverordnung Bundesdatenschutzgesetz, 3. Auflage, München 2022,
zitiert als: *Bearbeiter*, in: Gola/Heckmann, DS-GVO BDSG.

Hoeren, Thomas/Pinelli, Stefan

Das neue kalifornische Datenschutzrecht am Maßstab der DS-GVO - Auswirkungen des CCPA auf global agierende europäische Unternehmen, MMR 2018, 711-716,
zitiert als: *Hoeren/Pinelli*, MMR 2018.

House Committee on Energy and Commerce (Hrsg.)

Committee Chairs Rodgers, Cantwell Unveil Historic Draft Comprehensive Data Privacy Legislation, online abrufbar unter: https://energycommerce.house.gov/posts/committee-chairs-rodgers-cantwell-unveil-historic-draft-comprehensive-data-privacy-legislation,
zuletzt besucht am 11.1.2025.

IAPP (Hrsg.)

AMERICAN PRIVACY RIGHTS ACT cheat sheet, online abrufbar unter: https://iapp.org/media/pdf/resource_center/american_privacy_rights_act_cheat_sheet.pdf,
zuletzt besucht am 11.1.2025.

Duball, Joe

American Privacy Rights Act markup canceled, next US House steps uncertain, online abrufbar unter: https://iapp.org/news/a/american-privacy-rights-act-markup-canceled-next-us-house-steps-uncertain,
zuletzt besucht am 11.1.2025.

European General Court dismisses Latombe challenge, upholds EU-US Data Privacy Framework, online abrufbar unter: https://iapp.org/news/a/european-general-court-dismisses-latombe-challenge-upholds-eu-us-data-privacy-framework/,
zuletzt besucht am 25.09.2025.

Pelosi opposes proposed American Data Privacy and Protection Act, seeks new preemption compromise, online abrufbar unter: https://iapp.org/news/a/pelosi-rejects-proposed-american-data-privacy-and-protection-act-seeks-new-compromise/,
zuletzt besucht am 11.1.2025.

Proposed American Privacy Rights Act clears US House subcommittee, online abrufbar unter: https://iapp.org/news/a/proposed-american-privacy-rights-act-clears-us-house-subcommittee,
zuletzt besucht am 11.1.2025.

Stakeholders consider impacts of latest APRA draft text, online abrufbar unter: https://iapp.org/news/a/stakeholders-consider-impacts-of-latest-apra-draft-text,
zuletzt besucht am 11.1.2025.

State privacy prospects bring new paradigm in 2023, online abrufbar unter: https://iapp.org/news/a/2023-state-privacy-prospects-bring-new-paradigm,
zuletzt besucht am 11.1.2025.

Fazlioglu, Müge
US Federal Privacy Legislation Tracker Introduced in the 118th Congress (2023-2024), online abrufbar unter: https://iapp.org/media/pdf/resource_center/us_federal_privacy_legislation_tracker.pdf,
zuletzt besucht am 11.1.2025.

US State Comprehensive Privacy Laws Report - Overview, online abrufbar unter: https://iapp.org/resources/article/us-state-privacy-laws-overview/,
zuletzt besucht am 11.1.2025.

Fischer, Luke/Folks, Andrew
The American Privacy Rights Act's definition of covered data, online abrufbar unter: https://iapp.org/news/a/the-american-privacy-rights-acts-definition-of-covered-data,
zuletzt besucht am 11.1.2025.

Folks, Andrew
Defining 'comprehensive': Florida, Washington and the scope of state tracking, online abrufbar unter: https://iapp.org/news/a/defining-comprehensive-florida-washington-and-the-scope-of-state-tracking,
zuletzt besucht am 11.1.2025.

Folks, Andrew/Olivero, Amy
FTC enforcement trends: From straightforward actions to technical allegations, online abrufbar unter: https://iapp.org/resources/article/ftc-enforcement-trends/,
zuletzt besucht am 11.1.2025.

Kibby, C
US State Privacy Legislation Tracker, online abrufbar unter: https://iapp.org/resources/article/us-state-privacy-legislation-tracker/,
zuletzt besucht am 11.1.2025.

Lamont, Keir/Stauss David
Retrospective: 2024 in comprehensive state data privacy law, online abrufbar unter:
https://iapp.org/news/a/retrospective-2024-in-comprehensive-state-data-privacy-law,
zuletzt besucht am 11.1.2025.

Maldoff, Gabriel
The Risk-Based Approach in the GDPR: Interpretation and Implications, online abrufbar unter:
https://iapp.org/media/pdf/resource_center/GDPR_Study_Maldoff.pdf,
zuletzt besucht am 11.1.2025.

