I Z A Institute
of Labor Economics
Initiated by Deutsche Post Foundation

RESEARCH REPORT SERIES

IZA Research Report No. 104

Datenschutzrechtliche Dimensionen Datentreuhänder

Kurzexpertise im Auftrag des Bundesministeriums für Arbeit und Soziales

Jürgen Kühling (Universität Regensburg)
Florian Sackmann (Roding/München)
Hilmar Schneider (IZA)

NOVEMBER 2020

Bundesministerium
für Arbeit und Soziales

FORSCHUNGSBERICHT

550

Datenschutzrechtliche Dimensionen Datentreuhänder

– Kurzexpertise –

Oktober 2020

ISSN 0174-4992

I Z A Institute
of Labor Economics
Initiated by Deutsche Post Foundation

Kurzexpertise

Datenschutzrechtliche Dimensionen Datentreuhänder

Prof. Dr. Jürgen Kühling, LL.M. (Universität Regensburg)

Dr. Florian Sackmann (Roding/München)

Prof. Dr. Hilmar Schneider (IZA)

September 2020

Erstellt im Auftrag des Bundesministeriums für Arbeit und Soziales.

Kurzbeschreibung

Im Zuge fortschreitender technischer Möglichkeiten durch entsprechende Prozessorleistungsfähigkeit, Speicherkapazitäten und digitale Vernetzung erlangt die Nutzung und Verarbeitung personenbezogener Daten eine zunehmende kommerzielle Bedeutung in der allgemeinen Wertschöpfungskette. Die Wahrnehmung des Rechts auf informationelle Selbstbestimmung erlangt damit auch eine ökonomische Dimension. Der Markt für datenbasierte Dienstleistungen zeichnet sich jedoch durch eine ausgeprägte Asymmetrie der Verhandlungsmacht zwischen Dienste-Nutzern, die Informationen über sich preisgeben, und Dienste-Anbietern, die diese Informationen vermarkten, aus. Datentreuhänder könnten eine Möglichkeit bieten, das vorhandene Machtungleichgewicht durch eine Kollektivierung individueller Nutzerinteressen neu zugunsten der Dienste-Nutzer auszutarieren. Das vorliegende Gutachten untersucht, welche rechtlichen Voraussetzungen dafür gegeben oder zu schaffen sind, sowie welche ökonomischen Aspekte dabei zu berücksichtigen sind.

Abstract

In the course of advancing technical possibilities through corresponding processor performance, storage capacities and digital networking, the use and processing of personal data is gaining increasing commercial significance in the general value-added chain. The realization of the legal right to informational self-determination thus also involves an economic dimension. However, the market for data-based services is characterized by a pronounced asymmetry of bargaining power between service users, who disclose information about themselves, and service providers, who market this information. Data trustees could offer a way to rebalance this imbalance in favor of service users by collectivizing individual user interests. The present report examines the legal prerequisites that are existing or have to be created for this, as well as the economic aspects that should be considered.

Inhaltsverzeichnis

Abkürzungsverzeichnis

AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AGB	Allgemeine Geschäftsbedingungen
App	Applikation / Anwendungssoftware
BAG	Bundesarbeitsgericht
BB	Betriebs-Berater
BDSG	Bundes-Datenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des Bundesgerichtshofes in Zivilsachen
BMAS	Bundesministerium für Arbeit und Soziales
BRAO	Bundesrechtsanwaltsordnung
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfGK	Kammerentscheidungen des Bundesverfassungsgerichts
BvR	Richter des Bundesverfassungsgerichts
CNIL	Commission Nationale de l'Informatique et des Libertés
CR	Computer und Recht
DS-GVO	Datenschutz-Grundverordnung
DSRL	Datenschutzrichtlinie
DuD	Datenschutz und Datensicherheit
EDSA	Europäischer Datenschutzausschuss
EDSB	Europäischer Datenschutzbeauftragter
EG	Europäische Gemeinschaft
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EWG	Europäische Wirtschaftsgemeinschaft
FAZ	Frankfurter Allgemeine Zeitung
GDPR	General Data Protection Regulation
GesR	GesundheitsRecht
GG	Grundgesetz
GrCh	Charta der Grundrechte der Europäischen Union

IT	Informationstechnik
IZA	Forschungsinstitut zur Zukunft der Arbeit
LDSG	Landesdatenschutzgesetz
LG	Landgericht
LPK	Lehr- und Praxiskommentar
MedR	Medizinrecht
MMR	Multimedia und Recht
MüKo	Münchener Kommentar
NJW	Neue Juristische Wochenschrift
NZA	Neue Zeitschrift für Arbeitsrecht
PIMS	Personal Information Management Systems
RDG	Rechtsdienstleistungsgesetz
SGB	Sozialgesetzbuch
TKG	Telekommunikationsgesetz
TVG	Tarifvertragsgesetz
UKlaG	Unterlassungsklagengesetz
URL	Uniform Resource Locator
WWW	World Wide Web
ZD	Zeitschrift für Datenschutz

Abbildungsverzeichnis

Zusammenfassung

Online-Dienste haben inzwischen einen festen Platz in der Lebenswelt vieler Menschen erlangt. Die Nutzung solcher Dienste ist für die Nutzer in den meisten Fällen kostenlos. Finanziert wird die Bereitstellung solcher Dienste stattdessen auf indirektem Weg, etwa über Werbeeinnahmen, dem Verkauf von datenbasierten Modellen zur Produktwerbung oder zur Steuerung politischer Kampagnen, aber auch über Spenden oder eine staatliche Förderung. Die Finanzierung auf der Basis datenbasierter Modelle verdankt ihren wirtschaftlichen Erfolg in erster Linie der Bereitschaft der Dienste-Nutzer dem Dienste-Anbieter Informationen über sich selbst und/oder ihr Nutzungsverhalten zur kommerziellen Verwertung zu überlassen. Dabei geht es weniger um die kommerzielle Verwertung konkreter personenbezogener Daten als vielmehr um die Entwicklung und Vermarktung von darauf aufbauenden Modellen, die typische Verhaltensmuster abbilden. Die Verfahren, mit denen entsprechende Muster ermittelt werden, sind teilweise hochkomplex und bedienen sich nicht zuletzt neuester Techniken aus dem Bereich der künstlichen Intelligenz. Der so geschaffene Mehrwert eignet sich in vielfältiger Form zur kommerziellen Verwertung und stellt die ökonomische Basis dar, die es den Anbietern von Online-Diensten überhaupt erst erlaubt, ihr Dienste-Angebot bereit zu stellen.

Die indirekte Finanzierung von Online-Diensten auf der Basis eines aus Nutzerdaten bestehenden Rohstoffs bildet ein konstitutives Element der Ökonomie von Online-Diensten. Dabei hat sich im Laufe der Zeit relativ schnell eine Situation herauskristallisiert, bei der einer weltweiten Gemeinschaft von Dienste-Nutzern eine vergleichsweise geringe Zahl von Dienste-Anbietern gegenübersteht. Die damit einhergehenden Monopolstrukturen werfen die Frage auf, inwiefern die damit verbundene Asymmetrie der Verhandlungsmacht zwischen Dienste-Anbietern und Dienste-Nutzern zu Marktunvollkommenheiten führt, die sich mit Hilfe geeigneter regulatorischer Eingriffe beseitigen ließen.

Eine Möglichkeit zur Stärkung der Verhandlungsmacht der Dienste-Nutzer könnte in der Einschaltung von Datentreuhändern bestehen, die als unabhängige Instanz die kollektive Vertretung von Nutzerinteressen gegenüber den Dienste-Anbietern wahrnehmen könnten. Eine wichtige Voraussetzung hierfür ist, dass Datentreuhänder kein darüber hinaus gehendes Verwertungsinteresse an den ihnen überlassenen Daten ausüben dürfen. Auch wenn auf der politischen Fachebene an Konzepten der Datentreuhänderschaft großes Interesse besteht, hat es sich in der Praxis bislang nicht nennenswert etablieren können. Dabei könnten sowohl rechtliche als auch ökonomische Hürden eine Rolle spielen.

Das vorliegende Gutachten geht beiden Aspekten nach und kommt zu dem Schluss, dass eine Mandatierung von Datentreuhändern zur Wahrung und Durchsetzung des individuellen Rechts auf informationelle Selbstbestimmung bereits weitestgehend durch den bestehenden rechtlichen Rahmen gedeckt ist. Besonderer gesetzgeberischer Handlungsbedarf ist in dieser Hinsicht nicht gegeben. Die Hürden für eine Etablierung von Datentreuhändern liegen vielmehr darin, dass bislang die finanziellen Voraussetzungen für ein tragfähiges Geschäftsmodell fehlen.

Damit ist nicht nur die Wahrnehmung des Rechts auf informationelle Selbstbestimmung beeinträchtigt, sondern auch die Funktionsfähigkeit des Markts für Online-Dienste. Datentreuhänder könnten in diesem Kontext eine wichtige Rolle spielen. Damit diese zur Entfaltung kommen kann, bedarf es allerdings einer geeigneten Form der staatlichen Förderung, entweder durch die Schaffung einer unabhängigen öffentlichen Instanz oder durch die Förderung privater Dienstleister im staatlichen Auftrag. Eine solche Förderung sollte zunächst zeitlich befristet werden, um die daraus resultierenden Erfahrungen nach einer angemessenen Zeit einer Bewertung zu unterziehen und die eingesetzten Instrumente gegebenenfalls zielführend weiterentwickeln zu können.

1. Einleitung

Im Zuge fortschreitender technischer Möglichkeiten durch entsprechende Prozessorleistungsfähigkeit, Speicherkapazitäten und digitale Vernetzung erlangt die Nutzung und Verarbeitung personenbezogener Daten eine zunehmende kommerzielle Bedeutung in der allgemeinen Wertschöpfungskette. Personenbezogene Daten erlauben unter anderem eine gezieltere Steuerung von kommerzieller Werbung, politischen Kampagnen, staatlichen Informationsprogrammen oder ähnlichen Informationen als es ansonsten möglich wäre. Das Erheben von personenbezogenen Daten und deren Weiterverarbeitung zu kommerziellen Zwecken avanciert damit immer mehr zu einem eigenständigen Wirtschaftszweig. Insbesondere durch die Nutzung von Online-Diensten werden enorme Mengen an nutzerbezogenen Informationen generiert, die entweder durch die Dienste-Anbieter selbst oder durch Dritte zum jeweiligen Zweck einer entsprechenden Weiterverarbeitung unterzogen werden.

Die betroffenen Personen müssen dazu zwar ihre Einwilligung erteilen, tun dies aber häufig in Unkenntnis dessen, welche konkreten Verarbeitungsschritte und Verwertungsinteressen mit der Erfassung und Speicherung ihrer Nutzungsdaten verbunden sind. Zudem befinden sie sich typischerweise in einer schwachen Verhandlungsposition gegenüber denjenigen, die diese Einwilligung einfordern. So ist etwa die Nutzung nahezu aller Online-Dienste an die Zustimmung zu entsprechenden Klauseln gekoppelt, und wer sich der Zustimmung verweigert, kann den entsprechenden Dienst entweder gar nicht oder nur eingeschränkt nutzen. Die Wahrnehmung des Rechts auf informationelle Selbstbestimmung durch das einzelne Individuum unterliegt damit einer mehr oder weniger starken Beeinträchtigung.

Datentreuhänder können in dieser Konstellation ein Instrument sein, um die Durchsetzungsmöglichkeit des Rechts auf informationelle Selbstbestimmung zu stärken. Datentreuhänder sind dazu gedacht, anstelle einer Vielzahl von Einzelpersonen die kollektive Interessenswahrnehmung gegenüber einer datenerhebenden Einrichtung zu übernehmen. Einzelpersonen müssen dazu lediglich einen Datentreuhänder ihrer Wahl mandatieren. Dieser übernimmt dann an ihrer statt die Wahrung der jeweiligen Interessen. Damit Datentreuhänder die ihnen zugedachte Funktion ausüben können, dürfen sie keinem Interessenskonflikt ausgesetzt sein. Sie müssen dazu wirtschaftlich unabhängig sein und dürfen kein kommerzielles Eigeninteresse an der Verwertung der ihnen übertragenen Daten wahrnehmen.[1] Durch die Kollektivierung der Interessenswahrnehmung durch Datentreuhänder erhöht sich für Datenverarbeiter das Risiko einer Wertminderung der erhobenen Daten oder von Schadenersatzleistungen bei Fehlverhalten, und damit mutmaßlich die Bereitschaft zu Zugeständnissen im Sinne der Betroffenen.

Das vorliegende Gutachten beschäftigt sich vor diesem Hintergrund mit zwei Fragekomplexen. Der erste Teil widmet sich den rechtlichen Voraussetzungen für eine Datentreuhänderschaft und beleuchtet die Frage, ob der vorhandene Rechtsrahmen dafür bereits ausreicht oder ob es eines gesetzgeberischen Handelns bedarf. Die Bedeutung der Beantwortung dieser Frage geht dabei über den rein kommerziellen Bereich der Datenerhebung und Datenweiterverarbeitung weit hinaus. Sie ist beispielsweise auch für die Mandatierung des Rechts auf informationelle Selbstbestimmung im Rahmen einer arbeitsvertraglichen Beziehung oder im Rahmen der Verarbeitung von personenbezogenen Daten durch staatliche Behörden von Relevanz.

---

[1] Siehe dazu Blankertz A.; von Braunmühl P.; Kuzev P.; Richter F.; Richter H.; Schallbruch M. (2020): Datentreuhandmodelle - Themenpapier. Mimeo.

Der zweite Fragenkomplex geht den grundsätzlichen Fragen nach, welche volkswirtschaftliche Funktion den Datentreuhändern in der Welt der Datenökonomie zukommt, und welche ökonomischen Voraussetzungen dafür gegeben sein müssen. Zu den Grundvoraussetzungen für eine funktionierende Datentreuhänderschaft gehören die wirtschaftliche Unabhängigkeit der Datentreuhänder von Dienste-Anbietern und eine hinreichende Finanzierungsgrundlage.

Die Tatsache, dass sich die Datentreuhänderschaft bislang noch nicht in nennenswertem Umfang als marktgängige Dienstleistung etabliert hat, könnte ein Hinweis auf Störungen der Funktionalität von Märkten sein. Denkbar ist beispielsweise, dass Streitwerte im Zusammenhang mit der Wahrnehmung des Rechts auf informationelle Selbstbestimmung bei der Nutzung von Online-Diensten zu niedrig ist, um für kommerzielle Anwaltskanzleien lukrativ zu sein. Dem könnte mit einer geeigneten Form der öffentlichen Förderung von Datentreuhändern begegnet werden. Einmal etabliert, könnten Datentreuhänder aufgrund ihrer Verhandlungsmacht auch eine finanzielle Beteiligung von Online-Dienste-Nutzern am kommerziellen Ertrag der durch sie generierten Daten erstreiten und damit einen Beitrag zur Umverteilung der Gewinne zwischen Datenverarbeitern und Datengebern leisten.

In volkswirtschaftlicher Hinsicht geht es allerdings noch um mehr als nur die Wahrnehmung unmittelbarer Einzelinteressen der Dienste-Nutzer. Auch Wettbewerbsgesichtspunkte spielen hier eine Rolle. Auf dem Markt für datenbasierte Dienste haben sich relativ rasch monopolartige Strukturen herausgebildet, die eine Etablierung von neu in den Markt eintretenden Dienste-Anbietern erheblich behindern. Da die Monopolisten offenbar nur zu prohibitiv hohen Preisen bereit sind, den Datenzugang für potenzielle Wettbewerber zu öffnen, steht zur Debatte, die Dienste-Anbieter gesetzlich dazu zu verpflichten, Nutzerdaten in anonymisierter Form als öffentliches Gut für an der Entwicklung neuer Online-Dienste interessierten Unternehmen zur Verfügung zu stellen. Datentreuhänder könnten in diesem Zusammenhang gefordert sein, die Wahrung der Interessen der ursprünglichen Datenerzeuger zu überwachen.

2. Rechtliche Analyse

Prof. Dr. Jürgen Kühling, LL.M.
Dr. Florian Sackmann

Im Folgenden ist es zunächst erforderlich, in einem ersten Schritt die Vielfalt der verschiedenen Konzepte und Modelle der Datentreuhänder nicht nur in der Realwelt, sondern auch in der (rechtswissenschaftlichen) Literatur aufzubereiten (dazu Abschnitt 2.1). Davon ausgehend wird in einem weiteren Schritt untersucht, inwiefern das geltende Datenschutzrecht eine entsprechende Ausübung wesentlicher Gestaltungsrechte (Einwilligung, Betroffenenrechte etc.) durch einen Datentreuhänder zulässt (dazu Abschnitt 2.2). Mit umgekehrter Blickrichtung ist dann zu fragen, ob ein Ausschluss der Bevollmächtigung von Datentreuhändern über AGB möglich ist und welche korrelierenden vertraglichen Abwehrinstrumente insoweit bestehen (dazu Abschnitt 2.3). Schließlich sind die Anforderungen an die Datensicherheit in Bezug auf Datentreuhänder von Interesse (dazu Abschnitt 2.4). Dasselbe gilt für die Frage nach deren Verantwortung und Haftung (dazu Abschnitt 2.5).

Nach dieser Untersuchung des geltenden Rechts ist sodann zu klären, inwiefern etwaige Defizite einer normativen Anpassung bedürfen, um die Durchsetzung von Datentreuhänder-Modellen zu erleichtern und wenn ja, ob dies im EU-Recht oder im deutschen Recht zu erfolgen hat (dazu Abschnitt 2.6).

Im Ausblick sollen anschließend an die umfassenden Ausführungen zu den Vorgaben des allgemeinen Datenschutzrechts zu Datentreuhändern noch zwei Spezialbereiche betrachtet und auf ihr Potenzial für Datentreuhänder-Modelle „abgeklopft“ werden, nämlich der Sozial- und der Beschäftigtendatenschutz (dazu Abschnitt 2.7).

2.1 Konzepte der Datentreuhänder in der (rechtswissenschaftlichen) Literatur

Ausgehend von knappen Hinweisen zur heterogenen Nutzung des Begriffs des Datentreuhänders und unterschiedlichen bereits anzutreffenden Business-Modellen in der Realwelt (dazu 2.1.1) werden auch in der (juristischen) Literatur eine Vielfalt verschiedener Konzepte und Modelle der Datentreuhänder diskutiert. Vor diesem Hintergrund ist eine präzise Beschreibung des Betrachtungsgegenstandes für die vorliegende Untersuchung erforderlich (dazu 2.1.2).

2.1.1 Unterschiedliche Verwendung des Begriffs des Datentreuhänders und heterogene Business-Modelle in der Realwelt

In der Realwelt lassen sich bereits verschiedene Business-Modelle und demzufolge teils gänzlich unterschiedliche Konzepte von Datentreuhändern beobachten. Der verbindende Kern dieser sehr heterogenen Anwendungsfälle ist die Einschaltung eines Dritten.

Bis vor Kurzem etwa vermarktete Microsoft ein Cloud-Angebot für datenschutzbewusste deutsche Unternehmen als Datentreuhänder-Modell. Allerdings ging es nur darum, dass die gespeicherten Daten in Rechenzentren der Deutschen Telekom und damit auf europäischem Territorium verarbeitet werden und Mitarbeiter von Microsoft hierauf nur im Ausnahmefall Zugriff erhalten. Gleichwohl hat dieses Angebot in der juristischen Fachliteratur und auch in der Datenschutzpraxis Aufmerksamkeit erlangt, ging es doch um die spannende Frage, inwiefern dadurch die Daten vor extraterritorialen Zugriffen US-amerikanischer Ermittlungsbehörden

geschützt werden können.[2] Dies entspricht jedoch nicht dem vorliegenden Verständnis von „Datentreuhändern".

Das gilt auch für die im Zuge der Gestaltung des autonomen Fahrens teilweise anzutreffende Verwendung des Begriffs des „Datentreuhänders" für Anwendungsfälle, in denen die Kfz-Daten bei einer neutralen Stelle gespeichert werden, um bei einem Unfall einen privilegierten Zugang einer der Parteien (Fahrzeugführer/Hersteller) zu vermeiden.[3]

Ausgangspunkt ist also in diesen Konstellationen stets, dass ein Datentreuhänder als dritte Person zwischen verschiedene Akteure geschaltet wird. Dies gilt auch für Angebote, die in der Praxis anzutreffen sind, um das Datenschutzmanagement als Mittler für die Betroffenen zu verbessern, und die im Fokus der vorliegenden Untersuchung stehen. Ein zentraler Aspekt ist dabei oftmals eine Unterstützung bei der Abgabe von Einwilligungserklärungen im Sinne des Betroffenen. Jene Angebote sind in Deutschland teils aus Forschungsprojekten heraus entstanden.[4] Dem vorliegenden Verständnis eines Datentreuhänders nahe kommen etwa Angebote wie „MyData.org". Kerngedanke der Dienste jener Non-Profit-Organisation ist es, Betroffene transparent darüber zu informieren, wer was wann über sie weiß, ihnen zu helfen, festzulegen, wer die Daten nutzen darf, und diese Entscheidungen im Laufe der Zeit einfach anpassen zu können.[5] Dabei sollen auch Schnittstellen mit Daten verarbeitenden Unternehmen und anderen Akteuren hergestellt werden, so dass eine Kollaboration zwischen dem Intermediär auf beiden Seiten – Verantwortliche und Betroffene – erfolgen soll, im beiderseitigen Interesse aber primär zur Verwirklichung der informationellen Selbstbestimmung der Betroffenen. Teilweise fokussieren einzelne Anbieter auch auf spezifische Teilelemente, indem sie etwa Daten ankaufen, anonymisieren und weiterverkaufen. So wirbt der Anbieter „Datacoup" damit, dass die Internet-Giganten persönliche Daten wie ein öffentliches Gemeingut zu ihren Gunsten ausgebeutet haben, ohne die Betroffenen an den dabei entstehenden Gewinnen angemessen zu beteiligen. Deshalb will „Datacoup" die Betroffenen als Intermediär bei der Monetarisierung unterstützen.[6] Etwas abweichend davon, aber von der Zielrichtung durchaus vergleichbar, fokussiert das Diensteangebot von „Weople" vor allem darauf, in großem Umfang das Recht auf Datenportabilität aus Art. 20 DS-GVO für die Betroffenen geltend zu machen, um diese Daten anschließend anonymisiert und unter Beteiligung der Betroffenen am Gewinn zu kommerzialisieren.[7]

---

[2] Dazu ausführlich auch unter Analyse der umstrittenen rechtlichen Bewertung in der US-amerikanischen Gerichtspraxis Schwartz/Peifer, Datentreuhändermodelle – Sicherheit vor Herausgabeverlangen US-amerikanischer Behörden und Gerichte?, CR 2017, S. 165 ff.; vgl. ferner Rath/Kuß/Maiworm, Die neue Microsoft Cloud in Deutschland mit Datentreuhand als Schutzschild gegen NSA & Co.? Eine erste Analyse des von Microsoft vorgestellten Datentreuhänder-Modells, CR 2016, S. 98 ff.

[3] Siehe dazu die Analyse bei Brockmeyer, Treuhänder für Mobilitätsdaten – Zukunftsmodell für hoch- und vollautomatisierte Fahrzeuge? Erwägungen zur ausstehenden Regulierung des Speicherorts für die Daten nach § 63a Abs. 1 StVG, ZD 2018, S. 258 ff.

[4] Siehe insoweit die Darstellung bei Horn/Riechert/Müller, in: Stiftung Datenschutz (Hrsg.), Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen, 2017, S. 12 ff., abrufbar im WWW unter der URL https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_Studie_Neue_Wege_zur_Einwilligung_final.pdf (zul. aufgerufen am 12.8.2020), unter Hinweis insbesondere auf digi.me, LETsmart (Legalisation, Exchange, Transparency), Constent Management for Federated Data Sources (CoMaFeDS), MesInfos, Mydata, MyPermissions, Accesss my Info, Citizenme, Datacoup, personiq, PGuard, Humada, Consberry.

[5] Siehe nähere Informationen im WWW abrufbar unter https://mydata.org/mydata-101/ (zul. aufgerufen am 12.8.2020).

[6] Siehe nähere Informationen im WWW abrufbar unter https://datacoup.com/#first-stop (zul. aufgerufen am 12.8.2020).

[7] Siehe nähere Informationen im WWW abrufbar unter https://weople.space/en/ (zul. aufgerufen am 12.8.2020).

2.1.2 Begriffselemente eines „Datentreuhänders“ im vorliegenden Kontext und Modelle/Konzepte in der (rechtswissenschaftlichen) Literatur in Deutschland

In der vorliegenden Betrachtung geht es von diesen zuletzt genannten, exemplarischen ersten „Business“-Modellen für Datentreuhänder ausgehend spezifisch um Intermediäre zwischen den beiden Hauptakteuren des Datenschutzrechts, nämlich den Datenverarbeitern einerseits und den betroffenen Personen andererseits. Nach dem hier zugrunde liegenden Verständnis wird der Datentreuhänder als Vertrauensperson von der betroffenen Person eingesetzt, um die informationelle Selbstbestimmung einschließlich kommerzieller Verwertungsinteressen des Persönlichkeitsrechts gegenüber den Verantwortlichen besser wahrzunehmen.[8] Dies ist etwa denkbar, um Daten an einen Datentreuhänder als Mittelsmann zu übergeben, der sie pseudonymisiert und anschließend dem Verantwortlichen zur Verfügung stellt. Damit kann beispielsweise gewährleistet werden, dass, wenn keine Re-Pseudonymisierung möglich ist, die Daten für den dritten Verantwortlichen gar keine personenbezogenen Daten darstellen. Dieser Dritte kann dann mit den – für ihn nicht personenbezogenen – Daten ohne die Restriktionen des Datenschutzrechts agieren. Darüber hinaus kann der Datentreuhänder umfassender in die Datenschutzpräferenzen des Betroffenen eingeweiht werden, um anschließend als Agent für diesen eingesetzt zu werden. So kann der Betroffene die informationelle Selbstbestimmung mit Blick auf die Vielzahl von Datenverarbeitungsprozessen bei der Nutzung diverser Angebote im Internet besser wahrnehmen und von einer Vielzahl von datenschutzrechtlich relevanten Aktionen – insbesondere von Einwilligungserklärungen, aber auch der Nutzung von Betroffenenrechten – entlastet werden. Das ist gerade auch mit Blick auf die immer schnelleren, umfangreicheren und häufigeren Datenverarbeitungsprozesse und erst recht beim Einsatz von Künstlicher Intelligenz von Relevanz. Zugleich soll es dabei insbesondere um die kollektive Durchsetzung des Datenschutzrechts durch Datentreuhänder gehen.

Mit diesem Begriffsverständnis besteht eine weitreichende Überlappung mit dem verbreiteten Verständnis der sogenannten „Personal Information Management Systems (PIMS)“. Im Ausgangspunkt geht es bei entsprechenden Diensteanbietern vor allem um ein besseres Management der Einwilligung – gerade in ihrer dynamischen Perspektive – und der Datenschutzpräferenzen. Zugleich können diese jedoch gleichermaßen auf weitere Datenschutzrechte wie die Betroffenenrechte erweitert werden.[9]

Die Komplexität der datenschutzrechtlichen Anforderungen hängt dabei stark davon ab, in welchem Umfang der Datentreuhänder selbst Daten der Betroffenen verarbeitet. So ist denkbar, dass der Diensteanbieter – gleichsam wie die Einstellungen im Browser – nur sehr grob den Betroffenen bei der Durchsetzung seiner Datenschutzpräferenzen unterstützt und daher nur in geringem Umfang Daten der Betroffenen verarbeitet und insbesondere nicht mit den umfangreichen Daten, die anschließend von den dritten Verantwortlichen verarbeitet werden, „in Berührung“ kommt. Lediglich bei sehr einfach strukturierten Angeboten, die etwa tatsächlich nur die Datenschutzpräferenzen im Auftrag der betroffenen Person an die Verantwortlichen

---

[8] Siehe dazu etwa das Verbraucherzentrale Bundesverband, Positionspapier vom 19.2.2020, abrufbar im WWW unter der URL https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (zul. aufgerufen am 12.8.2020).

[9] Siehe dazu insbesondere Verbraucherzentrale Bundesverband, Positionspapier vom 19.2.2020, S. 7 f., abrufbar im WWW unter der URL https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (zul. aufgerufen am 12.8.2020); siehe ferner Europäische Kommission, An emerging offer of „personal information management services“, 2016, abrufbar im WWW unter der URL https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=40118 (zul. aufgerufen am 12.8.2020) und Datenethikkommission, Gutachten der Datenethikkommission der Bundesregierung, 2019, S. 133 f., abrufbar im WWW unter der URL https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.pdf (zul. aufgerufen am 12.8.2020); Europäischer Datenschutzbeauftragter, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), Stellungnahme 9/2016, S. 6, abrufbar im WWW unter der URL https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_de.pdf (zul. aufgerufen am 12.8.2020).

übermitteln, könnte sich im Einzelfall die Verarbeitung auf Kontaktdaten der betroffenen Person und deren Präferenzen beschränken. Insoweit ist allerdings schon fraglich, ob dann überhaupt der Begriff des Datentreuhänders gerechtfertigt ist.

