# ZdiW

ISSN 2702-4040

## ZEITSCHRIFT FÜR DAS RECHT DER DIGITALEN WIRTSCHAFT



AUS DEM INHALT

**Industrie 4.0**

*Weibel,* 3 Fragen – 3 Antworten zur Europäischen KI-Strategie

**E-Commerce**

*Schirmbacher,* Chat-Funktionen auf E-Commerce-Websites
*Filusch,* Digitale Souveränität in Europa dank Schrems II?
*Benedikt,* Datenübermittlung in die USA – Weshalb sich nach Schrems II nichts geändert hat

**Digital Finance**

*Voß,* Der Regierungsentwurf des eWpG und das Depotrecht – Ein Warnruf
*v. Goldbeck,* Das eWpG und Immobilieninvestments

**Digital HR**

*Kuhrau,* Der Mensch – Das vergessene Risiko für die Informations- und Datensicherheit
*Diercks,* Organisatorische Maßnahmen i.S.v. Art. 32 DSGVO – Das unterschätzte »Must-Have« eines jeden Unternehmens

**M&A/Corporate digital**

*Bonhage/Hoffmann,* Technologische Souveränität und deutsche Investitionsprüfung

**Querschnitt**

*Klaas,* Geldbußen bei unternehmensbezogenen Datenschutzverstößen

1

Heft 1
Januar 2021
Seiten 1–36
1. Jahrgang
Art.-Nr. 09672101

Wolters Kluwer

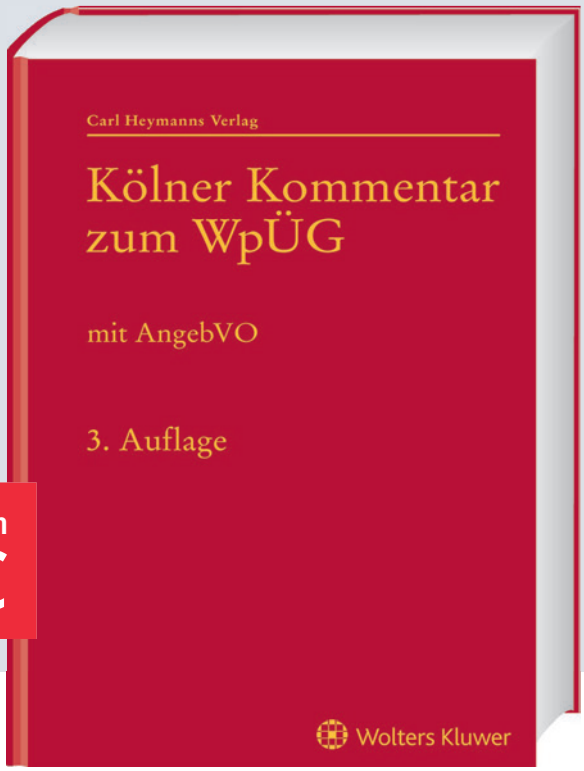
Wolters Kluwer

# Wertpapiererwerbs- und Übernahmerecht

**Mit der 3. Auflage auf dem neuesten Stand im Bank- und Kapitalmarktrecht:**

Die Neuauflage mit neuem Herausgeber Dr. Christoph Seibt berücksichtigt folgende Gesetzesänderungen:

- FiMaNoG
- Übernahmerichtlinien-UmsetzungsG
- Transparenzrichtlinien-UmsetzungsG
- ARUG II
- FGG-Reformgesetz


**Jetzt vorbestellen**
**ca. 289 €**

**Hirte/Seibt, *Kölner Kommentar zum WpÜG* - im Modul Bank- und Kapitalmarktrecht auf wolterskluwer-online.de.**

Profitieren Sie im Abonnement von einer sowohl wissenschaftlich fundierten, wie auch praxisorientierten Zusammenstellung von Fachinformationen von Carl Heymanns. Hohe Qualität und Top-Autoren bieten eine zuverlässige, lösungsorientierte Grundlage für eine erfolgreiche Beratungspraxis - inkl. der Wolters Kluwer Recherche mit Zugriff auf die kostenlose Rechtsprechungs- und Gesetzesdatenbank.

Jetzt QR-Code scannen und mehr erfahren.

wolterskluwer-online.de

ALLES, WAS EXPERTEN BEWEGT.

# ZdiW

## ZEITSCHRIFT FÜR DAS RECHT DER DIGITALEN WIRTSCHAFT




## Inhalt 1 · 2021


ZdiW aktuell **0.2**
Impressum **0.4**

### Editorial

Das Recht der digitalen Wirtschaft: Struktur und Profil
Schriftleitung und Verlag **1**

### Industrie 4.0

3 Fragen – 3 Antworten zur Europäischen KI-Strategie
Beat Weibel, München **3**

### E-Commerce

Chat-Funktionen auf E-Commerce-Websites
Dr. Martin Schirmbacher, Berlin **4**

Digitale Souveränität in Europa dank Schrems II?
Karina Filusch, Berlin **9**

Datenübermittlung in die USA – Weshalb sich nach Schrems II nichts geändert hat
Kristin Benedikt, Regensburg **12**

### Digital Finance

Der Regierungsentwurf des eWpG und das Depotrecht – Ein Warnruf
Dr. Thorsten Voß, Frankfurt am Main **16**

Das eWpG und Immobilieninvestments
Axel v. Goldbeck, Berlin **20**

### Digital HR

Der Mensch – Das vergessene Risiko für die Informations- und Datensicherheit
Sascha Kuhrau, Simmelsdorf **23**

Organisatorische Maßnahmen i.S.v. Art. 32 DSGVO – Das unterschätzte »Must-Have« eines jeden Unternehmens zur datenschutzrechtlichen Haftungsminimierung
Nina Diercks, M.Litt. (University of Aberdeen), Hamburg **27**

### M&A/Corporate digital

Technologische Souveränität und deutsche Investitionsprüfung
Dr. Jan D. Bonhage, LL.M. (NYU)/Erasmus Hoffmann, LL.M. (Cambridge), Berlin **30**

### Querschnitt

Geldbußen bei unternehmensbezogenen Datenschutzverstößen: Was bleibt von der datenschutzrechtlichen Verantwortlichkeit auf der Haftungsseite?
Dr. Arne Klaas, Berlin **34**

ZdiW aktuell

**Redaktion:**
Leah Ngabi, Rechtsanwältin
Wolters-Kluwer-Str. 1, 50354 Hürth
Tel.: 02233/3760-7190
ZdiW-redaktion@wolterskluwer.com

# News

## ■ Europäische Kommission veröffentlicht Vorschläge zum Gesetz für digitale Dienste (Digital Services Act – DSA) und zum Gesetz für digitale Märkte (Digital Markets Act – DMA)

Die Europäische Kommission am 15.12.2020 zwei jeweils rund 85 Seiten starke Verordnungsvorschläge präsentiert, mit denen die Digitalwirtschaft fit für die Zukunft gemacht werden soll.

Der **DSA** übernimmt das Haftungsprivileg für und die Definition von Durchleitungs- bzw. Access-, Caching- und Hosting-Provider sowie das Verbot von allgemeinen Überwachungspflichten aus den Art. 12 bis 15 E-Commerce Richtlinie und soll diese aufheben. Zugleich wird mit Online Plattformen eine neue Unterkategorie der Hosting-Provider eingeführt. Den ganz großen Online Plattformen, sogenannten Very Large Online Platforms (»VLOP«) mit mindestens 45 Mio. Nutzern werden dabei spezielle Pflichten auferlegt. Neu eingeführt werden sollen unter anderem

- eine Regelung, nach der die Haftungsprivilegierung für sogenannte »Internet Society Services« (ISS) auch dann aufrecht erhalten werden soll, wenn diese freiwillige Maßnahmen zur Erkennung, Identifizierung, Entfernung oder Deaktivierung von Inhalten vornehmen (Art. 6);
- detaillierte Verpflichtungen für ISS zum Umgang mit Inhalten und zur Herausgabe von Informationen (u.a. Art. 8 und 9 DSA);
- die Verpflichtung zur Einrichtung eines sogenannten »Single Point of Contact« (Art. 10 DSA) oder zur Benennung eines rechtlichen Vertreters innerhalb der EU (Art. 11 DSA);
- die Verpflichtung, transparente Bestimmungen zum Umgang mit hochgeladenen Inhalten in den jeweiligen Geschäftsbedingungen der ISS vorzuhalten (Art. 12 DSA);
- die Verpflichtung zu regelmäßigen Transparenzberichten (außer Micro- und Kleinunternehmen) (Art. 13 DSA);
- für Hosting-Provider ein Notice & Action Mechanismus (Art. 14 DSA);
- für Online Plattformen ein Beschwerdeverfahren (Art. 17 DSA),
- die Rolle des nationalen »Digital Services Coordinator«, dem umfangreiche Befugnisse zur Kontrolle und Strafe auf Basis des DSA zukommen (Strafen von bis zu 6 % der Jahresumsatzes, Art. 42).

Mit dem **DMA** sollen Vorschriften für Plattformen eingeführt werden, die im digitalen Sektor als »Torwächter«, sog. Gatekeeper, fungieren. Gemäß dem Verordnungsentwurf handelt es sich bei Gatekeepern um Digitalkonzerne (u.a. Anbieter von Vermittlungsdiensten, Suchmaschinen, Video-Sharing, soziale Netzwerke und Messengerdienste), die

- aufgrund ihrer Größe einen erheblichen Einfluss auf den Binnenmarkt haben (Jahresumsatz von mind. 6,5 Mrd. € im EWR über die letzten drei Jahre oder ein Marktwert von mind. 65 Mrd. €);
- eine bedeutende Plattform betreiben, um Nutzer/Verbraucher zu erreichen (über 45 Mio. aktive Endnutzer und über 10.000 aktive gewerbliche Nutzer mit Niederlassung in der EU) und
- denen eine (voraussichtlich) gefestigte und dauerhafte Wettbewerbsposition im Markt zugeschrieben werden kann.

Wenn diese Schwellenwerte nicht erfüllt sind, soll die Kommission im Rahmen einer Marktuntersuchung die spezifische Situation eines bestimmten Unternehmens prüfen und beschließen können, es als Gatekeeper einzustufen.

Für die Nichteinhaltung der geplanten Wettbewerbsvorschriften sind Sanktionen, u.a. Geldstrafen von bis zu 10 % des weltweiten Umsatzes des jeweiligen Unternehmens (Art. 26 DSM), vorgesehen. Im Wiederholungsfall behält es sich die Kommission zudem vor, ebenso strukturelle Maßnahmen zu ergreifen (z.B. Verkauf oder Abspaltung von Geschäftsbereichen).

## ■ GAIA-X Gründung nimmt Form an

Das europaweite Cloud- und Dateninfrastrukturprojekt GAIA-X hat die Etablierung eines souveränen, europäischen Datenökosystems im Einklang mit europäischen Werten zum Ziel und strebt den Aufbau einer digitalen Infrastruktur »Made in Europe« an. Die aus dem Bundesministerium für Wirtschaft und Energie (BMWi) stammende Initiative mündete zwischenzeitlich in der Gründung einer Betreibergesellschaft in Form einer AISBL (*Association internationale sans but lucratif*) nach Belgischem Recht mit Sitz in Brüssel. Zu den 22 deutschen und französischen Gründungsmitgliedern zählen unter anderem Atos SE, das Fraunhofer Institut, Safran S.A. und SAP SE. Zweck und Ziel der AISBL wird die Konsolidierung und Erleichterung der Zusammenarbeit innerhalb der GAIA-X-Gemeinschaft und den teilnehmenden Unternehmen und Organisationen sein. Die Organisation wird nun die regulatorischen Rahmenbedingungen entwickeln, um ihre Mitglieder zu vertreten, die internationale Zusammenarbeit fördern zu können und die erforderlichen Dienste zur Verfügung stellen zu können. Der gewählte rechtliche Rahmen soll die Mitglieder innerhalb der Vereinigung auch zu den gemeinsamen Zielen wie digitaler

# Editorial

Prof. Dr. Mary-Rose McGuire,
M. Jur. (Göttingen)
Universität Osnabrück

Prof. Dr. Bernd J. Hartmann, LL.M.
(Virginia)
Universität Osnabrück

Jan Schmidt
Wolters Kluwer

Leah Ngabi, Rechtsanwältin
Wolters Kluwer

## Das Recht der digitalen Wirtschaft: Struktur und Profil

Liebe Leserin, lieber Leser,

die Zeitschrift für das Recht der digitalen Wirtschaft (ZdiW) startet mit ihrer Erstausgabe in einer Rekordphase der COVID-19-Pandemie. Die ohnehin schon zügig voranschreitende Digitalisierung des Wirtschafts- und Gesellschaftslebens hat im zurückliegenden Jahr 2020 eine erhebliche Intensivierung und Beschleunigung erfahren. Viele von Ihnen werden diese Zeilen im Homeoffice lesen – sei es auf Ihrem Computer, Tablet, Smartphone oder im gedruckten Heft, das Sie online bestellt haben.

Mit »digitaler Wirtschaft« verbinden gewerbliche Anbieter von Wirtschaftsleistungen einerseits innovative Produkte, Dienstleistungen, Fertigungsmethoden und Geschäftsmodelle. Andere, oft traditionelle Akteure sehen sich unter reaktivem Handlungsdruck. Ob eigenmotiviert oder unter äußeren Zwängen: Für Wirtschaftstreibende bedeuten die Begriffe »digitale Wirtschaft« und »digitale Transformation« vieles, wenn nicht, alles anders zu denken und zu betreiben als Jahrzehnte, ja Jahrhunderte zuvor.

Die digitale Wirtschaft und ihre Funktionsweise bringen schon auf tatsächlicher Ebene viele Fragen mit sich. Es beginnt mit der Schwierigkeit einer klaren Definition des Begriffs und geht bis hin zu konkreten Einzelfragen, wie etwa, was eine Smart Factory ist oder wie eine Kryptowährung technisch funktioniert.

Zugleich bewegt sich die digitale Wirtschaft in einem Rechtsraum, dessen Prinzipien und Systematik unabhängig von der Digitalisierung gelten. Der Einsatz neuer Technologien muss an den Grundsätzen insbesondere von Privatautonomie, Persönlichkeits- und Eigentumsschutz sowie fairen Wettbewerbs orientiert werden. Soweit der Gesetzgeber mit Digitalisierungsreformen reagiert, steht die Rechtspraxis vor der Aufgabe, die neuen Regeln zu lernen und zu verstehen; wo und solange eine Modernisierung des Rechts ausbleibt, ist der juristische Umgang mit neuen technisch-tatsächlichen Phänomenen erst recht schwierig. Der Ausweg, die ungelöste Frage offen zu lassen, ist dem Praktiker indes versperrt.

Die ZdiW verfolgt vor diesem Hintergrund das Ziel, dem Begriff der digitalen Wirtschaft Struktur und Profil zu verleihen, die spezifisch rechtlichen Fragestellungen aufzugreifen und konkret zu klären, welche Folgen sich aus neuen technischen Möglichkeiten und rechtlichen Vorgaben für die Beratungs- bzw. Spruchpraxis ergeben.

Charakteristisch für die ZdiW ist ihre Gliederung. Die sonst in juristischen Fachzeitschriften übliche Zweiteilung in »Beiträge« einerseits und »Rechtsprechung« andererseits wird abgelöst durch eine inhaltliche Gliederung in die fünf relevanten Praxisbereiche

- Industrie 4.0: Rechtsfragen der digital vernetzten Produktion
- E-Commerce: Rechtsfragen des digitalen Handels, Marketings und Vertriebs
- Digital Finance: Rechtsfragen der Digitalisierung von Finanzierung, Zahlungsverkehr und Rechnungswesen
- Digital HR: Rechtsfragen der Digitalisierung im Bereich der Personalgewinnung und -verwaltung
- M&A/Corporate digital: Rechtsfragen digitaler Technologien bei Unternehmensfusionen sowie der digitalen Organisation von Unternehmen.

Außerdem erscheinen Beiträge, die mehrere Rubriken und/oder grundlegende Rechtsfragen der digitalen Wirtschaft betreffen, in der Rubrik »Querschnitt«. Rechtsprechung wird nicht kommentarlos wiedergegeben, sondern analysiert, insbesondere ihre Reichweite und Bedeutung eingeordnet.

Aufbau und Inhalte der ZdiW zielen darauf ab, Ihnen effizient und verständlich eine Orientierung im Geflecht jener vielfältigen Rechtsfragen des digitalen Wirtschaftslebens zu bieten, die sich in Ihrem juristischen Arbeitsalltag stellen. In diesem Sinne wünschen wir Ihnen mit der Zeitschrift gute, neue Erkenntnisse, frohes Schaffen und viel Erfolg.

Bleiben Sie gesund!

Schriftleitung und Verlag

ZdiW
ZEITSCHRIFT FÜR DAS RECHT DER DIGITALEN WIRTSCHAFT

Heft 1/2021 · 1. Jahrgang





Interview

# 3 Fragen – 3 Antworten zur Europäischen KI-Strategie

Beat Weibel, Chief IP Counsel, Siemens AG, München

**1. Die Europäische Kommission hat 2018 eine KI-Strategie[1] vorgelegt, 2019 ein Weißbuch zur Künstlichen Intelligenz.[2] Im Oktober 2020 hat das Europäische Parlament eine Resolution zum Schutz von KI-Technologien[3] erlassen. Durch alle diese Dokumente zieht sich wie ein roter Faden das Ziel, einen neuen Rechtsrahmen zu schaffen, um den Herausforderungen und Chancen der KI zu »begegnen«. Der Fokus liegt darauf, einerseits das Vertrauen in KI-Technologien zu stärken, andererseits potenzielle Auswirkungen auf Bürger, Gesellschaft und Wirtschaft bestmöglich zu regulieren. Erst an dritter Stelle wird das Ziel genannt, ein wirtschaftliches Umfeld zu schaffen, in dem Forschung und Innovation florieren können. Als Beispiel für nötige Änderungen werden EU-Produktsicherheits- und Produkthaftungsvorschriften genannt.**

**Ist der Regelungsansatz zu ängstlich?**

**Beat Weibel:** Ja, Produktsicherheits- und -haftungsvorschriften sind sicher wichtig, um Vorbehalte gegenüber den neuen KI-basierten technologischen Entwicklungen zu entkräften. Es sollte aber nicht nur darum gehen, KI sicher zu machen, sondern auch sie zu fördern, da KI enormes Potential z.B. in der Analyse, Diagnostik oder Automatisierung birgt. Mit KI kann Energie gespart werden, Krankheiten können besser geheilt werden, der Verkehr kann effizienter geleitet werden oder die Verfügbarkeit von Zügen kann erhöht werden. Hinzu kommt, dass die EU im Moment bei der Entwicklung von KI nicht mehr führend ist. Die entsprechenden Hotspots findet man in China, Korea und den USA. Die Sicherheitsvorschriften sollten ergänzt werden durch KI-Innovationen fördernde und entsprechende Investitionen schützende Maßnahmen wie z.B. Patentschutz (siehe Frage 2) oder ein EU-Software-Register.