Richards, Neil
The Vermont veto is a step backward for privacy, online abrufbar unter:
https://iapp.org/news/a/the-vermont-veto-is-a-step-backward-for-privacy,
zuletzt besucht am 11.1.2025.

US State Comprehensive Privacy Laws Report 2024 LEGISLATIVE SESSION, online abrufbar unter:
https://iapp.org/media/pdf/resource_center/us_state_privacy_laws_report_2024_session_overview.pdf,
zuletzt besucht am 11.1.2025.

Strauss, David
State data privacy legislation: Takeaways from 2022 and what to expect in 2023, online abrufbar unter: https://iapp.org/news/a/state-data-privacy-legislation-takeaways-from-2022-and-what-to-expect-in-2023,
zuletzt besucht am 11.1.2025.

Zweifel-Keegan, Cobun

US Institutions Privacy Stakeholder Map, online abrufbar unter: https://iapp.org/media/pdf/resource_center/us_institutions_stakeholder_map.pdf,
zuletzt besucht am 11.1.2025.

IHK Regensburg für Oberpfalz / Kelheim (Hrsg.)

Anforderungen an Websites nach der DSGVO, online abrufbar unter: https://www.ihk.de/regensburg/fachthemen/recht/online-recht-und-datenschutz/eu-datenschutzgrundverordnung/anforderungen-an-websites-nach-der-ds-gvo-4158848,
zuletzt besucht am 11.1.2025.

Information Technology & Innovation Foundation (Hrsg.)

Johnson, Ash

How to Improve the American Privacy Rights Act, online abrufbar unter: https://itif.org/publications/2024/06/06/how-to-improve-the-american-privacy-rights-act/,
zuletzt besucht am 11.1.2025.

Lawyers' Committee for Civil Rights Under Law (Hrsg.)

Lawyers' Committee Opposes New Draft of American Privacy Rights Act, Urges Representatives to Vote No, online abrufbar unter: https://www.lawyerscommittee.org/lawyers-committee-opposes-new-draft-of-american-privacy-rights-act-urges-representatives-to-vote-no/,
zuletzt besucht am 11.1.2025.

Leadership Conference on Civil and Human Rights (Hrsg.)

Civil Rights Advocates Decry Removal of Civil Rights Protections in APRA, online abrufbar unter: https://civilrights.org/2024/06/21/advocates-decry-removal-civil-rights-protections-apra/,
zuletzt besucht am 11.1.2025.

Noyb (Hrsg.)

Europäische Kommission gibt EU-US-Datentransfers 3. Runde beim EuGH, online abrufbar unter: https://noyb.eu/de/european-commission-gives-eu-us-data-transfers-third-round-cjeu,
zuletzt besucht am 1.11.2025.

US-Cloud bald illegal? Trump schlägt erstes Loch in EU-US-Datenabkommen, online abrufbar unter: https://noyb.eu/de/us-cloud-soon-illegal-trump-punches-first-hole-eu-us-data-deal,
zuletzt besucht am 25.09.2025.

Pernot-Leplay, Emmanuel

EU Influence on Data Privacy Laws: Is the U.S. Approach Converging with the EU Model?, SSRN Volume 18 Nr. 1 2020, 101-124.
zitiert als: *Pernot-Leplay*, SSRN 2020.

Pew Research Center (Hrsg.)

Duggan, Meave/ Rainie, Lee

Privacy and Information Sharing - Many Americans say they might provide personal information, depending on the deal being offered and how much risk they face, online abrufbar unter:
https://www.pewresearch.org/internet/2016/01/14/privacy-and-information-sharing/,
zuletzt besucht am 11.1.2025.

Scholz, Lauren Henry

Private Rights of Action in Privacy Law, William & Mary Law Review Volume 63 (2021-2022) Issue 5, 1639- 1693,
zitiert als: *Scholz*, William & Mary Law Review William & Mary Law Review (2021-2022).

Spies, Axel

USA: Kentucky – 15. US-Bundesstaat mit einem Verbraucherdatenschutzgesetz, ZD-Aktuell 2024, 01626,
zitiert als: *Spies*, ZD-Aktuell 2024.

USA: Neues kalifornisches „Löschgesetz“ (Delete Act) für Datenhändler (Data Brokers), ZD-Aktuell 2024, 01505,
zitiert als: *Spies*, ZD-Aktuell 2024

USA: Umsetzung des California Consumer Privacy Rights Act schreitet voran, MMR 2022, 839 f.,
zitiert als: *Spies*, MMR 2022.

Zahlreiche neue Datenschutzgesetze in den US-Bundesstaaten - Schwierige Datenschutz-Compliance in den USA, MMR 2023, 69-73,
zitiert als: *Spies*, MMR 2023.