Schon der exemplarische Aufriss zumindest der ersten kommerziellen Diensteanbieter zeigt jedenfalls, dass das Angebotsspektrum eines typischen Datentreuhänders eher darüber hinaus geht und dieser zumindest in Teilen für die Bereitstellung seiner Dienste im größeren Umfang Daten der Betroffenen verarbeiten muss, wenn er diese etwa anonymisiert kommerzialisieren, nur konditioniert zur Verfügung stellen, die Rechtmäßigkeit von Datenverarbeitungsprozessen überwachen und Rechtsverstöße geltenden machen möchte, sei es im Rahmen der Ausübung der Betroffenenrechte (etwa Löschansprüche) oder etwa bei der Durchsetzung von Schadensersatzansprüchen. Diese „anspruchsvolleren" Aufgabenspektren der tatsächlich bereits im Markt befindlichen bzw. denkbaren Diensteanbieter werden im Folgenden stärker fokussiert, da sie die komplexeren rechtlichen Herausforderungen mit sich bringen.

Zu dem hier zugrunde gelegten Verständnis der „Datentreuhänder" fehlt es bislang an vertieften rechtswissenschaftlichen Untersuchungen, die über grobe Problem- und Lösungshinweise hinausgehen. Letztere sind bislang auch eher von Institutionen entwickelt worden.[10] Eine wissenschaftliche Diskussion in entsprechenden rechtswissenschaftlichen Publikationsorganen ist hingegen – soweit ersichtlich – bislang nicht erfolgt. Insoweit leistet die folgende Untersuchung „Pionierarbeit".

2.1.3 „Kontrollblick über den Atlantik": US-amerikanische Literatur

Der Vollständigkeit halber sei darauf hingewiesen, dass auch ein exemplarischer Blick in die US-amerikanische rechtswissenschaftliche Literatur einen überschaubaren Befund geliefert hat. Zwar sind hier durchaus einzelne Aufsätze in relevanten Journals publiziert, die das Thema der Datentreuhänder („Trustee") im Fokus haben und in teils interessante Kontexte, wie der Bedeutung zur Vertrauensgewährleistung („trust") in einer Welt des „Überwachungs-kapitalismus" („surveillance capitalism"[11]), rücken.[12] Sehr grundlegend haben etwa *Kang/Shilton/Estrin/Burke/Hansen* als Ergebnis eines interdisziplinären Projekts ein Plädoyer für Datentreuhänder entwickelt, die als „Privacy Data Guardian" die Daten Privater („Privacy Data Vaults") verwalten und eine stärker selbstbestimmte Datenverarbeitung ermöglichen sollen. Allerdings fokussiert dieser Beitrag primär Daten, die durch die Betroffenen selbst erhoben werden, etwa durch „Wearables" („self-surveillance"), und weniger die größere Herausforderung beim Einsatz gegenüber Dritten, die Daten erheben („third-party surveillance"). Zudem behandelt der Beitrag allenfalls am Rande die rechtlichen Hindernisse und etwaige Lösungsansätze. In der kritischen Reaktion auf diesen Beitrag ist daher die Frage aufgeworfen worden, ob bei der Datenverarbeitung durch Dritte diese einer strengeren Regulierung unterworfen werden sollten oder ob nicht eine Regulierung zwischengeschalteter Intermediäre zweckdienlicher ist. Der konkretere regulatorische Ansatz wird aber auch in diesem Beitrag von *Peppet* nicht näher ausbuchstabiert.[13] Ähnlich und auch mit einem spezifischen Fokus – nämlich

---

[10] Siehe dazu insbesondere die in den Fn. 4 und 9 zitierten Studien und Stellungnahmen.

[11] Der Begriff wurde geprägt von Zuboff, The Age of Surveillance Capitalism. The Figth for a Human Futer at the New Frontier of Power, 2019 (deutsche Ausgabe: Das Zeitalter des Überwachungskapitalismus, 2019); siehe auch als Kurzfassung dies., Surveillance Capitalism – Überwachungskapitalismus, APuZ 2019, S. 4.

[12] Zu letzterem etwa Richards/Hartzog, Taking Trust Seriously in Privacy Law, 19 Stan. Tech. L. Rev. 2016, S. 431; siehe ähnlich auch Waldman, Privacy as Trust: Sharing Personal Information in a Networked World, 69 U Miami L Rev 2015, S. 559.

[13] Peppet, Privacy & the Personal Prospectus: Should We Introduce Privacy Agents or Regulate Privacy Intermediaries, Iowa Law Review Bulletin 97 2012/2013, S. 77.

auf die Datenschutzrichtlinien des Unternehmens – nähert sich *Regan* dem Thema mit einer grundlegenden Analyse der Zweckmäßigkeit eines öffentlichen Datentreuhänder-Modells („Public Trustee Concept").[14]

Insgesamt ist demnach der Blick in die US-amerikanische Literatur für die theoretisch-konzeptionelle Analyse von Datentreuhänder-Modellen durchaus interessant, hilft jedoch bei der Identifikation normativer bzw. regulatorischer Herausforderungen und erst recht bei deren Bewältigung nur begrenzt weiter.

2.2 Datenschutzrechtliche Anforderungen an die Übertragung wesentlicher Gestaltungsrechte an Datentreuhänder

Mit Blick auf die Frage, inwiefern das geltende Datenschutzrecht eine entsprechende Ausübung wesentlicher Gestaltungsrechte durch einen Datentreuhänder zulässt, ist zunächst darauf hinzuweisen, dass der Datentreuhänder bereits sehr frühzeitig vor der ersten Datenverarbeitung durch dritte Verantwortliche eingesetzt werden kann. Dann geht es in materiell-rechtlicher Hinsicht v.a. um die Frage, inwieweit der Verantwortliche in die Erteilung der Einwilligung gegenüber den dritten Verantwortlichen nach Art. 7 DS-GVO für die Betroffenen eingeschaltet werden kann (dazu 2.2.1). Insofern ist gleichsam eine doppelte Legitimation der Datenverarbeitung erforderlich, nämlich einerseits die des Datentreuhänders selbst für dessen Datenverarbeitung und andererseits in Bezug auf dessen Rolle in der Legitimation der Datenverarbeitung durch dritte Verantwortliche. Vor allem um Letzteres geht es im Folgenden. In prozeduraler Perspektive steht die Ausübung der Betroffenenrechte im Vordergrund (dazu 2.2.2). Die Geltendmachung dieser Rechte ist sowohl in der Fallkonstellation denkbar, dass der Datentreuhänder – wie soeben skizziert – von vornherein in die Datenverarbeitung einbezogen wird und für die Betroffenen beispielsweise bereits das Einwilligungsmanagement gegenüber den dritten Verantwortlichen übernommen hat. Dann kann der Datentreuhänder in der Folge etwa durch die Nutzung von Auskunftsansprüchen kontrollieren, ob sich die dritten Verantwortlichen rechtskonform verhalten und sodann gegebenenfalls entsprechende Löschungsansprüche etc. geltend machen. Aber auch in der Variante, dass der Datentreuhänder erst später eingeschaltet wird, kann dies sehr hilfreich sein, um etwa die Rechtmäßigkeit zu überprüfen oder die Betroffenenrechte geltend zu machen.

2.2.1 Vermittlung der datenschutzrechtlichen Einwilligung über Datentreuhänder

Für die Bewertung einer Übertragung datenschutzrechtlicher Gestaltungsrechte an Datentreuhänder ist zu differenzieren. Stellt ein Datentreuhänder etwa nur ein Tool zur Verfügung, um dem Nutzer einen besseren Überblick über die bei unterschiedlichen Verantwortlichen verarbeiteten Daten zu bieten und diesen Prozess besser zu steuern, so ist das unproblematisch. Letztlich agiert der Diensteanbieter in diesem Fall lediglich als „Bote" des Nutzers, übermittelt also eine fremde Einwilligungserklärung. Dann sind die rechtlichen Herausforderungen gering, aber es liegt auch nur ein sehr begrenztes Aufgabenspektrum des Diensteanbieters vor, so dass durchaus fraglich ist, ob insoweit überhaupt von einem Datentreuhänder gesprochen werden sollte (siehe dazu bereits soeben unter 2.1.2). Komplexer werden die Fragen, wenn dem Datentreuhänder ein eigener Entscheidungsspielraum zusteht, er also eine eigene Einwilligung im fremden Namen abgibt und somit als „Stellvertreter" des Nutzers auftritt oder aber die datenschutzrechtlichen Gestaltungsrechte an sich selbst abtreten lässt und dann im eigenen Namen agiert (zur Übertragbarkeit auf die Ausübung der

[14] Siehe insbesondere Regan, Reviving the Public Trustee Concept and Applying It to Information Privacy Policy, Maryland Law Review 76 2017, S. 1025.

Betroffenenrechte und den Widerruf der Einwilligung auch für die Fallkonstellation der späteren Einschaltung des Datentreuhänders, siehe unten 2.2.2). Letztlich sind die denkbaren Konstellationen und Geschäftsmodelle noch zu unabsehbar, als dass eine Einordnung in die entsprechenden Kategorien möglich oder sinnvoll wäre. Für die rechtliche Bewertung ist insoweit auch nur von Bedeutung, welche Anforderungen an die Übertragung der Wahrnehmung von Rechten an einen Datentreuhänder zu stellen sind, dem selbst ein gewisser Entscheidungsspielraum zusteht. Diese Frage wird im Folgenden analysiert.

2.2.1.1 Prinzipielle Vertretungsmöglichkeit; allgemeine Anforderungen für Datentreuhänder

In Bezug auf die Einwilligung ergeben sich aus allgemeinen Grundsätzen dabei nähere Überlegungen zur Person des Einwilligenden, die so nicht ausdrücklich in der DS-GVO geklärt wurden. So umfasst das Recht auf informationelle Selbstbestimmung grundsätzlich auch die Befugnis des Einzelnen, zu entscheiden, ob er dieses Recht höchstpersönlich oder unter Einschaltung eines Vertreters ausüben möchte. Jedoch gelten für die Erteilung einer entsprechenden Vollmacht – soweit übertragbar – dieselben Voraussetzungen wie sie auch für die Einwilligung selbst gelten. Daher muss auch die Vollmacht insbesondere zweckbestimmt erteilt werden (dazu näher 2.2.1.3). Eine Generalvollmacht zur umfassenden und unbegrenzten Wahrnehmung des Rechts auf informationelle Selbstbestimmung wäre wegen Unbestimmtheit unwirksam. Ferner muss die Vollmacht ebenso wie die Einwilligung in informierter Weise erteilt werden (dazu näher 2.2.1.2) – jedenfalls insoweit, als die betroffene Person selbst eine Vorstellung von den grundsätzlichen Rahmenbedingungen haben muss, unter denen der Vertreter eine Einwilligung mit Wirkung für und gegen sie erteilt. Darüber hinaus gilt für die Vollmacht, ebenso wie für die Einwilligung selbst, der Grundsatz der jederzeitigen freien Widerrufbarkeit (dazu näher 2.2.1.4). Schließlich sind die Besonderheiten beim Einsatz im Rahmen der Verwaltung von Daten von Kindern zu beachten (dazu 2.2.1.5).

Im Übrigen müssen die weiteren Wirksamkeitsvoraussetzungen des Art. 7 Abs. 4 i.V.m. Art. 4 Nr. 11 DS-GVO erfüllt sein. Die Freiwilligkeit der Einwilligung weist dabei für sich betrachtet keine zusätzlichen Herausforderungen auf, da – gerade im Fall der Entwicklung verschiedener Treuhänder-Modelle[15] – die Betroffenen eine Auswahl bekommen und im Übrigen jederzeit auch auf das Einschalten eines Treuhänders verzichten können. Auch die Transparenz muss im Rahmen der Ausgestaltung der Einwilligungserklärung gewährleistet sein, so dass – trotz fehlenden Schriftformerfordernisses – angesichts der Komplexität nur eine schriftliche Einwilligung in Betracht kommt. Diese muss schon wegen des Nachweisbarkeitserfordernisses (Art. 7 Abs. 1 DS-GVO) angemessen dokumentiert werden, was jedoch ohnehin schon aus Transparenzgesichtspunkten von den Datentreuhändern gewährleistet sein sollte.

2.2.1.2 Herausforderung 1: Informiertheit der Einwilligung

Größere Schwierigkeiten mit Blick auf Datentreuhänder-Modelle wirft das im Unionsrecht in Art. 4 Nr. 11 DS-GVO ebenfalls geforderte Maß an hinreichender Informiertheit des Einwilligenden auf. Dies ist schon für einzelne Anbieter mit komplexen Datenschutzerklärungen und schwer verständlichen Datenverarbeitungsprozessen oftmals problematisch. Wenn nun der Datentreuhänder darüber hinaus in Bezug auf eine Vielzahl derartiger Akteure das Einwilligungsmanagement übernehmen soll, potenziert sich grundsätzlich das Ausmaß an Informationen. Wie hier der Spagat zwischen einer möglichst umfassenden Information des Betroffenen auf der einen und der Vermeidung der Überforderung auf der anderen Seite bewerkstelligt werden kann, lässt sich nicht abstrakt-generell beantworten. Vielmehr wird es hier

[15] Sollte es zu einem monopolistischen Anbieter kommen, wären allerdings besondere Anforderungen mit Blick auf das Koppelungsverbot nach Art. 7 Abs. 4 DS-GVO zu beachten; dazu und zum Folgenden Kühling/Klar/Sackmann, Datenschutzrecht, 4. Aufl. 2018, Rn. 499 ff.

an den Datentreuhändern liegen, entsprechende Informationsmechanismen zu entwickeln, die eine Komplexitätsreduktion vorsehen, aber gleichwohl das Ziel der Informiertheit erreichen. Gerade darum geht es ja im Kern bei Datentreuhänder-Modellen. So sollen die Betroffenen einerseits entlastet werden. Andererseits kann nur eine betroffene Person, die alle entscheidungsrelevanten Informationen kennt, Risiken und Vorteile der Einwilligung abschätzen und eine darauf basierende Entscheidung treffen. Ihre Einwilligung kann sich auch nur auf die Umstände beziehen, die ihr bekannt sind. In eine unbestimmte Datenverwendung kann sie daher nicht wirksam einwilligen. Die Datentreuhänder trifft daher wie jeden Verantwortlichen eine umfassende Informationspflicht, insbesondere hinsichtlich der Arten von verarbeiteten Daten, des Verarbeitungszwecks, der Identität des Verantwortlichen und dessen Erreichbarkeit und an welche Empfänger ggf. Daten übermittelt werden, die er *vor* Einholung der Einwilligung erfüllen muss (vgl. im Einzelnen Art. 12 und 13 DS-GVO).[16]

Der Datentreuhänder kann insoweit als Ausgangsquelle nur die Informationen der dritten Verantwortlichen verwenden und muss und darf sich grundsätzlich auf deren Richtigkeit verlassen. Die Schwierigkeit wird sodann darin bestehen, diese gegebenenfalls heterogenen Datenverarbeitungszwecke, Empfänger von Daten etc. in einem weiteren Schritt zu aggregieren und gleichwohl für die Betroffenen so aufzubereiten, dass ein hinreichendes Maß an Informiertheit gewährleistet wird. Nur in den bereits oben erwähnten sehr einfachen Fällen (siehe 2.1.2) von Diensteangeboten, die bestimmte Datenverarbeitungszwecke auszuschließen versuchen (etwa die Weitergabe von Daten an weitere Verantwortliche oder der pauschale Ausschluss einer Datenverarbeitung etwa zu Werbezwecken), sind die korrelierenden Einwilligungserklärungen deutlich weniger komplex. Allerdings stellt sich hier nicht nur die Frage der Marktgängigkeit eines solchen Diensteangebotes, sondern auch die nach einem effektiven Einsatz, da derartige Nutzerpräferenzen gegebenenfalls zum Ausschluss vom Dienstenangeboten führen können, ohne dass diese Fragen vorliegend abstrakt-generell bewertet werden kann.

Unabhängig davon lässt sich dabei nicht näher eingrenzen, welches Maß an Konkretheit erforderlich ist. Hier wird vielmehr im Rahmen der Entwicklung der Geschäftsmodelle der Daten-treuhänder deren Kreativität gefragt sein, die insoweit – im Zweifel im Kontakt mit den Datenaufsichtsbehörden – belastbare Ansätze entwickeln müssen. So stellt beispielsweise bereits die Pflicht zur Benennung der „Empfänger oder Kategorien von Empfängern“ nach Art. 13 Abs. 1 lit. e DS-GVO die dritten Verantwortlichen vor nicht unerhebliche Anforderungen: Sind bereits konkrete Empfänger zum Zeitpunkt der Einwilligungserteilung bekannt, müssen diese auch benannt werden. Ist insoweit dagegen eine gewisse Dynamik vorbehalten, reicht es, die Kategorien von Empfängern zu benennen.[17] Dies wird auch für den Datentreuhänder gelten, dem gegebenenfalls noch etwas größere Flexibilitätsspielräume zu gewähren sind.

Mit Blick auf das Ziel eines möglichst dynamischen Einsatzes von Datentreuhändern, müssen diese grundsätzlich auch sinnvolle Aktualisierungsmechanismen entwickeln.

---

[16] Vgl. Buchner/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 59 f.

[17] Bäcker, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 13 DS-GVO Rn. 29 f.

2.2.1.3 Herausforderung 2: (Zweck-)Bestimmtheit der Einwilligung

Gerade wenn die eingesetzten Technologien dynamische Einwilligungen ermöglichen sollen, wird die ohnehin schon komplexe Frage der Bestimmtheit der Einwilligung gegenüber dem Datentreuhänder besonders virulent. Letztlich geht es dabei auch um die Möglichkeit etwaiger Zweckänderungen. Insoweit ist in der DS-GVO jedenfalls eine gewisse Flexibilisierung angelegt.

Das Erfordernis der Bestimmtheit der Einwilligungserklärung (Art. 5 Abs. 1 lit. b und Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO), das sich unmittelbar aus dem Zweckbindungsgrundsatz ableitet,[18] steht dabei in engem Zusammenhang mit der Informiertheit. Die betroffene Person kann nur dann die Vorteile und Risiken der Einwilligung einschätzen, wenn sie zum einen in der Lage ist, den Inhalt der Einwilligung zu verstehen und wenn zum anderen die Einwilligungserklärung hinreichend konkret abgefasst ist. Blankoeinwilligungen und pauschal gehaltene Einwilligungserklärungen sind unwirksam.[19]

Dies ist bei einem Datentreuhänder, der über eine Einwilligung eine Vielzahl von Datenverarbeitungsprozessen einer Vielzahl anderer Verantwortlicher legitimieren soll, eine große Herausforderung. Auch insoweit müssen die Treuhänder komplexitätsreduzierende und dynamische Erläuterungsmechanismen entwickeln.

Denn um dem Gebot der Bestimmtheit zu genügen, sind nicht nur die Daten oder die Art der Daten zu benennen, sondern grundsätzlich auch die einzelnen konkreten Phasen der Datenverarbeitung. Das erforderliche Maß an Bestimmtheit lässt sich allerdings nur in der Zusammenschau mit der konkreten Verarbeitungssituation ausmachen. Bei einer Vielzahl von – unter Umständen auch noch komplexen – Verarbeitungsphasen kann nicht die Benennung eines jeden einzelnen Verarbeitungsschrittes gefordert werden. Es reicht dann aus, wenn die relevanten, für die Beurteilung der Tragweite der Erklärung wesentlichen Phasen der Verarbeitung beschrieben sind. Ein gewisser Grad an Unvollständigkeit muss dann schon aus Gründen der Klarheit und der Verständlichkeit hingenommen werden. Umgekehrt sind an das Maß an Bestimmtheit umso höhere Anforderungen zu stellen, je mehr der Persönlichkeitsschutz der betroffenen Person berührt wird.[20]

Dies kann gerade bei Datentreuhändern, die zur besseren Verwirklichung des Selbstbestimmungsrechts der betroffenen Personen eingesetzt und gegebenenfalls durch sinnvolle Kontrollmechanismen (etwa eine Governance-Struktur, die das auch absichert) überprüft werden, gewisse Vereinfachungen ermöglichen, während gegenüber Verantwortlichen, die in egoistischem Interesse handeln, eher keine Erleichterungen denkbar sind. Denn das Gebot der Bestimmtheit ist kein Selbstzweck, sondern soll der Verwirklichung des Datenschutzrechts bzw. des informationellen Selbstbestimmungsrechts dienen. Wenn Datentreuhänder gerade diesen Zweck verfolgen, muss eine an diesem Ziel orientierte Auslegung und Anwendung der normativen Anforderungen an die Einwilligung dies auch ermöglichen. Daher dürften insoweit Datentreuhänder zu privilegieren sein, die auf die Verfolgung der Interessen der Betroffenen fokussiert sind. So könnte beispielsweise eine Differenzierung nach den Zwecken der Datenverarbeitung erfolgen und der Betroffene beispielsweise weiter reichende Datenverarbeitungen zur Verfolgung „wissenschaftlicher Zwecke“ legitimieren, da hier gerade auch die DS-GVO Privilegierungen vorsieht (Stichwort „Broad Consent“). So kann eine Einwilligung in die

---

[18] Buchner/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 61.

[19] So zum BDSG a.F. BGH, Urteil vom 19.9.1985, III ZR 213/83 = BGHZ 95, S. 362 (367 f.); Urteil vom 10.7.1991, VIII ZR 296/90 = BGHZ 115, S. 123 (127); Urteil vom 11.12.1991, VIII ZR 4/91 = BGHZ 116, S. 268 (273).

[20] Zum BDSG a.F. Holznagel/Sonntag, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 4.8 Rn. 49.

Datenverarbeitung zu Forschungszwecken „breiter“ und damit unbestimmter ausfallen, wenn die Unbestimmtheit der Einwilligung durch technisch-organisatorische Maßnahmen zum Schutz der betroffenen Personen kompensiert wird.[21] Hier werden sich die Details aber erst in Reaktion auf entsprechende Treuhänder-Modelle in der Realität und deren Bewertung durch Datenschutzaufsichtsbehörden entwickeln können. Diese Entwicklung könnte durch klarstellende Hinweise in entsprechenden aufsichtsbehördlichen Dokumenten unterstützt werden (etwa des Europäischen Datenschutzausschusses zur Einwilligung, siehe dazu unten 2.7.2.3).

Sofern Datentreuhänder auch Gesundheitsdaten oder andere besondere Kategorien personenbezogener Daten verwalten, muss sich die Einwilligung gemäß Art. 9 Abs. 2 lit. a DS-GVO zudem ausdrücklich auf diese Daten beziehen.

2.2.1.4 Herausforderung 3: jederzeitige Widerrufbarkeit der Einwilligung

Ganz allgemein stellt das Erfordernis der jederzeitigen Widerrufbarkeit von Einwilligungserklärungen bei bereits begonnener Datenverarbeitung ein Problem dar; bei Datentreuhändern verschärft sich dieses. Die unter dem BDSG a.F. vertretene Auffassung, dass die betroffene Person nur widerrufen konnte, wenn ihr das Festhalten an der Einwilligung objektiv nicht länger zuzumuten war, etwa weil der Verantwortliche die vom Einwilligungsinhalt gezogenen Verarbeitungsgrenzen überschritt oder erforderliche Maßnahmen zur Datensicherheit nicht durchführte oder angesichts sensibler Daten ein Entscheidungswandel den überwiegenden berechtigten Interessen der betroffenen Person entsprach,[22] stößt sich an der Vorgabe der jederzeitigen Widerrufbarkeit in Art. 7 Abs. 3 S. 1 DS-GVO. Andererseits findet sich der Grundsatz von Treu und Glauben auch in der DS-GVO wieder (Art. 5 Abs. 1 lit. a DS-GVO). Ob sich Einschränkungen vor dem Hintergrund dieser scharfen Formulierung weiterhin aufrechterhalten lassen, ist gleichwohl zweifelhaft. Überzeugend erscheint es aber durchaus, jedenfalls in umfassenden Vertragsverhältnissen gewisse Einschränkungen im Interesse der Praktikabilität zuzulassen.[23] Unklar ist erst recht, inwiefern das für Datentreuhänder gilt. Auch insoweit wären allerdings klärende Hinweise von den Aufsichtsbehörden für Datentreuhänder hilfreich.

Im Übrigen gilt: Auch soweit ein Datentreuhänder erst involviert wird, wenn bereits eine Einwilligung unmittelbar von der betroffenen Person erteilt wurde, kann es Aufgabe des Datentreuhänders sein, die Rechtmäßigkeit der erteilten Einwilligung zu prüfen oder aber deren Widerruf zu erklären. Insoweit gelten für den Widerruf gleichsam als actus contrarius spiegelbildlich dieselben Anforderungen wie bei der Erteilung der Einwilligung selbst. Gerade durch den drohenden Widerruf für eine Vielzahl von Kunden kann ein Datentreuhänder auch eine erhebliche Verhandlungsmacht gegenüber den dritten Verantwortlichen ausüben.

2.2.1.5 Besonderheiten beim Einsatz im Rahmen der Verwaltung von Daten von Kindern

Angesicht der vielfältigen Angebote im Internet stellt sich schließlich die Frage, ob Datentreuhänder auch im Rahmen der Vertretung bei der Erteilung der Einwilligung von Kindern eingesetzt werden können. Hier sieht die DS-GVO in Art. 8 ausdrücklich Fälle vor, in denen es um die personenbezogenen Daten von Kindern geht, denen direkt sog. Dienste der Informationsgesellschaft angeboten werden.[24] Die Einwilligung muss hier nach Art. 8 Abs. 1 DS-

---

21 Buchner/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 64.

22 Vgl. zur Rechtslage unter dem BDSG a.F. Simitis, in: Simitis (Hrsg.), Kommentar zum BDSG, 8. Aufl. 2014, § 4a Rn. 99 f.; dem auch unter der DS-GVO folgend Schaffland/Holthaus, in: Schaffland/Wiltfang (Hrsg.), DS-GVO/BDSG, EL 10/17 Stand: Dezember 2017, Art. 7 DS-GVO Rn. 55.

23 Vgl. dazu Buchner/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 38 ff.

24 Buchner/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 8 DS-GVO Rn. 20 f.

GVO durch den Träger der elterlichen Verantwortung erteilt werden. Alternativ ist auch eine persönliche Einwilligung durch das Kind möglich, dann jedoch mit Zustimmung des Trägers elterlicher Verantwortung. Selbst einwilligungsfähig sind Kinder nach Art. 8 Abs. 1 DS-GVO erst ab Vollendung des 16. Lebensjahres. Diese Vorgaben gelten im Fall des Einsatzes eines Datentreuhänders gleichermaßen. Auch hier könnten Datentreuhänder sogar ein besonderes Potenzial entfalten, da sie die Träger der elterlichen Verantwortung von teils – zeitlich und/oder fachlich – überfordernden Legitimationsentscheidungen entlasten und viel besser eine strukturierende Legitimation generieren können.

2.2.2 Ausübung der Betroffenenrechte durch Datentreuhänder

Der Einsatz von Datentreuhändern erscheint sodann für die Ausübung sämtlicher Betroffenenrechte attraktiv. Als erstes sind hier das Recht auf Löschung (Art. 17 DS-GVO) und der Auskunftsanspruch (Art. 15 DS-GVO) zu nennen. So kann gerade durch die technische Versiertheit eines eingeschalteten Intermediärs eine intervallartige Kontrolle im Rahmen der Ausübung eines Auskunftsanspruchs erfolgen, welche Daten über die betroffene Person verarbeitet werden. Je stärker eine Automatisierung derartiger Kontrollanfragen erfolgt, desto eher kann sodann auch ein Abgleich unter Rechtsmäßigkeitsgesichtspunkten erfolgen (beispielsweise: Wurde die Einwilligung der Datenverarbeitung nicht bereits widerrufen?). Dieser Abgleich kann in der Folge kombiniert werden mit einem etwaigen Löschungsanspruch im Fall der rechtswidrigen Datenverarbeitung und insbesondere Datenspeicherung. Sollten fehlerhafte Daten identifiziert werden, könnte (automatisiert) das Recht auf Berichtigung (Art. 16 DS-GVO) bzw. im Streitfall eine Einschränkung der Verarbeitung (Art. 18 DS-GVO) bzw. das Widerspruchsrecht nach Art. 21 DS-GVO geltend gemacht werden.

Die Darstellung bereits angebotener Dienste lässt zudem erkennen, dass – gerade unter kommerziellen Gesichtspunkten – die Geltendmachung des Rechts auf Datenübertragbarkeit nach Art. 20 DS-GVO als Ansatzpunkt für die Kommerzialisierung des informationellen Selbstbestimmungsrechts sinnvoll sein kann. Dabei kann sich das Recht auf Datenportabilität als wirkungsvoller Hebel herauskristallisieren, um die Etablierung von Datentreuhänder-Modellen zu erleichtern. So müssen nach Art. 20 Abs. 1 DS-GVO die Daten der Betroffenen vom Verantwortlichen „ohne Behinderung“ durch diesen bereitgestellt werden. Dieses Behinderungsverbot kann positiv die Beseitigung technischer Hürden verlangen, so dass eine einfache Datenübertragung an den Datentreuhänder über geeignete Schnittstellen im Rahmen der Anwendung jener Norm erzwungen werden kann. Auch insoweit wären entsprechende Hinweise der Aufsichtsbehörden in Leitlinien spezifisch zu Datentreuhändern zu diesem Themenkomplex oder in den allgemeinen Leitlinien etwa zu Art. 20 DS-GVO mit näheren Hinweisen zu Datentreuhändern hilfreich (dazu unten allgemein 2.6.5).