**2. Die Entschließung des Europäischen Parlaments erwähnt die Notwendigkeit, das Recht des Geistigen Eigentums und insbesondere das Patentrecht für die neue Technologie zu öffnen. Das sei notwendig, um Anreize für KI-Erfindungen sowie Chancen für europäische Unternehmen und Start-Ups zu schaffen. Zugleich werden als mögliche Probleme angesprochen, dass es bei KI-Erfindungen häufig nicht möglich sei, die Erfindung so zu offenbaren, dass sie von einem Fachmann nachgearbeitet werden könne; andererseits dass das Patentrecht als Anreiz für eine schöpferische Leistung angesehen werde, sodass nach der klassischen Konzeption, durch KI erzeugte Schöpfungen ausgeschlossen wären.**

**Ist das Patentrecht aus Sicht der Industrie das passende Schutzrecht, um Innovation und Investition in KI zu fördern?**

**Beat Weibel:** Ja, denn KI-Erfindungen sind in erster Linie computerimplementierte Erfindungen (Computer Implemented Innovations, CII). Das europäische Patentrecht und die Rechtsprechung beim europäischen Patentamt haben eine verlässliche und anerkannte Praxis entwickelt, wie CII mit Patenten geschützt werden können. In einer ersten Näherung besteht somit kein Grund, KI-Erfindungen anders zu behandeln. Grundsätzlich ist zu unterscheiden zwischen Erfindungen, die KI als Unterstützung verwenden, grundlegenden KI-Technologien und durch KI unabhängig geschaffenen (gegenständlichen) Erfindungen. Probleme mit der Offenbarung treten nur bei der ersten Kategorie auf, und das Problem der Nacharbeitbarkeit sollte sich lösen lassen, indem z.B. die Trainingsdaten offenbart werden. Bei der zweiten Kategorie liegen die Probleme vielmehr im Bereich der Patentierbarkeit als solcher, da es sich meist um mathematische Methoden handelt, die technisch umgesetzt werden. Die dazu entwickelten Grundsätze der Patentierbarkeit von CII führen hier ebenfalls zum Erfolg. Bei der dritten Kategorie eröffnet sich ein weiteres Problem, nämlich dass der Erfinder oder die Erfinderin keine natürliche Person mehr darstellt. Wird der Patentschutz z.B. von durch ein KI-System unabhängig geschaffenen elektronischen Topologien aufgrund der mangelnden natürlichen Erfinderschaft verweigert, benachteiligt man Investitionen in solche

1 KOM (2018)237.
2 KOM (2020)65.
3 Entschließung des Europäischen Parlaments von 20.10.2020 zu den Rechten des Geistigen Eigentums bei der Entwicklung von KI-Technologien, EP(2020)277.

Technologien. Wird künstlich eine natürliche Person als Erfinder benannt, spiegelt man falsche Tatsachen vor und – insbesondere in Deutschland wichtig – vergütet möglicherweise Personen, die gar nicht kreativ tätig wurden. Solche Erfindungen mögen heute noch Zukunftsmusik sein, doch werden bei Siemens bereits jetzt elektronische Schaltungen zu einen hohen Autonomiegrad von KI-Systemen designt. Abhilfe könnte hier die Erweiterung des Erfinderbegriffes auf juristischen Personen sein, die das KI-System einsetzen und kontrollieren. Dass Erfinder derzeit nur natürliche Personen sein können, liegt darin begründet, dass es zur Zeit der Schaffung der Patentgesetze oder der PVÜ schlicht nicht denkbar war, dass ein System erfinderisch oder kreativ tätig sein könnte. Genauso wie eine Anpassung des Anmelderbegriffes im AIA[4] des US-Patentrechts überfällig war, wäre es ein wichtiger Schritt für die Zukunft, den Erfinderbegriff auf juristische Personen zu erweitern. Ein solcher Schritt wäre auf jeden Fall besser, als Maschinen Rechte und Privilegien zu erteilen.

**3. KI wird als neue Grundlagentechnik bezeichnet, die nicht nur zu großen Umwälzungen in Industrie und Privatleben führen, sondern auch bald in vielen Sektoren zum Standardrepertoire gehören wird. Das wirft die Frage auf, welche Bedeutung die Sicherung von Interoperabilität durch Standardisierung für neue KI-Technologien haben wird und ob die bisher von der Rechtsprechung im Kontext der Telekommunikation hierzu entwickelten Grundsätze auch für diese neue Technologie geeignet sind.**

**Sollte der Gesetzgeber eingreifen und einen verlässlichen Rahmen für die Lizenzierung von standardessentiellen Patenten (SEP) schaffen?**

**Beat Weibel:** Die Lizenzierung von SEP wird stark kontrovers diskutiert, weil im Bereich der mobilen Kommunikation tatsächlich einige Probleme bestehen. Es gibt aber auch andere SEP-dominierte Bereiche der Digitalisierung wie z.B. die Videokompression, -codierung oder das Videobroadcasting, wo die SEP-Lizenzierung zur Zufriedenheit aller Beteiligten funktioniert und auch KMU auf einfache Art und Weise Zugang zum größten Teil der SEPs erhalten. Der Unterschied zwischen mobiler Kommunikation und den erwähnten Videoanwendungen liegt darin, dass im letzten Fall funktionierende Pools bestehen, an denen nahezu alle SEP-Inhaber und -Lizenznehmer teilnehmen. Mit anderen Worten, funktionierende und breit abgestützte Pools sind ein Schlüssel zu einer funktionierenden SEP-Lizenzierung. Das gleiche gilt für die Essentialitätsprüfung durch die Pools, die den diesbezüglichen Goldstandard darstellen. Politik bzw. Gesetzgeber wären deshalb gut beraten, in einem ersten Schritt zu untersuchen und zu verstehen, wieso die Lizenzierung auf einem SEP-Gebiet funktioniert und auf einem anderen nicht. Daraus ließen sich günstige Rahmenbedingungen wie die steuerliche Incentivierung von qualifizierten oder zertifizierten Pools ableiten. Zum Beispiel könnten Lizenzeinnahmen eines solchen Pools steuerlich begünstigt oder Lizenzzahlungen als notwendige Forschungsausgaben steuerlich abgezogen werden. Solche Rahmenbedingungen wären m.E. viel erfolgreicher als gesetzlich oder politisch aufgesetzte, breite Essentialitätsprüfungen, die möglicherweise die Transparenz erhöhen, aber einem KMU nichts nützen, da die Lizenzgebühr davon nicht betroffen ist, oder Eingriffe in die Privatautonomie wie License-to-all-Konzepte. Durch transparent funktionierende, europäische Pools wäre der Zugang zu SEP z.B. für 5G für alle Marktteilnehmer gewährleistet. Darüber hinaus könnte sichergestellt werden, dass die Technologie in Europa bleibt. Das amerikanische Steuersystem macht es vor.

**Das Interview führte Prof. Dr. Mary-Rose McGuire.**

4 Leahy-Smith America Invents Act 2012 (Änderung des Patents Act 1952).

## E-Commerce

### Überblick

# Chat-Funktionen auf E-Commerce-Websites

Rechtsanwalt Dr. Martin Schirmbacher, Berlin*

Chat-Funktionen auf E-Commerce-Websites erfreuen sich zunehmender Beliebtheit. Um sie rechtssicher einzusetzen, gilt es allerdings zu prüfen, ob Verträge über diesen Kanal geschlossen werden können sollen. Außerdem sind die datenschutz- und wettbewerbsrechtlichen Vorgaben einzuhalten.

## I. Chat-Funktionen im E-Commerce

Immer öfter bieten Unternehmen ihren potenziellen Kunden die Möglichkeit, in direkte Kommunikation über geschriebene Nachrichten zu treten. Die Versicherungswirtschaft hat hier eine gewisse Vorreiterrolle.[1] Auch andere Branchen mit erklärungsbedürftigen Produkten setzen schon lange auf den Austausch von Direktnachrichten auf ihren Websites. Dieser Beitrag gibt einen Überblick über rechtliche Fragen bei der Einführung von Chat-Funktionen und Chatbots im E-Commerce.[2]

Chatfunktionen werden zu unterschiedlichen Zwecken eingesetzt. Häufig begegnen einem kleine Chat-Fenster unmittelbar auf der Startseite von Shops und erfüllen dort vor allem eine Beratungsfunktion. Aufgabe ist in der Regel, den Bedarf von Kunden zu ermitteln und diese auf die richtige Produktdetailseite weiterzuleiten, um dort einen Vertrag abzuschließen. Denkbar ist auch eine detaillierte Beratung der Nutzer:innen mit dem Ziel eines späteren Abschlusses. Bisweilen werden auch persönliche Daten (insbesondere Telefon-

* Fachanwalt für IT-Recht, HÄRTING Rechtsanwälte.

1 Vgl. *Barel* VW 2020, 62 zum Einsatz von Chatbots als vertrauensbildende Maßnahme in der Versicherungswirtschaft.

2 Zum Einsatz von unternehmens- und konzerninternen Chat- und Co-Working-Funktionen vgl. Hussain/Graue ITRB 2020, 96.

nummer oder E-Mail-Adresse) aufgenommen, um die potenziellen Kund:innen später erneut kontaktieren zu können.

Auch im After-Sales-Service wird Live-Chat eingesetzt, um Beschwerden und konkrete Fragen von Kund:innen adressieren zu können. Hier ist in der Regel erforderlich, die Kund:innen konkret zu identifizieren, um spezifische Aussagen zu in der Vergangenheit getätigten Käufen treffen zu können. Denkbar sind etwa konkrete Aussagen zu Stornierungen oder Ersatzlieferungen. Bisweilen werden auch weitere Verträge geschlossen, etwa über Ersatzteile, Zubehör oder andere ergänzende Produkte. Dass ein Chat-Tool grundsätzlich geeignet ist, spezifische Fragestellungen von Interessierten zu beantworten, haben nicht zuletzt auch EuGH[3] und BGH[4] festgestellt. Eine Chat-Funktion genügt – ähnlich wie ein Rückrufsystem – den Anforderungen an eine schnelle Kontaktaufnahme und kann eine effektive Kommunikation sicherstellen.

Chat-Funktionalitäten auf Websites können unmittelbar auf dem Server des Website-Anbieters laufen oder als Drittinhalt eingebunden sein. In letzterem Fall läuft die Kommunikation über den Server eines externen Anbieters – ohne, dass die Nutzer:innen dies bemerken. Häufig werden bei dem Einsatz von Chat-Funktionen zugleich Cookies gesetzt.[5] Diese dienen der Wiedererkennung der Nutzer:innen für den Fall, dass diese die Seite kurzfristig verlassen und dann zurückkehren. Ist der User eingeloggt, ist auch denkbar, den Chatverlauf zu dem Benutzerkonto zu speichern und dort dauerhaft abzulegen.

Derzeit noch der Normalfall ist die Echtzeitkommunikation mit den Nutzer:innen durch reale Personen. Immer häufiger werden aber auch Chatbots eingesetzt. Dabei versucht die hinter dem Bot stehende Software das Problem der Nutzer:innen zu verstehen und entsprechend zu reagieren.[6] Meist haben Chatbots noch eingeschränkte Funktionen. Es ist aber nur eine Frage der Zeit, bis diese deutlich besser werden und tatsächlich qualifizierte Antworten geben können.[7] Im E-Commerce werden häufig auch hybride Formen eingesetzt, bei denen scheinbar einfache Anliegen automatisiert und komplexere Anfragen durch Menschen beantwortet werden.[8]

## II. Vertragsschluss und Verbraucherrecht

### 1. Vertragsschluss und Dokumentation

Dass im Rahmen von Chat-Funktionen unmittelbar Verträge geschlossen werden können, steht außer Frage, ist aber bisher eher die Ausnahme. Umso wichtiger sind klare unternehmensinterne Regelungen zum Umgang mit einer Vertragsanbahnung im Chat. Lässt sich dies einfach realisieren, wird es aus juristischer Sicht häufig empfehlenswert sein, den Vertragsschluss im Chat auszuschließen und Kund:innen auf die Bestellseiten zu verweisen. E-Commerce-Unternehmen, die es gezielt auf Abschlüsse im Chat anlegen, sollten dagegen geeignete Maßnahmen dafür treffen, dass ein Vertragsschluss dokumentiert ist. Ist der Kunde eingeloggt, bietet es sich an, den Chat-Verlauf unmittelbar zu dem Kundenkonto des Kunden zu speichern.[9] Existiert kein Kundenkonto ist die Abwicklung eines Kaufs schwierig. Ist nicht einmal eine E-Mail-Adresse vorhanden, kommt wohl nur eine Vorkasse-Abwicklung in Betracht. Auch hier ist essentiell, den Chat-Verlauf in geeigneter Weise zu protokollieren.

Für bestimmte Branchen gelten zusätzliche Dokumentationspflichten, z.B. müssen nach § 83 Abs. 3 Satz 1 WpHG Wertpapierdienstleistungsunternehmen auch die elektronische Kommunikation (auch Chats)[10] mit ihren Kund:innen u.U. aufzeichnen (so. Taping).[11]

### 2. Fernabsatzrecht und Recht im elektronischen Geschäftsverkehr

Handelt es sich um einen B2C-Vertrag, ist grundsätzlich das Fernabsatzrecht einschlägig. Fraglich ist allein, ob der Vertragsschluss im Einzelfall im Rahmen eines für den Fernabsatz organisierten Vertriebs- und Dienstleistungssystems i.S.v. § 312c Abs. 1 BGB erfolgt.[12] Die Voraussetzungen dafür liegen bei E-Commerce-Unternehmen natürlich vor. Allerdings kommt es auf jeden einzelnen Vertriebskanal an. So mag die ausnahmsweise Ausführung einer E-Mail-Bestellung in einem Online-Shop nicht im Rahmen des Fernabsatzsystems »Shop« erfolgen.[13] Chat-Funktionen sind aber unmittelbar in die Website integriert und in der Regel kein gesonderter Vertriebsweg. Daher gilt in der Regel Fernabsatzrecht, wenn ausnahmsweise unmittelbar im Chat ein Vertrag geschlossen wird.

Neben dem Verbraucherwiderrufsrecht gelten damit auch die Informationspflichten. Denkbar ist, hier die Erleichterungen nach Art. 246a § 3 EGBGB eingreifen zu lassen, weil jedenfalls innerhalb des Chatfensters nur eine begrenzte Darstellungsmöglichkeit besteht.[14] Ist der Chat allerdings an einen Online-Shop »angeschlossen«, können ohne Weiteres Links zu den Produktdetails und sonstigen Informationen gesetzt werden.

Auch die Regelungen über die Pflichten im elektronischen Geschäftsverkehr sind grundsätzlich einschlägig.[15] Nach § 312i Abs. 1 Satz 1 Nr. 3 BGB muss der Zugang der Bestellung unverzüglich auf elektronischem Wege bestätigt werden. Zwar erfüllt die Chat-Funktion die Voraussetzungen von § 312i Abs. 1 BGB, doch greift die Ausnahme des § 312i Abs. 2 Satz 1 BGB, weil der Vertragsschluss über den Direktaustausch von Chat-Nachrichten als individuelle Kommunikation zu qualifizieren ist.[16] Das ist auch dann der Fall,

3 EuGH v. 10.07.2019, Az. C-649/17, CR 2019, 526, 528; vgl. *Becker/Rätze* WRP 2019, 1124, 1127.
4 BGH v. 19.12.2019, Az. I ZR 163/16, CR 2020, 464, 465 f. zu Art. 246a § 1 Abs. 1 Satz 1 Nr. 2 EGBGB.
5 Zum Einwilligungserfordernis für Cookies: BGH v. 28.05.2020, Az. I ZR 7/16, WRP 2020, 1009; *Ettig/Herbrich* K&R 2020, 719; *Kollmar/Schirmbacher* WRP 2020, 1015 ff.
6 Vgl. *Conrad* ITRB 2018, 116; *Köbrich/Froitzheim* WRP 2017, 1188; *Lorenz* K&R 2019, 1, 2 f.
7 So schon *Köbrich/Froitzheim* WRP 2017, 1188.
8 Vgl. *Barel* VW 2020, 62, 64 f.; *Becker/Rätze* WRP 2019, 1124, 1127.
9 Zu den datenschutzrechtlichen Voraussetzungen s.u. bei IV.2.b.
10 *Roth/Blessing* CCZ 2017, 8, 11.
11 Vgl. Ebenroth/Boujong/Joost/Strohn/*Pölzig*, WpHG, 4. Aufl. 2020, § 83 Rn. 3.
12 Vgl. zu den Voraussetzungen: BGH v. 19.11.2020, Az. IX ZR 133/19, BB 2020, 2881 (Ls.); BGH v. 21.10.2004, Az. III ZR 380/03, NJW 2004, 3699, 3770 f.; Spindler/Schuster/*Schirmbacher*, Recht der elektronischen Medien, 4. Aufl. 2019, § 312c BGB Rn. 16; *Ernst* NJW 2014, 817, 819.
13 *Schirmbacher* (s. Fn. 12), § 312c BGB Rn. 19.
14 So jedenfalls *Brunotte* CR 2017, 583, 586 f.
15 Vgl. *Schirmbacher* (S. Fn. 12) § 312i BGB Rn. 11 ff.; MüKoBGB/*Wendehorst*, 8. Aufl. 2019, § 312i Rn. 15.
16 Differenzierter im Ergebnis aber für herkömmliche Chat-Funktionen wie hier: MüKoBGB/*Wendehorst*, 8. Aufl. 2019, § 312i Rn. 48 f.; vgl. auch *Brunotte* CR 2017, 583, 587 f. am Beispiel von virtuellen Assistenten; anders für Sprachassistenten: *Winkelmann* CR 2020, 451, 455.

wenn im Rahmen des Chats Links zu Produktdetailseiten gepostet werden und die Nutzer:innen sich zugleich auf der Website umsehen. Solange Antrag und Annahme im Chat erklärt werden, greift die Ausnahmebestimmung. Auch die besonderen Pflichten von § 312j Abs. 3 BGB, wonach ein Bestell-Button in bestimmter Weise zu beschriften ist, greifen in Chat-Funktionen nicht. Es fehlt schlicht an der Schaltfläche, auf die die Norm Bezug nimmt.[17] Zudem sind gem. § 312j Abs. 5 BGB die besonderen Informationspflichten nicht anwendbar, wenn der Vertrag durch individuelle Kommunikation zustande kam.[18]

## III. UWG

Auch unter wettbewerbsrechtlichen Aspekten kann die Einführung von Chat-Funktionen problematisch sein.