State of California Department of Justice – Office oft the Attorney General (Hrsg.)

Attorney General Bonta, Governor Newsom and CPPA File Letter Opposing Federal Privacy Preemption, online abrufbar unter: https://oag.ca.gov/news/press-releases/attorney-general-bonta-governor-newsom-and-cppa-file-letter-opposing-federal,
zuletzt besucht am 11.1.2025.

California Consumer Privacy Act (CCPA), online abrufbar unter: https://oag.ca.gov/privacy/ccpa,
zuletzt besucht am 11.1.2025.

Texas Office of the Attorney General (Hrsg.)

Attorney General Ken Paxton Sues General Motors for Unlawfully Collecting Drivers’ Private Data and Selling It To Several Companies, Including Insurance Companies, online abrufbar unter: https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-

paxton-sues-general-motors-unlawfully-collecting-drivers-private-data-and,
zuletzt besucht am 11.1.2025.

The National Law Review (Hrsg.)

Vanderzanden, Danielle/Seigner, Scott A. u.a.

Comprehensive Data Privacy Law Brings Big Changes to Virginia, but Excludes Employee Personal Data, online abrufbar unter: https://natlawreview.com/article/comprehensive-data-privacy-law-brings-big-changes-to-virginia-excludes-employee,
zuletzt besucht am 11.1.2025.

Uber (Hrsg.)

Was ist Uber – von A bis Z, online abrufbar unter: https://www.uber.com/de/blog/was-ist-uber/,
zuletzt besucht am 11.1.2025.

USAGov (Hrsg.)

Federal Trade Commission (FTC), online abrufbar unter: https://www.usa.gov/agencies/federal-trade-commission,
zuletzt besucht am 11.1.2025.

U.S. Congress (Hrsg.)

All Actions: H.R.8152 — 117th Congress (2021-2022),
online abrufbar unter: https://www.congress.gov/bill/117th-congress/house-bill/8152/all-actions,
zuletzt besucht am 11.1.2025.

All Actions: H.R.8818 — 118th Congress (2023-2024),
online abrufbar unter: https://www.congress.gov/bill/118th-congress/house-bill/8818/all-actions,
zuletzt besucht am 11.1.2025.

H.R.8152 - American Data Privacy and Protection Act - 117th Congress (2021-2022), online abrufbar unter: https://www.congress.gov/bill/117th-congress/house-bill/8152,
zuletzt besucht am 11.1.2025.

H.R.8818 - American Privacy Rights Act of 2024118th Congress (2023-2024), online abrufbar unter:
https://www.congress.gov/bill/118th-congress/house-bill/8818/text,
zuletzt besucht am 11.1.2025.

Overview of the Legislative Process, online abrufbar unter:
https://www.congress.gov/legislative-process,
zuletzt besucht am 11.1.2025.

Verbraucherzentrale (Hrsg.)

Dark Patterns: So wollen Websites und Apps Sie manipulieren, online abrufbar unter: https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinedienste/dark-patterns-so-wollen-websites-und-apps-sie-manipulieren-58082,
zuletzt besucht am 1.11.2025.

Whitman, James Q.

The Two Western Cultures of Privacy: Dignity Versus Liberty, The Yale Law Yournal Volume 113 Nr. 6 2004, 1151– 221,
zitiert als: *Whitman*, The Yale Law Yournal 2004.

Wired (Hrsg.)

Cameron, Dell

Surprise! The Latest ‘Comprehensive’ US Privacy Bill Is Doomed, online abrufbar unter: https://www.wired.com/story/apra-privacy-bill-doomed/,
zuletzt besucht am 11.1.2025.

Rechtsprechungsverzeichnis

EuGH

Urteil vom 16.7.2020 – C-311/18, NJW 2020, 2613-2622.

Urteil vom 1.10.2019 – C-673/17, MMR 2019, 732-740.

Urteil vom 6.10.2015 – C-362/14, NJW 2015, 3151-3158.

EuG

Urteil vom 3.9.2025 – T-553/23, BeckRS 2025, 22446.

BGH

Urteil vom 16.5.2017 – VI ZR 135/13, ZD 2017, 424-427.

BVerfG

Urteil vom 15.12.1983 – 1 BvR 209/83 u. a., NJW 1984, 419-428.