Es zeigt sich damit, dass für alle Betroffenenrechte ein relevantes Potenzial für den Einsatz von Datentreuhändern besteht. Rechtlich erhebliche Probleme bei der Geltendmachung dieser Betroffenenrechte durch Datentreuhänder sind nicht ersichtlich. Denn im Ansatzpunkt gilt hier dasselbe wie in Bezug auf die Einwilligung. So gebietet es die informationelle Selbstbestimmung nachgerade, dass diese Rechte grundsätzlich auch über einen Vertreter geltend gemacht werden können. Allerdings fehlt hier eine entsprechende Diskussion in der Literatur wie bei der Einwilligung. Ergänzend sei darauf hingewiesen, dass für die Betroffenenrechte in Art. 23 DS-GVO eine (begrenzte) Öffnungsklausel für mitgliedstaatliche Regelungen greift. Vorliegend relevante Spezifika, die im nationalen Datenschutzrecht zu abweichenden Besonderheiten führen, sind jedoch nicht ersichtlich.

2.2.3 Geltendmachung von Schadensersatzansprüchen durch den Datentreuhänder

Der Datentreuhänder kann auch einen etwaigen Schadensersatz in der Folge von Datenschutzverstößen des Verantwortlichen für seine Nutzer mit geltend machen. Diese Möglichkeit ergibt sich bereits aus dem nationalen Recht durch die Instrumente der Stellvertretung oder der Abtretung. Problematisch ist dabei, dass ein geschäftliches Anbieten solcher Dienstleistungen den Restriktionen des grundsätzlichen Rechtsberatungsprivilegs der Rechtsanwaltschaft unterfällt. Diese kann wiederum eine Beratung gegen Erfolgshonorar nur unter den sehr eingeschränkten Möglichkeiten des § 4a BRAO anbieten. Bei Schäden nach Datenschutzverstößen handelt es sich jedoch um typische Streuschäden, die für den einzelnen Geschädigten kaum jemals wirtschaftlich individuell verfolgt werden können.

Art. 80 Abs. 1 DS-GVO schafft daher einen Rahmen für die Vertretung durch bestimmte Einrichtungen, Organisationen und Verbände, deren Tätigkeit ansonsten das Rechtsdienstleistungsgesetz entgegenstehen könnte. Dafür muss es sich allerdings um „eine Einrichtung, Organisationen oder Vereinigung ohne Gewinnerzielungsabsicht, die ordnungsgemäß nach dem Recht eines Mitgliedstaats gegründet ist, deren satzungsmäßige Ziele im öffentlichem Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist“, handeln. Diese Voraussetzung erfüllen in Deutschland etwa die Verbraucherzentralen. Für solche Entitäten normiert Art. 80 Abs. 1 DS-GVO eine unmittelbare unionsrechtliche Erlaubnis zur Erbringung außergerichtlicher Rechtsdienstleistungen i.S.v. § 3 RDG.[25] Für alle anderen Datentreuhänder bedarf es abhängig vom jeweiligen Geschäftsmodell noch einer eigenen gesetzlichen Regelung der diesbezüglichen Berechtigung. Die Beschränkung auf bestimmte Entitäten bzw. das Erfordernis eines spezifischen gesetzlichen Zulässigkeitstatbestandes verhindert daher wirksam, dass Datentreuhänder missbräuchlich und im Eigeninteresse zur Gewinnerzielung Schadensersatzansprüche unter erleichterten Voraussetzungen durchsetzen können. Ein echtes Verbandsklagerecht nach Maßgabe von Art. 80 Abs. 2 DS-GVO wurde im deutschen Recht hingegen nur in Ansätzen im UKlaG eingeführt und bleibt auf besondere Fälle beschränkt.[26]

2.3 Ausschluss der Bevollmächtigung von Datentreuhändern in den AGB von Verantwortlichen

Um Datentreuhänder-Modellen zum Durchbruch zu verhelfen, müssen diese am Markt akzeptiert werden und auch durchsetzbar sein. Dies kann gefährdet sein, wenn die Verantwortlichen den Einsatz von Datentreuhändern etwa mittels Allgemeinen Geschäftsbedingungen zu verhindern suchen. Das kann gegebenenfalls aus dem Interesse heraus erfolgen, dass sie durch Datentreuhänder „ertüchtigte“ betroffene Personen weniger leicht „übervorteilen“ können, da diese plötzlich „auf Augenhöhe“ mit ihnen agieren. Derartige Klauseln in Allgemeinen Geschäftsbedingungen, die die Inanspruchnahme von Diensten etwa davon abhängig machen, dass der Nutzer sich individuell registriert, also seine Daten ohne Einschaltung eines Datentreuhänders bereitstellt („Abwehrklauseln“), sind daher ein realistisches Szenario. Die Verwendung solcher Klauseln begegnet aus mehreren rechtlichen Gesichtspunkten Bedenken.

---

[25] Bergt, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 80 DS-GVO Rn. 19.

[26] Dazu Bergt, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 80 DS-GVO Rn. 13 und 18.

2.3.1 Recht der Allgemeinen Geschäftsbedingungen (§§ 305 ff. BGB)

Auch für datenschutzrechtlich Verantwortliche gilt der grundrechtlich verbürgte Schutz der Privatautonomie aus Art. 2 Abs. 1 des Grundgesetzes und die daraus resultierende Vertragsfreiheit. Sie können daher grundsätzlich freiverantwortlich darüber entscheiden, mit wem und unter welchen Voraussetzungen sie Verträge schließen wollen. Einen allgemeinen Kontrahierungszwang gibt es also gerade nicht. Auch der Nutzer muss jedoch freiverantwortlich entscheiden können, ob und ggf. zu welchen Konditionen er Geschäfte abschließen möchte. Das kann in der Praxis jedoch nicht immer gewährleistet werden, denn das Informations- und Motivationsgefälle zwischen AGB-Verwender und Kunden führt zu einem partiellen Marktversagen:[27] Für den Nutzer sind die Transaktionskosten für einen Vergleich unterschiedlicher Vertragsbedingungen verschiedener Anbieter zu hoch, so dass es für ihn letztlich nur wirtschaftlich ist, das Vertragswerk des Anbieters widerspruchslos zu akzeptieren oder ganz vom Vertragsschluss abzusehen.[28] Um dieser Problematik zu begegnen, sieht das Bürgerliche Gesetzbuch in den §§ 305 ff. Regelungen zum Schutz des Vertragspartners vor.

An diesen Regelungen müssen sich auch die eingangs skizzierten „Abwehrklauseln" datenschutzrechtlich Verantwortlicher gegen die Einschaltung von Datentreuhändern messen lassen. Dabei wird im Folgenden davon ausgegangen, dass tatsächlich Allgemeine Geschäftsbedingungen vorliegen, also für eine Vielzahl von Verträgen vorformulierte Vertragsbedingungen, die eine Vertragspartei (Verwender) der anderen Vertragspartei bei Abschluss eines Vertrags stellt (§ 305 Abs. 1 S. 1 BGB). Individualabreden mit einzelnen Nutzern (§ 305 Abs. 1 S. 3 BGB) sind insoweit nicht relevant, da sie einerseits kaum praktikabel umzusetzen wären und andererseits auch die Verbreitung von Datentreuhänder-Modellen nicht ernstlich behindern würden.

2.3.1.1 § 305c Abs. 1 BGB

Eine Abwehrklausel würde dann nicht wirksamer Bestandteil des Vertrages, wenn diese so ungewöhnlich ist, dass der Vertragspartner des Verwenders mit ihr nicht zu rechnen braucht („überraschende Klausel"). Dabei kommt es grundsätzlich auf die Vorstellungen und Erwartungen an, die sich ein durchschnittlich geschäftserfahrener und redlicher Kunde mit der gehörigen Aufmerksamkeit und Umsicht vom Inhalt des Vertrages gebildet hätte. Für die Vorstellungen und Erwartungen des Kunden gilt demnach ein durch subjektive Umstände überlagerter generalisierender objektiver Maßstab. Letztlich ist das wesentliche ausschlaggebende Kriterium allerdings, ob der Klausel ein „Überrumpelungseffekt" innewohnt. Aus der systematischen Stellung der Vorschrift ergibt sich, dass im Kern verhindert werden soll, dass dem Vertragspartner des Verwenders eine Klausel durch die Gestaltung des Vertrages „untergeschoben" werden soll.

Unter Anwendung der dargelegten Grundsätze wäre eine Abwehrklausel gegenüber Datentreuhändern wohl tendenziell nicht als überraschende Klausel zu qualifizieren. Zwar sind derartige Klauseln derzeit noch nicht gebräuchlich und wären folglich ungewöhnlich. Allerdings ist das für die Annahme einer überraschenden Klausel nicht hinreichend. Sobald sich allerdings Datentreuhänder-Modelle am Markt etabliert haben und weitere Verbreitung gefunden haben, könnte dies anders zu bewerten sein. Letztlich wird zunächst aber eher die Inhaltskontrolle (dazu sogleich) der entscheidende Maßstab sein müssen. Einen relevanten Unterschied macht das vorliegend gleichwohl eher nicht, da die Einschaltung bzw. Zulassung eines Datentreuhänders keine vertragliche Hauptleistungspflicht sein kann und daher die Einschränkung, dass über die

---

[27] Basedow, in: MüKo-BGB, 8. Aufl. 2019, vor § 305 Rn. 6.

[28] Basedow, in: MüKo-BGB, 8. Aufl. 2019, vor § 305 Rn. 7 f.

Inhaltskontrolle nicht die Angemessenheit der Hauptleistungspflichten geprüft werden kann, nicht zum Tragen kommt.

2.3.1.2 § 307 Abs. 1 S. 1 BGB

Vor diesem Hintergrund kommt der Inhaltskontrolle unter der Generalklausel des § 307 Abs. 1 BGB eine besondere Bedeutung zu. Demnach sind Bestimmungen in Allgemeinen Geschäftsbedingungen unwirksam, wenn sie den Vertragspartner des Verwenders entgegen den Geboten von Treu und Glauben (§ 242 BGB) unangemessen benachteiligen. Ob eine Klausel den Vertragspartner unangemessen benachteiligt, ist eine Frage des Einzelfalls. Im Kern geht es um einen umfassenden Interessenausgleich zwischen Verwender und Vertragspartner.[29] Damit bildet die Generalklausel das Kernstück des AGB-Rechts.[30] Es sind für die Bewertung einer Klausel zunächst die wechselseitigen Interessen zu eruieren und sodann zu gewichten. So hat einerseits der Verwender durchaus ein berechtigtes Interesse „an der Klarheit und Übersichtlichkeit der Vertragsabwicklung".[31] Insofern ist es nicht von vornherein unzulässig, in Allgemeinen Geschäftsbedingungen etwa ein vertragliches Abtretungsverbot vorzusehen mit dem Ziel, nicht mit wechselnden Gläubigern konfrontiert zu werden.[32] Gegenläufig hat jedoch auch der Nutzer als Vertragspartner ein erhebliches Interesse an der Einschaltung eines Datentreuhänders, da er seine Rechte so sehr viel effektiver wahrnehmen kann.

Abwehrklauseln können den Vertragspartner daher – abhängig vom Einzelfall – unangemessen benachteiligen (§ 307 Abs. 1 BGB), insbesondere wenn dieser ohne die Einschaltung eines Datentreuhänders seine Rechtsposition nicht angemessen wahrnehmen kann. Der Nutzer muss also, will der Verwender in seinen AGB die Einschaltung eines Treuhänders verhindern, obwohl diese genau da ansetzen und ihm Technologien an die Hand geben sollen, um einfacher ein eigenverantwortliches Management der personenbezogenen Daten durchführen zu können, effektive Möglichkeiten haben, über die Verwendung seiner Daten zu bestimmen. Da die Interessengewichtung sehr stark vom konkreten Modell und der jeweiligen Ausgestaltung der Datentreuhänderschaft abhängt, ist eine pauschale Aussage über die Zulässigkeit von Abwehrklauseln nicht seriös möglich.

Auch eine spezifische Kasuistik zu Abwehrklauseln gegenüber Datentreuhändern hat sich bisher in der Rechtsprechung noch nicht herausgebildet. Es gibt jedoch vergleichbare Konstellationen, in denen Verwender versuchen, die schlagkräftigere kollektivierte Wahrnehmung von Interessen durch spezialisierte Anbieter zu verhindern. Diese insoweit ergangenen Entscheidungen versprechen daher auch für die vorliegende Konstellation einen Erkenntnisgewinn. Mit der Betrauung eines Datentreuhänders mit der Wahrnehmung von Rechten vergleichbar ist die Situation der Geltendmachung von Leistungsstörungsrechten im Reiserecht und dort insbesondere im Flugreiserecht: Für einen einzelnen Reisenden ist es verhältnismäßig schwierig, berechtigte Ansprüche gegen Reiseanbieter durchzusetzen. Dies liegt an der geringen Forderungshöhe im Einzelfall und einem Informationsgefälle. Insbesondere Entschädigungsansprüche wegen Flugannullierung nach Art. 7 der EU-Fluggastrechte-Verordnung[33] erfordern häufig umfassendes Wissen, wenn sich die betroffene Fluggesellschaft auf außergewöhnliche

---

29 Vgl. BT-Drs. 7/3919, S. 22.

30 Vgl. BT-Drs. 7/3919, S. 22.

31 So explizit BGH, Urteil vom 17.4.2012 - X ZR 76/11, Rn. 9; so auch LG Nürnberg-Fürth, Hinweisbeschluss vom 30.7.2018, Az. 5 S 8340/17, Rn. 19.

32 BGH, Urteil vom 17.4.2012 - X ZR 76/11, Rn. 9.

33 Verordnung (EG) Nr. 261/2004 des Europäischen Parlaments und des Rates vom 11.2.2004 über eine gemeinsame Regelung für Ausgleichs und Unterstützungsleistungen für Fluggäste im Fall der Nichtbeförderung und bei Annullierung oder großer Verspätung von Flügen und zur Aufhebung der Verordnung (EWG) Nr. 295/91.

Umstände nach Art. 5 Abs. 3 der Verordnung beruft. In Summe sind die Ansprüche aller Reisenden jedoch durchaus von Relevanz. Diese Gemengelage hat dazu geführt, dass sich als Inkassodienstleister im Sinne des Rechtsdienstleistungsgesetzes organisierte Plattformen wie etwa flightright.de (sog. Claim-Handling-Companies) etabliert haben. Diese machen gegen eine Erfolgsprovision die Ansprüche für den Reisenden geltend. Abhängig vom Geschäftsmodell erfolgt dies entweder durch eine entsprechende Bevollmächtigung oder aber durch Abtretung der Ansprüche an den Claim-Handler. Die Claim-Handling-Companies erzielen in der Summe durchaus gewichtige Entschädigungsansprüche von den Fluggesellschaften. Letztere sind teilweise dazu übergegangen, in ihren Allgemeinen Geschäftsbedingungen entsprechende Abtretungsverbote vorzusehen. In diesen Klauseln hat jedoch die Rechtsprechung in Teilen eine unangemessene Benachteiligung erkannt.[34]

Auch bei Datentreuhändern liegt das Prinzip in der Anspruchs- und Kompetenzbündelung durch Einschaltung Dritter. Insoweit ist die Interessenlage der Beteiligten durchaus vergleichbar. Zwar stellen die Entscheidungen zum Abtretungsverbot bei Flugreiseverträgen teils spezifisch auf die Wertungen der Fluggastrechte-Verordnung und deren Zielsetzung eines hohen Verbraucherschutzniveaus ab.[35] Gleichwohl liegen letztlich auch dem Datenschutzrecht ähnliche Wertungen zugrunde, wie sich aus den Erwägungsgründen 6 und insbesondere 142 der DS-GVO ergibt. Gerade der zuletzt genannte Erwägungsgrund macht deutlich, dass auch eine aggregierte Interessenvertretung der Betroffenen – vergleichbar den Verbraucherschutzverbänden zur Durchsetzung des Verbraucherschutzes – durch die DS-GVO institutionell erleichtert werden soll. Wie beim Verbraucherschutz geht es also auch um den Ausgleich eines Verhandlungsungleichgewichts – dort zwischen Unternehmen und Verbrauchern, hier zwischen Verantwortlichen und Betroffen. Datentreuhänder können bei der Ertüchtigung der Position der Betroffenen und damit bei der Verringerung des Verhandlungsungleichgewichts eine entscheidende Rolle spielen und dabei auch die wirtschaftlichen Interessen der Betroffenen als kommerzielle Dimension des informationellen Selbstbestimmungsrechts schützen.

Nicht zuletzt deshalb sprechen gute Gründe für die Annahme einer unangemessenen Benachteiligung im Sinne von § 307 Abs. 1 S. 1 BGB im Falle von Abwehrklauseln gegen Datentreuhänder. Anders könnte das Ergebnis hingegen ausfallen, wenn der Verantwortliche eigens Schnittstellen für den Datentreuhänder bereitstellen muss. Insoweit sei nur am Rande bemerkt, dass sich schon aus dem Recht auf Datenportabilität tendenziell die Verpflichtung ergibt, jedenfalls Schnittstellen zur Übermittlung der Daten an Datentreuhänder vorzusehen (dazu oben 2.2.2). Gegebenenfalls könnten sich im Weiteren sogar noch allgemeiner die Bereitstellung von Schnittstellen als gute Datenschutzpraxis entwickeln, so dass auch die etwaige Notwendigkeit der Schaffung solcher Schnittstellen keinen hinreichenden Grund für die Verwendung von Abwehrklauseln mehr darstellen würde. Letztlich ist die rechtliche Bewertung der Abwehrklauseln stark von der konkreten Ausgestaltung und der Situation im Einzelfall abhängig. Solange jedoch der Datentreuhänder für den Verantwortlichen keinen relevanten Mehraufwand verursacht, spricht viel dafür, dass Abwehrklauseln in den AGB des Verantwortlichen unwirksam wären.

2.3.1.3 § 307 Abs. 2 Nr. 1 BGB

Als weiterer Prüfungsmaßstab kommt auch die Vorschrift des § 307 Abs. 2 Nr. 1 BGB in Betracht, nach welcher Klauseln unwirksam sind, die „mit wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird, nicht zu vereinbaren“ sind, denn das (grundrechtlich

[34] So etwa LG Nürnberg-Fürth, Hinweisbeschluss vom 30.7.2018, Az. 5 S 8340/17; siehe ferner AG Hannover, Urteil vom 8.2.2012, 531 C 10491/11.

[35] LG Nürnberg-Fürth, Hinweisbeschluss vom 30.7.2018, Az. 5 S 8340/17, Rn. 17.

vorgeprägte) gesetzgeberische Leitbild einer informationellen Selbstbestimmung legt das Verfügungsrecht in die Hände der betroffenen Person. Diese muss daher in der Lage sein, über die Ausübung ihrer datenschutzrechtlichen Rechte auch dergestalt zu disponieren, dass sie ein Dritter ausüben darf. Letztlich stellt sich daher die Frage, ob die erforderliche Freiwilligkeit einer datenschutzrechtlichen Einwilligung auch bedingt, dass die Ausübung datenschutzrechtlicher Rechte auf einen Dritten übertragen werden kann (dazu sogleich).[36]

2.3.2 Datenschutzrechtlicher Freiwilligkeitsvorbehalt der Einwilligung (Art. 7 DS-GVO)

Allgemeine Geschäftsbedingungen können nicht nur nach §§ 305 ff. BGB unwirksam sein, sondern auch dann, wenn sie gegen sonstiges zwingendes Recht verstoßen. Gemäß Art. 6 DS-GVO ist die Verarbeitung personenbezogener Daten nur zulässig, soweit eine Einwilligung vorliegt oder ein gesetzlicher Zulässigkeitstatbestand einschlägig ist.[37]

Art. 4 Nr. 11 DS-GVO definiert die Einwilligung als eine Willensbekundung, die freiwillig erfolgt. Die explizite Forderung der Freiwilligkeit der Einwilligung für ihre Wirksamkeit spiegelt die Erkenntnis aus der Rechtswirklichkeit wider, dass sich oftmals ungleiche Partner gegenüberstehen. Die Einwilligung des schwächeren Partners droht ihre Legitimationswirkung für den Eingriff in sein informationelles Selbstbestimmungsrecht zu verlieren, wenn er aufgrund der faktischen Verhältnisse gleichsam keine Wahl hat und einwilligen muss, um die begehrte Leistung, etwa einen Kredit, eine Versicherungspolice, einen Arbeitsplatz oder einen Versorgungsvertrag (Strom, Wasser) zu erhalten bzw. zu behalten.[38] Dasselbe gilt, wenn die betroffene Person durch „übermäßige Anreize finanzieller oder sonstiger Natur zur Preisgabe [ihrer] Daten verleitet wird".[39] Insgesamt sind für die Bewertung der Freiwilligkeit die Kriterien des Ungleichgewichts, der Erforderlichkeit, der vertragscharakteristischen Leistung, der zumutbaren Alternative und eines angemessenen Interessenausgleichs relevant.[40]

So kann eine Einwilligung unfreiwillig sein, wenn zwischen betroffener Person und Datenverarbeiter ein klares Ungleichgewicht besteht (vgl. Erwägungsgrund 43 der DS-GVO). Dies kann namentlich in Arbeitsverhältnissen, im Bürger-Staat-Verhältnis sowie bei Hinzutreten weiterer Umstände auch zwischen Unternehmer und Verbraucher der Fall sein.[41] In jüngerer Zeit führte das Bundesverfassungsgericht aus, dem Einzelnen müsse ein informationeller Selbstschutz auch tatsächlich möglich und zumutbar sein. Sei das nicht der Fall, bestehe eine staatliche Verantwortung, die Voraussetzungen selbstbestimmter Kommunikationsteilhabe zu gewährleisten. In einem solchen Fall könne der betroffenen Person staatlicher Schutz nicht unter Berufung auf eine nur scheinbare Freiwilligkeit der Preisgabe bestimmter Informationen versagt werden. Die aus dem Allgemeinen Persönlichkeitsrecht folgende Schutzpflicht gebiete den zuständigen staatlichen Stellen vielmehr, die rechtlichen Voraussetzungen eines wirkungsvollen informationellen Selbstschutzes bereitzustellen.[42] Ist es ersichtlich, dass in einem Vertragsverhältnis ein Partner ein solches Gewicht hat, dass er den Vertragsinhalt faktisch einseitig

---

[36] Siehe zu datenschutzrechtlichen Implikationen auf die Inhaltskontrolle auch Wurmnest, in: MüKo-BGB, 8. Aufl. 2019, § 307 Rn. 71.

[37] Die folgenden Absätze sind stark orientiert an Kühling/Klar/Sackmann, Datenschutzrecht, 4. Aufl. 2018, Rn. 499 ff.

[38] Vgl. Beschluss vom 25.3.1992, 1 BvR 1430/88 = BVerfGE 85, S. 386.

[39] BGH, Urteil vom 16.7.2008, VIII ZR 348/06 = BGHZ 177, 253, Rn. 21.

[40] Siehe dazu und zum Folgenden Buchner/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 41 ff.

[41] Vgl. Erwägungsgrund 43 der DS-GVO; dazu auch Buchner, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, S. 155 (158).

[42] BVerfG, Beschluss vom 23.10.2006, 1 BvR 2027/02 = BVerfGK 9, 353 = MMR 2007, S. 93 (93).

bestimmen kann, sei es Aufgabe des Rechts, auf die Wahrung der Grundrechtspositionen beider Vertragspartner hinzuwirken, um zu verhindern, dass sich für einen Vertragsteil die Selbstbestimmung in eine Fremdbestimmung verkehrt.[43] Auch wenn die DS-GVO als EU-Verordnung freilich nicht an den Maßstäben des Bundesverfassungsgerichts zu messen ist, dürften diese Grundsätze auch auf europäischer Ebene Anwendung finden. Für die Verwendung von Abwehrklauseln durch den Verantwortlichen kann diesen Maßstäben nur durch eine extensive Anwendung des Freiwilligkeitsvorbehalts der Einwilligung Rechnung getragen werden. Die Verwendung einer für die betroffene Person negative Klausel indiziert ein Verhandlungsungleichgewicht, das per se bereits die Wirksamkeit der Einwilligung in Frage stellt.

Mit Art. 7 Abs. 4 schreibt die DS-GVO die schon unter dem Regime von Richtlinie und nationalen Umsetzungsgesetzen[44] geltenden Grundsätze des sog. Koppelungsverbots fort und stellt auch sonst an die Freiwilligkeit der Einwilligung vergleichbare Anforderungen.[45] Das Koppelungsverbot wird verletzt, wenn die Erfüllung bzw. Eingehung eines Vertrages von einer Einwilligung abhängig gemacht wird, obwohl die Datenverarbeitung, in welche eingewilligt wird, für die Erfüllung des Vertrages nicht erforderlich ist.[46] Dem Datenverarbeiter ist es dabei zwar nicht versagt, seine Leistung von der Erteilung einer Einwilligung i.S.v. „take it or leave it" abhängig zu machen. Dafür müssen aber sämtliche Datenverarbeitungen, in die eingewilligt wird, für die Durchführung des Vertrages erforderlich sein.[47] Aus teleologischen Gesichtspunkten spricht viel dafür, diese Voraussetzung auch auf die konkreten Modalitäten der Datenverarbeitung zu erstrecken. Soweit also die Vertragsdurchführung auch unter Einbeziehung eines Datentreuhänders möglich wäre, kann die Erteilung der Einwilligung also richtigerweise nicht von der Akzeptanz der Abwehrklausel abhängig gemacht werden, ohne gegen das Koppelungsverbot zu verstoßen.

Die Regelungen zur datenschutzrechtlichen Einwilligung sind von der Stoßrichtung auch stark vergleichbar mit der eingangs skizzierten und ebenfalls unionsrechtlich vorgeprägten[48] AGB-Inhaltskontrolle. In beiden Fällen ist der Ausgangspunkt die Privatautonomie. Diese wird bei ungleichen Vertragspartnern gefährdet, da sich der unterlegene Teil letztlich nicht mehr wirklich frei entscheiden kann. Auch sind die Situationen insoweit vergleichbar, dass dem unterlegenen Teil häufig faktisch wenig Zeit bleibt, sich über die Tragweite seiner Erklärung klar zu werden. Insofern spricht einiges dafür, als wesentliches Kriterium für die Freiwilligkeit danach zu fragen, ob durch die Einwilligung die betroffene Person unangemessen benachteiligt wird (Rechtsgedanke des Art. 3 Abs. 1 der Richtlinie 39/13/EWG). Eine stark zulasten der betroffenen Person und gegen dessen objektive Interessen gerichtete Einwilligung indiziert subjektiv Zweifel an der Freiwilligkeit.[49] Je unvorteilhafter eine Einwilligung für die betroffene Person objektiv ist, umso mehr wird bei den anderen Kriterien kritisch zu prüfen sein, ob die Einwilligungserklärung wirklich Ausdruck einer freien Entscheidung der betroffenen Person ist. Im Ergebnis kann also nur dann von einer freien Entscheidung der betroffenen Person gesprochen werden, wenn die

---

43 BVerfG, Beschluss vom 23.10.2006, 1 BvR 2027/02 = BVerfGK 9, 353 = MMR 2007, S. 93 (93).

44 Vgl. insbesondere § 28 Abs. 3b BDSG a.F. sowie § 95 Abs. 5 TKG.

45 Vgl. Buchner/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 41 und 43; Buchner, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, S. 155 (158); sehr kritisch dazu Härting, Koppelungsverbot – der Einwilligungskiller nach der DS-GVO, CR-online.de Blog vom 11.10.2016, abrufbar im WWW unter der URL https://www.cr-online.de/blog/2016/10/11/ (zul. aufgerufen am 12.8.2020).

46 Vgl. Buchner, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, S. 155 (158); Heckmann/Paschke, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2017, Art. 7 Rn. 52.

47 Buchner/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 43.

48 Vgl. insoweit die Richtlinie 93/13/EWG des Rates vom 5.4.1993 über missbräuchliche Klauseln in Verbraucherverträgen.

49 In diese Richtung auch Buchner/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 54.

betroffene Person effektiv die Möglichkeit hat, selbst zu bestimmen, ob und wie ihre Daten verarbeitet werden.