### 1. Kein Einwilligungserfordernis nach § 7 UWG

Allerdings gelten die Anforderungen an das E-Mail-Marketing aus § 7 Abs. 2 Nr. 3 UWG nicht für Chats. Voraussetzung für die Einwilligungsbedürftigkeit ist nämlich, dass Werbung unter Verwendung elektronischer Post versendet wird. Dies bedingt, dass Nachrichten in ein Postfach gelangen, das die Empfänger:innen zeitversetzt abrufen können.[19] Daran fehlt es bei Chats, die in Echtzeit ausgetauscht und gerade nicht im Endgerät der Teilnehmenden dauerhaft gespeichert werden, bis diese die Nachrichten löschen.[20] Im Rahmen einer vertragsanbahnenden Chat-Kommunikation bedarf es also auch dann keiner Werbeeinwilligung, wenn einzelne Nachrichten als Werbung zu klassifizieren sein sollten.[21] Unternehmen müssen daher nicht dafür Sorge tragen, dass sich die Chat-Agents auf Beantwortung der Fragen der Anfragenden beschränken, ohne die – letztlich schwierig zu bestimmende und im Zweifel schnell erreichte – Grenze zur Werbung zu überschreiten.[22]

In besonderen Ausgestaltungen denkbar ist, dass in einer aktiven Ansprache durch einen Chatbot auf der Website ein hartnäckiges Ansprechen (§ 7 Abs. 2 Nr. 1 UWG)[23] oder eine Werbung zu sehen ist, obwohl erkennbar ist, dass der angesprochene Marktteilnehmer sie nicht wünscht (§ 7 Abs. 1 Satz 2 UWG). Dies kann z.B. der Fall sein, wenn die Nutzer:innen eine Chat-Funktionalität mehrfach wegklicken und sich damit dennoch immer wieder auseinandersetzen müssen, weil das Chat-Fenster erneut in aufdringlicher Weise auf sich aufmerksam macht.

### 2. Keine Qualifikation als aggressive geschäftliche Handlungen

Ähnlich unwahrscheinlich ist, dass Chat-Funktionalitäten von Unternehmerseite so aufdringlich eingesetzt werden, dass sie als aggressive geschäftliche Handlung im Sinne von § 4a UWG anzusehen sind.[24] Nutzer:innen können sich jederzeit leicht aus einer etwaigen Nötigungslage befreien, in dem sie schlicht das Browser-Fenster schließen, sodass es regelmäßig an der Erheblichkeit fehlt. Es ist auch kaum vorstellbar, dass die Einflussnahme per Chat-Nachricht so intensiv ausfällt wie bei der Direktansprache am Telefon. Dass Gutscheine angeboten oder Rabatte beworben werden, kann für sich genommen ebenso wenig genügen, wie ein abrupter Themenwechsel in einem Chat.[25]

### 3. Kennzeichnung als Werbung

Gem. § 5a Abs. 6 UWG muss kommerzielle Kommunikation als Werbung erkennbar sein[26] und gegebenenfalls gekennzeichnet werden. Chatbots auf E-Commerce-Websites stellen sich jedoch als Teil dieses Angebots dar und werden häufig auch als besonderer Service des Anbieters angepriesen. Solange der kommerzielle Charakter der Website als solcher erkennbar ist, stellt sich daher die Frage nach der Abgrenzung von redaktionellem und werblichem Inhalt nicht. Anders wäre dies, wenn die Chat-Funktion als (getarnte) Werbung auf einer redaktionellen Seite zum Einsatz kommt.

Auch innerhalb einzelner Chat-Verläufe ist für überraschende, weil nicht gekennzeichnete, Werbung kaum Raum. Nutzer:innen wissen, dass sie sich in der Sphäre des E-Commerce-Unternehmens bewegen und werden deshalb in aller Regel nicht überrascht sein, innerhalb eines Gesprächs auf Produkte des Unternehmens hingewiesen zu werden. Einer Kennzeichnung bedürfen Chat-Funktionalitäten im E-Commerce daher in aller Regel nicht.[27]

## IV. Datenschutz

Im Rahmen einer Chat-Funktion werden Daten der Nutzer:innen erhoben. Dies betrifft einerseits die Daten, die bei dem Besuch der Website und Nutzung der Chatfunktion unmittelbar anfallen (vor allem also die IP-Daten und Informationen über Browser und Endgerät der User:innen). Zum anderen fallen Inhaltsinformationen aus den Chats selbst an. Hier lässt sich nicht vorhersehen, welche Daten die Nutzer:innen von sich preisgeben. Von einem weitgehend anonym verlaufenden belanglosen Kurzgespräch bis hin zur Angabe von intimen Gesundheitsdaten ist alles denkbar.

### 1. Personenbezug

Ist dem Website-Betreiber bekannt, um welche Person es sich handelt (etwa weil diese in einem Benutzerkonto eingeloggt ist), sind alle erhobenen Daten unmittelbar personenbezogene Daten. Doch auch, wenn es sich um eine dem Shopbetreiber unbekannte, nicht identifizierbare Person handelt, ist von Personenbezug i.S.v. Art. 4 Nr. 1 DSGVO jedenfalls dann auszugehen, wenn zur Re-Identifikation Cookies gesetzt werden. Zudem muss der Chat-Betreiber darauf eingerichtet sein, dass die Nutzer:innen im Chat personenbezogene Daten von sich aus offenbaren, so dass man stets davon ausgehen sollte, dass anfallende Daten solche mit Personenbezug sind.

17 *Schirmbacher* (S. Fn. 12), § 312j BGB Rn. 45.
18 MüKoBGB/*Wendehorst*, 8. Aufl. 2019, § 312j Rn. 31.
19 *Micklitz/Schirmbacher* (s. Fn. 12), § 7 UWG Rn. 105; a.A. *Köbrich/Froitzheim* WRP 2017, 1188, 1189, die aber übersehen, dass es nicht allein auf die flüchtige Speicherung im Endgerät ankommt, sondern auch auf die dortige bestimmungsgemäße Speicherung bis zum Abruf.
20 *Micklitz/Schirmbacher* (s. Fn. 12), § 7 UWG Rn. 105.
21 A.A. *Köbrich/Froitzheim* WRP 2017, 1188, 1189.
22 So aber *Köbrich/Froitzheim* WRP 2017, 1188, 1189.
23 Vgl. BMJV RefE v. 04.11.2020 und die Bestrebungen, § 7 Abs. 2 Nr. 1 UWG aus europarechtlichen Erwägungen in Nr. 26 des Anhangs zu § 3 Abs. 3 UWG zu verschieben.
24 So auch *Wanderwitz* WRP 2020, 425, 429 für den Sonderfall des Einsatzes von Persuasive Technologies; vgl. zu denkbaren Fällen: *Köbrich/Froitzheim* WRP 2017, 1188, 1190.
25 Weitergehend: *Köbrich/Froitzheim* WRP 2017, 1188, 1190.
26 Vgl. auch 6 Abs. 1 Nr. 1 TMG.
27 Anders für Chatbots auf Facebook-Seiten *Köbrich/Froitzheim* WRP 2017, 1188, 1190.

## 2. Rechtsgrundlage für die Datenverarbeitung

Bekanntlich bedarf nach Art. 6 Abs. 1 DSGVO jede Verarbeitung personenbezogener Daten einer Rechtfertigung. Für die Daten, die innerhalb des Chats ausgetauscht werden, kommen insbesondere eine Einwilligung (Art. 6 Abs. 1 Satz 1 Buchst. a) DSGVO) und berechtigte Interessen des Shopbetreibers (Art. 6 Abs. 1 Satz 1 Buchst. f) DSGVO) in Betracht. Theoretisch denkbar wäre auch eine Rechtfertigung nach Art. 6 Abs. 1 Satz 1 Buchst. b) DSGVO, häufig wird es jedoch an der Vertragsanbahnung oder einem Vertragsschluss fehlen, so dass diese Rechtsgrundlage für viele Chats nicht hinreichend verlässlich ist.[28] Ob eine Einwilligung eingeholt werden sollte, hängt davon ab, welche Daten zu welchen Zwecken gespeichert werden und inwiefern dies für die Nutzer:innen erkennbar ist.

### a) Einfache Chat-Funktionen

Chat-Funktionen, bei denen es vor allem um allgemeine Auskünfte geht und eine Zusammenführung mit existierenden Kundenprofilen nicht stattfindet, bedürfen im Regelfall keiner Einwilligung.[29] Vielmehr kann die mit der Durchführung des Chats verbundene Datenverarbeitung auf berechtigte Interessen gestützt werden. Alle Informationen über die Nutzer:innen stammen unmittelbar von diesen. Es entspricht den vernünftigen Erwartungen der Nutzer:innen, dass die Fragen und alle damit im Zusammenhang stehenden personenbezogenen Daten übermittelt und jedenfalls kurzfristig zwischengespeichert werden. Dies ist zur Erreichung des Zwecks – Durchführung des Chats und bestmögliche Beantwortung der gestellten Fragen – auch erforderlich. Dass es der Anbieter nicht verhindern kann, dass vereinzelt besondere Kategorien personenbezogener Daten eingegeben werden (etwa Gesundheitsdaten oder Daten zur Religionszugehörigkeit), ändert daran nichts. Ist die Nutzung der Chat-Funktion nicht gerade darauf gerichtet, solche Informationen von den Nutzer:innen einzuholen, führt die theoretische Möglichkeit der Eingabe sensitiver Daten nicht zu einem Einwilligungserfordernis.

### b) Zusammenführung mit bestehenden Kundenprofilen

Wird eine automatische Zuordnung zu existierenden Kundenprofilen vorgenommen, ist eine Rechtfertigung mit berechtigten Interessen schwieriger. Liegt die Zusammenführung und dauerhafte Speicherung der Informationen im Interesse der jeweiligen Kund:innen, liegen aber die Voraussetzungen von Art. 6 Abs. 1 Satz 1 Buchst. f) DSGVO vor. Insbesondere bei Vertragsabschlüssen, Reklamationen oder konkreten Anfragen zum Benutzerkonto kann man dies annehmen. Dagegen werden die Nutzer:innen bei reinen Produktanfragen nicht mit einer Zusammenführung der Daten rechnen.

Problematisch ist häufig, dass das konkrete Anliegen der Nutzer:innen vorab nicht feststeht und deshalb auch die Frage, ob eine Zusammenführung der Informationen mit einem existierenden Kundenkonto jedenfalls nicht gegen die Interessen der Betroffenen verstößt, vorab nicht zuverlässig beantwortet werden kann. Insofern ist Shopbetreibern zu empfehlen, eine gesonderte Einwilligung in die Nutzung der Chat-Funktionalität und die damit verbundene dauerhafte Speicherung der Daten im betreffenden Kundenkonto einzuholen.

### c) Besonderheiten bei Chatbots?

Die datenschutzrechtliche Besonderheit bei Chatbots liegt in der intensiveren Datenverarbeitung auf Seiten des Website-Betreibers. Die Eingaben der Nutzer:innen müssen automatisiert verarbeitet und auf taugliche Antworten hin überprüft werden. Meist wird die Kommunikation zudem ausgewertet, um den Chatbot zu trainieren. Spezielle Gesetzgebung hierzu gibt es bisher nicht.[30]

Allerdings gilt für die Frage der datenschutzrechtlichen Rechtfertigung nichts grundsätzlich anderes als für den Einsatz sonstiger Chat-Funktionen. Solange die Nutzer:innen erkennen, dass es sich um einen Chatbot handelt, kann dessen Einsatz auf berechtigte Interessen gestützt werden, soweit es um die Datenverarbeitung zum Zwecke der Beantwortung der gestellten Fragen geht. Eine weitergehende Datenverarbeitung (z.B. gezielte Auswertung oder dauerhafte Speicherung) bedarf allerdings in der Regel der Einwilligung.[31]

Art. 35 DSGVO verpflichtet den Verantwortlichen, unter bestimmten Voraussetzungen eine Datenschutzfolgeabschätzung (DSFA) durchzuführen. Nach Ansicht der Datenschutzaufsichtsbehörden besteht bei dem Einsatz KI-gestützter Chatbots ein hohes Risiko.[32] Unternehmen, die Chatbot-Funktionalitäten einsetzen, müssen sich daher mit diesem Thema auseinandersetzen.[33] Anbieter sind gut beraten, ihre Kunden bei der Erstellung der DSFA zu unterstützen. In jedem Falle muss die Datenschutzerklärung um den Einsatz der Chatbot-Funktionalität erweitert werden.[34]

### d) Einbeziehung von Dienstleistern

In aller Regel bedienen sich Website-Betreiber, die Chat-Funktionen einsetzen, der Dienste Dritter. Hat der Dienstleister keinen Zugriff auf die erhobenen Daten und ausgetauschten Informationen, liegt keine Übermittlung an den Anbieter vor. Anders ist das, wenn der Dienst etwa als iFrame in die Website integriert werden soll. Hier erhält der Anbieter jedenfalls Zugriff auf die IP-Daten der Nutzer:innen. Häufig wird auch ein Zugriff auf die Inhalte möglich sein. Wenn – was so sein sollte – der Dienstleister keine eigenen Zwecke mit der Verarbeitung der Daten verfolgt, wird es sich in aller Regel um ein Auftragsverhältnis handeln und eine Vereinbarung nach Art. 28 DSGVO zu schließen.

Spätestens seit der *Schrems II*-Entscheidung des EuGH[35] problematisch ist eine Datenübermittlung in die USA, wo viele Anbieter ihren Sitz haben. Eine Datenübermittlung auf Basis des EU-US-Privacy Shield ist nicht mehr zulässig. Zwar hat der EuGH eine Datenübermittlung auf Basis von Standarddatenschutzklauseln nicht ausgeschlossen.[36] Verlangt werden aber zusätzliche Garantien, die einen Zugriff auf diese Daten durch U.S.-Behörden ausschließen oder wenigstens deut-

28 So schon für Kontaktformulare ohne unmittelbares Feedback: *Conrad/Hole* K&R 2019, 761, 763; kritisch auch *Gausling* ZD 2019, 335, 336; anders wohl *Conrad* ITRB 2018, 116, 117.

29 Ähnlich für Kontaktformulare: *Conrad/Hole* K&R 2019, 761, 763.

30 Vgl. aber *Wanderwitz* WRP 2020, 425, 426 ff. zu neuen Gesetzgebungsvorhaben aus Großbritannien (SMART Act), wonach auch Chatbots reguliert werden sollen.

31 *Conrad* ITRB 2018, 116, 117.

32 Datenschutzkonferenz, »Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist« Version 1.1 v. 17.10.2018, https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf, lfd.Nr. 11, S. 3 (Abfrage: 11.12.2020).

33 *Conrad* ITRB 2018, 116, 117.

34 Vgl. *Gausling* ZD 2019, 335, 337.

35 EuGH v. 16.07.2020, Az. C-311/18, NJW 2020, 2613; s.a. *Grasmück/Kollmar* IPRB 2020, 212 speziell zum Einsatz von Cloud-Diensten nach *Schrems II*.

36 EuGH v. 16.07.2020, Az. C-311/18, NJW 2020, 2613, 2616.

lich erschweren.[37] Solche Garantien sind schwer erreichbar. Rein rechtliche Maßnahmen – insbesondere Ergänzungen der Standarddatenschutzklauseln – sollen nicht ausreichen. Erforderlich seien auch technische Maßnahmen.[38] Eine Verschlüsselung wird hier in der Regel nicht möglich sein, da es gerade um den Umgang mit den personenbezogenen Daten geht. Immerhin denkbar ist aber eine pseudonyme Verarbeitung, wobei die Zuordnung zu konkreten Kund:innen dann nur der Website-Betreiber selbst vornehmen können darf. Ob das den Anforderungen genügt, ist eine Frage des Einzelfalls, aber jedenfalls denkbar, wenn standardmäßig keine sensiblen Daten Gegenstand der Chat-Kommunikation sind.

#### 3. Konkrete Ausgestaltung

Wird eine Einwilligung eingeholt, bedarf es einer eindeutigen bestätigenden Handlung des Betroffenen. Dabei genügt es, dass unmittelbar oberhalb oder unterhalb der Schaltfläche, die zum Start des Chats führt, eine entsprechend eindeutige Formulierung enthalten ist.[39] Nicht erforderlich ist ein gesondertes Häkchen. Die bestätigende Handlung liegt ggf. in der Nutzung der Schaltfläche.

Unabhängig von der Rechtsgrundlage, auf die der Einsatz der Chat-Funktionalität gestützt wird, ist eine unmittelbare Verlinkung der Datenschutzinformation sinnvoll.[40] Ist die Datenschutzerklärung in unmittelbarer Nähe, etwa in der Fußzeile der Seite, erreichbar, kann auf eine erneute Verlinkung verzichtet werden. Wird im Einwilligungstext auf weitere Informationen in der Datenschutzinformation verwiesen, sollte dagegen in jedem Falle eine Verlinkung erfolgen.

Die Datenschutzinformation ist um einen Passus zum Chat zu ergänzen. Anzugeben sind insbesondere, welche Daten zu welchen Zwecken erhoben, wie lange diese voraussichtlich gespeichert werden und die Rechtsgrundlage für die Datenverarbeitung. Zulässig ist es, in dem Absatz zur Chat-Funktion mehrere Rechtsgrundlagen anzugeben. Art. 6 Abs. 1 DSGVO sieht explizit vor, dass *mindestens eine* Rechtsgrundlage gegeben sein muss.[41] Ferner bedarf es ggf. der Benennung des Dienstleister und – sofern dieser seinen Sitz im EU-Ausland hat – die Garantien nach Art. 46 ff. DSGVO.

## V. Fazit und Praxisempfehlungen

Vor der Einführung von Chat-Funktionen und insbesondere von Chatbots bei E-Commerce-Unternehmen sollten einige rechtliche Fragen gestellt und beantwortet werden.

#### 1. Vertragsschluss und Verbraucherrecht

Unternehmen sollten entscheiden, ob über Chat-Funktionen Verträge geschlossen werden können sollen. In diesem Fall muss insbesondere die Beweisbarkeit des Vertragsschlusses sichergestellt werden. Zudem sind grundsätzlich die fernabsatzrechtlichen Bestimmungen anwendbar, ein Verbraucherwiderrufsrecht einzuräumen und die Informationspflichten einzuhalten.

**Praxisempfehlung:**

- Aufstellen klarer unternehmensinterner Regelungen zum Umgang mit Vertragsanbahnungen im Chat.
- Sicherstellung der Dokumentation von Vertragsschlüssen, z.B. über das Kundenkonto.
- Einbindung des Chats in den Online-Shop, um die fernabsatzrechtlichen Vorgaben einhalten zu können.

#### 2. Unlauterer Wettbewerb

Werbende Chat-Nachrichten, die in Echtzeit ausgetauscht werden, bedürfen regelmäßig anders als das E-Mail-Marketing keiner Einwilligung. Auch eine Kennzeichnung als Werbung ist nicht erforderlich, wenn die Chat-Funktion in einen Online-Shop eingebunden ist. Obacht ist geboten bei allzu aufdringlichen Chatbots.

**Praxisempfehlung:**

- Chatfenster sollten sich beim ersten Wegklicken schließen und nicht immer wieder erneut erscheinen oder in sonstiger aufdringlicher Weise auf sich aufmerksam machen.

#### 3. Datenschutz

Bei dem Angebot einer Chatfunktion sind datenschutzrechtliche Vorgaben zu beachten, insbesondere mit Blick auf die direkt bei den Nutzern erhobenen personenbezogenen Daten (wie IP-Daten und Informationen über Browser und Endgerät), den Inhalt der Chatnachrichten sowie die Informationen aus den gesetzten Cookies.

Je nachdem, welche Daten verarbeitet werden, kommen als Rechtsgrundlagen berechtigte Interessen des Shop-Betreibers und – eher selten – die Vertragserfüllung bzw. -anbahnung in Betracht. Andernfalls bleibt die Einholung einer Einwilligung der Nutzer:innen des Chats.