VERZEICHNIS DER BISHER ERSCHIENENEN BEITRÄGE DER HOCHSCHULE PFORZHEIM

Werner Pepels Aug. 1990

Integrierte Kommunikation

53. Martin Dettinger-Klemm Aug. 1990

Grenzen der Wissenschaftsfreiheit. Überlegungen zum Thema: Freiheit und Verantwortung des Wissenschaftlers

54. Werner Pepels Sept. 1990

Mediaplanung – Über den Einsatz von Werbegeldern in Medien

55. Dieter Pflaum Sept. 1990

Werbeausbildung und Werbemöglichkeiten in der DDR

56. Rudi Kurz (Hrsg.) Nov. 1990

Ökologische Unternehmensführung – Herausforderung und Chance

57. Werner Pepels Jan. 1991

Verkaufsförderung – Versuch einer Systematisierung

58. Rupert Huth, Ulrich Wagner (Hrsg.) Aug. 1991

Volks- und betriebswirtschaftliche Abhandlungen. Prof. Dr. Dr. h.c. Tibor Karpati (Universität Osijek in Kroatien) zum siebzigsten Geburtstag. Mit einem Vorwort von R. Huth und Beiträgen von H.-J. Hof, H. Löffler, D. Pflaum, B. Runzheimer und U. Wagner

59. Hartmut Eisenmann Okt. 1991

Dokumentation über die Tätigkeit einer Industrie- und Handelskammer – Dargestellt am Beispiel der IHK Nordschwarzwald

60. Ursula Hoffmann-Lange Dez. 1991

Eliten und Demokratie: Unvereinbarkeit oder notwendiges Spannungsverhältnis?

61. Werner Pepels Dez. 1991

Elemente der Verkaufsgesprächsführung

62. Wolfgang Berger Dez. 1991

Qualifikationen und Kompetenzen eines Europamanagers

63. Günter Staub Jan. 1992

Der Begriff „Made in Germany“ – Seine Beurteilungskriterien

64. Martin W. Knöll, Hieronymus M. Lorenz Mai 1992

Gegenstandsbereich und Instrumente der Organisationsdiagnose im Rahmen von Organisationsentwicklungs (OE)-Maßnahmen

65. Werner Lachmann Juni 1992

Ethikversagen – Marktversagen

66. Paul Banfield Juni 1993

Observations On The Use Of Science As A Source Of Legitimation In Personnel Management

67. Bernd Noll Aug. 1993

Gemeinwohl und Eigennutz. Wirtschaftliches Handeln in Verantwortung für die Zukunft – Anmerkungen zur gleichnamigen Denkschrift der Evangelischen Kirche in Deutschland aus dem Jahre 1991

68. Siegfried Kreutzer, Regina Moczadlo Aug. 1993

Die Entdeckung der Wirklichkeit – Integrierte Projektstudien in der Hochschulausbildung

69. Sybil Gräfin Schönfeldt Aug. 1993

Von Menschen und Manieren. Über den Wandel des sozialen Verhaltens in unserer Zeit. Vortrag gehalten im Rahmen des Studium Generale der Hochschule Pforzheim, Wintersemester 1992/93

70. Hartmut Löffler Dez. 1993

Geld- und währungspolitische Grundsatzüberlegungen für ein Land auf dem Weg zur Marktwirtschaft – Das Beispiel Kroatien

71. Hans-Georg Köglmayr, Kurt H. Porkert Nov. 1994

Festlegen und ausführen von Geschäftsprozessen mit Hilfe von SAP-Software

72. Alexa Mohl Febr. 1995

NLP-Methode zwischen Zauberei und Wissenschaft. Vortrag gehalten im Rahmen des Studium Generale der Hochschule Pforzheim, Wintersemester 1994/95

73. Bernd Noll Mai 1995

Marktwirtschaft und Gerechtigkeit: Anmerkungen zu einer langen Debatte

74. Rudi Kurz, Rolf-Werner Weber Nov. 1995

Ökobilanz der Hochschule Pforzheim. 2. geänderte Auflage, Jan. 1996

75. Hans Lenk Mai 1996

Fairneß in Sport und Wirtschaft. Vortrag gehalten im Rahmen des Studium Generale der Hochschule Pforzheim, Wintersemester 1995/96

76. Barbara Burkhardt-Reich, Hans-Joachim Hof, Bernd Noll Juni 1996

Herausforderungen an die Sozialstaatlichkeit der Bundesrepublik

77. Helmut Wienert März 1997

Perspektiven der Weltstahlindustrie und einige Konsequenzen für den Anlagenbau

78. Norbert Jost Mai 1997

Innovative Ingenieur-Werkstoffe

79. Rudi Kurz, Christoph Hubig, Ortwin Renn, Hans Diefenbacher Sept. 1997

Ansprüche in der Gegenwart zu Lasten der Lebenschancen zukünftiger Generationen

80. Björn Engholm Okt. 1997

Ökonomie und Ästhetik. Vortrag gehalten im Rahmen des Studium Generale der Hochschule Pforzheim, Wintersemester 1996/97. 2. geänderte Auflage. Jan. 1998