Bereits die Tatsache, dass mittels Abwehrklauseln versucht wird, die Position der betroffenen Personen zu schwächen, ist ein starkes Indiz für eine Überlegenheit des Verantwortlichen. In diesem Zusammenhang ist zu berücksichtigen, dass die DS-GVO ausweislich ihres Erwägungsgrundes 6 ein hohes Datenschutzniveau auch in der Praxis sicherstellen möchte. Dies bedingt eine effektive Durchsetzung der prozeduralen Datenschutzrechte. Daher lässt sich insoweit auch der in Art. 80 DS-GVO sowie Erwägungsgrund 142 DS-GVO zum Ausdruck kommende Rechtsgedanke fruchtbar machen, dass der betroffenen Person die Wahrnehmung ihrer Rechte so einfach wie möglich gemacht werden soll. Abwehrklauseln zielen indes genau auf das Gegenteil. Die mit dem Ausschluss von Datentreuhändern verbundene objektive Erschwernis der Geltendmachung und Durchsetzung der Rechte der betroffenen Person spricht daher gegen eine wirklich freie Entscheidung der betroffenen Person. Daher kann eine Einwilligung unwirksam und in der Folge die Datenverarbeitung mit allen daraus folgenden Konsequenzen rechtswidrig sein, sofern nicht zusätzlich eine gesetzliche Rechtsgrundlage besteht. Will der Verantwortliche die Datenverarbeitung auf eine Einwilligung stützen, so muss er auf Abwehrklauseln gegenüber Datentreuhändern verzichten. Andernfalls besteht das erhebliche Risiko, dass die Datenverarbeitung von den Aufsichtsbehörden und ggf. den Gerichten als rechtswidrig eingestuft wird. In der Konsequenz drohen dann neben Bußgeldern in sehr signifikanter Höhe auch Schadensersatzansprüche der betroffenen Personen.[50]

2.3.3 Kartellrechtliches Missbrauchsverbot (Art. 102 Abs. 2 lit. a AEUV)

Bei marktbeherrschenden Unternehmen könnte derartigen Klauseln ferner das kartellrechtliche Missbrauchsverbot aus Art. 102 Abs. 2 lit. a AEUV entgegenstehen. In der Abwehrklausel kann eine Geschäftsbedingung zu erkennen sein, die aufgrund der marktbeherrschenden Stellung erzwungen wurde. Im Regelfall werden solche Abwehrklauseln nur von Unternehmen mit einer sehr starken Marktposition durchsetzbar sein. Letztlich hängt insoweit jedoch alles vom konkreten Einzelfall ab.

2.3.4 Zivilvertragliche Instrumente gegen Abwehrklauseln

Sollten sich Abwehrklauseln etablieren und entgegen der hier vertretenen Auffassung von der Rechtsprechung als wirksam angesehen werden, könnten Datentreuhänder ihrerseits durch Ausgestaltung ihrer Vertragsbedingungen versuchen, diese zu umgehen. Dabei muss zunächst differenziert werden, mit welcher zivilrechtlichen Handlungsform der Datentreuhänder dem Verantwortlichen gegenüber auftritt. So kommt neben einer Abtretung von Ansprüchen (§ 398 S. 1 BGB) insbesondere die Stellvertretung (§§ 164 ff. BGB) in Betracht (siehe zu diesen Gestaltungsmöglichkeiten trotz des höchstpersönlichen Charakters von Datenschutzrechten bereits oben 2.2). Bei der Abtretung wird der Anspruch durch den Datentreuhänder im eigenen Namen geltend gemacht. Tritt er lediglich im fremden Namen, also als Bevollmächtigter der betroffenen Person auf, so kommt einer Abwehrklausel von vornherein keine Wirkung zu, denn die Stellvertretung ist in §§ 164 ff. BGB für Willenserklärungen gesetzlich vorgesehen. Nichts anderes kann gelten, wenn sonstige datenschutzrechtliche Rechte im fremden Namen geltend gemacht werden. Da (und soweit) also eine Geltendmachung datenschutzrechtlicher Rechte in fremdem Namen zulässig ist (dazu 2.2), stellt sich die Problematik der Abwehrklauseln ohnehin nicht, denn eine Geltendmachung in fremdem Namen ist unproblematisch zulässig. Daher ergeben sich für

[50] Dazu bereits Kühling/Sackmann, Die Musterfeststellungsklage nach Datenschutzverstößen – ein unkalkulierbares Risiko für Unternehmen?, DuD 2019, S. 347.

Datentreuhänder in jedem Fall Möglichkeiten, auch bei der Verwendung von Abwehrklauseln – ihre Wirksamkeit im Gegensatz zu der hier vertretenen Ansicht unterstellt – für die Betroffenen zu agieren. Damit ist also ein „Businessmodell“ für die Datentreuhänder sicher möglich.

Aber auch eine darüber hinaus gehende rein faktische Abschreckungswirkung durch unwirksame AGB-Klauseln dürfte bei den durch die Datentreuhänder vertretenen Betroffenen wenig problematisch sein, da die Datentreuhänder im Regelfall über hinreichende Rechtskenntnis und entsprechende Ressourcen verfügen werden, um sich gegebenenfalls gegen derartige Klauseln juristisch zu erwehren. Soweit allerdings die betroffenen Personen bereits abgehalten werden, einen Datentreuhänder hinzuzuziehen, stehen hierfür die effektiven Mechanismen des Wettbewerbs- und Verbraucherschutzrechts zur Verfügung, um gegen die unwirksamen AGB-Klauseln vorzugehen.

2.3.5 Zwischenergebnis

Verantwortliche könnten versuchen, in ihren Allgemeinen Geschäftsbedingungen „Abwehrklauseln“ vorzusehen, um die Einschaltung eines Datentreuhänders auf Seiten der betroffenen Person zu verhindern. Derartige Klauseln sind richtigerweise als unwirksam anzusehen. Selbst wenn dies von der Rechtsprechung anders bewertet werden sollte als hier vertreten, so hat der Datentreuhänder durch ein Auftreten im fremden Namen die Möglichkeit, derartige Klauseln zu umgehen. Abwehrklauseln in Allgemeinen Geschäftsbedingungen dürften daher kein wesentliches Hindernis für die Etablierung von Datentreuhändern darstellen.

2.4 Anforderungen an die Datensicherheit; Datenschutz-Folgenabschätzung

2.4.1 Anforderungen an die Datensicherheit

Datentreuhänder-Modelle werden nur dann gesellschaftliche Akzeptanz finden, wenn von ihnen echte Verbesserungen für die Privatsphäre der Nutzer ausgehen. Das Vertrauen der Nutzer in die Integrität der beauftragten Datentreuhänder ist daher das entscheidende Gut. In den letzten Jahren hat sich gezeigt, dass gerade große Datenskandale in Folge von Datensicherheits-problemen in hohem Maße geeignet sind, Vertrauen zu erschüttern. Daher muss gerade bei Datentreuhändern ein besonderes Augenmerk auf die Datensicherheit gelegt werden.

Die zentrale Norm für die Sicherheit der Datenverarbeitung ist Art. 32 DS-GVO. Demnach müssen „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen [...] geeignete technische und organisatorische Maßnahmen [getroffen werden], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.“

Datentreuhänder können eine Vielzahl von Daten verwalten und verfügen darüber hinaus teilweise über weitere Zugangsmöglichkeiten bei anderen Verantwortlichen. Daher besteht für die Privatsphäre der betroffenen Personen ein erhebliches Risiko, wenn auf Datenbestände des Datentreuhänders unberechtigt Zugriff erlangt wird. Spiegelbildlich sind entsprechend des risikobasierten Ansatzes in Art. 32 DS-GVO für Datentreuhänder die Anforderungen an die IT-Sicherheit besonders hoch. Dabei muss der Datentreuhänder diesen strengen Anforderungen nicht nur genügen, sondern dies auch nachweisen können, Art. 5 Abs. 2 DS-GVO („Rechenschaftspflicht“). In der Praxis kann dieser Nachweis vor allem durch eine Zertifizierung (Art. 32 Abs. 3 DS-GVO) durch eine nach Art. 43 Abs. 1 S. 1 DS-GVO i.V.m. § 39 BDSG akkreditierte Zertifizierungsstelle gelingen, wobei nicht ersichtlich ist, dass dies durch einen Datentreuhänder bereits erfolgreich durchlaufen ist. Jedenfalls sollte sich die Zertifizierung auch auf die besondere Verantwortung eines Datentreuhänders beziehen. Mit der zunehmenden Etablierung von

Datentreuhänder-Modellen dürften sich also eigens auf diese abgestimmte Zertifizierungsprogramme herausbilden. Diese können etwa durch klar erkennbare Siegel bei den Nutzern zusätzliches Vertrauen schaffen.

2.4.2 Notwendigkeit bzw. Zweckmäßigkeit einer Datenschutz-Folgenabschätzung

Ergänzend ist darauf hinzuweisen, dass für Datentreuhänder die Durchführung einer Datenschutz-Folgenabschätzung indiziert sein kann. So schreibt die DS-GVO in Art. 35 für bestimmte Verarbeitungsvorgänge verpflichtend vor, dass der Verantwortliche eine Datenschutz-Folgenabschätzung vornimmt. Deren Ziel ist es, dass sich der Verantwortliche in besonders sensiblen Bereichen durch ein strukturiertes Verfahren über die möglichen Folgen der Datenverarbeitungsvorgänge bewusst wird.[51] Die Datenschutz-Folgenabschätzung ist eine vom Verantwortlichen vorzunehmende, strukturierte und dokumentierte Risikoanalyse und -bewertung. Sie hat nach Art. 35 Abs. 7 DS-GVO mindestens eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen zu enthalten. Ferner müssen dabei eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck sowie die Risiken für die Rechte und Freiheiten der betroffenen Personen erfolgen und die zur Bewältigung dieser Risiken vorgesehenen Abhilfemaßnahmen dargelegt und bewertet werden. Der Gesetzestext nennt in Art. 35 Abs. 3 DS-GVO drei (nicht abschließende) Beispiele, in denen eine Datenschutz-Folgenabschätzung durchzuführen ist.[52] Diese Fälle greifen nicht zwingend für jede denkbare Konstellation der Datentreuhänder. Umfasst das Angebot jedoch beispielsweise in relevantem Umfang Gesundheitsdaten, so ist die Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 Abs. 3 DS-GVO zwingend. Vor diesem Hintergrund wäre es denkbar, dass die Aufsichtsbehörden im Rahmen der Erstellung der Liste für Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung zwingend durchzuführen ist, klarstellen, in welchem Umfang dazu auch Datentreuhänder gehören. Schon jetzt kann durch die Art der vom Datentreuhänder verarbeiteten Daten einer der gelisteten Verarbeitungsvorgänge erfasst sein. Sofern beispielsweise der Datentreuhänder in relevantem Umfang Daten verarbeitet und dabei eine „(z)entrale Speicherung der Messdaten von Sensoren, die in Fitnessarmbändern oder Smartphones verbaut sind“, vornimmt, wäre er schon deshalb Adressat einer verpflichtenden Datenschutz-Folgenabschätzung.[53]

2.5 Verantwortung und Haftung von Datentreuhändern

Im Übrigen sind Haftungsfragen von großer Relevanz, da die jüngst im Rahmen der Datenschutzgrundverordnung und der Begleitgesetzgebung im BDSG vorgenommene massive Verschärfung der Haftung von Datenverarbeitern die Frage aufwirft, ob dadurch die Realisierbarkeit von Datentreuhänder-Modellen gefährdet wird. Dies ergibt sich gerade vor dem Hintergrund, dass Datentreuhänder regelmäßig nicht nur zwischen einer Vielzahl von Betroffenen und *einem* dritten Verarbeiter vermitteln, sondern der Idee nach zwischen einer

---

[51] Vgl. Jandt, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 35 DS-GVO Rn. 1; siehe hierzu und zum Folgenden auch Kühling/Klar/Sackmann, Datenschutzrecht, 4. Aufl. 2018, S. 284 ff.

[52] Vgl. dazu im Einzelnen instruktiv und mit Beispielen Art.-29-Datenschutzgruppe, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk“ for the purposes of Regulation 2016/679, WP 248, 4.4.2017.

[53] Siehe dazu Position 15 auf der Liste des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg, abrufbar im WWW unter der URL https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Liste-von-Verarbeitungsvorgängen-nach-Art.-35-Abs.-4-DS-GVO-LfDI-BW.pdf (zul. aufgerufen am 12.8.2020).

Vielzahl von Betroffenen und einer *Vielzahl* von dritten Verantwortlichen. Das potenziert die Haftungsrisiken (dazu 2.5.2). Insoweit ist die zunächst zu klärende Frage besonders virulent, ob die Datentreuhänder lediglich als Intermediär für die durch sie vorgenommene Datenverarbeitung im datenschutzrechtlichen Sinne verantwortlich sind und entsprechend haften oder ob sie darüber hinaus einer gemeinsamen Verantwortung mit den eigentlichen Datenverarbeitern – in ihrer unbegrenzten Vielzahl – unterliegen (dazu 2.5.1).

2.5.1 Qualifikation der Rolle des Datentreuhänders als gemeinsame Verantwortlichkeit, als getrennte Verantwortlichkeit bzw. als Auftragsverarbeitung

2.5.1.1 Datentreuhänder als Verantwortliche statt als Auftragsverarbeiter

Vorliegend wird für die Datentreuhänder eine bloße Auftragsverarbeitung ausscheiden. Denn dem Auftragsverarbeiter kommt keine Eigenverantwortlichkeit und keine Entscheidungsbefugnis zu, die seine Tätigkeit über die reine Hilfsfunktion im Rahmen fremder Zwecke hinausheben würde. Er fungiert im Verhältnis zum Verantwortlichen gleichsam als „Datensklave“ oder als „Marionette“.[54] Dies kommt auch in der Definition des Auftragsverarbeiters in Art. 4 Nr. 8 DS-GVO zum Ausdruck, wonach Auftragsverarbeiter jede natürliche und juristische Person, Behörde, Einrichtung oder andere Stelle ist, die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet. Der Verantwortliche ist hingegen in Art. 4 Nr. 7 DS-GVO legal definiert. Er umfasst jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Da aber gerade der Datentreuhänder das überlegene Wissen über die Mittel der Datenverarbeitung haben soll, scheidet grundsätzlich eine bloße Auftragsverarbeitung aus. Denn die Betroffenen erhoffen sich ja genau diese Erleichterung durch den Rückgriff auf jenen Intermediär mit überlegenen technischen Mitteln zur Sicherung der informationellen Selbstbestimmung der Betroffenen vom Einwilligungsmanagement bis zur Ausübung der Betroffenenrechte. Nur in den wenig relevanten Fällen, dass die Datentreuhänder nur ganz geringwertige Unterstützungsleistungen für die Betroffenen unter deren Weisung und bei geringfügiger Bestimmung über die einzusetzenden Mittel leisten (etwa in ganz einfachen Fällen des Einsatzes des Diensteanbieters zur Dokumentation und Durchsetzung von standardisierten Privatsphärepräferenzen, dazu bereits oben 2.1.2), kommt eine Auftragsverarbeitung in Betracht. Dann liegt aber letztlich im Kern kein Datentreuhänder-Modell vor.

---

[54] Vgl. Ernst, in: Paal/Pauly (Hrsg.), DS-GVO, Kommentar, 2017, Art. 4 Rn. 56; vgl. näher zum Begriff des Auftragsverarbeiters auch Art.-29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, WP 169, 16.2.2010.

2.5.1.2 Verarbeitung personenbezogener Daten durch Datentreuhänder sachlogisch nicht vermeidbar

Sodann ist darauf hinzuweisen, dass selbst Angebote, die gleichsam lediglich eine Filterfunktion für die Betroffenen einnehmen und für die wunschgemäße Datenverarbeitung sorgen, nach gegenwärtigem Erkenntnisstand – wiederum abgesehen von den bereits erwähnten ganz einfachen Diensteangeboten, bei denen die Einordnung als „Datentreuhänder" bereits fraglich ist (dazu oben 2.1.2) – nicht ohne substantielle eigene Datenverarbeitung möglich sind. Dies liegt nicht zuletzt am weiten Begriff der Datenverarbeitung. So fasst die DS-GVO unter dem Begriff der Verarbeitung in Art. 4 Nr. 2 eine Vielzahl von Verarbeitungsformen zusammen. Danach bezeichnet „Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. Dabei ist der erste Schritt eines idealtypischen Verarbeitungsvorgangs das Erheben oder Erfassen von personenbezogenen Daten. Anschließend können die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung oder die Einschränkung der Daten folgen. Zum Schluss steht das Löschen oder die Vernichtung der personenbezogenen Daten. Ohne eine dieser Formen des Umgangs mit Daten wird nach dem gegenwärtigen Stand der Technik jedenfalls kein substantielles Datentreuhänder-Modell aufsetzbar sein.

Theoretisch denkbar wäre zwar der intelligente Einsatz von Anonymisierungstechniken, um zu vermeiden, dass der Datentreuhänder überhaupt selbst mit personenbezogenen Daten in Kontakt kommt. Denn nach Erwägungsgrund 26 der DS-GVO gelten die Grundsätze des Datenschutzrechts nicht für anonyme Informationen, d.h. für Informationen, die sich (von vornherein) nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die (nachträglich) in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.[55] Dies dürfte angesichts der hohen Anforderungen an die Anonymisierung und der Weite des Begriffs der personenbezogenen Daten in Art. 4 Nr. 1 DS-GVO jedoch unter Wahrung eines relevanten Aufgabenbereichs des Datentreuhänders regelmäßig kaum möglich sein.

2.5.1.3 Niedrige Schwelle zur Annahme einer gemeinsamen Verantwortlichkeit der Datentreuhänder mit dritten Verantwortlichen

Viel relevanter ist daher die Frage, ob der Datentreuhänder unter der Prämisse einer substantiellen Aufgabenwahrnehmung jenseits seiner eigenen Verantwortlichkeit einer gemeinsamen Verantwortlichkeit mit den verschiedenen anderen dritten Verantwortlichen unterworfen wird, gegenüber denen er die Rechte der Betroffenen wahrnimmt. Das Risiko einer gemeinsamen Verantwortlichkeit ist bislang – soweit ersichtlich – noch gar nicht im Rahmen der Diskussion von Datentreuhändern vertieft worden. Hintergrund ist insoweit die ausufernde Rechtsprechung des EuGH zur gemeinsamen Verantwortlichkeit. Sie zwingt dazu, zu prüfen, welche Verantwortung den Datentreuhänder trifft, wenn dieser Daten an Verantwortliche übermittelt und jene Verantwortliche anschließend gegen Datenschutzbestimmungen in einer Art und Weise verstoßen, die vom Datentreuhänder hätte erkannt werden können. Insoweit könnte eine gesamtschuldnerische Haftung (Art. 26 Abs. 3 DS-GVO) des Datentreuhänders mit dem bzw. den Verantwortlichen die Attraktivität dieses Modells und damit ihre Etablierung am Markt deutlich erschweren.

---

[55] Ausführlich Klar/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 1 DS-GVO Rn. 31 ff.

Die jüngere Rechtsprechungslinie des EuGH zur gemeinsamen Verantwortlichkeit[56] ist dabei so zu verstehen, dass gemeinsam in die Datenverarbeitung eingeschaltete Entitäten im Zweifel auch als gemeinsam Verantwortliche anzusehen sind. Entscheidend ist eine hinreichende, gegebenenfalls auch nur teils überlappende und teils komplementäre Mitwirkung hinsichtlich der für die Datenverarbeitung erforderlichen Mittel. Dasselbe gilt für die Verfolgung eines gemeinsamen Zweckes. Auch hier genügt eine Teilüberlappung und ein gemeinsames kommerzielles Ziel, auch wenn dazu unterschiedliche Interessen an der Datenverarbeitung bestehen. Das gilt insbesondere, wenn im Außenverhältnis eine Arbeitsteiligkeit bei der Datenverarbeitung erfolgt und ein Akteur in die Datenerhebung eingebunden ist und diese überhaupt erst ermöglicht, auch wenn die andere Entität für die technische Abwicklung der Datenverarbeitung gleichermaßen benötigt wird, etwa weil sie entsprechende technische Tools dafür liefert. Im Zweifel kann im Übrigen eine Ausdifferenzierung der gemeinsamen und alleinigen Verantwortung hinsichtlich der verschiedenen Datenverarbeitungsschritte erfolgen. Auch die Aufgaben- und Rollenverteilung bei den gemeinsamen Verarbeitungsschritten kann ausdifferenziert werden. Die gemeinsame Verantwortlichkeit ersetzt damit substantiell Fallkonstellationen, die nach der bisherigen Auslegung im deutschen Recht als Auftragsverarbeitung qualifiziert worden sind.[57] Schon bei einer geringeren Zweck- und Mittelgemeinsamkeit ist nunmehr stattdessen von einer gemeinsamen Verantwortung auszugehen. Die Konsequenzen dieser erst nach Inkrafttreten der DS-GVO eingeleiteten Klarstellung des Konzepts der gemeinsamen Verantwortung, wie es an sich schon vorher unter der DSRL 95/46/EG und damit für das BDSG a.F. und die LDSGe a.F. bereits galt, zeichnen sich erst nach und nach in der deutschen Anwendungspraxis von DS-GVO und BDSG n.F. bzw. LDSGe n.F. ab.

Die Frage nach den jeweiligen Rollen kann vor diesem Hintergrund für die Teilfragen der Bestimmung der Zwecke und der „wesentlichen" Mittel anhand folgender Leitfragen, die teilweise bereits in der Literatur zusammengestellt werden, weiter ausdifferenziert werden.[58] So ist für die Frage, wer über die Zwecke bestimmt, etwa relevant, wer die Verarbeitung initiiert, von ihren Zwecken primär profitiert, ihre Ausgestaltung steuert, die Kundenansprache vornimmt etc. Hinsichtlich der „wesentlichen" Mittel kommt es vor allem auf die Bereitstellung der entsprechenden Datenverarbeitungssysteme und vor allem der Software einschließlich deren Ausgestaltung und des Zugangs und des Zugriffs an.[59]

2.5.1.4 Anreize für Datentreuhänder zur Wahrnehmung der Interessen der Betroffenen zur Vermeidung einer gemeinsamen Verantwortlichkeit mit dritten Verantwortlichen

Es besteht vor diesem Hintergrund das Risiko, dass die Datentreuhänder, gerade im Fall eines kommerziellen Interesses an der Maximierung von Datenverarbeitungen durch andere Verantwortliche, auch wenn dies den Interessen der Betroffenen entspricht, im Rahmen eines kollaborativen Zusammenwirkens mit diesen anderen Verantwortlichen in die Rolle einer gemeinsamen Verantwortlichkeit mit diesen hineinwachsen. Allerdings bestehen genügend Gestaltungsmöglichkeiten für den Datentreuhänder, sich gleichsam „im Lager" der betroffenen Person anzusiedeln und an dessen Verarbeitungswünschen orientiert nur als Mittler Daten der betroffenen Personen an andere Verantwortliche nach den Wünschen der betroffenen Personen zu verwalten. Dann bestimmen im Wesentlichen diese anderen Verantwortlichen über die Zwecke der Datenverarbeitung und der Intermediär sorgt nur dafür, dass eine Datenverarbeitung

---

[56] EuGH, Urteil vom 5.6.2018 – C-210/16, Rn. 31 ff. – Facebook-Fanpages; Urteil vom 10.7.2018 – C-25/17, Rn. 65 ff. – Zeugen Jehovas; Urteil vom 29.7.2019 – C-40/17, Rn. 75 ff. – Fashion ID.

[57] So zutreffend Kremer, Gemeinsame Verantwortlichkeit: Die neue Auftragsverarbeitung, CR 2019, S. 225 ff.

[58] Siehe ähnlich Gierschmann, Gemeinsame Verantwortlichkeit in der Praxis, ZD 2020, S. 69 (72).

[59] Ähnlich wiederum Gierschmann, Gemeinsame Verantwortlichkeit in der Praxis, ZD 2020, S. 69 (72).

ausschließlich nach den Wünschen der betroffenen Personen erfolgt – oder eben gar nicht. Dasselbe gilt für die Wahrnehmung der Betroffenenrechte. Handelt der Datentreuhänder auch im Interesse anderer Verantwortlicher und stellt sich damit – zumindest auch – in deren Lager, so wird in vielen Fällen eine gemeinsame Verantwortlichkeit anzunehmen sein. Diese Differenzierung – gleichsam im Sinne einer „Lagertheorie" – kann für Datentreuhänder eine vergleichsweise rechtssichere Orientierung bieten, ob mit den anderen Verantwortlichen eine gemeinsame Verantwortlichkeit besteht oder nicht.

Damit sorgt das strenge Haftungsregime der gemeinsamen Verantwortlichkeit zugleich für eine Disziplinierung der Datentreuhänder als Agenten der Interessenwahrnehmung der sie einschaltenden betroffenen Personen. Verfolgen sie diese nicht konsequent, sondern orientieren sich an den Verarbeitungsinteressen der anderen Verantwortlichen, werden sie folgerichtig zu gemeinsamen Verantwortlichen. Dies führt – wie unter 2.5.2 noch darzulegen sein wird – in der Konsequenz zu erheblichen Haftungsrisiken. Das durch die gemeinsame Verantwortlichkeit hervorgerufene strenge Haftungsregime schafft daher Anreize, die Interessenkollisionen ausschließen. Um es noch einmal anders zu formulieren: Die verschiedenen bereits in der Praxis anzutreffenden Datentreuhänder-Modelle (dazu oben 2.1) stehen in unterschiedlichem Umfang in der Gefahr, einer gemeinsamen Verantwortlichkeit mit den dritten Datenverarbeitern zu geraten. Agieren sie eher als „Makler" zwischen den anderen Datenverarbeitern und den Betroffenen und versuchen, etwa durch die Optimierung der Schnittstellen mit den anderen Datenverarbeitern eine deren Bedürfnissen entsprechende, möglichst umfassende und reibungslose Datenübermittlung zu gewährleisten, spricht dies eher für die Annahme einer gemeinsamen Verantwortlichkeit mit diesen. Das kann dann auch für den Fall gelten, dass sie diese Optimierung durchaus im Sinne der Betroffenen vornehmen, um deren kommerziellen Interessen gerecht zu werden. Denn gleichwohl entscheiden sie maßgeblich über die Zwecke und Ausgestaltung der Datenverarbeitung mit und fungieren auch als Interface für die anderen Verantwortlichen, um die Daten der Betroffenen zu erlangen und aufzubereiten. Je stärker sich der Treuhänder dagegen im Lager der Betroffenen positioniert und die Zusammenarbeit mit den anderen Verantwortlichen funktional scharf auf das zur Wahrnehmung der Interessen der Betroffenen nötige beschränkt, desto eher scheidet eine Zuweisung einer gemeinsamen Verantwortlichkeit mit den anderen Verarbeitern aus. Im Einzelfall ist insoweit eine Grauzone markiert und erst die weitere Entwicklung der verschiedenen Geschäftsmodelle wird zur Ausdifferenzierung der hier in der Grundstruktur aufgezeigten rechtlichen Bewertung führen.

2.5.2 Haftungsrisiken für Datentreuhänder

Wesentliches Ziel der DS-GVO ist es, eine tatsächliche Beachtung ihrer materiell-rechtlichen Vorgaben sicherzustellen. Sie versucht das durch sehr scharfe Sanktionsmechanismen zu erreichen. Diese betreffen gerade auch Datentreuhänder, die große und teils sehr sensible Datenbestände verwalten. Rechtswidrige Handlungen können daher für Datentreuhänder schwerwiegende Konsequenzen nach sich ziehen.

2.5.2.1 Bußgeldrisiken

Ein wesentliches Element der Datenschutzreform 2018 war die drastische Erhöhung des Bußgeldrahmens für Datenschutzverstöße.[60] Bußgelder können gegenüber Verantwortlichen und Auftragsverarbeitern verhängt werden. Hintergrund war die unter der DSRL herrschende

[60] Dieser und die folgenden Absätze sind stark orientiert an Kühling/Klar/Sackmann, Datenschutzrecht, 4. Aufl. 2018, Rn. 760 ff.

sehr uneinheitliche und auch zurückhaltende Bußgeldpraxis der Aufsichtsbehörden.[61] Die in Art. 83 Abs. 5 DS-GVO normierte maximale Bußgeldhöhe liegt bei 20 Mio. Euro. Wenn der Verantwortliche ein Unternehmen ist – wie wohl im Regelfall – steigt die Obergrenze auf 4 % des Jahresumsatzes, wenn dieser Betrag höher als 20 Mio. Euro ist. Selbst für Verstöße, die die DS-GVO als weniger gravierend einstuft (z.B. reine Organisationsmängel)[62], droht Art. 83 Abs. 4 DS-GVO noch eine maximale Geldbuße von 10 Mio. Euro oder 2 % des Jahresumsatzes an. Es ist dabei auf den jeweiligen Konzern-[63] (!) Welt- (!) Jahresumsatz des vorangegangenen Geschäftsjahres abzustellen, also auf die Einnahmen, die der Konzern des jeweiligen Verantwortlichen im Jahr vor der Verhängung des Bußgeldes weltweit erzielt. Damit wird erkennbar auf die (häufig US-amerikanischen) Internetriesen mit hohen Milliardenumsätzen weltweit abgezielt. Aber auch für Datentreuhänder mit im Zweifel geringeren Umsätzen sind die Bußgelder durchaus empfindlich. Allein das macht die Vorschrift zu einer der wirkungsvollsten der DS-GVO überhaupt.