Insbesondere bei einfachen Chat-Funktionen bedarf es im Regelfall keiner Einwilligung. Ob auch weitergehende Chat-Funktionen und Chatbots auf Grundlage eines berechtigten Interesses verarbeitet werden können, hängt maßgeblich davon ab, ob die konkrete Datenverarbeitung von den Nutzer:innen erwartet wird und ggf. sogar in deren Interesse liegt.

**Praxisempfehlung:**

- Vor Einführung einer Chat-Funktionalität muss geprüft werden, auf welche datenschutzrechtliche Rechtfertigung dies gestützt werden kann.
- Die Einholung einer gesonderten Einwilligung empfiehlt sich insbesondere bei der Zusammenführung von Informationen mit einem existierenden Kundenkonto oder dem Einsatz von Chatbots, zumindest soweit keine verlässliche Einschätzung der Erwartungshaltung der Kund:innen erfolgen kann.
- Bei dem Einsatz KI-gestützter Chatbots sollte vor deren Einsatz eine Datenschutzfolgeabschätzung durchgeführt werden.
- Die Datenschutzerklärung ist um den Einsatz der Chat-Funktionalität zu ergänzen und in unmittelbarer Nähe zum Chat zu verlinken.
- Bei Einbeziehung von Dienstleistern muss in der Regel eine Auftragsverarbeitungsvereinbarung geschlossen werden.

37 EuGH v. 16.07.2020, Az. C-311/18, NJW 2020, 2613, 2616.
38 Vgl. EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data v. 11.11.2020, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en.
39 Vgl. *Conrad/Hole* K&R 2019, 761, 762 f.
40 So auch *Gausling* ZD 2019, 335, 337.
41 Vgl. für Kontaktformulare: *Conrad/Hole* K&R 2019, 761, 762.

- Bei der Einbeziehung von Anbietern aus den USA sind zumindest das Bestehen von Binding Corporate Rules (BCR) oder die Vereinbarung von Standard Contractual Clauses (SCC) sicherzustellen. Zur Zeit nur schwer umsetzbar ist die weitere Anforderung, für zusätzliche Garantien (z.B. wirksame Verschlüsselung oder zumindest Pseudonymisierung) gegen einen Zugriff durch U.S.-Behörden zu sorgen.
- Es muss geprüft werden, ob eine Einwilligung für die zum Einsatz kommenden Cookies erforderlich ist.

**Checkliste**

- Entscheiden, ob im Chat Verträge geschlossen werden können
- Saubere Dokumentation von Vertragsschlüssen
- Anbindung des Chats an den Online-Shop (Widerrufsrecht und Informationspflichten)
- Datenschutzrechtliche Prüfung
- Dokumentation der Interessenabwägung oder Formulierung einer Einwilligungserklärung
- Erweiterung der Datenschutzerklärung
- Verlinkung der Datenschutzerklärung
- Prüfung des Cookie-Consent
- Datenschutzfolgeabschätzung bei KI-gestützten Chatbots
- Abschluss einer datenschutzrechtlichen Vereinbarung mit dem Chat-Tool-Anbieter
- Zusätzliche Prüfung der Rechtslage, wenn der Anbieter ein U.S.-Unternehmen ist

## Entscheidungsanalyse

# Digitale Souveränität in Europa dank Schrems II?

## Zum Urteil des EuGH vom 16.07.2020, Rs. C-311/18

Rechtsanwältin Karina Filusch, LL.M., Berlin*

**Mit dem Schrems II-Urteil erklärt der EuGH den Privacy Shield für ungültig und fordert zusätzliche Maßnahmen für Standarddatenschutzklauseln im Falle der Übermittlung in die USA. Das erschwert den transatlantischen Datentransfer und stellt europäische Unternehmen angesichts der Dominanz US-amerikanischer Anbieter auf dem europäischen Markt vor eine schwierige Aufgabe.**

### I. Sachverhalt

Der Österreicher *Maximilian Schrems* nutzt Facebook seit 2008.[1] Europäischer Staatsbürger:innen schließen einen Vertrag mit der Facebook Ireland, einer Tochter des US-amerikanischen Unternehmens Facebook Inc., wodurch die Daten in den USA verarbeitet werden können.

2013 erhob Schrems bei der irischen Datenschutzaufsichtsbehörde (Data Protection Commissioner – DPC) eine Beschwerde mit dem Inhalt, Facebook die Übermittlung seiner personenbezogenen Daten in die USA zu untersagen, da es keinen ausreichenden Schutz vor der Überwachungstätigkeit der US-amerikanischen Behörden gebe. Diese Beschwerde wurde zurückgewiesen, da die Europäische Kommission mit der Safe-Harbor-Entscheidung[2] festgestellt habe, dass die USA über ein angemessenes Datenschutzniveau verfüge.

Gegen diese Entscheidung erhob *Schrems* Klage vor dem irischen High Court. Im Rahmen dieses Verfahrens legte der High Court dem EuGH Vorlagefragen vor, u.a. zur Auslegung der Gültigkeit von Safe Harbor, woraufhin Safe Harbor für ungültig erklärt wurde,[3] sodass der High Court seine Entscheidung aufhob und die Sache an den DPC zurückverwies.

2015 formulierte *Schrems* seine Beschwerde dahingehend um, dass Facebook nach US-amerikanischem Recht dazu verpflichtet sei, personenbezogene Daten u.a. der National Security Agency (NSA) und dem Federal Bureau of Investigation (FBI) offen zu legen. Dies verstieße gegen die Grundrechtecharta der Europäischen Union (GRCh), insbesondere gegen die Achtung des Privatlebens (Art. 7 GRCh), das Recht auf Schutz personenbezogener Daten (Art. 8 GRCh) und das Recht auf einen wirksamen Rechtsbehelf (Art. 47 GRCh). Aus diesem Grund solle die Übermittlung seiner Daten an Facebook verboten werden.

2016 entschied der DPC vorläufig, dass bei der Verarbeitung personenbezogener Daten von Unionsbürger:innen in den USA gegen Art. 7–8, 47 GRCh verstoßen würde. Zudem seien die Standarddatenschutzklauseln nicht dazu geeignet, diesen Mangel auszugleichen, da eine vertragliche Reglungen nur den Datenexporteur und den Datenimporteur, nicht aber die Behörden, binde.

Weil sich für den DPC nun die Frage aufwarf, ob er die Datenübermittlung in die USA verbieten dürfe und sich somit auch die Frage nach der Gültigkeit der Standarddatenschutzklauseln stellte, rief der DPC im Jahr 2016 den High Court an, damit dieser beim EuGH Vorlagefragen einreiche, was er auch tat.

### II. Entscheidung

In der Entscheidung positionierte sich der EuGH zum Schutzniveau, das Art. 46 Abs. 1 und Abs. 2 lit. c DSGVO für die Übermittlung personenbezogener Daten auf Grundlage der Standarddatenschutzklauseln in ein Drittland verlangt.[4] Aus Art. 45 Abs. 3 DSGVO ergebe sich, dass sofern kein Angemessenheitsbeschluss der Kommission für ein Drittland existiere, personenbezogene Daten nur dann in ein Drittland übermittelt werden dürfen, wenn geeignete Garantien vorlägen und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stünden. Die von der Kommission erlassenen Standarddatenschutzklauseln können solche Garantien darstellen.[5] Die Garantien seien im Lich-

* Die Autorin ist externe Datenschutzbeauftragte und Dozentin an der HWR Berlin. – Zum Urteil des EuGH s.a. den Beitrag von *Kristin Benedikt* in diesem Heft.

1 Das und das Folgende gem. EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 50 ff.
2 2000/520/EG.
3 EuGH 06.10.2015, C-362/14 – Schrems I.
4 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 90.
5 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 91.

te des Art. 44 DSGVO zu verstehen, wonach das durch die DSGVO und die Grundrechtecharta gewährleistete Schutzniveau nicht untergaben werden dürfe.[6]

Ferner führt der EuGH aus, dass solange ein Angemessenheitsbeschluss nicht für ungültig erklärt sei, die Aufsichtsbehörde keine diesem Beschluss zuwiderlaufenden Maßnahmen treffen dürfe.[7] Sofern aber kein gültiger Angemessenheitsbeschluss existiere, sei die Aufsichtsbehörde verpflichtet, eine auf Standarddatenschutzklauseln gestützte Übermittlung von personenbezogenen Daten in ein Drittland auszusetzen oder zu verbieten, wenn die Standarddatenschutzklauseln in einem Drittland nicht eingehalten werden oder nicht eingehalten werden können und folglich das nach der DSGVO und Grundrechtecharta garantierte Schutzniveau nicht eingehalten werden könne.[8]

Überdies beinhalte ein Beschluss über die Aufstellung von Standarddatenschutzklauseln nicht die Prüfung des Datenschutzniveaus in einem Drittland, sodass daraus nicht abgeleitet werden könne, dass die Kommission beim Erlass von Standarddatenschutzklauseln auch eine Prüfung der Angemessenheit des Schutzniveaus vornehmen müsse.[9] Deshalb ist es bei fehlenden Angemessenheitsbeschluss Aufgabe des Verantwortlichen oder des Auftragsverarbeiters geeignete Garantien zur Einhaltung des Schutzniveaus vorzusehen,[10] insbesondere indem die Standarddatenschutzklauseln durch zusätzliche Maßnahmen ergänzt würden.[11] Die Standarddatenschutzklauseln an sich enthielten bereits einige Mechanismen, um ein angemessenes Datenschutzniveau zu versichern.[12]

Ferner stellt das Gericht fest, dass so lange der Privacy Shield nicht für unwirksam erklärt würde, Aufsichtsbehörden die Übermittlung von personenbezogenen Daten an die auf der Liste des Privacy Shields stehenden Unternehmen nicht aussetzen oder verbieten dürfe.[13]

Problematisch am Privacy Shield seien vor allem die dort genannten Ausnahmen, wonach die Einhaltung der Privacy Shield-Grundsätze eingeschränkt werden können, wenn die nationale Sicherheit, das öffentlichen Interesse oder die Durchführung von Gesetzen es erfordern würden. Eingriffe gem. Art. 7–8, 47 GRCh in die Rechte von Unionsbürger:innen stellen z.B. FISA oder die Überwachungsprogramme PRISM und UPSTREAM dar,[14] wobei unerheblich sei, ob die Informationen über das Privatleben sensiblen Charakter hätten oder ob die betroffene Person durch den Eingriff Nachteile hätte erleiden können.[15] Ferner verweist der EuGH auf den Zweckbindungsgrundsatz aus Art. 8 Abs. 2 GRCh und die Tatsache, dass die Daten nur mit Einwilligung der betroffenen Person und auf einer gesetzlichen Grundlage verarbeitet werden dürfe.[16] Der Eingriff müsse zudem verhältnismäßig sein, klare und präzise Regelungen für die Tragweite und die Anwendung des betroffenen Maßnahme vorsehen und Mindesterfordernisse aufstellen, um einen wirksamen Schutz vor Missbrauchsrisiken zu ermöglichen.[17] Zudem fordere Art. 45 Abs. 2 Buchst. a) DSGVO wirksame und durchsetzbare Rechte der betroffenen Person.[18] Die US-amerikanischen Gesetze erfüllen diese Voraussetzungen jedoch nicht.[19] Zudem läge ein Verstoß gegen Art. 47 GRCh vor, da den Unionsbürger:innen kein wirksamer Rechtsschutz zur Verfügung stünde.[20] Schlussendlich stellt der EuGH fest, dass der Privacy Shield ungültig sei.[21]

## III. Folgen für die Praxis

Das Urteil hat enorme Auswirkungen, denn der transatlantische Datentransfer macht mehr als die Hälfte der Datenströme in Europa und etwa die Hälfte der Datenströme in den USA aus.[22] Nicht verwunderlich ist deshalb, dass sich die deutschen Aufsichtsbehörden schnell positionierten. Beispielhaft sei die Berliner Beauftragte für Datenschutz genannt, die in Berlin ansässigen Stellen dazu aufforderte, umgehend zu Dienstleistern in der Europäischen Union oder in einem Land mit angemessenem Datenschutzniveau zu wechseln.[23] Sie sagt: »Die Zeiten, in denen personenbezogene Daten aus Bequemlichkeit oder wegen Kostenersparnissen in die USA übermittelt werden konnten, sind nach diesem Urteil vorbei.«[24] – Die Prämisse, dass Unternehmen US-amerikanische Produkte einsetzen, weil sie zu bequem sind nach europäischen Alternativen zu suchen oder diese zu teuer seien, ist falsch. Für die ca. 5.000 unter den Privacy Shield zertifizierten Unternehmen[25] gibt es teilweise entweder keinen oder keinen gleichwertigen Ersatz.[26] Ein umgehender Wechsel ist deshalb oft nicht möglich. Europäische Alternativprodukte sind aber im Entstehen. Es wird Zeit brauchen, um einen Wechsel zu europäischen Produkten geordnet zu vollziehen.

Auch die Datenschutzkonferenz (Zusammenschluss der deutschen Datenschutzbehörden) erklärt, dass die »Übermittlung personenbezogener Daten in die USA auf der Grundlage des Privacy Shield […] unzulässig [ist] und […] unverzüglich eingestellt werden [muss].«[27] Der Präsident des Bundesverbands der Deutschen Industrie (BDI) hingegen bedauert das Urteil und sprach von erheblichen Auswirkungen auf den Datenaustausch von Firmen mit den USA.[28]

In der Literatur wird festgestellt, dass eine Fortsetzung der Datenübermittlung in die USA nun illegal sein dürfe.[29] Allerdings wird teilweise angenommen, die Datenübermittlung könne auf die Standardvertragsklauseln gestützt werden.[30]

6 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 92, 105.
7 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 118.
8 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 121.
9 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 130.
10 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 131.
11 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 133.
12 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 138–146.
13 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 156.
14 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 165.
15 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 171.
16 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 173.
17 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 176.
18 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 177.
19 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 178 ff.
20 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 187.
21 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 201.
22 *Weiß* ZD 2020, 485, 485.
23 https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf [21.12.2020]; vgl. *Kaufmann* IWRZ 2020, 216, 216.
24 https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf [21.12.2020].
25 *Heinzke* GRUR-Prax 2020, 436, 438; *Botta* CR 2020, 505, 507.
26 Vgl. *Spies* ZD-Aktuell 2020, 549, 549.
27 https://www.datenschutzkonferenz-online.de/media/pm/20200616_pm_schrems2.pdf [21.12.2020].
28 ZD-Aktuell 2020, 07240.
29 *Hoeren* MMR 2020, 608, 608 (»in vielen Fällen«); *Kaufmann* IWRZ 2020, 216, 216.
30 *Hoeren* MMR 2020, 608, 609.

Dies widerspricht jedoch dem Wortlaut des Urteils, in dem es heißt, dass die amerikanische Gesetzgebung gegen die Grundrechtecharta verstieße, unverhältnismäßig sei und Europäer:innen keine Rechtsbehelfe dagegen einwenden könnten.[31] Jedoch übersehe der EuGH, dass die Gesetzgebung zur nationalen Sicherheit in den Mitgliedstaaten nationalem Recht unterliege und gerade nicht der Grundrechtecharta, sodass schon innerhalb der EU verschiedene Maßstäbe anzusetzen seien.[32] Zudem urteile der EuGH, dass die Standarddatenschutzklauseln zwar weiterhin anwendbar seien, verrate jedoch nicht, wie die geforderten zusätzlichen Maßnahmen ausgestaltet werden müssen.[33] Die Standardvertragsklauseln eigneten sich überdies nicht dazu, um die durch den EuGH angeführten Defizite zu überwinden, sodass es eine Frage der Zeit sei, bis ein Gericht oder eine Aufsichtsbehörde die Übermittlung aufgrund der Standarddatenschutzklauseln verbiete,[34] was in Berlin bereits geschehen ist (s.o.).

In der Zwischenzeit hat die US-Regierung ein White Paper veröffentlicht, in dem es heißt, dass gewöhnliche Geschäftsinformationen von US-Geheimdiensten nicht gesammelt werden würden, dass das Urteil Reformen in der US-amerikanischen Gesetzgebung nicht einbezogen habe wie z.B., dass vor der Überwachung eine Genehmigung bei einem Richtergremium eingeholt werden müsse, und dass es eine Klagemöglichkeiten vor US-amerikanischen Zivilgerichten gebe.[35] Bisher ist auf dieses White Paper noch nicht nennenswert eingegangen worden.[36]

## IV. Arbeitshilfen[37]

Für Anwält:innen im Bereich Datenschutz und externe Datenschutzbeauftragte bedeutet das Urteil in der Praxis vor allem praktikable, datenschutzkonforme Lösungen, die ein Unternehmen gleichzeitig nicht finanziell zu Grunde richten, zu finden. Dies zeigt, dass das Thema auf die Unternehmen abgewälzt wurde.[38]

Eine Möglichkeit wäre es, die Daten gemäß der »Vogel-Strauß-Taktik« weiterhin in die USA zu übermitteln. In diesem Fall besteht allerdings die Verpflichtung sowohl die Nutzer:innen[39] als auch die Aufsichtsbehörden über den Datentransfer zu informieren.[40] Dies birgt das Risiko, dass eine Aufsichtsbehörde entweder von sich aus oder aufgrund einer Beschwerde einer betroffenen Person, ein Bußgeld verhängt. Da nicht alle Aufsichtsbehörden proaktiv handeln, ist das Risiko, dass eine Aufsichtsbehörde durch eine Beschwerde vom Verstoß erfährt, als höher einzustufen, als dass die Behörde dies selbst in Erfahrung bringen würde.

Eine weitere Lösung wäre es, die Datenübermittlung in die USA sofort zu stoppen. Das ist die von der Datenschutzkonferenz empfohlene Lösung (s.o.).[41] Dies ist jedoch praktisch allenfalls mit hohen wirtschaftlichen Verlusten umsetzbar.

Als weitere Maßnahmen werden bspw. vorschlagen, Fragebögen an die US-amerikanischen Anbieter zu senden[42] oder Content-Walls auf der Website einzurichten, um eine Einwilligung[43] der Nutzer:innen einzuholen. Auch eine komplette Verschlüsselung wird vorgeschlagen.[44] Diese Lösung wird jedoch einen man-in-the-middle-Angriff nicht verhindern können und ist nur für data in rest geeignet.[45] Auch die zuvor genannten Lösungen helfen nicht, das Hauptproblem zu überwinden, nämlich den Zugriff durch US-Behörden und das Fehlen von Rechtsbehelfen. Die Vorschläge eignen sich also bestenfalls dazu, ein Bußgeld zu reduzieren. Die Fragebögen verschlimmern sogar die Situation der Unternehmen: Wird ein Fragebogen an ein US-amerikanisches Unternehmen versandt und geht aus der Antwort hervor, dass Daten in den USA verarbeitet werden und dass das Unternehmen den Zugriff US-amerikanische Behörden nicht verhindern kann, kann sich die Frage nach der Strafbarkeit des Datenexporteurs stellen, sofern im Anschluss die Datenübermittlung nicht ausgesetzt wird. Stattdessen ist es ratsam, zunächst eine Bestandsaufnahme aller US-amerikanischen Dienstleister und der übermittelten Daten zu machen[46] und dann entsprechend der folgenden Empfehlungen eine gute, praktikable und wirtschaftliche Lösung zu finden.