81. Lutz Goertz Sept. 1998

Multimedia quo vadis? – Wirkungen, Chancen, Gefahren. Vortrag gehalten im Rahmen des Studium Generale der Fachhochschule Pforzheim, Wintersemester 1996/97

82. Eckhard Keßler Nov. 1998

Der Humanismus und die Entstehung der modernen Wissenschaft. Vortrag gehalten im Rahmen des Studium Generale der Hochschule Pforzheim, Wintersemester 1996/97

83. Heinrich Hornef Febr. 1998

Aufbau Ost – Eine Herausforderung für Politik und Wirtschaft. Vortrag gehalten im Rahmen des Studium Generale der Fachhochschule Pforzheim, Wintersemester 1997/98

VERZEICHNIS DER BISHER ERSCHIENENEN BEITRÄGE DER HOCHSCHULE PFORZHEIM

84. **Helmut Wienert** Juli 1998
50 Jahre Soziale Marktwirtschaft – Auslaufmodell oder Zukunftskonzept? Vortrag gehalten im Rahmen des Studium Generale der Hochschule Pforzheim, Sommersemester 1998

85. **Bernd Noll** Sept. 1998
Die Gesetzliche Rentenversicherung in der Krise

86. **Hartmut Löffler** Jan. 1999
Geldpolitische Konzeptionen - Alternativen für die Europäische Zentralbank und für die Kroatische Nationalbank

87. **Erich Hoppmann** Juni 1999
Globalisierung. Vortrag gehalten im Rahmen des Studium Generale der Hochschule Pforzheim, Sommersemester 1999

88. **Helmut Wienert (Hrsg.)** Dez. 1999
Wettbewerbspolitische und strukturpolitische Konsequenzen der Globalisierung. Mit Beiträgen von Hartmut Löffler und Bernd Noll

89. **Ansgar Häfner u.a. (Hrsg.)** Jan. 2000
Konsequenzen der Globalisierung für das internationale Marketing. Mit Beiträgen von Dieter Pflaum und Klaus-Peter Reuthal

90. **Ulrich Wagner** Febr. 2000
Reform des Tarifvertragsrechts und Änderung der Verhaltensweisen der Tarifpartner als Voraussetzungen für eine wirksame Bekämpfung der Arbeitslosigkeit

91. **Helmut Wienert** April 2000
Probleme des sektoralen und regionalen Wandels am Beispiel des Ruhrgebiets

92. **Barbara Burkhardt-Reich** Nov. 2000
Der Blick über den Tellerrand – Zur Konzeption und Durchführung eines „Studium Generale“ an Fachhochschulen

93. **Helmut Wienert** Dez. 2000
Konjunktur in Deutschland - Zur Einschätzung der Lage durch den Sachverständigenrat im Jahresgutachten 2000/2001

94. **Jürgen Wertheimer** Febr. 2001
Geklonte Dummheit: Der infantile Menschenpark. Vortrag gehalten im Rahmen des Studium Generale der Hochschule Pforzheim, Wintersemester 2000/01

95. **Konrad Zerr** März 2001
Erscheinungsformen des Online-Research – Klassifikation und kritische Betrachtung

96. **Daniela Kirchner** April 2001
Theorie und praktische Umsetzung eines Risikomanagementsystems nach KontraG am Beispiel einer mittelständischen Versicherung

97. **Bernd Noll** Mai 2001
Die EU-Kommission als Hüterin des Wettbewerbs und Kontrolleur von sektoralen und regionalen Beihilfen

Peter Frankenfeld
EU Regionalpolitik und Konsequenzen der Osterweiterung

98. **Hans Joachim Grupp** Juni 2001
Prozessurale Probleme bei Beschlussmängelstreitigkeiten in Personengesellschaften

99. **Norbert Jost (Hrsg.)** Juli 2001
Technik Forum 2000: Prozessinnovationen bei der Herstellung kaltgewalzter Drähte. Mit Beiträgen von Peter Kern, Wilhelm Bauer, Rolf Ilg; Heiko Dreyer; Johannes Wößner und Rainer Menge

100. **Urban Bacher, Mikolaj Specht** Dez. 2001
Optionen – Grundlagen, Funktionsweisen und deren professioneller Einsatz im Bankgeschäft

101. **Constanze Oberle** Okt. 2001
Chancen, Risiken und Grenzen des M-Commerce

102. **Ulrich Wagner** Jan. 2002
Beschäftigungshemmende Reformstaus und wie man sie auflösen könnte
Jürgen Volkert
Flexibilisierung durch Kombi-Einkommen? Die Perspektive der Neuen Politischen Ökonomie

103. **Mario Schmidt, René Keil** März 2002
Stoffstromnetze und ihre Nutzung für mehr Kostentransparenz sowie die Analyse der Umweltwirkung betrieblicher Stoffströme

104. **Kurt Porkert** Mai 2002
Web-Services – mehr als eine neue Illusion?