Erste Anwendungsfälle zeigen, dass die Aufsichtsbehörden durchaus auch bereit sind, die neuen Bußgeldrahmen zu nutzen. Zeigten die deutschen Aufsichtsbehörden anfangs noch eher Zurückhaltung, gingen die Aufsichtsbehörden in den anderen Mitgliedstaaten schneller voran. Ein erstes Signal setze die französische CNIL bereits im Januar 2019 mit einem Bußgeld in Höhe von 50 Mio. Euro gegen Google.[64] Noch schärfer ahndete die britische Aufsichtsbehörde zwei Verstöße gegen die Datensicherheit mit Bußgeldern von rund 205 Mio. Euro und 110 Mio. Euro gegen Unternehmen aus der Reisebranche.[65] Nachdem die deutschen Aufsichtsbehörden ihre Bußgeldpraxis auch nach Inkrafttreten der DS-GVO noch stark an der früheren Handhabung orientierten und die Höhe nur moderat anpassten,[66] änderten sie ihr Vorgehen relativ schnell und auch in Deutschland kam es zu hohen Bußgelder auch für vergleichsweise weniger bedeutende Verstöße.[67] Nachdem sich die Aufsichtsbehörden auf Bundes- und Landesebene auf einen einheitliches Bußgeldkonzept[68] geeinigt haben, das sich primär am erzielten Jahresumsatz orientiert, dürften drakonisch anmutende Bußgeldhöhen auch künftig eher die Regel als die Ausnahme sein. Bei den Zumessungskriterien kommt es neben Art, Schwere und Dauer des Verstoßes auch auf die Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens an. Da Datentreuhänder eine Vielzahl auch sensibler Daten verarbeiten, sind die Bußgeldrisiken für Datentreuhänder sehr erheblich, auch wenn Datentreuhänder nicht in jedem Fall große Umsätze erzielen werden.

---

61 Bergt, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 83 DS-GVO Rn. 1.

62 Neun/Lubitzsch, EU-Datenschutzgrundverordnung – Behördenvollzug und Sanktionen, BB 2017, S. 1538 (1542).

63 Erwägungsgrund 150 der DS-GVO; vgl. Bergt, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 83 DS-GVO Rn. 28; im Einzelnen ist dies umstritten, da der Wortlaut nur von Unternehmen spricht und erst in der Zusammenschau mit den Erwägungsgründen klar wird, dass der Begriff nicht i.S.d. Art. 4 Nr. 18 DS-GVO, sondern i.S.d. Art. 101 f. AEUV verstanden werden muss; kritisch insoweit Piltz, Die Datenschutz-Grundverordnung, K&R 2017, S. 85 (92); a.A. auch mit durchaus beachtlichem Hinweis auf das Bestimmtheitsgebot Neun/Lubitzsch, EU-Datenschutzgrundverordnung – Behördenvollzug und Sanktionen, BB 2017, S. 1538 (1543).

64 Siehe https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (zul. aufgerufen am 12.8.2020).

65 Dazu und zu weiteren anschaulichen Beispielen https://www.enforcementtracker.com/ (zul. aufgerufen am 12.8.2020).

66 Siehe etwa https://www.heise.de/newsticker/meldung/Passwoerter-im-Klartext-20-000-Euro-Bussgeld-nach-DSGVO-gegen-Knuddels-de-4229798.html (zul. aufgerufen am 12.8.2020).

67 Siehe etwa https://www.heise.de/newsticker/meldung/DSGVO-Verstoss-1-1-muss-knapp-10-Millionen-Euro-Strafe-zahlen-4608676.html (zul. aufgerufen am 12.8.2020).

68 Abrufbar im WWW unter der URL https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf (zul. aufgerufen am 12.8.2020).

2.5.2.2 Zivilrechtliche Haftungsrisiken

Neben den Risiken durch Bußgelder tritt das oft weniger beachtete zivilrechtliche Haftungsregime. [69] Denn der datenschutzrechtlich Verantwortliche und der Auftragsverarbeiter, darunter auch Datentreuhänder, sind auch „verantwortlich" im zivilrechtlichen Sinne.[70] Werden Rechte der betroffenen Person verletzt und entsteht ihr hierdurch ein Schaden, so steht ihr ein Ausgleich zu. Eine Besonderheit bei der datenschutzrechtlichen Haftung gegenüber der betroffenen Person ist der im Regelfall fehlende kausale materielle Schaden durch den Datenschutzrechtsverstoß. Unter der DS-GVO wird diesem Umstand dahingehend Rechnung getragen, dass auch ein immaterieller Schaden für ersatzfähig erklärt wird, Art. 82 Abs. 1 DS-GVO. Diese Vorschrift entspricht daher einer gesetzlichen Normierung gemäß § 253 Abs. 1 BGB im nationalen Recht und steht damit nicht im Widerspruch zur allgemeinen Schadenersatzrechtsdogmatik. Ein immaterieller Schaden ist in verschiedenen Konstellationen denkbar. Er dürfte aber jedenfalls dann ausgeschlossen sein, wenn lediglich gegen reine Ordnungsvorschriften verstoßen wird (wie etwa die Pflicht zur Führung eines Verarbeitungsverzeichnisses oder bloße Formalia in Datenschutzklauseln). Aufgrund der Möglichkeit, Ausgleich auch für immaterielle Schäden verlangen zu können, werden sich Verantwortliche und Auftragsverarbeiter künftig vermehrt Ansprüchen Geschädigter ausgesetzt sehen. Die Risiken, die sich daraus ergeben, können je nach Fallkonstellation unter Umständen sogar diejenigen aus der öffentlich-rechtlichen Bußgeldhaftung übersteigen.

Wie bei großen Compliance-Fällen in anderen Bereichen, z.B. dem sog. LKW-Kartell oder der Diesel-Abgas-Thematik bei den großen Fahrzeugherstellern, könnten zukünftig auch im Datenschutzrecht die im Vergleich zu möglichen öffentlich-rechtlichen Sanktionen größeren Risiken in einer massenhaften Geltendmachung von Schadensersatzansprüchen liegen. Für Datentreuhänder mit einer Vielzahl von Endkunden könnte ein Verstoß gegen Datenschutznormen dann künftig einen ernstzunehmenden Großschaden bedeuten. Gerade bei solchen Datentreuhändern, die mit umfangreichen Datenbeständen einer Vielzahl von Personen arbeiten, ist das ein realistisches Szenario. Dies gilt insbesondere vor dem Hintergrund, dass sich Unternehmen gegen Klagen von betroffenen Personen aufgrund einer faktischen Beweislastumkehr nach Art. 82 Abs. 3 DS-GVO mit einer abgestuften Darlegungs- und Beweislastverteilung[71] nur schwer verteidigen können, denn Verantwortliche haben die Einhaltung der Datenschutzvorschriften darzulegen und gegebenenfalls zu beweisen.[72] Dies gilt insbesondere in Kombination mit dem zivilprozessualen Instrument der Musterfeststellungsklage.[73] Ob es in der Praxis tatsächlich zu „Klagewellen" kommen wird, lässt sich derzeit noch nicht zuverlässig abschätzen. Jedenfalls die Möglichkeit der Geltendmachung von Ausgleichen für immaterielle Schäden sollte aber gerade für datenverarbeitungsgeprägte Unternehmen wie Datentreuhänder ein Ansporn sein, den Datenschutz ernst zu nehmen.

---

69 Dieser und die folgenden Absätze sind stark orientiert an Kühling/Klar/Sackmann, Datenschutzrecht, 4. Aufl. 2018, Rn. 765 f.

70 Hierzu und zum gesamten Abschnitt vertiefend auch Sackmann, Die Beschränkung datenschutzrechtlicher Schadensersatzhaftung in Allgemeinen Geschäftsbedingungen, ZIP 2017, S. 2450; allgemein zum Schadensersatz nach der DS-GVO Wybitul/Haß/Albrecht, Abwehr von Schadensersatzansprüchen nach der Datenschutzgrundverordnung, NJW 2018, S. 113.

71 Siehe dazu detaillierter auch Kühling/Sackmann, DuD 2019, 347, 350.

72 Vgl. dazu im Einzelnen Wybitul, DS-GVO veröffentlicht – Was sind die neuen Anforderungen an die Unternehmen, ZD 2016, S. 253 (254); siehe auch Kühling, Neues Bundesdatenschutzgesetz – Anpassungsbedarf bei Unternehmen, NJW 2017, S. 1985.

73 Dazu auch Kühling/Sackmann, Die Musterfeststellungsklage nach Datenschutzverstößen – ein unkalkulierbares Risiko für Unternehmen?, DuD 2019, S. 347.

Ein weiterer wesentlicher Aspekt bei der Beurteilung der Haftungsrisiken für Datentreuhänder ist die relativ strenge Außenhaftung gegenüber den betroffenen Personen. So ergibt sich direkt aus Art. 82 Abs. 4 DS-GVO, dass mehrere an einem Datenverarbeitungsvorgang beteiligte Verantwortliche als Gesamtschuldner auf Schadensersatz haften. Trifft einen der beteiligten Verantwortlichen ein höherer Verschuldensgrad, so findet ein Innenausgleich nach Art. 82 Abs. 5 DS-GVO statt. Dabei ist der Begriff der Beteiligung an der Datenverarbeitung weit zu verstehen.[74] Damit soll nach dem Wortlaut des Gesetzes ein wirksamer Schadensersatz für die betroffene Person sichergestellt werden, Art. 82 Abs. 4 a.E. DS-GVO.

Bei Einschaltung eines Datentreuhänders ist einerseits dieser an der Datenverarbeitung beteiligt und andererseits auch der Verantwortliche. Das gilt nach dem Wortlaut der Norm grundsätzlich auch unabhängig von der Frage, ob bei dem konkreten Geschäftsmodell eine gemeinsame Verantwortlichkeit mit dem Datentreuhänder anzunehmen ist. Allerdings sprechen die besseren Gründe dafür, dass die Vorschrift des Art. 82 Abs. 4 DS-GVO aus teleologischen Gesichtspunkten eine Einschränkung erfährt, wenn der Datentreuhänder keine eigenen Interessen an der Datenverarbeitung hat, also rein „im Lager“ der betroffenen Person steht. Es gibt dann kein sachlich zu rechtfertigendes Argument, den Datentreuhänder mithaften zu lassen. Letztlich würde er sonst unkalkulierbaren und vor allem nicht sachgerechten Risiken ausgesetzt: Obwohl er als „Agent“ der betroffenen Person agiert, müsste er ansonsten für das Fehlverhalten der „Gegenseite“ einstehen. Das kann ersichtlich vom Verordnungsgeber nicht gewollt sein. Bei einem sachgerechten Verständnis bietet damit das gegenwärtige Rechtssystem auch ein sinnvolles Anreizregime, um Interessenkollisionen beim Datentreuhänder zu vermeiden.

2.5.3 Zwischenergebnis

Datentreuhänder sehen sich erheblichen Haftungsrisiken ausgesetzt. Bei Verletzung datenschutzrechtlicher Vorschriften drohen erhebliche Bußgelder, die jedoch vor allem von der Höhe des Umsatzes abhängen. Die verhältnismäßig noch größeren Risiken ergeben sich aus der möglichen massenhaften Geltendmachung von Schadensersatzansprüchen durch die Nutzer, gegen die sich Datentreuhänder nach einer Datenschutzverletzung nur schwer verteidigen können. Besondere Risiken ergeben sich aus einer möglichen gemeinsamen Verantwortlichkeit. Bei einem sachgerechten Verständnis bietet das gegenwärtige Rechtssystem ein sinnvolles Anreizregime, um Interessenkollisionen beim Datentreuhänder zu vermeiden.

2.6 Mögliche Anpassungsbedürfnisse des geltenden Rechts

Während die bisherigen Ausführungen das geltende Recht und damit die gegenwärtigen „Spielregeln“ für den Einsatz und gegebenenfalls die Abwehr von Datentreuhändern skizziert und analysiert haben, stellt sich nunmehr in einem weiteren Schritt die Frage, inwiefern vor diesem Hintergrund Vorschläge indiziert sind, den Rechtsrahmen in einzelnen oder mehreren Punkten de lege ferenda zu modifizieren, da er sich als defizitär für den sinnvollen Einsatz von Datentreuhändern erwiesen hat und diesen behindert.

2.6.1 Belastbarkeit und Funktionsfähigkeit des rechtlichen Rahmens; Vorschläge sektorspezifischer Regelungen

Insoweit hat sich zwar gezeigt, dass angesichts der Vielfalt der bereits jetzt erkennbaren Dienste und der Komplexität der aufgeworfenen Rechtsfragen die im Datenschutzrecht gerade bei innovativen Angeboten übliche Rechtsunsicherheit zu konstatieren ist. Das gilt exemplarisch für

[74] Bergt, in: Kühling/Buchner, DS-GVO/BDSG, 2. Auflage 2018, Art. 82 DS-GVO Rn. 22.

die dargestellte Grauzone bei der Rollenzuweisung der Datentreuhänder als allein Verantwortliche für die von ihnen durchgeführte Datenverarbeitung oder als gemeinsam Verantwortliche in Kollaboration mit den anderen Datenverarbeitern (dazu 2.5.1). Genau diese Restunsicherheiten ergeben sich jedoch aus der Vielfalt der Angebote und der notwendig abstrakt zu fassenden Regeln in der DS-GVO. Ähnliches gilt für die weiteren aufgezeigten rechtlichen Herausforderungen von der Ausübung der Gestaltungsrechte bis hin zu den Haftungsfragen. Im Übrigen hat sich gezeigt, dass der Rechtsrahmen und im exemplarischen Fall der Frage der gemeinsamen Verantwortlichkeit auch die Rechtsprechung des EuGH hinreichend klare Hinweise geben, unter welchen Voraussetzungen eher eine gemeinsame Verantwortlichkeit anzunehmen ist. Es konnte sogar gezeigt werden, dass die Unsicherheiten in der Grauzone eher den positiven Anreiz setzen sollten, im Zweifel eine starke Ausrichtung des Treuhänder-Modells an den Interessen der Betroffenen und nicht der anderer Verantwortlicher auszurichten. Dasselbe wurde für die Anreizwirkungen des Haftungsregimes gezeigt (dazu 2.5.2.2).

Zudem ist darauf hinzuweisen, dass sich die verschiedenen Angebote und Geschäftsmodelle von Datentreuhändern gerade erst im Markt entwickeln, so dass eine Regelung zum gegenwärtigen Zeitpunkt zwangsläufig ein noch unklares Phänomen normieren müsste. Gleichwohl ist die Schaffung eines rechtlichen Rahmens etwa vom Verbraucherzentrale Bundesverband für die PIMS als zentrales Modell der Datentreuhänder vorgeschlagen worden.[75] Darin sollen etwa Haftungsfragen, Qualitätsanforderungen, Regeln zu den Treuepflichten, zu verbotenen Koppelungen bis hin zu Bestimmungen zur Insolvenz oder Auflösung von Datentreuhändern geklärt werden. Ferner soll normativ verhindert werden, dass sich auf diesem Markt Monopolstellungen ergeben sowie positiv gewährleistet werden, dass PIMS „unabhängig, neutral und ohne ein wirtschaftliches Eigeninteresse“ an der Datenverarbeitung handeln. Die vorliegende nähere Prüfung hat jedoch ergeben, dass das geltende Recht insoweit genügend Spielräume bietet, dafür zu sorgen, dass entsprechende Angebote im Markt vorhanden sind.

2.6.2 Zweck- statt phänomenbezogene Ausrichtung des Rechtsrahmens

Im Übrigen ist ganz allgemein Vorliegendes zu beachten: Die Rechtsordnung ist nicht phänomenbezogen, sondern zweckbezogen strukturiert.[76] Das bedeutet, dass die Rechtsbeziehungen zwischen Rechtssubjekten im Mittelpunkt stehen und nicht um einzelne Lebenssituationen herum ausgestaltet werden und jedes denkbare Verhalten in Bezug auf diese in einem Regelungskontext zusammengefasst ist. Insofern entspricht es der Struktur der Rechtsordnung, dass es konsolidierte phänomenbezogene Regelungen für das Phänomen „Datentreuhänder“ ebenso wenig gibt wie beispielsweise ein eigenes Regelungswerk, das alle Vorgänge im Gesundheitssektor erfasst. Vielmehr unterliegt auch dieser Lebensbereich unterschiedlichen Normen aus verschiedenen Rechtsgebieten. Die Rechtsordnung ist vielmehr so strukturiert, dass durch Rechtsnormen menschliche Verhaltensweisen adressiert werden, die im Grundsatz erlaubt (Art. 2 Abs. 1 GG) und ausnahmsweise untersagt werden. Ein überzeugendes Regulierungsregime im Hinblick auf einzelne Phänomene kann daher kaum in einzelnen phänomenbezogenen Gesetzen gesucht werden, die dann ihrerseits alle denkbaren Konstellationen abdecken. Gerade in Sektoren mit hoher Änderungsgeschwindigkeit der realen

---

[75] Verbraucherzentrale Bundesverband, Positionspapier vom 19.2.2020, S. 3, abrufbar im WWW unter der URL https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (zul. aufgerufen am 12.8.2020).

[76] Dieser Absatz ist stark orientiert an Kühling/Sackmann, Rechte an Daten, S. 9, abrufbar im WWW unter der URL https://www.vzbv.de/sites/default/files/downloads/2018/11/26/18-11-01_gutachten_kuehling-sackmann-rechte-an-daten.pdf (zul. aufgerufen am 12.8.2020).

Bedingungen sind legislative Handlungsformen oftmals zu träge, um auf sich ändernde Umstände zu reagieren.[77] Allgemeine Rechtsbegriffe und eine gute Begleitung im exekutiven Vollzug sind insoweit besser geeignet. Es entstünde zudem fast unweigerlich eine Parallelstruktur zu bestehenden Normsystemen mit erheblichen Friktionsflächen zu anderen Regelungsgebieten. Die Folge wäre eine höhere Regelungskomplexität und damit einhergehend eine geringere Rechtssicherheit. Denn auch die gegenwärtigen rechtlichen Vorgaben für die Datenverarbeitung erfolgen sektoral und schutzzweckorientiert. Sie passen sich damit in den verhaltensbezogenen Regelungsansatz der Rechtsordnung ein. Lösungen, die sich in dieses gewachsene Regelungsregime einfügen, versprechen den größeren Nutzen durch hohe Rechtssicherheit und große Akzeptanz. Die Zweckmäßigkeit eines konsolidierten Regelungsbedarfs ist deshalb nicht nur nicht erkennbar. Eine Regulierung in einem Spezialgesetz wäre sogar kontraproduktiv. Denn sie würde die Komplexität im Regelungsgefüge weiter steigern.

2.6.3 Regelungen nur auf unionaler Ebene (sinnvoll) möglich

Darüber hinaus würde eine derart weit gefasste Regelung eine Fülle rechtlicher Schwierigkeiten mit sich bringen. So wäre zunächst für jede einzelne Regelung zu klären, inwiefern diese auf nationaler Ebene überhaupt zulässig ist, oder ob insoweit eine Änderung bzw. Konkretisierung der DS-GVO erforderlich ist. Sodann wäre zu prüfen, auf welcher Verbandsebene (EU oder Mitgliedstaat) entsprechende Vorgaben in der Sache rechtlich zulässig sind und ob sie etwa gegen Grundrechte verstoßen. Die erste Frage hängt stark davon ab, inwieweit die DS-GVO korrelierende Öffnungsklauseln für mitgliedstaatliche Konkretisierungsmaßnahmen vorsieht.[78] Dies wäre für die vorgeschlagenen Regelungsinhalte im unterschiedlichen Umfang der Fall. Beispielsweise enthält Art. 7 Abs. 4 DS-GVO bereits ein Koppelungsverbot. Eine korrelierende Öffnungsklausel besteht nicht. Insoweit wäre eine normative Konkretisierung also nur auf unionaler Ebene möglich. Zwar bietet die gegenwärtige deutsche Ratspräsidentschaft insoweit ein gutes Fenster für einen deutschen Impuls. So könnte die Europäische Kommission aufgefordert werden, einen entsprechenden Rechtsakt vorzuschlagen. Die Verabschiedung der DS-GVO ist 2016 jedoch ein großer Kraftakt gewesen und eine zeitnahe Ergänzung mit Blick auf den Aspekt der Datentreuhänder erscheint nicht sehr wahrscheinlich. Dementsprechend hat die Kommission in ihrem jüngsten Bericht zur Evaluierung der DS-GVO nach Art. 97 DS-GVO – zu Recht – aufscheinen lassen, dass kurzfristig der Fokus stärker auf der Anwendung und Durchsetzung der geltenden DS-GVO liegen sollte als auf deren Modifikation.[79]

Jedenfalls gilt, dass angesichts des notwendig umfassenden Ansatzes der Datentreuhänder, möglichst weitgehend zahlreiche Datenverarbeitungsvorgänge im In- und Ausland zu erfassen, eine nationale Regelung, auch sofern entsprechende Kompetenzen partiell bestehen, wenig zielführend wäre.

---

[77] Dazu Sackmann, Datenschutz bei der Digitalisierung der Mobilität, 2020, S. 195.

[78] Dazu grundlegend Kühling/Martini et. al., Die Datenschutz-Grundverordnung und das nationale Recht. Erste Überlegungen zum innerstaatlichen Regelungsbedarf, 2016, abrufbar im WWW unter der URL http://www.uni-regensburg.de/rechtswissenschaft/oeffentliches-recht/kuehling//medien/k__hling_martini_et_al.-die_dsgvo_und_das_nationale_recht_-_.pdf (zul. aufgerufen am 12.8.2020) und Kühling/Martini, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, S. 448 ff.

[79] Siehe Europäische Kommission, GDPR - the fabric of a success story - Europe fit for the digital age, abrufbar im WWW unter der URL https://ec.europa.eu/commission/presscorner/detail/de/ip_20_1163 (zul. aufgerufen am 12.8.2020).

2.6.4 Gegenwärtig kein Regelungsbedürfnis

Unabhängig von der Realisierungswahrscheinlichkeit einer Novelle der DS-GVO ist eine auf Datentreuhänder bezogene Spezialregelung auch gar nicht wünschenswert. Das lässt sich exemplarisch am Beispiel des Koppelungsverbots aufzeigen. Dieses wirft als allgemeine horizontale Regelung in einer Fülle von Rechtskonstellationen nach wie vor erhebliche Schwierigkeiten auf, insbesondere was die Anwendung auf die anderen Verantwortlichen selbst – wie etwa soziale Netzwerke wie Facebook – anbelangt.[80] Dass nun gerade die gleichsam „abgeleitete" Frage, wie unzulässige Koppelungen der Datentreuhänder normativ unterbunden werden können, zuvor geklärt werden sollte, erscheint wenig zielführend. Es würde insoweit der zweite Schritt vor dem ersten gemacht.

Dies ist nur ein Beispiel für die fehlende Zweckmäßigkeit normativer Anpassungen zum gegenwärtigen Zeitpunkt. Denn insgesamt ist darauf hinzuweisen, dass jegliche normative Umhegung die ohnehin schon hohe (durch das normative Nebeneinander von DS-GVO und nationalem Datenschutzrecht verschärfte) datenschutzrechtliche Komplexität weiter steigern würde. Das gilt erst recht für einen Ausbau der normativen Vorsteuerung auf nationaler Ebene. Sollte sich im weiteren Verlauf eine Regulierung einzelner Fragen als erforderlich erweisen, so sollte dies in jedem Fall auf unionaler Ebene erfolgen.

Der Ansatz der DS-GVO ist es aber zu Recht, gerade für den Bereich der Datenverarbeitung durch Unternehmen einen abstrakt-generellen Rahmen zu schaffen – ohne bereichsspezifische Regelungen für einzelne Business-Modelle auf unionaler und erst recht nicht auf nationaler Ebene.[81] Dementsprechend sind auch sektorspezifische Datenschutzregelungen für andere Bereiche der Datenverarbeitung nicht indiziert, wie etwa im Bereich der Mobilität (Stichwort „autonomes Fahren").[82] Dieser allgemeine Rahmen soll vielmehr von den Vollzugsbehörden im Rahmen der Anwendung konkretisiert werden – unter der Kontrolle der Rechtsprechung.

2.6.5 Empfehlungen und Leitlinien der Datenschutzaufsichtsbehörden sinnvoll

Daher sind auch auf dieser Ebene weitere Empfehlungen angezeigt. So sind insbesondere weitere Aktivitäten der Datenschutzaufsichtsbehörden hilfreich, die in den bisherigen Ausführungen schon zum Teil adressiert wurden. So könnten auf nationaler Ebene die Aufsichtsbehörden bzw. die unabhängigen Datenschutzbehörden des Bundes und der Länder gemeinsam über die Datenschutzkonferenz eine Orientierungshilfe veröffentlichen, um die hier aufgezeigten oder sich im Laufe der Zukunft noch als problematisch erweisenden Aspekte der rechtlichen Einordnung der und die Anforderungen an Datentreuhänder näher zu bewerten. Dabei könnten sie beispielsweise – wie bereits vorgeschlagen (siehe dazu oben 2.4.2) – klarstellen, in welchen Fällen Datentreuhänder zwingend Datenschutz-Folgeabschätzungen durchzuführen haben. Sie können im Weiteren etwa darlegen, in welchem Umfang zur Beseitigung technischer Hindernisse Schnittstellen geschaffen werden müssen, insbesondere zur Wahrnehmung des Rechts auf Datenportabilität aus Art. 20 DS-GVO (siehe dazu oben 2.2.2). Eine Vielzahl unklarer Fragen in Bezug auf den Einsatz von Datentreuhändern muss also – statt im normativen Wege – auf der Ebene exekutiver Leitlinien etc. geklärt werden.

Auf europäischer Ebene wären ebenfalls entsprechende Leitlinien des Europäischen Datenschutzausschusses (EDSA) hilfreich. Ferner könnten auch im Rahmen der Aktualisierung

---

[80] Buchner/Kühling, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 61.

[81] Siehe dazu Kühling, Neues Bundesdatenschutzgesetz - Anpassungsbedarf bei Unternehmen, NJW 2017, S. 1985 ff.

[82] Siehe dazu grundlegend Sackmann, Datenschutz bei der Digitalisierung der Mobilität, 2020.

der relevanten Leitlinien die besonderen Probleme von Datentreuhänder-Modellen jeweils bezogen auf entsprechende Teilaspekte thematisiert werden. So hat der EDSA beispielsweise gerade erst Anfang Mai eine aktualisierte Fassung zur Einwilligung veröffentlicht.[83] Diese könnte im Zuge einer späteren erneuten Aktualisierung Hinweise und Beispiele zu den spezifischen Problemen von Datentreuhändern aufnehmen. Bislang existiert auf unionaler Ebene – soweit ersichtlich – nur die sehr allgemein gehaltene Stellungnahme des Europäischen Datenschutzbeauftragten zu PIMS.[84]

2.7 Ausblick: Bedeutung von Treuhänder-Modellen im Zusammenhang mit dem Sozial- und Beschäftigtendatenschutz

Im Ausblick sollen abschließend mit dem Sozial- und der Beschäftigtendatenschutz noch zwei Spezialbereiche betrachtet und auf ihr Potenzial für Datentreuhänder-Modelle „abgeklopft" werden. Da es sich in beiden Bereichen um komplexe, vielschichtige und umfassende Regelungsmaterien handelt, kann im Folgenden nur eine knappe Analyse geleistet werden, die grobe Tendenzaussagen beinhaltet und damit Anregungen und erste Hinweise für weiterführenden Forschungsbedarf geben kann.

2.7.1 Hohe Regelungskomplexität im Sozialdatenschutzrecht; begrenztes Potenzial für Treuhänder-Modelle

2.7.1.1 Für beide Rechtsmaterien gilt dabei, dass in der DS-GVO umfassende Öffnungsklauseln vorgesehen sind. Diese werden im deutschen Datenschutzrecht gerade im Sozialdatenschutzbereich auch umfassend genutzt.Beispiel: Komplexität und besondere Herausforderungen für Datentreuhänder-Modelle im Gesundheitswesen

Die – bereits andernorts durchgeführte[85] – exemplarische Bestandsaufnahme des Datenschutzes im Gesundheitswesen unter der Wirkung der DS-GVO ergibt dabei mit Blick auf die weite Öffnungsklausel insbesondere in Art. 9 Abs. 2 DS-GVO ein unbefriedigendes Bild. Statt einer Vereinfachung der ohnehin schon hypertrophen Datenschutzordnung ist eine weitere normative Ebene hinzugetreten, die zentrale Steuerungsimpulse gibt. Gerade auch auf Wunsch der deutschen Regierung sind im Zuge der Verhandlungen der Verordnung in der Endphase auch für den Sozialdatenschutz im Allgemeinen und den Gesundheitsdatenschutz im Besonderen eine Vielzahl von Öffnungsklauseln aufgenommen worden, die im Gesundheitswesen in besonderer Weise ihre desintegrierende Wirkung entfalten. Von einer unionsweiten Harmonisierung des Datenschutzes im Gesundheitswesen kann daher mitnichten die Rede sein. Es bleibt vielmehr bei einem normativen „Flickenteppich" aus Bundes- und Landesregelungen, die sogar noch ergänzt werden durch kirchenrechtliche Spezialbestimmungen. Schon das Auffinden der einschlägigen Zulässigkeitstatbestände im komplexen Zusammenspiel der Akteurstrias im Gesundheitswesen aus „Patient, Leistungserbringer und Leistungsträger" ist oftmals nicht trivial. Das gilt erst recht, wenn es um innovative Datenverarbeitungen unter Beteiligung verschiedener Akteure über die Grenzen verschiedener Bundesländer hinweg geht.