Ein möglicher Ausweg ist es, die US-amerikanischen Produkte durch Produkte aus dem Europäischen Wirtschaftsraum (EWR) oder einem Land mit Angemessenheitsbeschluss (wie bspw. Kanada, Israel, Neuseeland, Japan, Schweiz usw.) zu ersetzen. – Dieser Ansatz stellt eine große Chance für europäische Unternehmen dar, um unabhängiger von US-amerikanischen Unternehmen zu werden.

Bei der Auswahl des Produkts ist zudem nicht nur darauf zu achten, dass der Server in der EWR steht, sondern auch, dass der Unternehmenssitz im EWR liegt und das Unternehmen keine Tochter in einem US-amerikanischen Konzern ist.[47] Denn dies genügt schon, damit US-amerikanische Behörden auf die personenbezogene Daten von Unionsbürger:innen zugreifen können. Es bringt also nichts, sich einen deutschen Anbieter auszusuchen, wenn dieser seine Daten in Irland bei Amazon Webservices (AWS) hostet.

Seit dem Urteil ist viel im EWR passiert. Deutsche Unternehmen arbeiten an Alternativen zu Salesforce, einem populären US-amerikanischen Customer-Relationship-Manage-

31 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 171 ff.; vgl. *Moos/Rothkegel* ZD 2020, 522, 523; *Botta* CR 2020, 505, 506 f.
32 *Moos/Rothkegel* ZD 2020, 522 ff.
33 *Moos/Rothkegel* ZD 2020, 522, 524, *Schreiber* GRUR-Prax 2020, 379; *Kirschhöfer* ZVertriebsR 2020, 366, 368; *Botta* CR 2020, 505, 510.
34 Vgl. *Moos/Rothkegel* ZD 2020, 522, 527; *Tribess* GWR 2020, 308; *Streinz* JuS 2020, 1085, 1088.
35 *Spies* ZD-Aktuell 2020, 07327.
36 Vgl. *Spies* ZD-Aktuell 2020, 07327.
37 Zu aktuellen Alternativen zu US-amerikanischen Tools siehe den Blog unter www.kanzlei-filusch.de [21.12.2020].
38 *Spies* ZD-Aktuell 2020, 549, 549.
39 Vgl. *Jungkind/Raspé/Schramm* NZG 2020, 1056, 1059; vgl. *Paal/Kumkar* MMR 2020, 733, 738.
40 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 138–146.
41 https://www.datenschutzkonferenz-online.de/media/pm/20200616_pm_schrems2.pdf [21.12.2020].
42 *Schreiber* GRUR-Prax 2020, 379.
43 Zur Problematik der Einwilligung *Paal/Kumkar* MMR 2020, 733, 737; *Moos/Rothkegel* ZD 2020, 522, 527; *Spies* ZD-Aktuell 2020, 549, 550; *Botta* CR 2020, 505, 511; *Weiß* ZD 2020, 485, 486.
44 *Schreiber* GRUR-Prax 2020, 379; *Moos/Rothkegel* ZD 2020, 522, 526 f.; *Streinz* JuS 2020, 1085, 1088; *Kirschhöfer* ZVertriebsR 2020, 366, 368; *Paal/Kumkar* MMR 2020, 733, 738; *Heinzke* GRUR-Prax 2020, 436, 438; *Jungkind/Raspé/Schramm* NZG 2020, 1056, 1058.
45 https://www.datenschutz-notizen.de/wie-sicher-sind-verschluesselnde-cloud-speicher-dienste-0526776/?s=09 [21.12.2020].
46 Ähnlich *Jungkind/Raspé/Schramm* NZG 2020, 1056, 1057.
47 Vgl. *Paal/Kumkar* MMR 2020, 733, 738.

ment(CRM)-Tool. Andere europäische Unternehmen haben ihr Hosting von AWS auf europäische Server verlagert.

Schwierig wird es bei Betriebssystemen. Diese übersenden sog. Telemetriedaten in die USA. Bei Windows Pro kann man diese jedoch teilweise ausschalten[48] und bei Windows Enterprise sogar vollständig.[49] Einige Firmen haben auf Linux umgestellt.

Es gibt aber Produkte, die schnell und mit geringen Kosten ersetzt werden können wie z.B. Newsletter-Dienstleister. Hier gibt es eine Vielzahl von europäischen Anbietern, die gleichwertig sind zu den US-amerikanischen Konkurrenzprodukten. So lässt sich MailChimp schnell gegen das deutsche Pendant CleverReach austauschen. Auch kollaborative Tools wie Google Docs lassen sich durch das französische Cryptpad.fr ersetzen, und auch für Videokonferenz-Dienstleister gibt es europäische Alternativen. Aus Zoom und Co. können so schnell eudip, spreed, TeamViewer oder Tools der Telekom (alle aus Deutschland!) werden.

Anhand der Videokonferenz-Dienstleister offenbart sich eine weitere Lösung, nämlich Lizenzen von amerikanischen Produkten zu erwerben und sie auf europäischen Servern im EWR zu hosten (on premise). So kann man z.B. Big Blue Button über einen deutschen Server hosten, ohne dass US-Behörden Zugriff auf die Daten hätten. Dies funktioniert auch mit Cloud-Diensten.

In einigen Bereichen gibt es also bereits gute europäische Alternativen, in anderen gibt es sie hoffentlich bald, sodass Europa in Zukunft über mehr digitale Souveränität verfügen kann.

48 https://www.heise.de/newsticker/meldung/Windows-10-Enterprise-Version-1909-Telemetrie-komplett-abschaltbar-4652535.html [21.12.2020].

49 https://www.datenschutzkonferenz-online.de/media/dskb/TOP_30_Beschluss_Windows_10_mit_Anlagen.pdf und https://www.lda.bayern.de/media/baylda_report_09.pdf [21.12.2020].

## Überblick

# Datenübermittlung in die USA – Weshalb sich nach Schrems II nichts geändert hat

## Zum Urteil des EuGH vom 16.07.2020, Rs. C-311/18

Richterin am Verwaltungsgericht Kristin Benedikt, Regensburg*

**Die Entscheidung des EuGH im Verfahren »Schrems II« war ein Paukenschlag. Das Urteil war vielfach Gegenstand von Urteilsbesprechungen, Vorträgen und wissenschaftlichen Fachbeiträgen. Auch die Datenschutzaufsichtsbehörden veröffentlichten Hinweise, wie mit der Entscheidung umzugehen ist, und doch hat sich seit Juli 2020 nichts geändert. Der Datentransfer zwischen der EU und den USA ist nach wie vor von größter Bedeutung – erst recht in der Covid-19-Pandemie. Weshalb sich auch in Zukunft wenig ändern wird, Verantwortliche weiterhin beanstandungsfrei Daten in die USA und andere Drittländer übermitteln können und Datenschutzaufsichtsbehörden an die Grenzen des Vollzugs stoßen, wird in diesem Beitrag erläutert.**

### I. EuGH-Entscheidung überbewertet? – Was der EuGH entschieden hat und was gerade nicht

Voreilig wurde angenommen, die Entscheidung des EuGH bedeute das Ende des Datentransfers zwischen den USA und Europa. Diese Schlussfolgerung ergebe sich nicht nur aus dem Ende des Privacy Shield, nachdem der EuGH in seiner Entscheidung die Angemessenheitsentscheidung für ungültig erklärt hat.[1] Die Feststellung des EuGH, dass im Falle der USA kein angemessenes Datenschutzniveau bestehe, habe auch Auswirkungen auf Standard Contractual Clauses (SCC) und Binding Corporate Rules (BCR). Doch diese Schlussfolgerung verkennt einerseits die beschränkte Aussagekraft einer Entscheidung des EuGH im Vorabentschiedungsverfahren gem. Art. 267 AEUV (a) sowie andererseits, welcher Sachverhalt der EuGH-Entscheidung zugrunde lag (b). Ebenso ist für die praktischen Folgen der Rechtsprechung relevant, aus welchen Gründen der EuGH ein angemessenes Datenschutzniveau im Falle der USA verneint hat (c).

a) Bei der Interpretation einer Entscheidung des EuGH ist zunächst zu berücksichtigen, dass der EuGH im Vorabentscheidungsverfahren den zugrundeliegenden Sachverhalt nicht letztinstanzlich entscheidet, sondern sich lediglich mit der Anwendung europäischen Rechts befasst. Für den Fall, dass die Auslegung einer europäische Rechtsnorm zu unterschiedlichen Ergebnissen führt und dies für die Beurteilung des zugrundeliegenden Sachverhalt entscheidungserheblich ist, klärt der EuGH, wie eine europäische Norm auszulegen ist. Aufgabe des EuGH im Vorabentscheidungsverfahren ist es, die einheitliche Anwendung einer europäischen Rechtsnorm zu gewährleisten. Für das Verfahren »Schrems II« bedeutet das, dass der EuGH »lediglich« die Angemessenheitsentscheidung der Kommission, das EU-US-Privacy Shield, für ungültig erklärt und festgestellt hat, dass SCC grundsätzlich weiterhin gültig sind.[2] Der EuGH hat jedoch nicht darüber entschieden, ob die Facebook Ireland Ltd. weiterhin Daten europäischer Nutzer an die in den Vereinigten Staaten ansässige Facebook Inc. übermitteln darf. Erst recht hat der EuGH keine Entscheidung darüber getroffen, ob Datenübermitt-

* Die Autorin, Richterin am VG Regensburg, leitete zuvor den Bereich »Internet« beim Bayerischen Landesamt für Datenschutzaufsicht. – Zum Urteil des EuGH s.a. den Beitrag von *Karina Filusch* in diesem Heft.

1 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 199.

2 EuGH 16.07.2020, C-311/18 – Schrems II, Rn. 148.

lungen in die USA auf Grundlage der SCC in jedem Fall ergänzender Maßnahmen bedürfen, gar unmöglich sind oder welche Konsequenzen sich mit Blick auf andere Drittländer wie China oder Russland ergeben.

b) Weiterhin ist zu berücksichtigen, welcher Sachverhalt dem EuGH zugrunde lag. Im Verfahren »Schrems II« wurden personenbezogene Daten des Nutzers des sozialen Netzwerks Facebook, Maximilians Schrems, zunächst in Europa von der Facebook Ireland Ltd. verarbeitet und anschließend ganz oder teilweise an die Facebook Inc. in die USA übermitteln, wo die weitere Datenverarbeitung erfolgte. Es handelt sich demnach um ein Verhältnis zwischen drei Akteuren: Maxilimas Schrems als Nutzer sowie der Facebook Ireland Ltd. und der Facebook Inc. Der EuGH prüfte dabei das Verhältnis zwischen der Facebook Inc. und der Facebook Irland Ltd. unter Berücksichtigung des US-amerikanischen Rechts. Hiervon unterscheiden sich die Sachverhalte, die oftmals im Zusammenhang mit der Nutzung US-amerikanischer Dienste, z.B. Cloud-Services, Videokonferenzsysteme, E-Mail-Dienste oder weitere Dienste der elektronischen Kommutation diskutiert wurden. In diesem Szenario ist der in der EU/EWR ansässige Unternehmer, der diese Dienste nutzt, häufig nicht selbst der Verantwortliche, sondern auch »nur« ein Nutzer wie Maximilian Schrems. Die datenschutzrechtliche Rolle der Unternehmen wird daher häufig fehlerhaft bewertet, weil die DSGVO den Schutzbereich nur auf natürliche Personen erstreckt. Bei den o.g. Diensten handelt es sich jedoch um Dienste der elektronischen Kommunikation, die unter den Regelungsbereich des europäischen Kodex für die elektronische Kommunikation fallen. In den Schutzbereich der Regelungen zur elektronischen Kommunikation fallen nicht nur natürliche Personen, sondern auch juristische Personen, wenn natürliche Personen im Namen dieser juristischen Personen handeln oder zumindest auf einer Seite an der Kommunikation beteiligt sind.[3] Folglich gehören Unternehmen bei der Nutzung von Videokonferenzsystemen, Cloud-Diensten etc. zum geschützten Personenkreis. Erst dann, wenn sie unter Verwendung dieser Dienste personenbezogene Daten von betroffenen Personen, z.B. Kundendaten, verarbeiten, nehmen sie zugleich die Rolle des Verantwortlichen i.S.d. Art. 4 Nr. 7 DSGVO ein.

c) Der EuGH wurde unter anderem dafür kritisiert, dass er das EU-US-Privacy Shield für ungültig erklärte, jedoch bei den SCC den Aufsichtsbehörden, aber vor allem dem Datenimporteur und -exporteur eine umfassende Pflicht zur Einzelfallprüfung auferlegte und feststellte, dass gegebenenfalls ergänzende Maßnahmen zu ergreifen sind, um ein gleichwertiges Datenschutzniveau sicherzustellen. Vorschnell neigten einige Beobachter zu der Schlussfolgerung, wenn schon das Privacy Shield ungültig sei, dann können auch die SCC kein geeignetes Instrument für die Übermittlung personenbezogener Daten in die USA darstellen.[4] Doch diese Schlussfolgerung ergibt sich nicht denklogisch aus der EuGH-Entscheidung im Verfahren »Schrems II«. Eine Angemessenheitsentscheidung der Kommission gem. Art. 45 DSGVO ist eine abstrakt-generelle Prüfung anhand festgelegter Kriterien, vgl. Art. 45 Abs. 2 DSGVO. Bei den SCC hingegen handelt es sich zunächst um ein Vertragsverhältnis, dass zwischen Datenimporteur- und Exporteur besteht und auch nur zwischen den Vertragsparteien eine Bindungswirkung entfaltet. Die vertraglich verpflichteten Parteien müssen sicherstellen, dass sie für ein geeignetes Datenschutzniveau sorgen. Ob es den Parteien gelingt, mithilfe der SCC ein geeignetes Datenschutzniveau sicherzustellen, ist einer Einzelfallprüfung vorbehalten. Eine solche Einzelfallprüfung durfte der EuGH im Vorabentscheidungsverfahren nicht vornehmen, da ihm hierfür gem. Art. 267 AEUV die Kompetenz fehlte. Eine gerichtliche Einzelfallentscheidung obliegt ausschließlich den nationalen Gerichten.
Im Falle der USA kam der EuGH zu dem Ergebnis, dass kein angemessenes Datenschutzniveau gem. Art. 45 DSGVO besteht, da u.a. die amerikanischen Rechtsvorschriften Überwachungsmaßnahmen nicht auf das zwingend erforderliche Maß beschränken und somit unverhältnismäßig sind. Außerdem stellte der EuGH fest, dass den betroffenen Personen kein wirksamer Rechtsschutz i.S.v. Art. 47 GRCh zur Verfügung steht.

Fazit: Der EuGH hat in seiner Entscheidung im Verfahren »Schrems II« nicht ausdrücklich festgestellt, dass im Falle der USA ein Datentransfer auf Grundlage der SCC ausscheidet. Für Verantwortliche ist entscheidend, wie das Ergebnis einer Einzelfallprüfung hinsichtlich eines geeigneten Datenschutzniveaus ausfällt, ob die SCC ausreichend sind, unter welchen Umständen ergänzende Maßnahmen zu ergreifen sind und ob ergänzende Maßnahmen die vom EuGH festgestellten Defizite kompensieren können.

## II. Einzelfallprüfung mit vorhersehbarem Ergebnis

Der EUGH hat betont, dass Datenimporteur und -exporteur im Einzelfall prüfen müssen, ob das erforderliche Schutzniveau im betreffenden Drittland eingehalten wird und ob die Parteien die SCC einhalten können. Können die SCC nicht eingehalten werden, muss der Exporteur die Datenübermittlung aussetzen und/oder vom Vertrag mit dem Datenimporteur zurücktreten. Ergibt eine Einzelfallprüfung, dass das erforderliche Schutzniveau (noch) nicht besteht, müssen die SCC um zusätzliche Maßnahmen ergänzt werden.

Der vom EuGH auferlegten Prüfpflicht kann nur der konkrete Einzelfall zugrunde gelegt werden. Das bedeutet, dass keinesfalls pauschal eine mögliche allumfassende Überwachung der US-Geheimdienste zugrunde zu legen ist, sondern die Parteien ermitteln müssen, ob beim Datenimporteur Überwachungsmaßnamen stattgefunden haben, noch stattfinden oder unmittelbar bevorstehen. Diese Prüfung dürfte schnell zu einem Ergebnis führen: Es bestehen keine Anhaltspunkte für die Ausübung der Befugnisse nach Section 702 FISA und Executive Order 12333 im konkreten Fall. Die Begründung liegt auf der Hand. Es liegt zum einen in der Natur der Sache, dass Geheimdienstaktivitäten geheim sind. Zum anderen unterliegen die US-amerikanischen Unternehmen einer strafbewehrten Ver-

3 Richtlinie (EU) 2018/1972 des europäischen Parlaments und des Rates v. 11.12.2018 über den europäischen Kodex für die elektronische Kommunikation, Erwg. 17.

4 Kritisch dazu *Caspar*, Hamburgischer Beauftragte für Datenschutz und Informationsfreiheit, Pressemitteilung v. 16.07.2020; *Hasse*, Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Pressemitteilung v. 16.07.2020.

schwiegenheitspflicht (»Gag Order«), sodass der Verantwortliche in der EU/EWR jedenfalls vom Datenimporteur nicht aktiv informiert werden dürfen. Im Übrigen zeigen die Transparenzberichte einiger US-Anbieter, die unter Section 702 FISA fallen, dass jedenfalls keine Totalüberwachung aller EU-Bürger vorliegt, sondern sich die Anzahl der Geheimdienstersuchen auf wenige hundert Fälle pro Jahr beschränkt.[5]

Fazit: Im Rahmen der Einzelfallprüfung muss der Datenexporteur bewerten, ob das in dem Drittland ansässige Unternehmen Adressat eines Ersuchens der Geheimdienste werden kann. Wie dieses Risiko bewertet werden kann, zeigt das folgende Praxisbeispiel im Fall der USA: Einen Online-Glücksspielanbieter in Frankreich, der mit seinen Nutzern über Facebook-Dienste kommuniziert, dürfte wohl ein höheres Risiko treffen, da bei Online-Glücksspielen die Bekämpfung von Geldwäsche und Finanzierung des Terrorismus im Fokus der Behörden steht. Hingegen dürfte eine Bäckerei, die lediglich eine Website betreibt und Google-Marketing-Tools verwendet, eher keinen Beitrag zur Finanzierung des Terrorismus leisten, weshalb das Risiko eines Ersuchens deutlich geringer erscheint.

## III. Ergänzende Maßnahmen empfehlenswert, aber wirkungslos

Für den Fall, dass der Verantwortliche zu dem Ergebnis kommen, dass (noch) kein gleichwertiges Schutzniveau besteht, soll er ergänzende Maßnahmen ergreifen. Um es vorweg zu nehmen: Die von den Datenschutzaufsichtsbehörden vorgeschlagenen Maßnahmen sollten in jedem Fall in Betracht gezogen werden. In jeder Beratungspraxis gilt es, den sichersten Weg zu gehen. Selbst wenn die Einzelfallprüfung ergibt, dass das Risiko gering ist, sollten in jedem Fall zusätzliche Maßnahmen zu den SCC vereinbart werden. Allerdings dienen die Maßnahmen allenfalls dazu »wenigstens [den] Willen zu rechtskonformem Handeln zu demonstrieren«.[6] Die vom EuGH zurecht festgestellten Defizite im Falle der USA – die unverhältnismäßigen Befugnisse der US-Geheimdienste aufgrund von Section 702 FISA und Executive Order 12333 sowie der fehlende Rechtsschutz – dürften in den seltensten Fällen mit technischen organisatorischen Maßnahmen oder gar rein vertraglichen Maßnahmen kompensiert werden können. Die vom Europäischen Datenschutzausschuss vorgeschlagenen technischen Maßnahmen[7] dienen allenfalls dazu, einen Zugriff US-amerikanischer Geheimdienste zu erschweren.