105. **Helmut Wienert** Juni 2002
Der internationale Warenhandel im Spiegel von Handelsmatrizen

106. **Robert Wessolly, Helmut Wienert** Aug. 2002
Die argentinische Währungskrise

107. **Roland Wahl (Hrsg.)** Sept. 2002
Technik-Forum 2001: Weiterentwicklungen an Umformwerkzeugen und Walzdrähten. Mit Beiträgen von Roland Wahl, Thomas Dolny u.a., Heiko Pinkawa, Rainer Menge und Helmut Wienert

108. **Thomas Gulden** April 2003
Risikoberichterstattung in den Geschäftsberichten der deutschen Automobilindustrie

109. **Günter Altner** Mai 2003
Lasset uns Menschen machen – Der biotechnische Fortschritt zwischen Manipulation und Therapie. Vortrag gehalten im Rahmen des Studium Generale der Hochschule Pforzheim, Sommersemester 2003

110. **Norbert Jost (Hrsg.)** Juni 2003
Technik-Forum 2002: Innovative Verfahren zur Materialoptimierung. Mit Beiträgen von Norbert Jost, Sascha Kunz, Rainer Menge/Ursula Christian und Berthold Leibinger

111. **Christoph Wüterich** Februar 2004
Professionalisierung und Doping im Sport. Vortrag gehalten im Rahmen des Studium Generale der Hochschule Pforzheim, Sommersemester 2003

112. **Sabine Schmidt** Mai 2004
Korruption in Unternehmen – Typologie und Prävention

113. **Helmut Wienert** August 2004
Lohn, Zins, Preise und Beschäftigung – Eine empirische Analyse gesamtwirtschaftlicher Zusammenhänge in Deutschland

114. **Roland Wahl (Hrsg.)** Sept. 2004
Technik-Forum 2003: Materialentwicklung für die Kaltumformtechnik. Mit Beiträgen von Andreas Baum, Ursula Christian, Steffen Nowotny, Norbert Jost, Rainer Menge und Hans-Eberhard Koch

115. **Dirk Wenzel** Nov. 2004
The European Legislation on the New Media: An Appropriate Framework for the Information Economy?

VERZEICHNIS DER BISHER ERSCHIENENEN BEITRÄGE DER HOCHSCHULE PFORZHEIM

116. **Frank Morelli, Alexander Mekyska, Stefan Mühlberger** Dez. 2004
Produkt- und prozessorientiertes Controlling als Instrument eines erfolgreichen Informationstechnologie-Managements

117. **Stephan Thesmann, Martin Frick, Dominik Konrad** Dez. 2004
E-Learning an der Hochschule Pforzheim

118. **Norbert Jost (Hrsg.)** Juni 2005
Technik-Forum 2004: Innovative Werkstoffaspekte und Laserbehandlungstechnologien für Werkzeuge der Umformtechnik

119. **Rainer Gildeggen** Juni 2005
Internationale Produkthaftung

120. **Helmut Wienert** Oktober 2005
Qualifikationsspezifische Einkommensunterschiede in Deutschland unter besonderer Berücksichtigung von Universitäts- und Fachhochschulabsolventen

121. **Andreas Beisswenger, Bernd Noll** Nov. 2005
Ethik in der Unternehmensberatung – ein vermintes Gelände?

122. **Helmut Wienert** Juli 2006
Wie lohnend ist Lernen? Ertragsraten und Kapitalendwerte von unterschiedlichen Bildungswegen

123. **Roland Wahl (Hrsg.)** Sept. 2006
Technik-Forum 2005: Umformwerkzeuge - Anforderungen und neue Anwendungen. Mit Beiträgen von Edmund Böhm, Eckhard Meiners, Andreas Baum, Ursula Christian und Jörg Menno Harms

124. **Mario Schmidt** Dez. 2006
Der Einsatz von Sankey-Diagrammen im Stoffstrommanagement

125 **Norbert Jost (Hrsg.)** Okt. 2007
Technik-Forum 2006: Innovative neue Techniken für Werkzeuge der Kaltverformung. Mit Beiträgen von Franz Wendl, Horst Bürkle, Rainer Menge, Michael Schiller, Andreas Baum, Ursula Christian, Manfred Moik und Erwin Staudt.

126 **Roland Wahl (Hrsg.)** Okt. 2008
Technik-Forum 2007: Fortschrittsberichte und Umfeldbetrachtungen zur Entwicklung verschleißreduzierter Umformwerkzeuge. Mit Beiträgen von Klaus Löffler, Andreas Zilly, Andreas Baum und Paul Kirchhoff.