---

[83] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4.5.2020, abrufbar im WWW unter der URL https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf (zul. aufgerufen am 12.8.2020).

[84] Europäischer Datenschutzbeauftragter, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), Stellungnahme 9/2016, S. 6, abrufbar im WWW unter der URL https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_de.pdf (zul. aufgerufen am 12.8.2020); vgl. ferner der Bericht über eine Konsultation der Europäischen Kommission, An emerging offer of „personal information management services", 2016, abrufbar im WWW unter der URL https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=40118 (zul. aufgerufen am 12.8.2020).

[85] Siehe dazu umfassend Kühling, Datenschutz im Gesundheitswesen, MedR 2019, S. 611 ff.

Vor diesem Hintergrund zeigt sich exemplarisch, dass die Etablierung von Datentreuhänder-Modellen gerade im Gesundheitsbereich, der jedenfalls für die Datenverarbeitung durch gesetzliche Krankenkassen im Gesundheitswesen zum Sozialrecht gehört, vor besonderen normativen Herausforderungen steht.

Dabei greifen zwar eine Reihe der oben angeführten allgemeinen rechtlichen Rahmenbedingungen auch für etwaige Datentreuhänder im Gesundheitssektor. So gelten etwa die Grundsätze zur gemeinsamen Verantwortlichkeit oder zur Haftung prinzipiell auch für diesen Sektor. In relevanten Bereichen gibt es jedoch sektorspezifische Besonderheiten, die auch von den Datentreuhändern zu beachten wären. Das gilt etwa für die Reichweite der Einwilligungserklärung, die beispielsweise vom Bundessozialgericht traditionell besonders eng interpretiert wird.[86] Dies schränkt die Betätigungsmöglichkeiten privater Unternehmen und damit auch der Datentreuhänder bei der Verarbeitung von Gesundheitsdaten, sofern es um Sozialdaten geht, ein.

2.7.1.2 Ähnliche Situation im übrigen Sozialdatenschutzrecht

2.7.1.2.1 Ausgangspunkt: vielschichtige Grundstruktur des Sozialdatenschutzrechts und besonderer Schutz des Sozialgeheimnisses

Dasselbe Bild ergibt sich mit Blick auf das übrige Sozialdatenschutzrecht. Um das besser zu verstehen, ist eine knappe Skizze der Struktur des Sozialdatenschutzrechts erforderlich. Sozialdaten sind dabei im Sozialgesetzbuch (§ 67 Abs. 2 SGB X) vom Gesetzgeber wie folgt definiert worden[87]: „(2) Sozialdaten sind personenbezogene Daten (Artikel 4 Nummer 1 der Verordnung (EU) 2016/679), die von einer in § 35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden." Diese Legaldefinition stellt eine Kombination der Definition der personenbezogenen Daten in Verbindung mit den in § 35 SGB I genannten Leistungsträgern und anderen, in § 35 Abs. 1 S. 4 SGB I aufgezählten Stellen dar. Somit sind Sozialdaten personenbezogene Daten, die von Sozialleistungsträgern erhoben, verarbeitet oder genutzt werden. Sie stellen also eine Unterkategorie personenbezogener Daten dar, genauer gesagt eine besonders qualifizierte Form.[88] Sozialdaten unterliegen dem Sozialgeheimnis aus § 35 SGB I und ihr Umgang ist gemäß § 35 Abs. 2 SGB I nur unter den Voraussetzungen der §§ 67-85a SGB X zulässig. Adressaten von § 35 SGB I sind grundsätzlich nur die dort aufgeführten Leistungsträger.[89] Allerdings muss zwingend ein funktionaler Zusammenhang bestehen, also muss der Umgang im Rahmen der gesetzlichen Aufgabenerfüllung erfolgen, und nicht etwa zu arbeitsrechtlichen oder fiskalischen Zwecken.[90]

Eine abschließende Aufzählung der denkbaren Einzelangaben, die als Sozialdaten zu qualifizieren sein können, ist unmöglich.[91] Beispielhaft zu nennen sind Name, Alter, Familienstand, Staatsangehörigkeit, Einkommen, Arbeitgeber, Religionszugehörigkeit, Krankenkassenzugehörigkeit oder auch Überzeugungen und Charaktereigenschaften.[92] Der Sinn

---

[86] Siehe besonders problematisch BSG, Urteil vom 10.12.2008 – B 6 KA 37/07 R und dazu kritisch Kühling/Seidel, Die Abrechnung von Gesundheitsleistungen im Spannungsfeld von Datenschutz und Berufsfreiheit - Handlungsbedarf für den Gesetzgeber?, GesR 2010, S. 231.

[87] Siehe hierzu und zum Folgenden Kühling/Seidel, in: Kingreen/Kühling (Hrsg), Gesundheitsdatenschutzrecht, 2015, S. 38 ff.

[88] Knut/Seidel, in: Diering/Timme/Waschull (Hrsg.), LPK-SGB X, 3. Aufl. 2011, § 67 Rn. 2.

[89] Dazu näher Kircher, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, Teil 2, A. V. 2. b) bb).

[90] Stähler, in: Krahmer (Hrsg.), Sozialdatenschutz nach SGB I und X, 2. Aufl. 2011, § 67 SGB X Rn. 7.

[91] Vgl. Knut/Seidel, in: Diering/Timme/Waschull (Hrsg.), LPK-SGB X, 3. Aufl. 2011, § 67 Rn. 3.

[92] Siehe mit weiteren Beispielen Bieresborn, in: von Wulffen/Schütze (Hrsg.), SGB X, 8. Aufl. 2014, § 67 Rn. 5 und 7; Knut/Seidel, in: Diering/Timme/Waschull (Hrsg.), LPK-SGB X, 3. Aufl. 2011, § 67 Rn. 3.

und Zweck des Erhebens dieser Daten durch die verschiedenen Leistungsträger kann diverse Gründe haben. Einer wäre etwa die Ermittlung, ob die Voraussetzungen eines Anspruchs auf eine Sozial(versicherungs-)leistung gegeben sind. Allerdings sind die Verarbeitungskontexte so vielfältig wie das Sozialrecht selbst,[93] das alle diejenigen Normen des öffentlichen Rechts erfasst, die auf die Absicherung sozialer Risiken ausgerichtet sind. Relevante soziale Risiken sind dabei insbesondere die Krankheit und Pflegebedürftigkeit, aber auch die des Verlustes der Arbeit oder des Einkommens, sowie die Versorgung im Alter und die mit dem Tod verbundenen Versorgungsrisiken.

Das Sozialgeheimnis als Rechtsanspruch des Bürgers aus § 35 SGB I i.V.m. den §§ 67 - 85a SGB X, die Erlaubnistatbestände und vor allem Öffnungsklauseln (§§ 67a - c) für Einzelregelungen in den einzelnen Sozialgesetzbüchern enthalten, bilden im Zusammenspiel mit den unionsrechtlichen Vorgaben ein dichtes Regelungswerk.

2.7.1.2.2 Begrenztes Potenzial für den Einsatz von Treuhänder-Modellen

Diese ausgeprägte normative Komplexität erschwert die Entfaltung innovativer Treuhänder-Modelle zusätzlich. Angesichts der hohen Pfadabhängigkeit dürfte sich an dieser legislativen Situation jedenfalls mittelfristig auch kaum etwas ändern. Unabhängig davon unterliegt die Datenverarbeitung im Sozialbereich aber auch den aufgezeigten Besonderheiten einer öffentlich-rechtlichen Fundierung der zulässigen Datenverarbeitung. Diese hoheitliche Steuerung der Datenverarbeitungsprozesse zur gemeinwohlorientierten Absicherung gegenüber sozialen Risiken prägt die Ausgestaltung der Datenverarbeitungslogik und -regeln. Datentreuhänder passen insoweit nicht recht ins Bild, da für die Leistungsträger ohnehin eine Datenverarbeitung unter der Bindung des Gesetzesvorbehalts zur Erfüllung der öffentlichen Aufgaben indiziert ist. Es ist daher bislang eher unklar, wie hier sinnvoll ein Treuhänder mit welcher Funktion zwischen die Verantwortlichen und die Betroffenen geschaltet werden soll. Am ehesten wäre auf den ersten Blick noch ein Einsatz im Bereich der Durchsetzung der Betroffenenrechte denkbar. Die Aktivierung im Rahmen der Geltendmachung von Einwilligungen mit dem Ziel einer Kommerzialisierung gerade der besonders sensiblen und vom Sozialgeheimnis zusätzlich geschützten Sozialdaten erscheint hingegen deutlich fraglicher als in anderen Bereichen.

Die teils in der öffentlichen Diskussion anzutreffenden Vorschläge, etwa die Daten aus der Corona-App in ein spezifisches Treuhänder-Modell mit einer entsprechenden Gemeinwohl-Orientierung zu überführen,[94] sind vor diesem Hintergrund wenig überzeugend. Gerade bei der Corona-App kommt im Übrigen hinzu, dass sich Deutschland für das dezentrale System und gegen den zentralen Ansatz entschieden hat, so dass ein Großteil der Daten ohnehin dezentral auf dem Endgerät des Nutzers liegt und gar nicht im zentralen, vom Robert-Koch-Institut verantworteten App-System.[95] Erst im Fall einer Infektionsmeldung erfolgt eine – anonymisierte – Weitergabe der Daten über die App. Eine Kommerzialisierung gerade dieser Daten erscheint wiederum eher fernliegend. Insofern ist auch darauf hinzuweisen, dass die eingangs angeführten bisherigen Datentreuhänder-Modelle zwar durchaus – etwa im Bereich der Gesundheitsdaten – eine relevante Rolle spielen können (beispielsweise im Fall von Messdaten von Sensoren in Fitnessarmbändern oder Smartphones), aber eher weniger im Bereich des öffentlichen Gesundheitswesens als Teil des Sozialbereichs. Anders kann sich die Sachlage im Beschäftigtenbereich darstellen (dazu sogleich 2.7.2).

---

[93] Siehe dazu ausführlich Stolleis, Geschichte des Sozialrechts in Deutschland. Ein Grundriss, 2003.

[94] Siehe etwa Fezer, FAZ vom 26.5.2020, S. 13, der für eine „digitale Bürgerplattform“ plädiert.

[95] Siehe dazu Kühling/Schildbach, Corona-Apps — Daten- und Grundrechtsschutz in Krisenzeiten, NJW 2020, S. 1545 ff.

Gemäß diesen ersten Einschätzungen dürfte daher der Einsatz von Datentreuhänder-Modellen im Sozialdatenschutzbereich vor zusätzlichen normativen Hürden stehen, die gesondert näher aufbereitet werden müssten, und zugleich dürfte die Verbreitung entsprechender Modelle auch phänotypisch in diesen Bereich nicht besonders gut passen. Daher ist dieser Sektor allenfalls in einer reiferen Phase der Verbreitung von Treuhänder-Modellen relevant.

2.7.2 Anwendungspotenzial für Treuhänder-Modelle im Bereich der Beschäftigtendaten

2.7.2.1 Weniger komplexe Struktur des Rechtsrahmens

Etwas aussichtsreicher scheint insoweit das Anwendungspotenzial für Treuhänder-Modelle im Bereich der Beschäftigtendaten. Der Beschäftigtendatenschutz ist geprägt vom Zusammenspiel aus der Grundregelung und Öffnungsklausel in Art. 88 DS-GVO sowie der nationalen Strukturierung in § 26 BDSG nebst weiterer Spezifika wie Regelungen in Tarifverträgen sowie Betriebs- und Dienstvereinbarungen. Letztere können auf der Basis der einschlägigen arbeitsrechtlichen Kompetenzgrundlagen wie insbesondere § 1 Abs. 1 TVG geregelt werden.[96] Auch wenn der Beschäftigtendatenschutz aufgrund der starken Abhängigkeit von der konkretisierenden arbeitsgerichtlichen Rechtsprechung und dem Zusammenspiel der genannten normativen Ebenen ebenfalls durchaus komplex ist, besteht mit den genannten Kernnormen jedoch keine vergleichbar amorphe Struktur wie im Sozialdatenschutzrecht. Dem Grunde nach gelten im Übrigen zahlreiche der aufgezeigten allgemeinen rechtlichen Rahmenbedingungen für Datentreuhänder für den Beschäftigtendatenschutz gleichermaßen. Das gilt etwa für die Frage der gemeinsamen Verantwortung oder der Haftung. Auch die Ausübung der Betroffenenrechte erfolgen entsprechend der oben aufgezeigten Linien.

2.7.2.2 Relevante Besonderheiten für Datentreuhänder insbesondere hinsichtlich der Einwilligung

Für besondere Kategorien personenbezogener Daten – also etwa Gesundheitsdaten – finden sich in § 26 Abs. 3 BDSG dagegen spezifische, auf die Arbeitswelt zugeschnittene Vorgaben. Vorliegend besonders wichtige Spezifika ergeben sich ferner hinsichtlich der Frage der Freiwilligkeit der Einwilligung, da diese im Abhängigkeitsverhältnis „Arbeitgeber – Arbeitnehmer“ besonders prekär ist. Dies wird auch in § 26 Abs. 2 BDSG adressiert. Ein Indikator für die Freiwilligkeit ist es, wenn durch die Einwilligung ein wirtschaftlicher Vorteil erlangt wird. In diesem Kontext wäre ein Ansatz für die wirtschaftliche Betätigung von Datentreuhändern denkbar. Gleichwohl stellt sich die Frage, ob die Komplexität und Vielfalt der Datenverarbeitung so groß ist, dass sich der Einsatz von Datentreuhändern als hilfreich erweist. Das gilt etwa für die komplexen Probleme des Fragerechts des Arbeitgebers vor Begründung des Beschäftigten-verhältnisses genauso wie für die etwaigen Daten aus (Gesundheits-)Untersuchungen und Einstellungstests. Wenig umfangreich dürften auch die Stammdaten bzw. die Daten der Personalakte sein. Interessanter könnten hingegen Mobilitätsdaten oder solche der Mitarbeiterkontrolle sein.[97] Auch bei der Nutzung von Betroffenenrechten, um den angemessenen Datenschutz des Arbeitgebers zu prüfen, könnten Datentreuhänder-Modelle einen (begrenzten) Einsatz finden.

---

[96] Zu den Details siehe Maschmann, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 88 DS-GVO Rn. 81 ff.

[97] Siehe zu all diesen Spezifika jeweils umfassend statt vieler die Hinweise bei Maschmann, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, § 26 BDSG Rn. 29 ff.

2.7.2.3 Flankierende Funktion von Datentreuhändern neben etablierten kollektiven Legitimationsinstrumenten zur Datenverarbeitung

Ein mit Blick auf den Einsatz von Datentreuhändern weiterer interessanter Unterschied ist im Übrigen mit den Zulässigkeitstatbeständen bereits genannt. Denn mit den Tarifverträgen sowie Betriebs- und Dienstvereinbarungen liegen bereits kollektive Instrumente der Verwirklichung der informationellen Selbstbestimmung vor. Insoweit spricht einiges dafür, dass womöglich Datentreuhänder eine stärkere Individualisierung der Interessendurchsetzung eröffnen und damit gerade die informationelle Selbstbestimmung verbessern können.

Denn die Legitimationswirkung von Tarifverträgen, Betriebs- und Dienstvereinbarungen lässt sich nicht eindeutig der Kategorie einer gesetzlichen Ermächtigung oder der einer Einwilligung zuordnen, da sie Charakteristika von beiden aufweist: Die getroffene Betriebsvereinbarung gilt nicht nur für die an der Aushandlung beteiligten Personen, sondern für alle Arbeitnehmer, die in ihren Anwendungsbereich fallen. Dabei ist das verhandelnde Gremium[98] von den betriebsangehörigen Arbeitnehmern gewählt worden[99] und erfährt dadurch eine gewisse repräsentative Legitimation, die allerdings mit einer demokratischen Legitimation des Normgebers allenfalls ansatzweise zu vergleichen ist. Augenscheinlich ist auch, dass der die Betroffenen unmittelbar selbst treffende Datenumgang legitimiert wird, und nicht abstrakt ein Zulässigkeitstatbestand im Gesetz verankert wird. Dies entspricht eher der Wirkung einer Einwilligung.

Vor dem Hintergrund dieser Ambivalenz ist die Reichweite der Legitimationswirkung von Tarifverträgen, Betriebs- und Dienstvereinbarungen auch durchaus offen. Umstritten ist dabei insbesondere, ob und inwieweit der in der DS-GVO und im BDSG festgelegte Standard durch diese Rechtsgestaltungsform unterschritten werden darf. Verfassungs- und unionsprimärrechtlich spricht vieles für einen strengen Maßstab, da Tarifverträge, Betriebs- und Dienstvereinbarungen keine hinreichende Legitimation aus der Sicht des Gesetzesvorbehalts oder des Selbstbestimmungsrechts zu generieren vermögen. So mag mit Blick auf das Selbstbestimmungsrecht zwar – ähnlich einer freiwilligen Einwilligung – das normalerweise zwischen Arbeitgeber und -nehmer bestehende Machtgefälle durch die auf Augenhöhe verhandelnden Parteien abgemildert werden, wobei schon dies vor allem für Tarifverträge und nur begrenzt für Betriebs- und Dienstvereinbarungen gilt.[100] Unabhängig davon findet aber gerade keine persönliche Legitimation durch den Rechtsträger statt, sondern nur eine kollektive durch die repräsentierende Verhandlungspartei, was an die Legitimationskraft einer Individualvereinbarung nicht heranreicht. Eine quasi-legislative Legitimation wird ebenso wenig generiert. Daher ist die verfassungs- und unionsprimärrechtliche Legitimationskraft von Tarifverträgen, Betriebs- und Dienstvereinbarungen insgesamt fraglich, sofern durch sie das Recht auf informationelle Selbstbestimmung gegenüber der gesetzlichen Regelung Einschränkungen unterworfen wird. Für dieses Ergebnis spricht auch der Wortlaut des Art. 8 Abs. 2 GrCh, der neben der Einwilligung nur eine solche Datenverarbeitung zulässt, die auf einer „gesetzlich geregelten legitimen Grundlage“ basiert.

---

98 Das verhandelnde Gremium ist hier der Betriebsrat. Dessen allgemeine Aufgaben sind in § 80 BetrVG geregelt.

99 §§ 7 ff. BetrVG.

100 So ist zum einen darauf hinzuweisen, dass Tarifverträge eine verfassungsrechtliche Legitimation aus Art. 9 Abs. 3 GG erlangen, die im Rahmen der Abwägung mit dem Recht auf informationelle Selbstbestimmung zu berücksichtigen ist. Bei Betriebsvereinbarungen ist darauf hinzuweisen, dass gegebenenfalls eine Einigungsstelle befasst wird, mit der Folge einer denkbaren Durchsetzung von Datenschutzeingriffen gegeben den Willen des Betriebsrates auf der Grundlage der Stimme des Vorsitzenden der Einigungsstelle, vgl. § 76 BetrVG.

Vor diesem Hintergrund ist davon auszugehen, dass Tarifverträge, Betriebs- und Dienstvereinbarungen heute wohl keine Unterschreitung des datenschutzrechtlichen Standards legitimieren können – trotz einer dies partiell ermöglichenden Entscheidung[101] des Bundesarbeitsgerichts von 1986.[102] Es ist danach zu erwarten, dass das Bundesarbeitsgericht bei einem ähnlich gelagerten Fall heute strenger judizieren würde: Denn mittlerweile rückt auch das Bundesarbeitsgericht den Schutz des informationellen Selbstbestimmungsrechts stärker in den Mittelpunkt seiner Überlegungen und stellt daher strengere Anforderungen an die Betriebsparteien, wie sich beispielsweise anhand der Entscheidungen zur Videoüberwachung[103] feststellen lässt. Auch die übrige höchstrichterliche Rechtsprechung stellt strenge Anforderungen an die Bestimmtheit von Ermächtigungsgrundlagen und an die Freiwilligkeit der Einwilligung.[104] Vor dem Hintergrund dieser Rechtsprechungsentwicklung und den verschärften Anforderungen gerade des Bundesverfassungsgerichts sind an die Möglichkeit datenschutzreduzierender Tarifverträge, Betriebs- und Dienstvereinbarungen jedenfalls hohe Anforderungen zu stellen.[105]

Je nach weiterer Entwicklung dieser Einordnung unter der Geltung der DS-GVO wäre jedenfalls eine zusätzliche legitimierende Kraft der Einwilligung durch den Einsatz von Datentreuhändern denkbar. Dies wäre jedoch näher unter Beachtung auch der weiteren arbeitsrechtlichen Implementierung etwa von Kommerzialisierungsaspekten in diesem Kontext gesondert im Rahmen weiterer Untersuchungen vertieft zu betrachten. Dazu wäre auch eine vollständige Anamnese der relevanten Datenverarbeitungskonstellationen geboten, um die jeweiligen Potenziale für Datentreuhänder vor dem Hintergrund der (zusätzlichen) spezifischen rechtlichen Rahmenbedingungen des Beschäftigtendatenschutzes herauszuarbeiten.

Dabei könnte – anders als im Sozialdatenschutzsektor (dazu oben 2.7.1.2.2) – der Einsatz differenzierter Hardware einschließlich entsprechender Apps zur Kontrolle der Einhaltung von Sicherheitsabständen und der Nachverfolgung von Kontakten mit Corona-Infizierten gemäß den spezifischen Gegebenheiten in Betrieben[106] möglicherweise ein Testfall für den Einsatz von Datentreuhänder-Modellen im Bereich des Beschäftigtendatenschutzes sein. Datentreuhänder könnten gleichsam als neutrale zwischengeschaltete Entität einerseits Vertrauen für den Einsatz entsprechender Technologien schaffen, aber zugleich auch eine Nutzung zum Nachteil der Beschäftigten vermeiden helfen. So ließe sich gegebenenfalls an diesem Beispiel die Möglichkeiten einer Einbettung entsprechender Diensteangebote in die durch institutionelle Besonderheiten geprägte Organisation der Interessen von Beschäftigten in der Arbeitswelt analysieren – unter Beachtung der datenschutzrechtlichen und arbeitsrechtlichen Spezifika.

---

101 BAG, Beschluss vom 27.5.1986 – 1 ABR 48/84, NZA 1986, S. 643.

102 So auch Brandt, Betriebsvereinbarungen als datenschutzrechtliche „Öffnungsklauseln"?, DuD 2010, S. 213 (215), allerdings noch unter der Geltung des vorangegangenen Datenschutzrechtsrahmens.

103 BAG, Beschluss vom 29.6.2004 – 1 ABR 21/03; Beschluss vom 26.6.2008 – 1 ABR 16/07.

104 Siehe etwa die Entscheidung des BSG vom 10.12.2008, SGb 2009, S. 717.

105 Etwas weiter gehend Maschmann, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 88 DS-GVO Rn. 84, der letztlich eine Verhältnismäßigkeitsprüfung genügen lässt, die auch Beschränkungen des Rechts auf informationelle Selbstbestimmung zugunsten betrieblicher Interessen vor dem Hintergrund der unternehmerischen Freiheit aus Art. 12 GG ermöglicht; dort auch weitere Nachweise zur Rechtsprechung des BAG.

106 Siehe zu entsprechenden Möglichkeiten exemplarisch die Diensteangebote von Kinexon abrufbar im WWW unter der URL https://kinexon.com/de/safezone (zul. aufgerufen am 12.8.2020).

2.8 Ergebnisse der rechtlichen Analyse

1. In der vorliegenden Untersuchung geht es um die Frage, inwiefern das geltende Recht bereits einen angemessenen datenschutzrechtlichen Ordnungsrahmen für den Einsatz von Datentreuhändern gewährleistet und ob es insofern normativer Anpassungen bedarf.
2. Datentreuhänder werden dabei verstanden als Intermediäre zwischen den beiden Hauptakteuren des Datenschutzrechts, nämlich den Datenverarbeitern einerseits und den betroffenen Personen andererseits. Der Datentreuhänder wird als Vertrauensperson von der betroffenen Person eingesetzt, um die informationelle Selbstbestimmung einschließlich kommerzieller Verwertungsinteressen des Persönlichkeitsrechts gegenüber den Verantwortlichen besser wahrzunehmen. So kann der Betroffene angesichts der Vielzahl von Datenverarbeitungsprozessen und einer Vielzahl von datenschutzrechtlich relevanten Aktionen – insbesondere von Einwilligungserklärungen, aber auch der Nutzung von Betroffenenrechten – entlastet werden.
3. Zu dem hier zugrunde gelegten Verständnis der Datentreuhänder fehlt es bislang an vertieften rechtswissenschaftlichen Untersuchungen, die über grobe Problem- und Lösungshinweise hinausgehen. Letztere sind bislang auch eher von Institutionen entwickelt worden. Eine umfassendere Diskussion in entsprechenden rechtswissenschaftlichen (deutschsprachigen) Publikationsorganen ist hingegen bislang nicht erfolgt. Insoweit leistet die vorliegende Untersuchung „Pionierarbeit".
4. Auch der ergänzende Blick in die US-amerikanische Literatur ist zwar für die theoretisch-konzeptionelle Analyse von Datentreuhänder-Modellen durchaus interessant, hilft jedoch bei der Identifikation normativer bzw. regulatorischer Herausforderungen und erst recht bei deren Bewältigung nur begrenzt weiter.

Im Einzelnen hat die Analyse hinsichtlich der aufgeworfenen Rechtsfragen folgende Detailergebnisse geliefert:

5. Die wesentlichen datenschutzrechtlichen Gestaltungsrechte können auch durch Datentreuhänder ausgeübt werden. Insofern stehen dem Einsatz entsprechender Modelle keine durchgreifenden rechtlichen Hindernisse entgegen. In Bezug auf die Einwilligung umfasst das Recht auf informationelle Selbstbestimmung grundsätzlich auch die Befugnis des Einzelnen, zu entscheiden, ob er dieses Recht höchstpersönlich oder unter Einschaltung eines Vertreters ausüben möchte. Auch für Kinder können die Träger elterlicher Verantwortung entsprechend Art. 8 DS-GVO Datentreuhänder einsetzen und sich so von zeitlich aufwendigen und technisch anspruchsvollen Einzelausübungen der diesbezüglichen Gestaltungsrechte entlasten.
6. Jedoch gelten für die Erteilung einer entsprechenden Vollmacht – soweit übertragbar – die gleichen Voraussetzungen wie sie auch für die Einwilligung selbst gelten. Daher muss auch die Vollmacht insbesondere zweckbestimmt erteilt werden. Eine Generalvollmacht zur umfassenden und unbegrenzten Wahrnehmung des Rechts auf informationelle Selbstbestimmung durch Datentreuhänder wäre wegen Unbestimmtheit unwirksam. Ferner muss die Vollmacht ebenso wie die Einwilligung in informierter Weise erteilt werden – jedenfalls insoweit, als die betroffene Person selbst eine Vorstellung von den grundsätzlichen Rahmenbedingungen haben muss, unter denen der Vertreter eine Einwilligung mit Wirkung für und gegen sie erteilt. Darüber hinaus gilt für die Vollmacht, ebenso wie für die Einwilligung selbst, der Grundsatz der jederzeitigen freien Widerrufbarkeit. Diese rechtlichen Voraussetzungen stellen nicht unerhebliche Anforderungen an die

Datentreuhänder, die von diesen durch innovative Ausgestaltungen der Einwilligungserklärungen bewältigt werden müssen, aber auch bewältigbar sind.

7. Diese Entwicklung könnte durch klarstellende Hinweise in entsprechenden aufsichtsbehördlichen Dokumenten auf nationaler Ebene und durch den Europäischen Datenschutzausschuss unterstützt werden.

8. Sofern Datentreuhänder auch Gesundheitsdaten oder andere besondere Kategorien personenbezogener Daten verwalten, muss sich die Einwilligung der Betroffenen gegenüber den Datentreuhändern zur Legitimierung der Datenverarbeitung durch dritte Verantwortliche gemäß Art. 9 Abs. 2 lit. a DS-GVO zudem ausdrücklich auf diese Daten beziehen.

9. Darüber hinaus besteht hinsichtlich aller Betroffenenrechte ein relevantes Potenzial für den Einsatz von Datentreuhändern. Rechtlich erhebliche Probleme bei der Geltendmachung dieser Betroffenenrechte durch Datentreuhänder sind nicht ersichtlich. Denn im Ansatzpunkt gilt hier dasselbe wie in Bezug auf die Einwilligung. So gebietet es die informationelle Selbstbestimmung nachgerade, dass diese Rechte grundsätzlich auch über einen Vertreter geltend gemacht werden können. In diesem Zusammenhang kann der Datentreuhänder auch für seine Nutzer Schadensersatzansprüche geltend machen. Unter bestimmten Voraussetzungen kann dies unter den erleichterten Bedingungen des Art. 80 Abs. 1 DS-GVO erfolgen und eine separate gesetzliche Zulässigkeitsvorgabe nach dem Rechtsdienstleistungsgesetz ist dann nicht mehr erforderlich.