Noch weniger geeignet erscheinen vertraglichen Maßnahmen, wie bspw. die vom Europäischen Datenschutzausschuss (EDSA) vorgeschlagenen Informationspflichten oder gar die Vereinbarung eines Schadensersatzanspruchs.[8] In den meisten Fällen dürfte der Datenimporteur dem Verbot unterliegen, über einen Zugriff durch US-Geheimdienste zu informieren (»Gag Order«). Eine Transparenzpflicht wäre daher vom Datenimporteur nicht erfüllbar, da die Transparenzpflicht im Konflikt mit dem nationalen Recht des Drittlandes steht.[9] Auch die vorgeschlagene Beschreitung des Rechtswegs durch den Datenimporteur scheint zunächst eine geeignete Maßnahme zu sein. Doch bei genauerem Blick entpuppt sich dies schnell als Farce, da auch in anderen Rechtsregimen der Grundsatz gilt, dass gerichtliche Entscheidungen nur zwischen den Beteiligten (inter partes) wirken und jedenfalls betroffene Personen in der EU/im EWR hieraus keine Rechte, insbesondere nicht das Recht auf gerichtlichen Rechtsschutz, herleiten können. Noch weniger geeignet ist ein Schadensersatzanspruch, der zwischen Datenimporteur- und Exporteur vereinbart wird, um eventuell erlittene Schäden des Betroffenen auszugleichen.[10]

Grund für das fehlende Datenschutzniveau in den USA sind die fehlende Rechtsschutzmöglichkeit für die betroffene Person und die unverhältnismäßigen Befugnisse der US-amerikanischen Geheimdienste. Auf den Punkt gebracht hat der EuGH rechtswidrige Grundrechtseingriffe im Falle der USA festgestellt. Dieses rechtswidrige staatliche Handeln – erst recht schwerwiegende Eingriffe in die Grundrechte gem. Art. 7, 8 und 47 GRCh – können jedoch nicht im Innenverhältnis zwischen nichtstaatlichen Beteiligten kompensiert werden. Im Übrigen dürfte sich der Datenimporteur zur Verteidigung immer auf die Beweislastregelung des Anspruchsinhabers stützen. Eine betroffene Person müsste demzufolge darlegen, dass ein rechtswidriges staatliches Handeln durch US-Geheimdienste stattgefunden hat und dass ihm daraus ein bezifferbarer Schaden entstanden ist. Dabei muss es sich stets um einen konkreten Schaden handeln, d.h. der bloße Verweis auf die Erkenntnisse und die Enthüllungen durch *Edward Snowden* dürften keinesfalls ausreichen, um einen Schadensersatzanspruch zu begründen. Wenn man diese erheblichen Beweisschwierigkeiten berücksichtigt, läuft der vertraglich vereinbarte Schadensersatzanspruch regelmäßig ins Leere. Demzufolge kann eine Regelung zum Schadensersatzanspruch die oben genannten Defizite – keine Rechtsschutzmöglichkeit und unverhältnismäßige Befugnisse der US-Geheimdienste – keinesfalls kompensieren.

Fazit: Es gilt die uneingeschränkte Empfehlung, ergänzende Maßnahmen, insbesondere die vom EDSA vorgeschlagenen, zu vereinbaren. Die Parteien sollten sich aber darüber im Klaren sein, dass es sich hier allenfalls um »good will«-Maßnahmen handelt, die keinesfalls geeignet sind, die Defizite eines niedrigeren Datenschutzniveaus auszugleichen.

## IV. Grenzen des Vollzugs

Bisher wenig im Fokus der Diskussion stand die Frage, ob die Datenschutzaufsichtsbehörden eine Datenübermittlung in ein Drittland im Einzelfall untersagen können. Zwar hat

5 Vgl. Transparenzbericht Google, https://transparencyreport.google.com/user-data/us-national-security?hl=de [22.12.2020]; Transparenzbericht Facebook, https://transparency.facebook.com/government-data-requests/country/US [22.12.2020]; Transparenzbericht Apple, https://www.apple.com/legal/transparency/pdf/requests-2019-H1-en.pdf [22.12.2020].

6 *Brink*, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Orientierungshilfe: Was jetzt in Sachen internationaler Datentransfer?, 2. Aufl., Stand: 07.09.2020.

7 EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, S. 21.

8 EDSA, a.a.O., S. 28.

9 Eine solche Verschwiegenheitspflicht auch nach dem deutschen Recht soll § 173 Abs. 6 TKG-E in der Fassung des Telekommunikationsmodernisierungsgesetzes vorsehen. Die Bundesregierung hat den Gesetzesänderungsentwurf am 16.12.2020 verabschiedet, siehe https://www.bmwi.de/Redaktion/DE/Artikel/Service/Gesetzesvorhaben/telekommunikationsmodernisierungsgesetz.html [28.12.2020].

10 Einen begrüßenswerter Vorstoß hinsichtlich einer solchen Regelung wagt Microsoft: »Neue Maßnahmen zum Schutz Ihrer Daten«, 20.11.2020, https://news.microsoft.com/de-de/neue-massnahmen-zum-schutz-von-daten/ [22.12.2020].

der EuGH die Aufsichtsbehörden deutlich dazu ermahnt, aufsichtliche Maßnahmen zu ergreifen. Ein Vollzug der Entscheidung im nationalen Recht dürfte jedoch schnell an Grenzen stoßen.

Bevor die deutschen Datenschutzaufsichtsbehörden eine Maßnahme gem. Art. 58 Abs. 2 DSGVO treffen können, müssen sie nach dem Grundsatz der Amtsermittlung gem. § 24 VwVfG[11] den Sachverhalt vollumfänglich aufklären. Dazu gehört es auch, den Verstoß im konkreten Einzelfall festzustellen. Für eine Untersagung einer Datenübermittlung in die USA wäre das der folgende Verstoß: Der Verantwortliche übermittelt, ohne die Voraussetzungen des Art. 44 ff. DSGVO einzuhalten, personenbezogene Daten in ein Drittland. Die Aufsichtsbehörde müsste darüber hinaus feststellen, dass die SCC sowie gegebenenfalls getroffene ergänzende Maßnahmen nicht ausreichend sind, um ein gleichwertiges Datenschutzniveau sicherzustellen. Diese Feststellung setzt allerdings voraus, dass die Datenschutzaufsichtsbehörde selbstständig eine Einzelfallprüfung angestellt hat. Die Behörde muss darlegen können, dass tatsächlich ein rechtswidriger Eingriff in die Grundrechte der betroffenen Person stattgefunden hat oder noch stattfindet. Ein bloß abstrakter Verweis auf die bestehenden Befugnisse US-amerikanischer Geheimdienste ist dafür keinesfalls ausreichend. Die Aufsichtsbehörde muss im Einzelfall ermitteln, dass der Datenimporteure Adressat eines Ersuchens der US-Geheimdienste war oder die US-Geheimdienste anderweitig unbefugt auf personenbezogene Daten zugegriffen haben.

Fazit: Für das Ergreifen aufsichtlicher Maßnahmen gem. Art. 58 Abs. 2 DSGVO ist die bloße abstrakte Gefahr, dass ein unbefugter Zugriff erfolgt sein oder stattfinden könnte, nicht ausreichend. Der Amtsermittlungsgrundsatzes gebietet es, dass die Behörde den Sachverhalt vollumfänglich ermittelt. Ein Verstoß ist erst dann festgestellt, wenn tatsächlich ein unberechtigter Zugriff von US-amerikanischen Geheimdiensten erfolgte. Bereits anhand dieses Kriteriums ergibt sich, dass die Anforderungen für ein aufsichtliches Handeln insbesondere im Falle einer Untersagung der Datenübermittlung sehr hoch sind.

Darüber hinaus muss jede Maßnahme der Datenschutzaufsichtsbehörde gem. § 40 VwVfG ermessensfehlerfrei getroffen werden, d.h. insbesondere verhältnismäßig sein. Hier deutet sich die nächste scheinbar unüberwindbare Hürde an. Unmittelbar nach der EuGH Entscheidung im Verfahren »Schrems 2« riefen die Aufsichtsbehörden dazu auf, Verantwortliche sollen prüfen, ob sie statt US-amerikanischer Dienste nicht auf europäische Anbieter zurückgreifen könnten. Ein Großteil der Office-Anwendungen sind cloud-basierte Dienste US-amerikanischer Anbieter. Insbesondere für Klein- und mittelständische Unternehmen dürfte es keine praktikable Alternative zu den großen US-amerikanischen Diensteanbietern geben. Selbst wenn es theoretisch eine Alternative wäre, eigene Server innerhalb der EU/EWR zu betreiben, bedeutet dies für eine Vielzahl der Verantwortlichen einen enormen finanziellen und personellen Aufwand. Dieser Aufwand muss im Rahmen der Ermessensausübung berücksichtigt werden. Die Aufsichtsbehörde muss im Falle einer Untersagung zu dem Ergebnis kommen, dass dem Verantwortlichen ein rechtmäßiges Handeln – Verzicht auf US-amerikanische Dienstleister – nicht nur tatsächlich möglich (vgl. § 44 Abs. 2 Nr. 4 VwVfG), sondern als im Einzelfall angemessene Regelung auch tatsächlich zumutbar ist. Schon diese Voraussetzung dürfte unter Berücksichtigung der Monopolstellung der US-amerikanischen Dienste selten vorliegen.

Die von der Behörde getroffene Maßnahme muss auch sonst verhältnismäßig sein. Art. 58 Abs. 2 DSGVO sieht einen Maßnahmenkatalog vor, der mit den geringsten Intensität beginnt und an deren Ende das letzte Mittel steht, und zwar die Anordnung, eine Übermittlung auszusetzen. Eine Untersagung, US-amerikanische Dienste zu verwenden, dürfte vor allem im Zeitalter der Digitalisierung und erst recht während der Covid-19-Pandemie in vielen Fällen einer Betriebsuntersagung gleichkommen. Die Aufsichtsbehörde müsste darlegen, dass es kein gleich geeignetes milderes Mittel gibt als die Anordnung, die Übermittlung in die USA auszusetzen. Ein milderes Mittel dürfte es jedoch sein, wenn die Aufsichtsbehörde ergänzende Maßnahmen im Einzelfall anordnet. An dieser Stelle wird klar, dass sich das Blatt schnell wendet und die Aufsichtsbehörde prüfen muss, ob und welche ergänzenden Maßnahmen gleich geeignet und daher vorrangig zu ergreifen sind. Die Aufsichtsbehörde müsste prüfen, weshalb eine Verschlüsselung, die Verwendung von Pseudonymisierungsverfahren oder weitere technische Maßnahmen nicht ebenso geeignet sind, um einen konkreten Zugriff der Geheimdienste auf personenbezogene Daten zu unterbinden.

Fazit: Zunächst muss der Verantwortlichen prüfen, ob die SCC ausreichend sind. Gegebenenfalls ergreift er ergänzende Maßnahmen und orientiert sich dabei an den Empfehlungen des EDSA. Gelangt er zu dem Ergebnis, dass ein gleichwertiges Schutzniveau besteht und ergreift er die vom EDSA vorgeschlagenen Maßnahmen, so bleibt unter Berücksichtigung der verwaltungsrechtlichen Grundsätze kaum ein Raum für eine Untersagung der Datenübermittlung. Die Datenschutzaufsichtsbehörden müssten nicht nur einen konkreten Verstoß US-amerikanischer Geheimdienste feststellen, sondern zugleich auch ermessensfehlerfrei zu dem Ergebnis kommen, dass der Verantwortliche alternative Mittel der Datenverarbeitung in Anspruch nehmen kann, ohne dass seine wirtschaftliche Betätigung unverhältnismäßig eingeschränkt wird.

## VI. Zusammenfassung

Führt man sich dieses Ergebnis vor Augen, ist klar, dass eine Lösung ausschließlich auf politischer Ebene erfolgen kann. Zwar entbindet dies keinesfalls den Verantwortlichen in jedem Fall eine Einzelfallprüfung durchzuführen. Allerdings zeigt sich, dass die mahnenden Worte des EuGH, die Datenschutzaufsichtsbehörden mögen nun endlich aufsichtliche Maßnahmen treffen, an rechtliche Grenzen stoßen. Die verwaltungsverfahrensrechtlichen Anforderungen sind derart hoch, dass eine vollständige Untersagung der Datenübermittlung in die USA äußerst unwahrscheinlich ist. Doch dies bedeutet keinesfalls einen Freibrief für Verantwortliche. Wer noch heute ausschließlich seine Datenübermittlung auf das Privacy Shield stützt, handelt rechtswidrig. Wer hingegen SCC nutzt, eine Einzelfallprüfung hinsichtlich des Datenschutzniveaus durchgeführt und dokumentiert sowie ergänzende Maßnahmen getroffen hat, der darf sich entspannt zurücklehnen und die Verhandlungen zu neuen EU-US-Datenschutzabkommen verfolgen.

11 Entsprechendes gilt nach den landesspezifischen Verwaltungsverfahrensvorschriften im Falle der Datenschutzaufsichtsbehörden der Länder.

Digital Finance

Überblick

# Der Regierungsentwurf des eWpG und das Depotrecht – Ein Warnruf

Rechtsanwalt Dr. Thorsten Voß, Frankfurt am Main*

**Mit dem Regierungsentwurf für ein Gesetz zur Einführung elektronischer Wertpapiere betritt der deutsche Gesetzgeber in vielerlei Hinsicht Neuland, um einen angemessenen Rechtsrahmen für die Digitalisierung des Wertpapierhandels zu schaffen. Das Gesetz über elektronische Wertpapiere (eWpG) soll und muss sich dabei in ein bestehendes komplexes kapitalmarktrechtliches Regime aus genuin nationalen, europäisch veranlassten sowie unmittelbar in den Mitgliedstaaten geltenden europäischen Regelwerken einfügen, wobei depotrechtliche Aspekte zentral sind. Die im vorgelegten Entwurf hierzu gemachten Vorschläge werden indessen quasi-monopolistische Strukturen festigen und innovative Start-ups wie auch einen gewünschten Wettbewerb ungebührlich behindern.**

## I. Einleitung

Der am 16.12.2020 beschlossene Regierungsentwurf eines Gesetzes zur Einführung von elektronischen Wertpapieren[2] ist derzeit der Hotspot für kapitalmarktrechtliche Fragestellungen in der Blockchain- und FinTech-Community schlechthin. Der Kern dieses Artikelgesetzes ist das gänzlich neue Gesetz über elektronische Wertpapiere (eWpG),[3] wonach für private Emittenten die Begebung »papierloser Wertpapiere«[4] rechtlich möglich gemacht werden soll. Flankierend hierzu sind Modifikationen des WpPG, des DepotG, des SchVG sowie weiterer Gesetze vorgesehen.

Die Fragestellungen, die sich aus einer derart komplexen Ergänzung des Wertpapierrechts ergeben, sind naturgemäß äußerst vielfältig und reichen von Haftungsfragen bei Verlust von elektronischen Wertpapieren, etwa infolge von Hackerangriffen, über das Verhältnis zum Kryptoverwahrgeschäft nach dem KWG bis zur Behandlung von Investmentvermögen nach dem KAGB.[5] Dieser Beitrag nimmt die Aspekte in den Fokus, die sich für »sammelverwahrte« elektronische Wertpapiere stellen, also solche, die bei einer Wertpapiersammelbank hinterlegt werden, um im Anschluss in den »stückelosen« Effektengiroverkehr einbezogen zu werden. Er wird zugleich aufzeigen, dass der Gesetzesentwurf im Hinblick auf diesen Regelungskomplex für die Hebung der Potentiale der Distributed Ledger-Technologie kontraproduktiv ist.

## II. Öffnung des deutschen Rechts für elektronische Wertpapiere

### 1. Anwendungsbereich

Die geplante Öffnung des deutschen Rechts für elektronische Wertpapiere beschränkt sich zunächst auf Inhaberschuldverschreibungen.[6] Dies geschieht dergestalt, dass die zwingende urkundliche Verkörperung von Wertpapieren abgeschafft wird. Der Regierungsentwurf sieht keinen Zwang zum Umstieg auf elektronische Wertpapiere vor,[7] sondern möchte den Emittenten lediglich eine zusätzliche Gestaltungsoption eröffnen. Ihnen bleibt die Entscheidung überlassen, ob sie *»am bewährten System der Wertpapierurkunden«*[8] festhalten oder die Emission von Schuldverschreibungen auf elektronischem Wege bevorzugen.[9] Auch sieht § 6 Abs. 2 bzw. 3 eWpG-E die Möglichkeit eines Formwechsels von der alten in die neue Welt vor, d.h. von nicht-elektronischen zu elektronischen Wertpapieren, und *vice versa*.[10] So soll ein Gleichgewicht zwischen der Aufrechterhaltung existierender Strukturen – die volkswirtschaftliche Notwendigkeit hierzu ist nicht von der Hand zu weisen – und der Förderung neuer dezentraler Strukturen, die insbesondere von Start-ups vorangetrieben werden und für etablierte Finanzinstitute gleichermaßen interessant sind, erreicht werden.

### 2. Begebung und Übertragung elektronischer Wertpapiere

Die Begebung eines elektronischen Wertpapiers erfolgt durch Eintragung in ein Wertpapierregister anstelle der Ausstellung einer Urkunde, § 2 Abs. 1 eWpG-E. Damit eröffnet der RegE neben der klassischen Begebungs- und Verwahrpraxis die Möglichkeit, anstelle der physischen Skriptur einer (Global-)Urkunde einen elektronischen Eintrag in einem Register zur Emission vorzunehmen.

* Partner der Sozietät Schalast & Partner in Frankfurt am Main, Bankkaufmann, Lehrbeauftragter an der Frankfurt School of Finance & Management und Dozent im Fachanwaltslehrgang für Bank- und Kapitalmarktrecht. Alle Internet-Fundstellen wurden zuletzt am 27.12.2020 abgerufen.

2 Der Referentenentwurf wurde am 10.08.2020 vorgelegt und ist abrufbar unter https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Einfuehrung_elektr_Wertpapiere.html. Der Entwurf ist Teil der am 18.09.2020 veröffentlichten Blockchain-Strategie der Bundesregierung (abrufbar unter Blockchain-Strategie der Bundesregierung (bmwi.de)) und entspricht i.Ü. sehr weitgehend den Reflexionen des gemeinsamen Eckpunktepapiers von BMF und BMJV für die regulatorische Behandlung von elektronischen Wertpapieren und Krypto-Token v. 07.03.2019 (abrufbar unter Eckpunkte für die regulatorische Behandlung von elektronischen Wertpapieren und Krypto-Token (bundesfinanzministerium.de)); vgl. hierzu statt aller *Casper* BKR 2019, 209.