127. **Julia Tokai, Christa Wehner** Okt. 2008
Konzept und Resultate einer Online-Befragung von Marketing-Professoren an deutschen Fachhochschulen zum Bologna-Prozess

128 **Thomas Cleff, Lisa Luppold, Gabriele Naderer, Jürgen Volkert** Dez. 2008
Tätermotivation in der Wirtschaftskriminalität

129 **Frank Thuselt** Juni 2009
Das Arbeiten mit Numerik-Programmen. MATLAB, Scilab und Octave in der Anwendung.

130 **Helmut Wienert** August 2009
Wachstumsmotor Industrie? Zur Bedeutung des verarbeitenden Gewerbes für die Entwicklung des Bruttoinlandsprodukts

131 **Sebastian Schulz** Sept. 2009
Nutzung thermodynamischer Datensätze zur Simulation von Werkstoffgefügen (aus der Reihe „Focus Werkstoffe“, Hrsg. Norbert Jost).

132 **Hanno Beck; Kirsten Wüst** Sept. 2009
Gescheiterte Diäten, Wucherzinsen und Warteprämien: Die neue ökonomische Theorie der Zeit.

133 **Helmut Wienert** Sept. 2009
Was riet der Rat? Eine kommentierte Zusammenstellung von Aussagen des Sachverständigenrats zur Regulierung der Finanzmärkte und zugleich eine Chronik der Entstehung der Krise

134 **Norbert Jost (Hrsg.): Technik-Forum 2008**
Werkstoffe und Technologien zur Kaltverformung

135 **Frank Morelli** Januar 2010
Geschäftsprozessmodellierung ist tot – lang lebe die Geschäftsprozessmodellierung!

136 **T. Cleff, L. Fischer, C. Sepúlveda, N. Walter** Januar 2010
How global are global brands? An empirical brand equity analysis

137 **Kim Neuer** Juni 2010
Achieving Lisbon – The EU’s R&D Challenge The role of the public sector and implications of US best practice on regional policymaking in Europe

138 **Bernd Noll** Sept. 2010
Zehn Thesen zur Corporate Governance

139 **Pforzheim University** März 2011
Communication on progress.
PRME Report 2008

140 **Rainer Maurer** März 2011
Unternehmensverantwortung für soziale und ökologische Nachhaltigkeit – darf man auch anderer Meinung sein? Einige kritische Anmerkungen zum PRME-Report der Hochschule

141. **Barbara Reeb, Malte Krome** Okt. 2011
Arm trotz Arbeit? Zum Für und Wider von Mindestlöhnen

142. **Daniel Wyn Müller** Mai 2012
Titanschäume als Knochenimplantat (aus der Reihe „Focus Werkstoffe“, Hrsg. Norbert Jost).

143. **Alexander Martin Matz, Norbert Jost** Mai 2012
Fouling an offenporigen zellulären Werkstoffen auf Al-Basis unter beheizten wässrigen Bedingungen (aus der Reihe „Focus Werkstoffe“, Hrsg. Norbert Jost).

144. **Norbert Jost, Roman Klink (Hrsg.)** Sept. 2012
Tagungsband zum 1. Pforzheimer Werkstofftag

145. **Norbert Jost, Roman Klink (Hrsg.)** Sept. 2012
Tagungsband zum 2. Pforzheimer Werkstofftag. Aus der Reihe „Leichtbau“, Hrsg.: N. Jost, R. Klink.

146. **Helmut Wienert** Febr. 2014
Zur Entwicklung der Hochschulen für Angewandte Wissenschaften (Fachhochschulen) in Deutschland

147. **Jürgen Antony** April 2014
Technical Change and the Elasticity of Factor Substitution

148. **Stephanie Görlach** April 2014
Ressourceneffizienz in Deutschland

149. **Norbert Jost (Hrsg.)** Sept. 2014

VERZEICHNIS DER BISHER ERSCHIENENEN BEITRÄGE DER HOCHSCHULE PFORZHEIM

Focus Werkstoffe. Tagungsband zum 3. Pforzheimer Werkstofftag

150. Bernd Noll Aug. 2014
Unternehmenskulturen – entscheidender Ansatzpunkt für wirtschaftsethisches Handeln?

151. Human Resources Competence Center April 2015
50 Jahre Personalmanagement an Der Hochschule- Jubiläumsband

152. Rainer Maurer Mai 2015
Auf dem Weg zur weltanschaulichen Bekenntnisschule: Das wirtschaftspolitische Leitbild der Hochschule Pforzheim