10. Verantwortliche könnten versucht sein, in ihren Allgemeinen Geschäftsbedingungen „Abwehrklauseln“ vorzusehen, um die Einschaltung eines Datentreuhänders auf Seiten der betroffenen Person zu verhindern. Derartige Klauseln sind richtigerweise als unwirksam anzusehen.

11. Selbst wenn dies von der Rechtsprechung anders bewertet werden sollte als hier vertreten, so hätte der Datentreuhänder durch ein Auftreten in fremden Namen die Möglichkeit, derartige Klauseln zu umgehen. Denn das Auftreten in fremdem Namen ist unproblematisch möglich.

12. Abwehrklauseln in Allgemeinen Geschäftsbedingungen dürften daher kein wesentliches Hindernis für die Etablierung von Datentreuhändern darstellen.

13. Für Datentreuhänder sind die Anforderungen an die IT-Sicherheit besonders hoch. Dabei muss der Datentreuhänder den strengen Anforderungen nicht nur genügen, sondern dies auch nachweisen können („Rechenschaftspflicht“). In der Praxis kann der Nachweis vor allem durch eine Zertifizierung gelingen.

14. Datentreuhänder unterfallen unter Umständen der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO. Hier kann es sinnvoll sein, dass die Aufsichtsbehörden im Rahmen der Erstellung der Liste für Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung zwingend durchzuführen ist, klarstellen, in welchem Umfang dazu auch die Angebote von Datentreuhändern gehören. Schon jetzt kann durch die Art der vom Datentreuhänder verarbeiteten Daten einer der gelisteten Verarbeitungsvorgänge erfasst sein.

15. Hinsichtlich der Verantwortlichkeit sind Datentreuhänder grundsätzlich als Verantwortliche und nicht als bloße Auftragsverarbeiter zu qualifizieren, da sie ja gerade das überlegene Wissen über die Mittel der Datenverarbeitung haben. Denn die Betroffenen erhoffen sich genau diese kognitive Erleichterung durch den Rückgriff auf jenen Intermediär.

16. Es besteht darüber hinaus das Risiko, dass Datentreuhänder, gerade im Fall eines kommerziellen Interesses an der Maximierung von Datenverarbeitungen durch andere Verantwortliche im Rahmen eines kollaborativen Zusammenwirkens mit diesen, in die Rolle einer gemeinsamen Verantwortlichkeit hineinwachsen. Allerdings bestehen genügend Gestaltungsmöglichkeiten für den Datentreuhänder, sich gleichsam „im Lager" der betroffenen Person anzusiedeln und an dessen Verarbeitungswünschen orientiert nur Daten der betroffenen Personen an andere Verantwortliche nach den Wünschen der betroffenen Personen zu verwalten. Eine gemeinsame Verantwortlichkeit scheidet dann aus. Dasselbe gilt für die Wahrnehmung der Betroffenenrechte: Handelt der Datentreuhänder auch im Interesse anderer Verantwortlicher und stellt sich damit – zumindest auch – in deren „Lager", so wird in vielen Fällen eine gemeinsame Verantwortlichkeit anzunehmen sein. Diese Differenzierung – gleichsam im Sinne einer „Lagertheorie" – kann für Datentreuhänder eine vergleichsweise rechtssichere Orientierung bieten, ob mit den anderen Verantwortlichen eine gemeinsame Verantwortlichkeit besteht oder nicht.

17. Damit sorgt das strenge Haftungsregime der gemeinsamen Verantwortlichkeit zugleich für eine Disziplinierung der Datentreuhänder als Agenten zur Interessenwahrnehmung der sie einschaltenden betroffenen Personen. Verfolgen sie deren Interessen nicht konsequent, sondern orientieren sich an den Verarbeitungsinteressen der anderen Verantwortlichen, werden sie folgerichtig zu gemeinsamen Verantwortlichen mit diesen Dritten. Dies führt in der Konsequenz zu erheblichen Haftungsrisiken. Das durch die gemeinsame Verantwortlichkeit hervorgerufene strenge Haftungsregime schafft daher Anreize, derartige Interessenkollisionen ausschließen.

18. Datentreuhänder sehen sich aber auch unabhängig von einer gemeinsamen Verantwortlichkeit mit den anderen Verantwortlichen erheblichen Haftungsrisiken ausgesetzt. Bei Verletzung datenschutzrechtlicher Vorschriften drohen erhebliche Bußgelder, die jedoch vor allem von der Höhe des Umsatzes abhängen. Die verhältnismäßig noch größeren Risiken ergeben sich aus der möglichen massenhaften Geltendmachung von Schadensersatzansprüchen durch die Nutzer, gegen die sich Datentreuhänder nach einer Datenschutzverletzung nur schwer verteidigen können. Auch insoweit werden starke Anreize zu einem sorgfältigen Umgang mit den Daten der Betroffenen gesetzt.

19. Mit Blick auf die etwaige Anpassung des geltenden Rechts ist zunächst zu konstatieren, dass angesichts der sinnvollerweise grenzüberschreitend angelegten Datentreuhänder-Modelle eine flankierende Regelung schon prinzipiell allenfalls auf unionaler Ebene sinnvoll ist. Teilweise sieht die DS-GVO auch gar keine Öffnungsklauseln für mitgliedstaatliche Regelungen in den hier untersuchten datenschutzrechtlichen Regularien vor.

20. Abgesehen von der geringen mittelfristigen Realisierungswahrscheinlichkeit entsprechender Anpassungen auf unionaler Ebene zur normativen Begleitung von Datentreuhänder-Modellen sind diese auch gar nicht wünschenswert. Denn der Rechtsrahmen hat sich als grundsätzlich passend erwiesen.

21. Erforderlich sind vielmehr exekutive Konkretisierungen durch nationale Datenschutzaufsichtsbehörden und den Europäischen Datenschutzausschuss. Dies kann in den jeweils relevanten allgemeinen Dokumenten – etwa in den Leitlinien des Europäischen Datenschutzausschusses zur Einwilligung – erfolgen oder in Form eines rechtsproblemübergreifenden Dokuments bezogen auf Datentreuhänder. Aber selbst insoweit sollte die weitere Entwicklung entsprechender Modelle eher noch abgewartet werden.

22. Der abschließende Blick auf die besonderen Sektoren des Sozial- und des Beschäftigtendatenschutzes offenbart, dass der Einsatz von Datentreuhänder-Modellen im Sozialdaten-

schutzbereich vor zusätzlichen normativen Hürden steht, die gesondert näher aufbereitet werden müssten. Zugleich wird deutlich, dass die Verbreitung entsprechender Modelle phänotypisch in diesen Bereich nicht besonders gut passen dürfte. Daher ist dieser Sektor allenfalls in einer reiferen Phase der Verbreitung von Treuhänder-Modellen relevant.

23. Etwas aussichtsreicher scheint insoweit das Anwendungspotenzial für Treuhänder-Modelle im Bereich der Beschäftigtendatenverarbeitung. So könnten etwa Datentreuhänder-Modelle bei der Ausübung von Betroffenenrechten der Beschäftigten eingesetzt werden. Gegebenenfalls können Datentreuhänder eine stärkere Individualisierung der Interessendurchsetzung eröffnen und damit gerade die informationelle Selbstbestimmung verbessern, teils als Substitut oder Flankierung von kollektivrechtlichen Regelungen in Tarifverträgen sowie Betriebs- und Dienstvereinbarungen. Dies wäre jedoch näher unter Beachtung auch der weiteren arbeitsrechtlichen Implementierung etwa von Kommerzialisierungsaspekten in diesem Kontext gesondert im Rahmen weiterer Untersuchungen vertieft zu betrachten. Dazu wäre auch eine vollständige Anamnese der relevanten Datenverarbeitungskonstellationen geboten, um die jeweiligen Potenziale für Datentreuhänder vor dem Hintergrund der (zusätzlichen) spezifischen rechtlichen Rahmenbedingungen des Beschäftigtendatenschutzes herauszuarbeiten.

3. Volkswirtschaftliche Analyse

Prof. Dr. Hilmar Schneider

3.1 Der Markt für Online-Dienste

Online-Dienste dürften die mit Abstand wichtigste Quelle für die Erhebung personenbezogener Nutzungsdaten darstellen, die für zahlreiche Zwecke weiterverarbeitet werden können und in aufbereiteter Form einen beträchtlichen kommerziellen Wert erhalten können. Bei der Nutzung von Online-Diensten haben sich Geschäftsmodelle etabliert, die partiell auf einem Naturaltausch zwischen Dienste-Anbietern und Dienste-Nutzern beruhen. Die Dienste-Nutzer beziehen dabei Informationen und Services, für die sie teilweise oder ganz mit Informationen über sich und ihr Nutzungsverhalten quasi bezahlen. Mit diesen Informationen allein ließe sich die notwendige Infrastruktur zur Dienste-Bereitstellung vermutlich nicht finanzieren. Damit daraus ein funktionierendes Geschäftsmodell wird, werden die Informationen von den Dienste-Anbietern mit Hilfe von Mustererkennungsverfahren zu kommerziellen Zwecken weiterverarbeitet. Während es sich dabei in den Anfängen der Datenökonomie in erster Linie um Werbezwecke handelte, gehen die Anwendungsgebiete heutzutage weit darüber hinaus. Insbesondere der Einsatz von Nutzerdaten zum Training KI-basierter Algorithmen in immer neuen Einsatzgebieten begründet ihren großen Wert. So vielfältig die Einsatzgebiete für Nutzungsdaten von Online-Diensten sind, so vielfältig sind auch die ökonomischen Wirkkanäle die das Marktgeschehen beeinflussen und Verteilungsergebnisse bedingen. Im Folgenden soll diese Vielfalt exemplarisch am Beispiel der Datennutzung zu Werbezwecken und anderer direkter Kundenansprache beleuchtet werden.

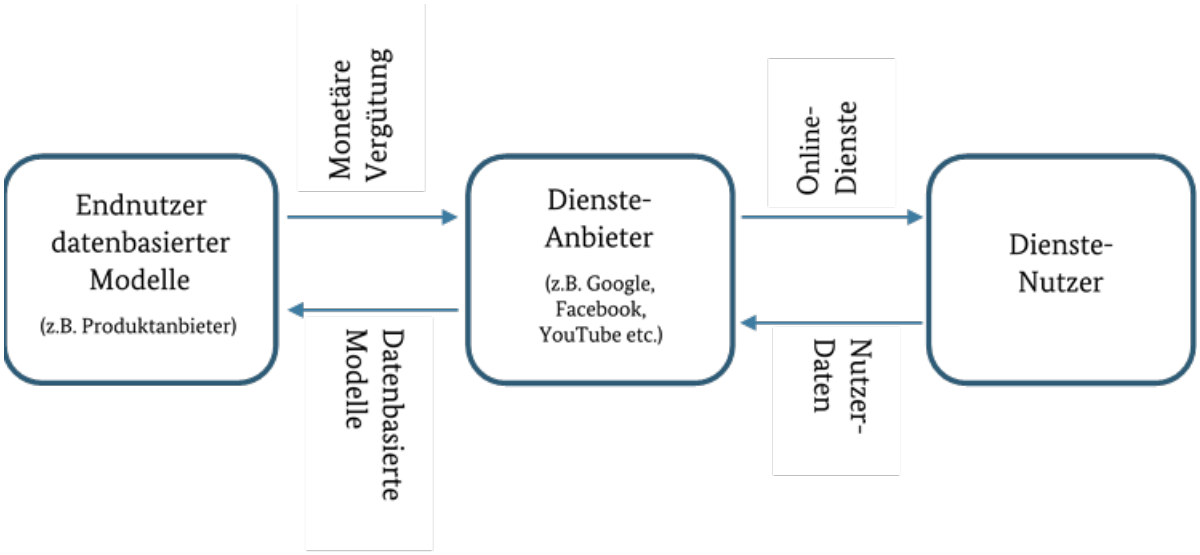
Ein typischer Anwendungsfall besteht darin, im Auftrag von Produktanbietern nutzerspezifische Werbeangebote auf Webseiten und in Web-Applikationen einzublenden. Neben Werbezwecken können die Daten aber auch zur Steuerung politischer Kampagnen oder Aufklärungskampagnen im Auftrag des Staates oder anderer Organisationen genutzt werden. Auch in diesem Fall wird ein kommerzielles Geschäftsinteresse bedient, denn politische Parteien, Nichtregierungsorganisationen oder der Staat entwickeln die datengetriebenen Steuerungsmodelle in der Regel nicht selbst, sondern beauftragen damit ein entsprechend spezialisiertes Unternehmen.

Die Nachfrager nach datenbasierten Steuerungsmodellen – meist handelt es sich hier um Produktanbieter – zahlen dafür einen entsprechenden Preis an die Dienste-Anbieter oder die Datenverarbeiter. Dienste-Anbieter agieren in diesem Sinne als Vermittler zwischen den kommerziellen End-Nutzern der datenbasierten Modelle und den Dienste-Nutzern. Die Bezahlung durch die kommerziellen End-Nutzer stellt die finanzielle Grundlage für die Bereitstellung von Online-Diensten dar. Damit daraus ein tragfähiges Geschäftsmodell resultiert, müssen die kommerziellen Einnahmen höher sein als die Kosten für die Bereitstellung des Online-Dienste-Angebots. Man hat es hier folglich mit einem zweiseitigen Markt zu tun, was eine Beurteilung im Hinblick auf faire Preisbildung und Informationsasymmetrien erheblich erschwert. Abbildung 1 illustriert die grundlegende Funktionslogik.

In der Praxis sind zahlreiche Varianten des Grundmodells zu beobachten. So kann beispielsweise ein Datenverarbeitungsdienstleister zwischen Dienste-Anbieter und End-Nutzer eingeschaltet sein. Dienste-Anbieter wie Amazon fungieren als Dienste-Anbieter und End-Nutzer zugleich. Online-Dienste wie Wikipedia finanzieren sich nicht über die Produktion kommerzieller

Datenprodukte, sondern über Spenden. Allen gemeinsam ist jedoch, dass das Dienste-Angebot überwiegend aus einer anderen Quelle finanziert wird als dem Dienste-Nutzer selbst.

Abbildung 1 Schema eines zweiseitigen Markts für das Angebot von Online-Diensten



Quelle: Eigene Darstellung des IZA.

Die indirekte ökonomische Beziehung zwischen Dienste-Anbieter und Dienste-Nutzer unterscheidet den Markt für Online-Dienste ganz grundsätzlich von anderen Märkten, etwa dem Arbeitsmarkt.[107] Auf dem Arbeitsmarkt treten Arbeitgeber und Arbeitnehmer unmittelbar miteinander in eine vertragliche Beziehung, die Art und Umfang der zu erbringenden Leistung und den dafür zu zahlenden Lohn regelt. Machtungleichheiten zwischen den beiden Vertragsparteien legitimieren Staat und Gewerkschaft als Sachwalter für einen angemessenen Interessensausgleich. Ihr Wirken beugt ausbeuterischen Arbeitsverhältnissen vor und schützt Arbeitnehmer vor unzumutbaren Gefährdungen.

Im Markt für Online-Dienste verhält sich die Interessenslage anders. Zwar liegt auch hier ein Machtungleichgewicht zwischen den Dienste-Anbietern und Dienste-Nutzern vor, aber anders als in einer bilateralen Vertragsbeziehung haben die Anbieter von Online-Diensten keinen ökonomischen Vorteil davon, Qualität und Umfang ihres Angebots zu Lasten der Dienste-Nutzer zu reduzieren. Würden sie es tun, schmälerten sie damit eher die Attraktivität ihres Angebots und reduzierten damit den kommerziellen Wert der erhobenen Daten. Gleichwohl haben sie einen Anreiz, möglichst viele und für die Erzielung von kommerziellen Einnahmen möglichst wertvolle Nutzerinformationen zu gewinnen.

Die Preisbildung für den Informationswert erfolgt deshalb nicht in einem Aushandlungsprozess zwischen Dienste-Anbietern und Dienste-Nutzern, sondern auf dem Markt für Datensätze oder datenbasierte Modelle. Dort werden sowohl die individuellen Nutzerdaten selbst angeboten als auch die auf den individuellen Nutzerdaten basierenden Vorhersagemodelle.

[107] Es gibt zwar auch Online-Plattformen für die Vermittlung von Arbeitsleistungen, aber die darüber hergestellte Beziehung zwischen dem Anbieter einer Dienstleistung und dem Nachfrager nach einer Dienstleistung ist zu unterscheiden von dem grundsätzlichen Vermittlungsdienst durch die Plattform. Im vorliegenden Kontext interessiert in erster Linie die Vermittlungsdienstleistung und deren Finanzierungsgrundlage.

Nutzerspezifische Informationen stellen in diesem Sinne ein Vorprodukt dar, das für die Herstellung des Endprodukts – etwa einem Modell zur optimalen Steuerung von Werbeeinblendungen – verwendet wird. Es findet jedoch kein expliziter Preisbildungsprozess für das Vorprodukt statt. Die Dienste-Nutzer erteilen lediglich ihr Einverständnis zur Nutzung ihrer Daten durch den Dienste-Anbieter im Gegenzug für die Nutzung des Online-Dienstes.

3.2 Der ökonomische Wert von individuellen Nutzerdaten

Die Tatsache, dass sich auf der Grundlage von datenbasierten Steuerungsmodellen äußerst lukrative Gewinne erzielen lassen, gibt Anlass zu der Frage, ob Dienste-Nutzer ihre Daten möglicherweise unter Wert preisgeben. Um dies beurteilen zu können, müsste sowohl der Wert der individuellen Nutzerinformationen für die Dienste-Anbieter als auch der Wert der Dienste-Nutzung für die Nutzer abgeschätzt werden können. Beides ist äußerst schwierig und mit erheblichen Unsicherheiten behaftet.

Der ökonomische Wert von Informationen über Nutzer oder deren Nutzungsverhalten kommt erst in der Masse durch Strukturierung und Systematisierung mittels mathematisch-statistischer Verfahren durch einen Dienste-Anbieter zur vollen Entfaltung.

Dabei setzen die Dienste-Anbieter Mustererkennungsverfahren ein, um aus der Fülle an Einzelinformationen systematische Modelle zu entwickeln, die eine möglichst gute Vorhersage etwa für erfolgreiche Werbeeinblendungen liefern. Ist ein solches Modell gefunden, sind nur noch rudimentäre Einzelinformationen erforderlich, um den interessierenden Prozess zu steuern. So lässt sich beispielsweise aus der Information, dass ein hoher Prozentsatz von Kundinnen oder Kunden, die eine Reise zu einem bestimmten Ort gebucht haben, auch einen Reiseführer für die entsprechenden Region gekauft haben, ableiten, dass entsprechende Werbeeinblendungen im Zusammenhang mit Reisebuchungen gewisse Erfolgsaussichten haben dürften. Ob ein einzelner Nutzer die Preisgabe seiner personenbezogenen Informationen verweigert, hat für den Wert des Vorhersagemodells dann praktisch keine Relevanz mehr, solange es genügend Nutzer gibt, deren Nutzungsinformationen für die Erstellung des Vorhersagemodells herangezogen werden können.[108]

Ein darauf basierendes Modell für die effektive Steuerung von Werbeeinblendungen ist für Produktanbieter von hohem Wert. Dienste-Anbieter bzw. die Entwickler solcher Modelle schaffen in diesem Sinne einen eigenständigen Mehrwert, der über die Summe des Werts aller dazu notwendigen Einzelinformationen hinaus geht. Die Algorithmen, mit denen aus einer Vielzahl von Einzelinformationen Modelle zur effektiven Platzierung von Werbeeinblendungen oder zur Steuerung von politischen Kampagnen generiert werden, können aus urheberrechtlicher Sicht als Geschäftsgeheimnis der Online-Dienste gelten. Wissenschaftlich fundierte Schätzungen darüber, wie hoch der Anteil des dadurch geschaffenen Mehrwerts am Gesamtwert der vorhandenen Daten ist, liegen bislang jedoch nicht vor. Auf dem Markt für datenbasierte Steuerungsmodelle wird nur das Endprodukt angeboten. Der dabei erzielte Preis lässt keine Rückschlüsse auf die relative Bedeutung der daran beteiligten Komponenten zu.[109]

---

[108] In diesem Sinne argumentieren beispielsweise Acemoglu D.; Makhdoumi A.; Malekian A.; Ozdaglar A. (2020): Too Much Data: Prices and Inefficiencies in Data Markets. Mimeo. Der marginale Wert eines zusätzlichen Nutzerdatensatzes sinkt mit der Zahl der bereits vorhandenen Nutzerdatensätze.

[109] Einige punktuelle Preisangaben finden sich in Schneider I. (2019): Regulierungsansätze in der Datenökonomie. Aus Politik und Zeitgeschichte, 24-26/2019, S. 35-41. Spitzenreiter dürfte Google sein. Umgelegt auf den einzelnen Nutzer erwirtschaftet Google einen Ertrag aus Werbeeinnahmen, der etwa 150 Euro pro Jahr ausmacht. Unklar ist jedoch, wie viel davon nach Abzug der Kosten für Diensteangebot und Datenweiterverarbeitung übrigbleibt.

Man könnte argumentieren, dass sich eine Abschätzung des ökonomischen Werts individueller Nutzerinformationen ableiten ließe, wenn Nutzer wählen könnten zwischen einem Nutzungsmodell, bei dem sie für die Dienste-Nutzung mit der Preisgabe von Nutzerinformationen „bezahlen" und einem Modell, bei dem sie für den gleichen Nutzungsumfang einen monetären Betrag entrichten und der Dienste-Anbieter dafür auf die Erhebung und Verarbeitung individueller Nutzerdaten verzichtet. Der Preis, zu dem ein Dienste-Anbieter bereit ist, den gleichen Nutzungsumfang zur Verfügung zu stellen wie im Falle einer bezahlfreien Datennutzung könnte ein geeigneter Indikator für den Wert sein, den der Dienste-Anbieter der Nutzerinformation beimisst.

In der Tat gibt es am Markt Beispiele für solche Wahloptionen, auch wenn sich die Bezahlvarianten bislang nur schlecht etabliert haben. So bieten etwa Zeitungsverlage an, den Nutzern das Leseangebot gegen Entgelt bereit zu stellen und dafür auf Werbeeinblendungen zu verzichten. Ähnliches gilt für zahlreiche Apps, bei denen man zwischen einer „Light"-Version mit Werbeeinblendungen und einer Bezahl-Version ohne Werbeeinblendungen wählen kann. De facto bevorzugen die weitaus meisten Nutzer die bezahlfreien Versionen, was etwa die Zeitungsverlage dazu zwingt, parallel zu ihrem traditionellen Leseangebot in elektronischer Form ein breit genutztes und bezahlfreies Leseangebot bereit zu stellen, das sich auf dem beschriebenen Umweg über die Generierung von Werbeeinnahmen refinanziert.

Ein Grund für die Präferenz zahlreicher Nutzer für die bezahlfreien Varianten der Dienste-Nutzung dürfte darin bestehen, dass aus der Preisgabe von Informationen für die Nutzer keine direkten Budgetwirkungen entstehen. Die Nutzer behalten ihre volle Freiheit im Hinblick auf andere Kaufentscheidungen, egal, wie häufig sie den Dienst in Anspruch nehmen. Sie erleiden auch keinen offensichtlichen Schaden durch die Preisgabe ihrer Daten. Die Entscheidung für ein Bezahlmodell zieht dagegen Liquiditätsbeschränkungen nach sich und zwingt die Nutzer zur Güterabwägung.

Es ist daher schwer einzuschätzen, inwieweit die beobachtbaren Preise für Bezahldienste aufgrund einer eingeschränkten Zahlungsbereitschaft seitens der Dienste-Nutzer womöglich nach unten verzerrt sind. Dies gilt umso mehr, als Bezahlmodelle in der Praxis nicht automatisch an einen Verzicht des Dienste-Anbieters auf Nutzerinformationen gekoppelt sind. Es könnte sogar sein, dass die Preise für Bezahldienste höher sind als es die Kosten zur Bereitstellung der Dienste erfordern würden, weil sie sich gezielt an ein Kundensegment richten, das sich durch eine hohe Präferenz für die Zeitersparnis bei der Dienste-Nutzung ohne Werbeeinblendungen auszeichnet.

De facto reflektiert die Wahlmöglichkeit zwischen Bezahlmodell und kostenfreier Nutzung mehr als nur den Preis der individuellen Nutzerinformation. Der Preis für Bezahldienste kann daher bestenfalls einen groben Anhaltspunkt für den Wert der individuellen Nutzerinformation liefern, keineswegs aber eine verlässliche Schätzung.[110]

Eine andere Möglichkeit zur Bestimmung des Werts von individuellen Nutzerdaten wäre gegeben, wenn öffentlich beobachtbare Marktangebote für die gleichen Nutzerdaten sowohl in verarbeiteter als auch in nicht-verarbeiteter Form vorlägen. Davon ist in der Praxis nicht auszugehen. Selbst wenn es so wäre, müsste berücksichtigt werden, dass aufgrund der Monopolstruktur des Marktes mit überteuerten Preisen für die reinen Nutzerdaten zu rechnen wäre. Das ist zumindest das Argument der EU-Kommission und der Kommission Wettbewerbsrecht 4.0, die daraus die Forderung ableiten, die Online-Dienste zur Preisgabe anonymisierter Nutzerdaten

[110] Dies deckt sich mit den Schlussfolgerungen von Acemoglu et al. (a.a.o.).

als öffentliches Gut zur Verfügung zu stellen.[111] Erschwerend kommt hinzu, dass sich der ökonomische Wert eines einzelnen Nutzerdatensatzes an dessen Marginalwert orientieren müsste, der mutmaßlich geringer ist als der ökonomische Wert des vollen Datensatzes dividiert durch die Summe der darin enthaltenen Einzeldatensätze.

Zusammenfassend ist somit festzustellen, dass die Bestimmung des ökonomischen Werts von nutzerspezifischen Informationen mit schwer lösbaren Schwierigkeiten verbunden ist. Das verbietet nicht das Anliegen, im Interesse der Dienste-Nutzer eine Vergütung für die dafür bereit gestellten Nutzerinformationen zu fordern, schwächt jedoch die argumentative Grundlage für die Festsetzung einer angemessenen Höhe.

3.3 Der ökonomische Wert der Dienste-Nutzung

Der Wert der Dienste-Nutzung für die Nutzer kommt auf vielfältige Art zustande. Dabei macht der direkte Nutzen der entsprechenden Dienstleistung nur einen Bruchteil aus. Darüber hinaus beeinflussen viele weitere Wirkkanäle auch indirekt den Nutzen, der auf individueller oder gesamtwirtschaftlicher Ebene entsteht. Die Nutzung von Online-Diensten in Form von Preisportalen etwa verschafft den Nutzern – zumindest der Intention nach – eine transparente Marktübersicht, die ihnen dabei hilft, Geld zu sparen. Markttransparenz erschwert es den Produktanbietern, Informationsasymmetrien zu ihren Gunsten nutzen zu können. In der Praxis lässt sich zwar beobachten, dass Produktanbieter mit gezielten Verschleierungsstrategien darauf reagieren, etwa indem sie sie Produktversionen marginal und laufend aktualisieren und damit die Vergleichbarkeit von Produkttests entwerten. Der Preisdämpfungseffekt scheint dennoch zu überwiegen, möglicherweise auch deshalb, weil mit der zunehmenden Verlagerung des Einzelhandels in den Online-Bereich Preisvorteile durch geringere Lager- und Personalkosten entstehen. Forscher vermuten die Ursache für die seit Jahren niedrige Inflationsrate in genau solchen Effekten.[112] Weitere Kanäle, die den ökonomischen Wert der Dienst-Nutzung beeinflussen , sind insbesondere dort zu vermuten, wo die gesammelten Nutzerdaten im Zusammenspiel mit anderen Datensätzen in ganz anderen Wirtschaftsbereichen zu Einsatz kommen. Eine vollständige Darstellung oder gar Quantifizierung all dieser Effekte ist unmöglich, auch deshalb, weil einmal erhobene Daten auch in Zukunft vielfältig wertschöpfend zum Einsatz kommen können.

3.4 Vergütung für die Übermittlung von Nutzerdaten

Sollte der Wert der übermittelten Nutzerdaten dagegen größer sein als der Nutzen der Dienste-Nutzung, stellt sich die Frage, wie sich die Differenz zugunsten des Dienste-Nutzers ausgleichen ließe. Es müsste eine geeignete Form der Vergütung gefunden werden, die sich sowohl am Wert der übermittelten Nutzerdaten als auch am Wert der Dienste-Nutzung festmacht.

Ob die Dienste-Nutzer ihre Daten unter Wert weitergeben, ist aufgrund der geschilderten Probleme nicht von vorneherein ersichtlich. Sollte dies der Fall sein, gäbe es eine Begründung für eine Kollektivierung der Nutzerinteressen, um diese gegenüber den Dienste-Anbietern effektiv

---

111 Siehe Europäische Kommission (2020): Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Eine europäische Datenstrategie. Brüssel; sowie Bundesministerium für Wirtschaft und Energie (Hrsg.): Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft – Bericht der Kommission Wettbewerbsrecht 4.0. September 2019.