3 Art. 1 des Regierungsentwurfs eines Gesetzes zur Einführung von elektronischen Wertpapieren (im Folgenden »eWpG-E«).

4 So die Diktion von *Segna* WM 2020, 2301.

5 Hierzu *von Goldbeck* in diesem Heft.

6 Verwiesen wird auf *»das praktische Bedürfnis des Finanzmarkts«*, das *»bei dieser Finanzierungsform am größten«* sei. Krit. insb. zur Auslassung von Aktien *Segna* WM 2020, 2301.

7 Die Ausrichtung des Entwurfs auf »das praktische Bedürfnis des Finanzmarkts« dürfte ein Verständnis nahelegen, wonach Nutzungs-Token bzw. Utility Token, die typischerweise digitale Gutscheine sind, nicht vom eWpG umfasst sind, selbst wenn sie im Einzelfall ein Leistungsversprechen i.S.v. § 793 Abs. 1 Satz 1 BGB repräsentieren. Nur erwähnt sei, dass die Schweiz hier schon weiter ist, wie ein Blick auf das schweizerische Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register v. 25.09.2020 zeigt. Denn lt. dessen Begründung sind auch Nutzungs-Token, die zivilrechtlich eine Forderung darstellen, einer Ausgestaltung als Registerwertrechte i.S.d. neuen Art. 973d OR zugänglich. Vor dem Hintergrund, dass maßgebliche neue Blockchains, wie etwa das LUKSO-Projekt (www.lukso.network) von der BaFin als Utility-Token eingestuft wurden, dürften hier empfindliche Regelungslücken bestehen.

8 So die Diktion im Eckpunktepapier, S. 2.

9 Hierzu bereits *Kreße* WM 2015, 463, 465.

10 *Linardatos* ZBB 2020, 329, 331.

Es ändert sich so – von analogem Papier hin zu einem digitalen Registereintrag – lediglich das Speichermedium. Der Gesetzgeber verhält sich hier bewusst technologieneutral und wählt einen jedweder Form von Dematerialisierung Rechnung tragenden Regulierungsansatz – das eWpG ist keine *lex Blockchain*.[11]

Zudem enthält § 2 Abs. 2 eWpG-E eine Klarstellung, wonach ein elektronisches Wertpapier dieselbe Rechtswirkung auslöst, wie ein mittels Urkunde begebenes, es wird mithin nur die Entstehungsform desselben erweitert.[12] Gleichwohl ist ein elektronisches Wertpapier ein Wertpapier im juristischen Sinne und damit eines i.S.d. CSD-VO.[13] Hierzu stellt das im eWpG neu eingeführte sog. Kryptowertpapier eine Unterform dar. Der Unterschied zum »konventionellen« Wertpapier besteht allein darin, dass die Eintragung in ein sog. Kryptowertpapierregister erfolgt.[14] Somit liegt der wesentliche Unterschied zur traditionellen Begebung im Austausch des Datenträgers der Gedankenerklärung – von der Papierform hin zu einem digitalen Eintrag in ein kryptografisches Register.

Von Belang ist zudem, dass der Gesetzgeber für den zivilrechtlichen Rahmen eine sachenrechtliche Fiktion vorgesehen hat: So werden elektronische – d.h. körperlose – Schuldverschreibungen im Wege einer Fiktionslösung *ipso iure* zu Sachen erklärt; vgl. § 2 Abs. 3 eWpG-E, so dass sich die Übertragung nach den §§ 929 ff. BGB richtet – lt. *Casper* die »Gretchenfrage« des Rechts elektronischer Wertpapiere.[15] Auch für elektronische Wertpapiere in Sammeleintragung bleibt es bei den allgemeinen sachenrechtlichen Prinzipien, was für die rechtssichere Integration elektronischer Wertpapiere in das herkömmliche Wertpapierrecht begrüßenswert ist.[16] Weiter können Kryptowertpapiere i.S.d. § 4 Abs. 3 eWpG-E auch im Wege der Einzeleintragung emittiert werden; ihre Übertragung richtet sich nach einem Geflecht sachenrechtlicher Ausnahmeregelungen in den §§ 24 ff. eWpG-E.

Zentral ist insoweit das Übereignungserfordernis gem. § 25 eWpG-E, wonach es zur Übertragung des Eigentums einer dinglichen Einigung sowie der Umtragung des Erwerbers im Wertpapierregister auf Weisung des Berechtigten bedarf. In § 24 eWpG-E findet sich dann der Grundsatz *»keine Verfügung außerhalb des Registers«*. Dieser sieht die Unwirksamkeit von nicht im Register eingetragenen Verfügungen vor. Damit werden die zivilrechtlichen Grundsätze der Übertragung insoweit ergänzt, als dass die Übergabe durch Eintragung ersetzt wird.[17] Für elektronische Wertpapiere in Sammeleintragung gelten über § 9 eWpG-E die sachenrechtlichen Regelungen für den Wertpapiersammelbestand.

Explizite Regelungen sind im Hinblick auf die für den Rechtsverkehr zentrale Frage des gutgläubigen Erwerbs eines elektronischen Wertpapiers in Einzeleintragung vorgesehen. So gilt zunächst der Inhalt des Wertpapiers für den redlichen Erwerber als vollständig und richtig, indessen enthält § 26 Nr. 2 eWpG-E eine Klarstellung, wonach derjenige, der als Inhaber des elektronischen Wertpapiers eingetragen ist, als materieller Rechtsinhaber gilt.[18] Erreicht wird dies durch die Eigentumsvermutung des § 27 eWpG-E für den als Inhaber Eingetragenen. Dagegen gilt für elektronische Wertpapiere in Sammeleintragung das allgemeine Sachenrecht und der dort verankerte Gutglaubensschutz; vgl. § 9 eWpG-E.

## III. Die Register

Soweit die dogmatische Bereitung des Bodens für Entstehung und Übertragung elektronischer Wertpapiere – die Musik für die Hebung des Potentials der Distributed Ledger Technologie spielt indessen in der Dogmatik der Register und hier in den Vorgaben für die Sammelverwahrung. Unterschieden wird zwischen dem zentralen Register für elektronische Wertpapiere und dem dezentralen Register für Kryptowertpapiere. Wer kann solche Register – realistisch – betreiben? Richtig ist, dass aufgrund der großen Bedeutung eines solchen Wertpapierregisters für die Rechtssicherheit und die Schaffung von Publizität an die Verlässlichkeit der Registerführung sowie die Richtigkeit des Registerinhalts hohe Anforderungen zu stellen sind, um die Authentizität, mithin die Feststellung des »Urhebers« des Wertpapiers, und die Integrität, mithin die Unverfälschtheit seit der Herstellung, zu gewährleisten. Das Führen der Wertpapierregister soll nach dem Konzept des eWpG-E unter Aufsicht gestellt werden, um dem Anlegerschutz sowie der Integrität, Transparenz und der Sicherstellung der Funktionsfähigkeit des Finanzmarktes Rechnung zu tragen.

### 1. Das Zentralregister

Das zentrale Wertpapierregister soll die erstmalige Eintragung elektronischer Wertpapiere sowie die Dokumentation über Änderungen des niedergelegten Inhalts des Rechts sicherstellen. Es dient somit in dem Gesamtkonzept als Medium der Entstehung eines solchen elektronischen Wertpapiers in Ersetzung der physischen Papierurkunde. Damit einhergehend ist durchaus für den Bereich des zentralen Wertpapierregisters eine Senkung der Transaktionskosten zu erwarten, entfallen doch die Kosten für die physische Verwahrung der Urkunden. Zudem fungiert das zentrale Wertpapierregister als eine Art Wertpapiersammelbank und sorgt für die notwendige Publizität, indem die §§ 13 f. eWpG-E den Inhalt sowie die Änderung des Registers festlegen.

Der normative Rahmen wird durch die §§ 12 ff. eWpG-E abgesteckt und es ist vorgesehen, dass bereits bestehende Anbieter ihr Angebot um die Registerführung erweitern könnten. Insoweit beschränkt der RegE wie auch schon der RefE die registerführenden Stellen auf Zentralverwahrer, die eine Kerndienstleistung i.S.d. Abschnitts A des Anhangs zur CSD-VO im Inland erbringen, zu-

11 Vgl. auch Stellungnahme Bundesverband Blockchain zum RefE, S. 5; im Internet abrufbar unter Bundesblock Stellungnahme zum Referentenentwurf eines Gesetzes zur Einführung von elektronischen Wertpapieren – Blockchain Bundesverband.

12 Vgl. RegBegr. eWpG S. 43. Erfreulicherweise verzichtet der RegE – sehenden Auges – auf eine originäre Definition der Begebung und vermeidet so eine normative Festlegungen zu den verschiedenen Begebungstheorien. Dies verhindert insb. ein Auseinanderfallen zwischen den herrschenden Begebungstheorien bzgl. via Urkunde begebener Wertpapiere sowie einer normativen Festlegung bzgl. elektronischer Wertpapiere. Es mag nach der herrschenden Vertragstheorie ein Wertpapier durch Einigung zwischen Emittent und Inhaber sowie dem Skripturakt der Urkundenerstellung entstehen, woran der RegE keine Änderung vornimmt, kann doch jetzt nur der Skripturakt auch durch Eintragung in ein Wertpapierregister erfolgen. Wie hier und die positive Einschätzung teilend *Segna* WM 2020, 2301, 2306.

13 Verordnung (EU) Nr. 909/2014 des Europäischen Parlaments und des Rates v. 23.07.2014 zur Verbesserung der Wertpapierlieferungen und -abrechnungen in der Europäischen Union und über Zentralverwahrer sowie zur Änderung der Richtlinien 98/26/EG und 2014/65/EU und der Verordnung (EU) Nr. 236/2012; im Internet abrufbar unter EUR-Lex - 32014R0909 - EN - EUR-Lex (europa.eu).

14 Vgl. RegBegr § 8 eWpG, S. 57 f.

15 *Casper* BKR 2019, 209, 214.

16 Vgl. *Preuße/Wöckener/Gillenkirch* BKR 2020, 551, 554; die Sammeleintragung wird im RegE. selbst als die *»digitale Abbildung des institutionellen Effektengiroverkehrs, bei dem im derzeit praktisch relevantesten Fall die Dauerglobalurkunde durch die Wertpapiersammelbank verwahrt wird«*, bezeichnet.

17 S. für Einzelheiten *Preuße/Wöckener/Gillenkirch* BKR 2020, 551, 554; *Linardatos* ZBB 2020, 329, 332.

18 Im Gegensatz zum RefE ist nach dem RegE kein über das Herkömmliche hinausgehender Gutglaubensschutz an die Vertretungsbefugnis, Verfügungsbefugnis oder gar an die Geschäftsfähigkeit des Veräußerers sowie des Vertreters mehr vorgesehen.

dem sollen im Gegensatz zum RefE nunmehr auch Depotbanken als Zentralregisterführer tätig werden können, wenn die dort eingetragenen Papiere nicht in das Effektengiro eingebucht werden. Die Beaufsichtigung der Führung eines solchen zentralen Registers soll gem. § 11 eWpG-E der BaFin obliegen. Die Inbezugnahme der CSD-VO hat einen derart hohen aufsichtsrechtlichen Maßstab zur Folge, dass weitergehende Vorgaben obsolet sind.[19]

### 2. Dezentrale Register

Hinter dem in §§ 16 ff. eWpG-E normierten Kryptowertpapierregister versteckt sich im Grunde das häufig geforderte, wenn von der Community nicht gar ersehnte »Blockchain-Register«. Auch und gerade insoweit vermisst man im RegE Festlegungen im Hinblick auf eine bestimmte Technologie. Um gewisse Mindeststandards festzuschreiben, die für die Annahme eines Gutglaubensschutzes auch erforderlich sind, ist vorgesehen, dass das Aufzeichnungssystem als dezentrale Datenstruktur ausgestaltet ist, in welcher Daten in der Zeitfolge protokolliert sowie gegen unbefugte Löschung und nachträgliche Veränderung geschützt abgebildet sind.[20] Es muss folglich eine Verhinderung von Manipulationen sowie eine Nachvollziehbarkeit jeder Änderung der Daten in ihrer konkreten zeitlichen Abfolge gewährleistet sein. Dies ist alles so offen und technologieneutral formuliert, dass auch der Blockchain-Technologie nachfolgende, vergleichbare Systeme bei Entsprechung der gesetzgeberseitig aufgestellten Anforderungen als dezentrales Register für elektronische Wertpapiere fungieren können. In einem solchen Register ist es möglich, so gut wie alle Arten von Daten in einem Peer-to-Peer-Netzwerk zu teilen und zu handeln, werden doch elektronisch nahezu in Echtzeit auf mehreren Rechnern gleichzeitig verschlüsselte Datenblocks erstellt, aktualisiert und koordiniert. Von allen Rechnern eines Netzwerks wird jede Transaktion oder Veränderung registriert, geprüft, bestätigt und dokumentiert. Daher sind solche Systeme jedenfalls vom Grundsatz her effizient, transparent und im Vergleich zu herkömmlichen Systemen recht fälschungssicher. Die Identität der Nutzer wird durch Verschlüsselungsmechanismen geschützt.

Hervorzuheben ist, dass es im Gegensatz zum zentralen Wertpapierregister keines zugelassenen Zentralverwahrers bedarf. Vielmehr kann die Verwaltung und Fortschreibung des Registers automatisiert und algorithmenbasiert erfolgen. Gleichwohl bedarf es, um die Einhaltung der Verwaltungspflichten bezüglich Kryptowertpapierregistern zu gewährleisten, einer registerführenden Stelle als Normadressat. Die Konsequenz hieraus ist, dass sogar der Emittent selbst – in der Sache können dies etwa auch Industriekonzerne sein – das Register für die eigenen Wertpapiere führen können und dürfen. Es ist insoweit kein zentrales Kryptowertpapierregister vorgesehen, weil – und das hat der Gesetzgeber sehr zutreffend erkannt – die *ratio* hinter der Distributed Ledger-Technologie gerade die originäre Ersetzung zentraler Strukturen ist. Das ändert jedoch nichts daran, dass die Führung eines Kryptowertpapierregisters gesetzgeberseitig eine Einstufung als Finanzdienstleistung erfährt. Damit bedarf die registerführende Stelle aber auch einer Erlaubnis durch die BaFin. Aus Gründen des Anlegerschutzes, der Geldwäscheprävention, der Marktintegrität sowie der Transparenz und dem Funktionsschutz der Kapitalmärkte ist dies als legislative Grundsatzentscheidung jedenfalls nicht zu beanstanden, die konkrete Ausgestaltung in der Verwaltungspraxis (Stichwort: *»Aufsicht mit Augenmaß«*) wird sich insbesondere am Angemessenheitserfordernis messen lassen müssen.

Wasser in den Wein schüttet der Gesetzgeber der Community allerdings mit § 16 Abs. 2 i.V.m. § 7 eWpG-E, ist doch hiernach die registerführende Stelle oder eben der Emittent für die Registerführung zivilrechtlich haftbar. Beim Betrieb insbesondere einer sog. public Blockchain ist dies ein durchaus valides Risiko – hier werden sich womöglich Versicherungslösungen etablieren müssen, damit eine entsprechende Anbieterakzeptanz entsteht.

### 3. Warnruf

Soweit, so gut – indessen gibt der RegE im Hinblick auf seine marktpolitische Ausgestaltung nicht nur Anlass zur Kritik, sondern auch für einen Warnruf. Stein des Anstoßes ist der Umstand, dass der RegE nach wie vor vorsieht, dass *ausschließlich* zugelassene Zentralverwahrer registerführende Stelle bei einer Sammelverwahrung sein können. Erste Stimmen bewerten dies als positiv, etwa wenn in diesem Kontext davon gesprochen wird, dies überzeuge, *»insbesondere im Hinblick auf die effektive Vermeidung von Manipulationsmöglichkeiten, die mit dem hohen aufsichtsrechtlichen Maßstab einhergeht. Ebenso ist das Schaffen von Wettbewerb auf diesem Marktsegment positiv zu bewerten, so sind hierdurch unmittelbar sinkende Transaktionskosten zu erwarten, was wiederum der Attraktivität des deutschen Finanzstandortes zuträglich ist.«*[21]

Das Gegenteil ist richtig. Zutreffend ist, dass bei elektronischen Schuldverschreibungen, die an einer Börse oder einem anderen Handelsplatz gehandelt werden sollen, eine »Verwahrung« bei einem Zentralverwahrer unverzichtbar ist; vgl. Art. 3 Abs. 1 CSD-VO. Nicht zu übersehen ist jedoch, dass es in Zukunft auch papierlose Emissionen geben kann, bei denen die Einbeziehung in den Handel und/oder den Effektengiroverkehr überhaupt nicht angestrebt wird. Damit wäre die Inanspruchnahme eines Zentralverwahrers, also der *Clearstream Banking AG* als der einzigen Einrichtung, die in Deutschland überhaupt über eine entsprechende Zulassung verfügt, wohl bereits regelmäßig aus Kostengründen nicht erwünscht. Dann mag die Eintragung in ein Kryptowertpapierregister als Alternative zur Verfügung stehen, aber auch diese Begebungsform wird – nicht fernliegend – sowohl bei Emittenten als auch Investoren auf Vorbehalte stoßen. Zwar besteht nunmehr, weil gem. § 12 Abs. 2 Nr. 2 WpG-E ein Verwahrer ein zentrales Register führen kann, grundsätzlich die Möglichkeit, elektronische Wertpapiere nach Art der Haussammelverwahrung gem. § 5 Abs. 1 Satz 2 DepotG bei einem Kreditinstitut zu »hinterlegen«. Vor dem Hintergrund des § 9a Abs. 1 Satz 1 DepotG (*»Zwangsgiro«*) ist dies durchaus folgerichtig, sollte man ein elektronisches Wertpapier in Sammeleintragung als Gegenstück zur Globalurkunde begreifen.

Indessen muss dieses Ergebnis im Interesse eines gewünschten Wettbewerbs von Anbietern überdacht werden, wenn bestehende quasi-monopolistische Strukturen nicht vertieft und gefestigt werden sollen. Auch die angestrebte Technologieneutralität gebietet einen anderen, offeneren Regelungsansatz. Was spricht dagegen, nicht nur Kreditinstitute mit einer Erlaubnis zum Depotgeschäft gem. § 1 Abs. 1 Satz 2 Nr. 5 KWG als taugliche Registerführer vorzusehen, sondern einen neuen Tatbestand sui generis zu schaffen, der Start-ups realistisch, so wie etwa beim Kryptoverwahrgeschäft, einen Markteintritt ermöglicht? Denn

19 *Preuße/Wöckener/Gillenkirch* BKR 2020, 551, 556.
20 Vgl. RegBegr zu § 16 eWpGE 70.
21 So etwa *Preuße/Wöckener/Gillenkirch* BKR 2020, 551, 556.

dort sind die tatsächlichen Innovationen zu erwarten, in seiner aktuellen Fassung übt sich das Gesetz im Bestandsschutz.[22]

Gestützt wird diese Forderung durch den Blick ins Ausland. So existieren bspw. in der *Confoederatio Helvetica* Regulierungsansätze von noch höherem Liberalitätsgrad: Bekanntlich entstehen nach Schweizer Recht Wertrechte mit konstitutiver Eintragung in das grundsätzlich vom Emittenten selbst zu führende Wertrechtebuch; vgl. Art. 973c Abs. 2 und 3 OR. Im Rahmen der Begebung tritt an die Stelle der bei verbrieften Titeln erforderlichen Übergabe einer Urkunde die Eintragung; das nicht öffentliche Wertrechtebuch ist vom öffentlichen Hauptregister gem. Art. 6 Abs. 2 BEG zu unterscheiden, das von einer Verwahrungsstelle i.S.v. Art. 4 Abs. 2 BEG zu führen ist. Dessen Funktion ist in der Herstellung von Publizität hinsichtlich der in einem Effektengirosystem zirkulierenden Bucheffekten zu verorten.