153. Norbert Jost (Hrsg.) Okt. 2015
Tagungsband Pforzheimer Werkstofftag

154. Jessica Elena Balzer Nov. 2015
Spielen mit guten Gewissen: Ein Vorschlag zur Zertifizierung der deutschen Spielwarenindustrie und ein Schritt näher zum Schachmatt des Greenwashing

155. Jaqueline Paasche Jan. 2016
Kopieren, transformieren, kombinieren – Ideenklau und Plagiarismus in der Werbung

156. Vanessa Zeiler Jan. 2016
Mobile User Experience – Der Einfluss von kognitivem Entertainment auf die Nutzung mobiler Anwendungen

157. Mario Kotzab, Maximilian Pflug Jan. 2016
Das bedingungslose Grundeinkommen

158. Marco C. Melle Jan 2016
Harmonisierung der heterogenen Unternehmensteuern in Europa? Plädoyer für einen Mittelweg

159. Klaus Möller, Julian Gabel, Frank Bertagnolli Aug. 2016
fischer Befestigungssysteme: Change Management in der Distributionslogistik – eine Fallstudie

160. Klaus Möller, Julian Gabel, Frank Bertagnolli Aug. 2016
fischer Befestigungssysteme: Change Management in der Distributionslogistik – eine Fallstudie

161. Wolfgang Heinz Nov. 2016
Die Ethik des Strafens

162. Norbert Jost, Simon Kött (Hrsg.) Okt. 2016
Pforzheimer Werkstofftag 2016

163. Bettina C.K. Binder
Kennzahlenmanagement und –controlling Prozessorientiertes Performance Management in internationalen Unternehmen

164. Stefan Walz, Jonas Tritschler, Reinhard Rupp
Erweitertes Management Reporting mit SAP S/4HANA auf Basis des Universal Journals

165. Simone Harriehausen
Wenn ich zwanzig Ziegen will und Du mir keine geben magst – Ein Überblick über die Möglichkeiten und Methoden der Streitbeilegung

166. Norbert Jost, Simon Kött (Hrsg.) Okt. 2017
Pforzheimer Werkstofftag 2017

167. Helmut Wienert Dez. 2017
Pforzheim: Alles Schmuckstadt – oder was?

168. Norbert Jost; Simon Kött
Pforzheimer Werkstofftag 2018 September 2018

169. Bernd Noll
21. Juni 1948 – Startschuss mit Folgen November 2018

170. Katja Flosdorff April 2019
Identifikation und Evaluation von Bewertungskriterien zur optimalen Auswahl von Ideen während des Innovationsprozesses

171. Theresa Süß Juni 2019
Inwiefern kann Behavioral Economics das Ernährungsverhalten erklären und beeinflussen?

172. Viktor Waldschmidt Juni 2019
Clickbait, der ganz große Wurf? Eine Studie über die Verwendung von Clickbaits durch Online-Nachrichtenportale und deren Konsequenzen

173. Rainer Maurer Oktober 2019
Normative Werturteile und Wirtschaftswissenschaft

174. Kristina Weber Oktober 2019
Künstliche Intelligenz im werteorientierten Marketing – Konzeptualisierung des „Value in Context“ und eine Bewertung KI-gestützter Marketingaktivitäten

175. Klaus Möller, Fritz Gairing, Daniel Mezger, Thomas Jehnichen Oktober 2019
Design of Training Processes in Manual Order Picking

176. Martin Leroch Oktober 2021
Moral Institutions and Evolution: In Search of Equilibria

177. Shirin Mayasilci LL.B. Juli 2022
Inhalt und Bedeutung der neu ins bürgerliche Recht eingeführten Update-Pflicht

178. Vanessa Schweikert LL.B. Juli 2022
Das Lieferkettensorgfaltspflichtengesetz

179. Tsjalle van der Burg Oktober 2022
Competitive Balance and Demand for Football:
A Review of the Literature

180. Hans-Joachim Grupp Dezember 2023
Weihnachtsgeschichten aus dem Schwarzwald

181. Tobias Brändle, René Kalweit und Marcel Reiner
Die Reform des Arbeitnehmerüberlassungsgesetze und Tarifautonomie Januar 2024

182. Annalena Secci LL.B. Februar 2024
Erstellen und Veröffentlichen von Fotos nach der DSGVO - eine kritische Auseinandersetzung mit Anforderungen am Beispiel von Kinderfotos

183. Denise Flattich LL.B. November 2024
Die CE-Kennzeichnungspflicht im Fokus des neuen Sachmangelbegriffs

184. Melanie Mitschke LL.B. Februar 2025
Einziehung von Gegenständen des rechtswidrigen

185. Heiko Steffens Mai 2025
Von der Arbeitsgemeinschaft der Verbraucherverbände **(**AgV) zum Verbraucherzentrale Bundesverband