112 Aulsbee und Klenow (2018) schätzen, dass die Inflationsrate in den USA im Zeitraum 2014-2017 ohne Online-Handel um 2% höher ausgefallen wäre. Aulsbee A.D.; Klenow P.J. (2018): Internet Rising, Prices Falling: Measuring Inflation in a World of E-Commerce. NBER Working Paper No. 24649. Cambridge, MA.

zur Geltung bringen zu können. Datentreuhänder könnten dafür ein geeignetes Instrumentarium sein.[113] Deren Ziel müsste dann darin bestehen, den Dienste-Nutzern in geeigneter Form ein über das Recht zur Dienste-Nutzung hinausgehendes Entgelt für die Bereitstellung ihrer Daten zu verschaffen.

Dazu müsste ein geeignetes Verfahren zur Ermittlung des individuellen Nettoschadens des Dienste-Nutzers definiert werden, der zu kompensieren wäre. Aufgrund der geschilderten Messproblematik kommen dafür allenfalls pragmatische Heuristiken in Betracht, aber auch diese dürften sich in der Praxis als untauglich erweisen. Man könnte beispielsweise eine Wertzumessung realisieren, die sich am messbaren Datenvolumen festmacht. Allerdings eröffnet das zahlreiche Manipulationsmöglichkeiten – sowohl auf Seiten der Dienste-Anbieter als auch auf Seiten der Dienste-Nutzer. Dienste-Anbieter könnten dann beispielsweise versucht sein, ein möglichst hohes Datenvolumen zu generieren, ohne den Nutzen des Dienstes zu verbessern, um so den fiktiven Wert der Daten-Nutzung in die Höhe zu treiben. Dienste-Nutzer könnten umgekehrt versucht sein, durch automatisierte Apps ein möglichst hohes Volumen an möglicherweise völlig sinnlosen Nutzungsdaten zu übermitteln. Im Ergebnis würden überflüssige Kosten für Rechnerkapazitäten und den davon ausgehenden Energieverbrauch generiert werden, ohne den Wert der Dienste-Nutzung zu erhöhen. Abgesehen davon, dass das im Extremfall sogar zu einer Entwertung der individuellen Nutzerinformationen führen könnte, wäre es in jedem Fall mit einem volkswirtschaftlichen Effizienzverlust verbunden.

Praktikabel wäre allenfalls eine pauschale monetäre Vergütung für die Dienste-Nutzer im Gegenzug für die Bereitstellung ihrer Nutzungsdaten. Zu deren Durchsetzung wären Datentreuhänder zweifellos eine geeignete Möglichkeit. In der Praxis dürfte aber schwer begründbar sein, warum Intensiv-Nutzer und Gelegenheits-Nutzer Anspruch auf die gleiche Pauschalvergütung haben sollten. Außerdem müsste sichergestellt sein, dass Nutzer nicht allein durch die parallele Nutzung mehrerer Nutzerkonten den individuellen Vergütungsanspruch künstlich nach oben treiben könnten. Selbst eine einfache Lösung könnte sich damit schnell als praktisch undurchführbar erweisen.

Darüber hinaus bleibt die Frage offen, in welcher Form Datentreuhänder die ihnen zugedachte Interessenwahrnehmung ausüben könnten. In Analogie zum Streikrecht zur Durchsetzung von Arbeitnehmerinteressen müsste den Datentreuhändern gegenüber den Dienste-Anbietern eine wirksame Möglichkeit zur Untersagung der Nutzung der Daten der von ihnen vertretenen Dienste-Nutzer zur Verfügung stehen. Das dürfte sich in der Praxis äußerst schwierig gestalten. Zwar mag eine solche Untersagung rechtlich durchsetzbar sein, aber wirksam wäre sie nur, wenn sie nicht zugleich von den Dienste-Nutzern selbst unterlaufen würde. Eine Bestreikung der Datennutzungserlaubnis könnte für die vertretenen Dienste-Nutzer einen zumindest vorübergehenden Ausschluss von der Dienste-Nutzung zur Folge haben. Dienste-Nutzer könnten daher versucht sein, sich durch erneute Erteilung der Datennutzungserlaubnis wieder Zugang zur Dienste-Nutzung zu verschaffen, was die Verhandlungsposition des Datentreuhänders schwächen würde.

3.5 Datentreuhänderschaft als Geschäftsmodell

In der Praxis haben sich bislang nur sehr wenige Datentreuhändermodelle am Markt etabliert. Voraussetzung für eine nachhaltige Etablierung ist die Erzielung eines dauerhaften Geschäftsertrags. Dieser könnte aus Provisionen bestehen, die die von ihnen vertretenen Dienste-Nutzer

[113] Acemoglu et al. (a.a.o) diskutieren theoretische Modelle, bei denen der Einsatz von Datentreuhändern wohlfahrtssteigernde Effekte nach sich ziehen kann.

an den Datentreuhänder abführen. Dazu wiederum müssten die Datentreuhänder erfolgreich ein Vergütungsmodell für individuelle Nutzerinformationen bei den Dienste-Anbietern durchsetzen können. Die möglichen Gründe für die faktische Nicht-Verbreitung dürften maßgeblich in den beschriebenen praktischen Umsetzungshürden für ein solches Vergütungsmodell zu suchen sein. Solange dafür keine praktikablen Lösungen gefunden werden, dürfte sich an der bestehenden Situation wenig ändern.

Datentreuhänder als Instanz zur Wahrnehmung des Rechts auf informationelle Selbstbestimmung haben sich bislang ebenfalls nicht etablieren können. Zwar steht der Rechtsweg prinzipiell jedem offen, der seine diesbezüglichen Rechte verletzt sieht, aber in der Praxis werden Einzelpersonen möglicherweise aus Kostengründen davon abgehalten, ihr Recht gegenüber den Dienste-Anbietern wahrzunehmen. Es könnte beispielsweise sein, dass der Streitwert in solchen Angelegenheiten systematisch zu niedrig angesetzt wird und es deshalb für Anwaltspraxen nicht hinreichend lukrativ ist, sich in solchen Fällen zu engagieren. Das könnte für den Gesetzgeber Anlass sein, entsprechend tätig zu werden, etwa durch die Schaffung einer unabhängigen öffentlichen Instanz, die datenbezogene Nutzeranliegen gegenüber den Dienste-Anbietern kollektiv bündelt und vertritt.[114] Eine solche Instanz versuchsweise und zeitlich befristet zu etablieren, wäre ein denkbarer Weg, um den Umfang von marktlich womöglich nicht hinreichend abgedecktem Vertretungsbedarf ermitteln zu können. Sollte sich auf diese Weise zeigen, dass der Bedarf für die Wahrnehmung persönlicher Datenschutzinteressen merklich höher ist als es sich bis dato gezeigt hat, wäre dies ein Indiz für Markthemmnisse für Datentreuhänder, die sich entweder durch die dauerhafte Etablierung der entsprechenden öffentlichen Instanz oder einer öffentlichen Finanzierung privater Datentreuhänder überwinden ließen. Die Unabhängigkeit einer entsprechenden Instanz – egal ob öffentlich oder privat auf der Basis öffentlicher Förderung – wäre im Übrigen auch ein wirksamer Beitrag, um Vorbehalten gegenüber staatlichen Datenerfassungsaktivitäten – etwa durch die sogenannte Corona-App – glaubwürdig entgegen wirken zu können. Ähnliches gilt für die Nutzung von amtlicherseits erhobenen Sozialdaten zu wissenschaftlichen Zwecken.

Auffallend ist in diesem Zusammenhang, dass Gewerkschaften die bestehenden rechtlichen Möglichkeiten zur Umsetzung des Datentreuhändermodells bislang noch nicht systematisch für ihre Zwecke zu nutzen scheinen. Ähnlich wie eine unabhängige staatliche Instanz zur Durchsetzung des Rechts auf informationelle Selbstbestimmung könnten Gewerkschaften ihren Mitgliedern eine Datentreuhänderschaft anbieten, die interessierten Arbeitnehmern Zugang und Kontrolle über die über sie erhobenen Daten bei ihrem Arbeitgeber verschafft. Ob es daran liegt, dass sich die Gewerkschaften über ihre rechtlichen Möglichkeiten noch zu wenig im Klaren sind, oder ob es Hemmnisse anderer Art gibt, die Gewerkschaften von diesen Möglichkeiten abhalten, ist bislang eine offene Frage.

Eines der wenigen Beispiele für bereits existierende Datentreuhändermodelle im Zusammenhang mit der Nutzung von Online-Diensten ist Verimi. Es handelt sich hier um einen Anbieter, der damit wirbt, Nutzer-Konten bei verschiedenen Dienste-Anbietern über ein einziges Nutzer-Konto bei Verimi zu verwalten. Der daraus erwachsende Vorteil für Dienste-Nutzer dürfte vergleichsweise gering sein und wirft für sich genommen auch noch keinen Ertrag für das Unternehmen ab. Formal handelt es sich bei Verimi zwar um eine Form der Datentreuhänderschaft, aber Verimi sieht sich nicht als eine Instanz, die im Interesse der Dienste-Nutzer monetäre Ansprüche gegenüber den Dienste-Anbietern geltend machen will. Verimi sieht sein Geschäftsmodell eher darin, eine rechtssichere Online-Abwicklung von Vorgängen zu ermöglichen, die

[114] In diesem Sinne hat sich die Kommission Wettbewerbsrecht 4.0 dafür ausgesprochen, den Einsatz von Datentreuhändern zu prüfen. Siehe Bundesministerium für Wirtschaft und Energie (Hrsg.), a.a.o.

eine besondere Legitimierung der persönlichen Identität erfordern, etwa durch Vorlage eines Personalausweises. Erst durch diesen besonderen Service entsteht eine mögliche Geschäftsgrundlage, mit der sich monetäre Einnahmen erzielen lassen. Diese generiert die Plattform aus Beiträgen der Partner-Dienste wie Banken und Versicherungen, deren Zahlungsbereitschaft aus dem Einsparpotenzial durch die Online-Abwicklung von Geschäftsvorgängen resultiert.

3.6 Gleiche Wettbewerbschancen für die Anbieter von Online-Diensten

Wenn im vorliegenden Zusammenhang ein Marktversagen zu konstatieren ist, dann in erster Linie deswegen, weil die Akkumulation von individuellen Nutzerinformationen proprietär bei einigen wenigen monopolartigen Dienste-Anbietern wie Google und Facebook erfolgt und diese Unternehmen dadurch eine marktbeherrschende Stellung bei der Weiterentwicklung neuer Online-Dienste erlangt haben. Neu in den Markt eintretende Unternehmen, und darunter insbesondere kleine Start-Ups, haben dadurch kaum eine realistische Chance, ein innovatives Geschäftsmodell auf der Grundlage von individuellen Nutzerinformationen zu entwickeln. Um hier faire Wettbewerbschancen herzustellen, müssten die sogenannten „Internet-Riesen“ von staatlicher Seite zur Herausgabe anonymisierter Datensätze mit individuellen Nutzerdaten verpflichtet werden, die in geeigneter Form als öffentliches Gut bereit zu stellen wären (Interoperabilität). [115] [116] Im Rahmen der dafür zu schaffenden Dateninfrastruktur wären Datentreuhänder die Instanz, der die Wahrung der Nutzerinteressen im Zusammenhang mit der Verarbeitung der Daten durch die entsprechenden Dienste-Anbieter zukommen müsste.

3.7 Zusammenfassung und Ausblick

Online-Dienste haben inzwischen einen festen Platz in der Lebenswelt vieler Menschen erlangt. Die Nutzung solcher Dienste ist für die Nutzer in den meisten Fällen kostenlos. Finanziert wird die Bereitstellung solcher Dienste stattdessen auf indirektem Weg, etwa über Werbeeinnahmen, dem Verkauf von datenbasierten Modellen zur Produktwerbung oder zur Steuerung politischer Kampagnen, aber auch über Spenden oder eine staatliche Förderung. Die Finanzierung auf der Basis datenbasierter Modelle verdankt ihren wirtschaftlichen Erfolg in erster Linie der Bereitschaft der Dienste-Nutzer, dem Dienste-Anbieter Informationen über sich selbst und/oder ihr Nutzungsverhalten zur kommerziellen Verwertung zu überlassen. Dabei geht es weniger um die kommerzielle Verwertung konkreter personenbezogener Daten als vielmehr um die Entwicklung und Vermarktung von darauf aufbauenden Modellen, die typische Verhaltensmuster abbilden. Die Verfahren, mit denen entsprechende Muster ermittelt werden, sind teilweise hochkomplex und bedienen sich nicht zuletzt neuester Techniken aus dem Bereich der künstlichen Intelligenz. Der so geschaffene Mehrwert eignet sich in vielfältiger Form zur kommerziellen Verwertung und stellt die ökonomische Basis dar, die es den Anbietern von Online-Diensten überhaupt erst erlaubt, ihr Dienste-Angebot bereitzustellen.

Die indirekte Finanzierung von Online-Diensten auf der Basis eines aus Nutzerdaten bestehenden Rohstoffs bildet ein konstitutives Element der Ökonomie von Online-Diensten. Dabei hat sich im Laufe der Zeit relativ schnell eine Situation herauskristallisiert, bei der einer weltweiten Gemeinschaft von Dienste-Nutzern eine vergleichsweise geringe Zahl von Dienste-Anbietern gegenübersteht. Die damit einhergehenden Monopolstrukturen stellen eine Marktunvollkommenheit dar. Daher stellt sich die Frage, inwiefern sich die damit verbundene

---

[115] In diesem Sinne argumentiert auch die Kommission Wettbewerbsrecht 4.0 (siehe Bundesministerium für Wirtschaft und Energie (Hrsg.), a.a.o.).

[116] Ähnliche Gedanken liegen auch den wettbewerbstheoretischen Ausführungen der europäischen Datenstrategie zugrunde.

Asymmetrie der Verhandlungsmacht zwischen Dienste-Anbietern und Dienste-Nutzern mit Hilfe geeigneter regulatorischer Eingriffe beseitigen ließe.

Eine Möglichkeit zur Stärkung der Verhandlungsmacht der Dienste-Nutzer könnte in der Einschaltung von Datentreuhändern bestehen, die als unabhängige Instanz die kollektive Vertretung von Nutzerinteressen gegenüber den Dienste-Anbietern wahrnehmen könnten. Eine wichtige Voraussetzung hierfür ist, dass Datentreuhänder kein darüber hinaus gehendes Verwertungsinteresse an den ihnen überlassenen Daten ausüben dürfen. Festzustellen ist, dass sich am Markt bislang keine Form etabliert hat, die die Datentreuhänderschaft als tragfähiges Geschäftsmodell erkennen ließe. Dafür scheint die Finanzierungsgrundlage zu fehlen, die beispielsweise dann gegeben wäre, wenn es Datentreuhändern gelänge, mit den Dienste-Anbietern Vergütungsmodelle zugunsten der Dienste-Nutzer auszuhandeln, auf deren Grundlage Datentreuhänder ihrerseits Provisionszahlungen von den Dienste-Nutzern verlangen könnten. Die hier angestellte volkswirtschaftliche Analyse zeigt, dass ein solches Vorhaben nicht ohne Weiteres zu begründen ist und im Hinblick auf die praktische Umsetzung mit kaum lösbaren Problemen behaftet wäre.

Eine andere Form zur der Marktunvollkommenheit ergibt sich daraus, dass Dienste-Nutzer, die als Einzelne gegenüber den Dienste-Anbietern das Recht auf informationelle Selbstbestimmung wahrnehmen möchten, auf nahezu unüberwindliche Hürden treffen. Für Anwaltskanzleien scheint dies kein hinreichend lukratives Geschäftsfeld zu sein; möglicherweise, weil der Streitwert in solchen Fällen nicht hoch genug ist. Datentreuhänder könnten in diesem Zusammenhang eine bedeutende Rolle spielen, sofern durch eine staatliche Förderung entsprechende finanzielle Anreize gesetzt würden. Um den Bedarf und den Stellenwert einer Datentreuhänderschaft in diesem Zusammenhang besser einschätzen zu können, erscheint es gerechtfertigt, sie in zeitlich befristeter Form als unabhängige staatlich geförderte Institution zu etablieren. Dies könnte in Form einer staatlichen Instanz, aber auch privatwirtschaftlicher Organisationen mit staatlicher Förderung erfolgen. Die staatliche Finanzierung würde eine für die Dienste-Nutzer weitgehend kostenfreie Mandatierung zur Wahrnehmung des Rechts auf informationelle Selbstbestimmung ermöglichen. Auf der Basis der so gesammelten Erfahrungen ließen sich belastbare Einschätzungen im Hinblick auf künftigen Marktregulierungsbedarf ableiten.

Die Tendenz zur Monopolbildung am Markt für Online-Dienste liefert noch eine weitere volkswirtschaftliche Begründung für das Institut der Datentreuhänder. Die marktbeherrschende Stellung durch einige wenige Online-Dienste behindert den Marktzugang für neu eintretende Wettbewerber. Um diese Eintrittsbarrieren abzubauen, müssten marktbeherrschende Dienste regulatorisch dazu verpflichtet werden, den Zugang zum Rohstoff Nutzerinformationen in anonymisierter Form als öffentliches Gut bereit zu stellen. Datentreuhänder wären hier als unabhängige Instanz gefragt, um die Einhaltung der entsprechenden Datenschutzbestimmungen zu gewährleisten.

Literaturverzeichnis

Acemoglu D.; Makhdoumi A.; Malekian A.; Ozdaglar A. (2020): Too Much Data: Prices and Inefficiencies in Data Markets. Mimeo.

Art.-29-Datenschutzgruppe (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk“ for the purposes of Regulation 2016/679. WP 248.

Art.-29-Datenschutzgruppe (2010). Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“. WP 169.

Aulsbee A.D.; Klenow P.J. (2018): Internet Rising, Prices Falling: Measuring Inflation in a World of E-Commerce. NBER Working Paper No. 24649. Cambridge, MA.

Brandt, J. (2010). Betriebsvereinbarungen als datenschutzrechtliche „Öffnungsklauseln“? DuD, S. 213.

Brockmeyer, H. (2018). Treuhänder für Mobilitätsdaten – Zukunftsmodell für hoch- und vollautomatisierte Fahrzeuge? Erwägungen zur ausstehenden Regulierung des Speicherorts für die Daten nach § 63a Abs. 1 StVG. ZD, S. 258.

Buchner, B. (2016). Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO. DuD, S. 155.

Bundesministerium für Wirtschaft und Energie (Hrsg.): Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft – Bericht der Kommission Wettbewerbsrecht 4.0. September 2019.

CNIL (2019). The CNIL’s restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC. abrufbar im WWW unter der URL: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (zul. aufgerufen am 12.8.2020).

Datenethikkommission. (2019). Gutachten der Datenethikkommission der Bundesregierung. Berlin. abrufbar im WWW unter der URL: https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.pdf (zul. aufgerufen am 12.8.2020).

Diering, B., Timme, H. & Waschull, D. (Hrsg.). (2011). Sozialgesetzbuch X: Sozialverwaltungsverfahren und Sozialdatenschutz - Lehr- und Praxiskommentar. 3. Aufl.: Baden-Baden.

Ehmann, E. & Selmayr, M. (Hrsg.). (2017). Datenschutz-Grundverordnung Kommentar. 1. Aufl.: München.

Europäische Kommission. (2020). GDPR - the fabric of a success story - Europe fit for the digital age. abrufbar im WWW unter der URL: https://ec.europa.eu/commission/presscorner/detail/de/ip_20_1163 (zul. aufgerufen am 12.8.2020).

Europäische Kommission. (2016). An emerging offer of „personal information management services". abrufbar im WWW unter der URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=40118 (zul. aufgerufen am 12.8.2020).

Europäischer Datenschutzbeauftragter. (2016). Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM). Stellungnahme 9/2016. abrufbar im WWW unter der URL: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_de.pdf (zul. aufgerufen am 12.8.2020).

Europäische Kommission (2020): Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Eine europäische Datenstrategie. Brüssel.

European Data Protection Board. (2020). Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4.5.2020. abrufbar im WWW unter der URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf (zul. aufgerufen am 12.8.2020).

Fezer, K. (2020). Wir brauchen eine digitale Bürgerplattform. FAZ vom 26.5.2020, S. 13.

Gierschmann, S. (2020). Gemeinsame Verantwortlichkeit in der Praxis. ZD, S. 69.

Härting, N. (2016). Koppelungsverbot – der Einwilligungskiller nach der DS-GVO. CR-online.de Blog vom 11.10.2016. abrufbar im WWW unter der URL https://www.cr-online.de/blog/2016/10/11/ (zul. aufgerufen am 12.8.2020).

Holland, M. & Krempl, S. (2019). DSGVO-Verstoß: 1&1 muss knapp 10 Millionen Euro Strafe zahlen. heise online 09.12.2019. abrufbar im WWW unter der URL: https://www.heise.de/newsticker/meldung/DSGVO-Verstoss-1-1-muss-knapp-10-Millionen-Euro-Strafe-zahlen-4608676.html (zul. aufgerufen am 12.8.2020).

Holland, M. (2018). Passwörter im Klartext: 20.000 Euro Bußgeld nach DSGVO gegen Knuddels.de. heise online 22.11.2018. abrufbar im WWW unter der URL: https://www.heise.de/newsticker/meldung/Passwoerter-im-Klartext-20-000-Euro-

Bussgeld-nach-DSGVO-gegen-Knuddels-de-4229798.html (zul. aufgerufen am 12.8.2020).

Horn, N., Riechert, A. & Müller, C. (2017). Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen. Studie der Stiftung Datenschutz (Hrsg.). Leipzig. abrufbar im WWW unter der URL: https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_Studie_Neue_Wege_zur_Einwilligung_final.pdf (zul. aufgerufen am 12.8.2020).

Kingreen, T. & Kühling, J. (Hrsg.). (2015). Gesundheitsdatenschutzrecht. 1. Aufl. Studien zum öffentlichen Recht Bd. 13.: Baden-Baden.

Krahmer, U. (Hrsg.). (2011). Sozialdatenschutz – Kommentar nach SGB I und X. 2. Aufl.: Neuwied.

Kremer, S. (2019). Gemeinsame Verantwortlichkeit: Die neue Auftragsverarbeitung. CR, S. 225.

Kühling, J. (2019). Datenschutz im Gesundheitswesen. MedR, S. 611.

Kühling, J. (2017). Neues Bundesdatenschutzgesetz – Anpassungsbedarf bei Unternehmen. NJW, S. 1985.

Kühling, J. & Buchner, B. (Hrsg.). (2018). Datenschutzgrundverordnung/BDSG Kommentar. 2. Aufl.: München.

Kühling, J., Klar, M. & Sackmann, F. (2018). Datenschutzrecht. 4. Aufl.: Heidelberg.

Kühling, J. & Martini, M. et. al. (2016). Die Datenschutz-Grundverordnung und das nationale Recht. Erste Überlegungen zum innerstaatlichen Regelungsbedarf. Münster. abrufbar im WWW unter der URL: http://www.uni-regensburg.de/rechtswissenschaft/oeffentliches-recht/kuehling//medien/k__hling_martini_et_al.-die_dsgvo_und_das_nationale_recht_-_.pdf (zul. aufgerufen am 12.8.2020).

Kühling, J. & Martini, M. (2016). Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht? EuZW, S. 448.

Kühling, J. & Sackmann, F. (2019). Die Musterfeststellungsklage nach Datenschutzverstößen – ein unkalkulierbares Risiko für Unternehmen? DuD, S. 347.

Kühling, J. & Sackmann, F. (2018). Rechte an Daten – Regulierungsbedarf aus Sicht des Verbraucherschutzes? abrufbar im WWW unter der URL:

https://www.vzbv.de/sites/default/files/downloads/2018/11/26/18-11-01_gutachten_kuehling-sackmann-rechte-an-daten.pdf (zul. aufgerufen am 12.8.2020).

Kühling, J. & Schildbach, R. (2020). Corona-Apps — Daten- und Grundrechtsschutz in Krisenzeiten. NJW, S. 1545.

Kühling, J. & Seidel, C. (2010). Die Abrechnung von Gesundheitsleistungen im Spannungsfeld von Datenschutz und Berufsfreiheit - Handlungsbedarf für den Gesetzgeber? GesR, S. 231.

Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg. (2018). Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO für die gemäß Art. 35 Abs. 1 DS-GVO eine Datenschutz-Folgenabschätzung von Verantwortlichen im nicht-öffentlichen Bereich durchzuführen ist. abrufbar im WWW unter der URL: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Liste-von-Verarbeitungsvorgängen-nach-Art.-35-Abs.-4-DS-GVO-LfDI-BW.pdf (zul. aufgerufen am 12.8.2020).

Neun, A. & Lubitzsch, K. (2017). EU-Datenschutzgrundverordnung – Behördenvollzug und Sanktionen. BB, S. 1538.

Paal, B. & Pauly, D. (Hrsg.). (2017). Datenschutz-Grundverordnung Kommentar. 1. Aufl.: München.

Peppet, S. (2012). Privacy & the Personal Prospectus: Should We Introduce Privacy Agents or Regulate Privacy Intermediaries. 97 Iowa L. Rev. Bull., S. 77.

Piltz, C. (2017). Die Datenschutz-Grundverordnung. K&R, S. 85.

Rath, M., Kuß, C. & Maiworm, C. (2016). Die neue Microsoft Cloud in Deutschland mit Datentreuhand als Schutzschild gegen NSA & Co.? Eine erste Analyse des von Microsoft vorgestellten Datentreuhänder-Modells. CR, S. 98.

Regan, P. (2017). Reviving the Public Trustee Concept and Applying It to Information Privacy Policy. 76 Maryland L. Rev., S. 1025.

Richards, N. & Hartzog, W. (2016). Taking Trust Seriously in Privacy Law. 19 Stan. Tech. L. Rev., S. 431.

Roßnagel, A. (Hrsg.). (2003). Handbuch Datenschutzrecht. 1. Aufl.: München.

Säcker, F., Rixecker, R., Oetker, H., Limperg, B. (2019) Münchener Kommentar zum Bürgerlichen Gesetzbuch. 8. Aufl.: München.

Sackmann, F. (2020). Datenschutz bei der Digitalisierung der Mobilität – Eine sektorspezifische Analyse der Leistungsfähigkeit und des Weiterentwicklungsbedarfs der Datenschutzgrundverordnung. 1. Aufl. Recht der Informationsgesellschaft Bd. 43: Baden-Baden.

Sackmann, F. (2017). Die Beschränkung datenschutzrechtlicher Schadensersatzhaftung in Allgemeinen Geschäftsbedingungen. ZIP, S. 2450.

Schaffland, H & Wiltfang, N (Hrsg.). (2017) Datenschutz-Grundverordnung (DS-GVO)/Bundesdatenschutzgesetz (BDSG) Kommentar. EL 10/17 Stand: Dezember 2017: Berlin.

Schneider I. (2019): Regulierungsansätze in der Datenökonomie. Aus Politik und Zeitgeschichte, 24-26/2019, S. 35-41.

Schwartz, K. & Peifer, P. (2017). Datentreuhändermodelle – Sicherheit vor Herausgabeverlangen US-amerikanischer Behörden und Gerichte? CR, S. 165.

Simitis, S. (Hrsg.). (2014). Bundesdatenschutzgesetz Kommentar. 8. Aufl.: Baden-Baden.

Stolleis, M. (2003). Geschichte des Sozialrechts in Deutschland – Ein Grundriss: Stuttgart.

Verbraucherzentrale Bundesverband. (2020). Neue Datenintermediäre – Anforderungen des vzbv an „Personal Information Management Systems“ (PIMS) und Datentreuhänder. Positionspapier vom 19.2.2020: Berlin. abrufbar im WWW unter der URL: https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (zul. aufgerufen am 12.8.2020).

Waldman, A. (2015). Privacy as Trust: Sharing Personal Information in a Networked World, 69 U Miami L. Rev., S. 559.

von Wulffen, M. & Schütze, B. (Hrsg.). (2014) SGB X – Sozialverwaltungsverfahren und Sozialdatenschutz Kommentar. 8. Aufl.: München.

Wybitul, T. (2016). DS-GVO veröffentlicht – Was sind die neuen Anforderungen an die Unternehmen. ZD, S. 253.

Wybitul, T., Haß, D. & Albrecht, J. (2018). Abwehr von Schadensersatzansprüchen nach der Datenschutzgrundverordnung. NJW, S. 113.

Zuboff, S. (2019). The Age of Surveillance Capitalism. The Figth for a Human Futer at the New Frontier of Power. New York. (deutsche Ausgabe: Zuboff, S. (2019). Das Zeitalter des Überwachungskapitalismus: Frankfurt a.M., New York).

Erstellt im Auftrag des Bundesministeriums für Arbeit und Soziales.

Die Durchführung der Untersuchungen sowie die Schlussfolgerungen aus den Untersuchungen sind von den Auftragnehmern in eigener wissenschaftlicher Verantwortung vorgenommen worden. Das Bundesministerium für Arbeit und Soziales übernimmt insbesondere keine Gewähr für die Richtigkeit, Genauigkeit und Vollständigkeit der Untersuchungen.