#### 4. Einbeziehung in den Effektengiroverkehr

Auch eine Reflexion des Regelungsrahmens für die Einbeziehung in den Effektengiroverkehr unterstützt den Anlass für den Warnruf. So ermöglicht die zentrale Registrierung einer elektronischen Schuldverschreibung bei der *Clearstream Banking AG* die Einbeziehung in den Effektengiroverkehr; in welchen Schritten dies vonstatten zu gehen hat, ist § 12 Abs. 3 eWpG, der offensichtlich an Art. 3 Abs. 1 CSD-15 VO angelehnt ist, bedauerlicherweise nur andeutungsweise zu entnehmen. Es dürfte folgendes Verfahren angezeigt sein: Es muss die zur Aufnahme in den Effektengiroverkehr vorgesehene Schuldverschreibung in einem ersten Schritt wirksam zur Entstehung gebracht werden. Dabei entspricht funktional die hierfür erforderliche Eintragung in das von der *Clearstream Banking AG* geführte zentrale Register nach Maßgabe der §§ 8 Abs. 1 Nr. 1, 13 eWpG-E der Einlieferung und Hinterlegung von Urkunden, wie sie im bekannten System der Girosammelverwahrung notwendig ist. Die Verbuchung der wirksam begründeten Anteilsrechte an der Sammeleintragung auf Depotkonten wäre dann der zweite Schritt; es wird sich bei einer Anleiheemission typischerweise um die Depotkonten der Mitglieder des Emissionskonsortiums handeln.[23]

Nun geht aber die Gesetzesbegründung davon aus, dass die *Clearstream Banking AG* die zur Einbeziehung elektronischer Wertpapiere in den Effektengiroverkehr erforderlichen Schritte *»in den bestehenden Vertrags- und Kontenstrukturen«* vollziehen könne, ohne ein neues Registersystem einrichten zu müssen.[24] Das ist sicher richtig, insbesondere wenn man sich vor Augen führt, dass sich das hier beschriebene Procedere nicht wesentlich von dem hergebrachten Verfahren der Einlieferung und Einbuchung von (Global-)Urkunden in das CASCADE-System unterscheidet. Dann besteht aber nicht nur ein einziger Anbieter für die Sammelverwahrung, der bereits über die erforderliche Zulassung verfügt, sondern zudem auch nur ein einziger Anbieter, der über die hierfür erforderliche technische Infrastruktur verfügt. Für Anbieter, die in diesen Markt neu eintreten möchten, türmt sich damit nicht nur die Hürde eines Zulassungsverfahrens nach der CSD-VO auf, sondern zugleich die Programmierung und Etablierung eines technischen Systems mit Kosten in deutlich zweistelliger Millionenhöhe. Für Start-ups ist dies jedenfalls zeitnah nicht realistisch zu bewerkstelligen.

### IV. Zusammenfassende Bewertung

Trotz der Dematerialisierung des Effektenwesens erübrigen sich auch durch das eWPG diejenigen Fragen nicht, die aus der *Mediatisierung der Wertpapierverwahrung* folgen. Dies betrifft namentlich die Notwendigkeit, den Übertragungsvorgang im Effektengiroverkehr *»irgendwie in die Kategorien der §§ 929 ff. BGB zu pressen«*.[25]

Um es in aller Deutlichkeit zu formulieren: Ein Modell, das zwar einen Schritt zum »papierlosen Wertpapier« vollzieht, im Wesentlichen aber an der hergebrachten sachenrechtlichen Konstruktion des Effektengiroverkehrs meint festhalten zu müssen, trägt zur Lösung dieser seit Jahrzehnten bekannten Probleme wenig bei. Soweit das Regelungskorsett für elektronische Wertpapiere im zentralen Register betroffen ist, muss der Regierungsentwurf sogar mit dem Attribut *»rückwärtsgewandt«* charakterisiert werden.[26]

Dies ist umso weniger verständlich, als eine umfassende Reform des Depotrechts seit langem mit Nachdruck gefordert wird[27] – und welcher Zeitpunkt erscheint besser geeignet als derjenige der Öffnung des deutschen Rechts für elektronische Wertpapiere? Hinzu kommt, dass dies in einem früheren Eckpunktepapier des BMJ zur Diskussion gestellt worden war.[28] Damit verfehlt der Entwurf aber das erklärte und selbst gesteckte Ziel, *»das Wertpapierrecht zu modernisieren und damit den Finanzplatz Deutschland zu stärken«*. Die Innovationskraft, die bei der Regelung von Kryptowertpapieren spürbar wird, bleibt ein schwacher Trost.

Zu fordern bleibt eine umfassende Reform des Depotrechts, an deren Ende elektronische Wertpapiere nach dem Vorbild des schweizerischen Bucheffektengesetzes hoffentlich als ein neues Recht *sui generis* zu stehen. Gerade im Hinblick auf die ausweislich der Gesetzesbegründung geplante Neueinführung einer elektronischen Aktie[29] wäre dies äußerst wünschenswert, damit die Diskussion sich nicht in den ausgetretenen Bahnen fortsetzt.

### Fazit

**(1)** Das eWPG soll Privaten die Emission »papierloser Wertpapiere« ermöglichen, indem ein elektronisches Wertpapier als Sache i.S.d. § 90 BGB fingiert wird.

**(2)** Die bekannten Probleme, die sich aus der Mediatisierung der Wertpapierverwahrung ergeben, werden durch diesen Ansatz nicht gelöst, da die Übertragungsvorgänge im Effektengiroverkehr nach wie vor in das Korsett der §§ 929 ff. BGB gezwängt werden.

**(3)** Insbesondere im Hinblick auf in einem zentralen Register verwahrte elektronische Wertpapiere ist der RegE des eWPG in der Sache rückwärtsgewandt und festigt in den zu prognostizierenden praktischen Auswirkungen bestehende quasi-monopolistische Strukturen.

**(4)** Eine (derzeit rechtspolitisch unwahrscheinliche) gebotene umfassende Reform des deutschen Wertpapier- und Depotrechts gehört auf die Agenda, um einen zukunftsfähigen Rechtsrahmen für einen digitalisierten Wertpapierhandel zu schaffen.

22 I.d.S.a. *Segna* WM 2020, 2301, 2311.
23 Beide Schritte lassen sich unter dem Begriff der »notariellen Dienstleistung« i.S.d. CSD-Verordnung zusammenfassen.
24 RegBegr eWpG-E, S. 61.
25 *Canaris*, Bankvertragsrecht, 3. Aufl. 1988, Rn. 2053.
26 Dies teilend *Segna* WM 2020, 2301, 2311.
27 Vgl. nur *Einsele*, Wertpapierrecht als Schuldrecht, 1995, S. 561 ff.; *Lehmann*, Finanzinstrumente, 2009, S. 228 ff.
28 BMJ, Eckpunktepapier zur Reform des Depotrechts v. 29.05.2008.
29 RegBegr eWpG, S. 43.

## Überblick

# Das eWpG und Immobilieninvestments

Rechtsanwalt Axel v. Goldbeck, Berlin*

**Der Beitrag behandelt die Möglichkeiten zur Tokenisierung von Immobilieninvestments und den Einfluss des eWpG-E hierauf. Dargestellt werden die bestehenden Möglichkeiten sowie die auch nach Einführung des eWpG in der aktuellen Fassung bestehenden Beschränkungen.**

### A. Einführung

Die Digitalisierung der deutschen Wertpapierbranche schien vergleichsweise weit fortgeschritten zu sein. Technische Entwicklungen haben die Wertpapiermärkte geprägt, ihre Globalisierung gefördert und zu einer gewaltigen Expansion geführt: Elektronischer Wertpapierhandel, Automatisierung und Hochfrequenzhandel waren Schlagworte, die die Öffentlichkeit, Marktteilnehmer und Aufsichtsbehörden über Jahre beschäftigten.

Umso befremdlicher mag es anmuten, dass am Anfang jeder deutschen Wertpapieremission noch immer ein Relikt aus der vordigitalen Zeit steht: Die Wertpapierurkunde. Was in den meisten entwickelten Kapitalmärkten schon länger Geschichte ist, prägt das deutsche Wertpapierwesen bis heute. Die für angelsächsische Jurisdiktionen eigentümliche Trennung von Schuld- und Sachenrecht und die Anknüpfung der Übertragung von Wertpapieren an den Sachbegriff haben die gesamte Wertpapierdogmatik im deutschen Recht geprägt und seine Modernisierung gebremst.

Nun hat die normative Kraft des Faktischen gesiegt. Der Referentenentwurf eines Gesetzes zur Einführung von elektronischen Wertpapieren hat am 16.12.2020 das Kabinett passiert und liegt damit als offizieller Regierungsentwurf vor.[1] Der Gesetzentwurf beschränkt sich zwar auf Schuldverschreibungen und Anteilsscheine von Investment-Sondervermögen und damit auf die »niedrig hängenden Früchte« für die Zwecke der Digitalisierung. Aber dabei soll und wird es nicht bleiben.

Wie ein Vergleich zeigt, ist der Regierungsentwurf gegenüber dem Referentenentwurf noch einmal maßgeblich überarbeitet und teilweise erweitert worden. Wesentliche Neuerung ist die teilweise Öffnung des Kapitalanlagegesetzbuches (KAGB) für die elektronische Wertpapierform durch Art. 10 des Entwurfs. Offene inländische Investmentvermögen in Form von Sondervermögen sollen in Zukunft Anteilsscheine auch in elektronischer Form begeben können. Damit wurde auf vielfache Stellungnahmen zu dem Referentenwurf reagiert, die die Beschränkung auf Schuldverschreibungen als zu eng kritisierten.[2]

Um die Bedeutung dieser Erweiterung zu erfassen, lohnt ein Blick auf das Volumen des von deutschen Investmentsfonds verwalteten Kapitals: Die Mitglieder des BVI, der deutschen Branchenvertretung der Investmentbranche, verwalten nach den Verbandsstatistiken (Stand 30.09.2020) insgesamt ein Volumen von rd. 3,7 € Billionen. Rund 3 € Billionen werden in offenen Publikums- oder Spezialfonds gehalten, die in der Regel als Sondervermögen aufgelegt werden.[3] Von diesem Volumen entfallen rd. 116 € Milliarden auf Immobilien-Publikumsfonds, rd. 111 € Milliarden auf Spezial-Immobilienfonds und der große Rest auf Wertpapierfonds. Der mit Abstand größte Teil von Angeboten von Investmentvermögen könnte somit nunmehr elektronisch erfolgen.

Der vorliegende Beitrag nimmt den eWpG-E zum Anlass, die aktuellen Möglichkeiten elektronischer Immobilienbeteiligungen und den Einfluss des eWpG-E darauf darzustellen und zu bewerten.

### B. Digitale Immobilienbeteiligungen in Deutschland

Tatsächlich gibt es Immobilienbeteiligungen in digitaler Form bereits seit einiger Zeit in Deutschland in Form von sog. Immobilien-Token.

#### I. Immobilien-Token

Token entwickeln sich seit Jahren von einem Nischenthema der Kryptocommunity zu einem Thema, das Gesetzgeber und Aufsichtsbehörden in Bewegung setzt. Schon sprachlich ist der Tokenbegriff allerdings zunächst vielen ein Rätsel geblieben. Mittlerweile steht fest, dass es sich um den digitalen Repräsentanten eines Wertes bzw. eines – möglicherweise sehr kleinen – Teils eines körperlichen Assets oder sogar, wie bei sog. Kryptowährungen wie BitCoin, Ethereum & Co. um einen – digitalen – Wert selbst handelt. Diese digitalen Werte werden unter Einsatz von kryptografischen Technologien verschlüsselt und auf einer Blockchain registriert. Begrifflich präziser hat der deutsche Gesetzgeber mit der Erlaubnispflicht für die Kryptoverwahrung hierfür den Begriff »Kryptowert« eingeführt.

Immobilien-Token sind keine eigene Kategorie, sondern so gut wie immer eine Form von sog. Security- oder Wertpapiertoken, teilweise auch als Investment oder Asset Token bezeichnet. Immobilien-Token haben zuletzt einen deutlichen Aufschwung erfahren. Ihre vermeintliche Stabilität gerade im Gegensatz zu den zumeist volatilen Kryptowährungen hat ihnen eine hohe Aufmerksamkeit beschert.

Die Zahl der Anbieter und der spezialisierten technischen Plattformen hierfür ist stetig gewachsen. Brickblock, Bloxxter, Exporo u.a. bieten technische Unterstützung bei Tokenisierungen von Immobilien bzw. Immobilienfonds an. Der Erfolg der sog. Eigen-Emissionen, also Angeboten von Immobilienbestandshaltern mit eigenen Immobilien hält sich bisher jedoch regelmäßig in Grenzen. Bei den wenigen Vollplatzierungen ging es in der Regel um kleinere, d.h. einstellige

* Partner im Bereich Real Estate & Finance der DWF Germany Rechtsanwaltsgesellschaft mbH.

1 https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Einfuehrung_elektr_Wertpapiere.html.

2 Vgl. Stellungnahme Bundesverband Blockchain v. 11.08.2020, www.bundesblock.de; zumindest für Anteile an Sondervermögen vgl. BVI-Stellungnahme v. 14.09.2020.

3 https://www.bvi.de/fileadmin/user_upload/Statistik/Investmentstatistik_2009_Gesamtmarkt_DE.pdf.

Millionenbeträge, die oftmals ohne oder vor einem öffentlichen Angebot an bekannte Investoren verteilt wurden. Echte öffentliche Angebote hat es kaum gegeben. Grund hierfür sind nicht allein rechtliche Gründe, sondern vor allem die Finanzierungslogik von Immobilien: von Kleinanlegern lassen sich – mit vergleichsweise hohem Aufwand – regelmäßig lediglich recht geringe Beträge einsammeln. Große Volumina werden zumeist von institutionellen Investoren gezeichnet, die Tokenemissionen bisher aber skeptisch gegenüberstehen.

## II. Immobilien-Token und Schuldverschreibungen

In der Öffentlichkeit und auch in der Vermarktung von Immobilien-Token wird teilweise aus Unkenntnis, teilweise aber auch gezielt, der eigentliche Charakter von Immobilien-Tokenemissionen verschleiert. In Abgrenzung von den risikobehafteten Kryptowährungen wird auf das stabile Asset, d.h. die Immobilie verwiesen, die für die Sicherheit der Investition Sorge trage. Dabei wird immer wieder der – falsche – Eindruck erweckt, der Investor erwerbe »ein Stück Immobilie« (fractionized ownership) oder einen Anteil an einer immobilienhaltenden Gesellschaft. Tatsächlich können Immobilieneigentum und Beteiligungen an Immobiliengesellschaften in Deutschland wegen der bestehenden Registerpflichten bisher nicht tokenisiert werden. Investoren erhielten bei den bisherigen Tokenisierungen weder dingliche, noch gesellschaftsrechtliche, sondern ausschließlich schuldrechtliche und regelmäßig unbesicherte Ansprüche gegen den Emittenten.

Dabei werden die emittierten Instrumente häufig als Schuldverschreibungen bezeichnet. Ob dies in Anbetracht des Urkundenerfordernisses des § 793 BGB überhaupt möglich ist, ist für die zumeist nicht-professionellen Investoren dabei von untergeordneter Bedeutung. Tatsächlich handelt es sich nicht um Schuldverschreibungen oder Wertpapiere im zivilrechtlichen Sinne. Vielmehr ist es der Kautelarpraxis gelungen, ein vertragsrechtliches Pendant zur Schuldverschreibung zu entwickeln, das eine rechtlich wirksame Ausgabe von Immobilientoken erlaubt. Der Sache nach werden häufig Genussrechte »tokenisiert«, die eine eingeschränkte Beteiligung am Erfolg einer Immobilie(ngesellschaft) einräumen. Dies zeigt sich an den Übertragungsregelungen, die entweder dem Abtretungs- oder Vertragsübernahmeregime folgen; jedenfalls nicht der »wertpapiermäßigen« Übertragung einer Sache. Der »Trick« der Kautelarpraxis liegt darin, die Übertragung des Tokens bzw. des entsprechenden Schlüssels in einer Weise mit der Übertragung der vertraglichen Ansprüche zu verbinden, die ein Auseinanderfallen von Token und Forderung im Normalfall verhindert. Sofern vorgegeben wird, es handele sich um eine Schuldverschreibung, ist das zwar inkorrekt, aber irrelevant: Der Inhalt des emittierten Instruments ist in den Emissionsbedingungen zutreffend beschrieben und eine Falschbezeichnung schadet bekanntlich nicht.

Trotz dieser vertraglichen Konstruktion betrachtet die BaFin die emittierten Instrumente wegen ihrer Standardisierung und Handelbarkeit aufsichtsrechtlich als Wertpapiere im Sinne der MiFID. Dass zivilrechtliche Beurteilung und aufsichtsrechtliche Beurteilung auseinanderfallen, ist gewöhnungsbedürftig aber nicht verboten; allerdings auch folgenreich für alle Dienstleister, die an der Emission und dem Handel derartiger Instrumente beteiligt sind. Denn mit dieser Einordnung unterfallen Immobilien-Token dem umfangreichen wertpapierrechtlichen Aufsichtsregime.

## III. Immobilien-Token und das KAGB

### 1. eWpG und KAGB

Auf ihrem Weg ans Licht der Öffentlichkeit müssen Immobilien-Token allerdings eine weitere Hürde nehmen: Das Einsammeln von Mitteln einer Anzahl von Anlegern zum Zwecke der gemeinsamen Anlage entsprechend einer festgelegten Anlagestrategie qualifiziert einen Emittenten als Investmentvermögen nach § 1 Abs. 1 KAGB. Entsprechende Aktivitäten fallen damit in den Anwendungsbereich des KAGB mit seinen zahlreichen Verpflichtungen, insbesondere der Verwaltung des Fondsvermögens durch eine lizensierte Kapitalverwaltungsgesellschaft und den Formvorschriften für die angebotenen Instrumente.

Das KAGB lässt für Tokenemissionen so gut wie keinen Spielraum. Alle zulässigen Emissionsformen, seien es Immobilien-Investment-Aktien, Anteile an Sondervermögen und Investment-Kommanditanteile, verlangen bisher die Urkundsform bzw. die Eintragung ins Handelsregister. Bei offenen und geschlossenen Investment-Kommanditanteilen wird zudem die indirekte Beteiligung über einen Treuhänder, die unter Tokenisierungsgesichtspunkten Spielräume eröffnet hätte, weitgehend ausgeschlossen. Lediglich für die geschlossene Publikumsinvestmentkommanditgesellschaft ist eine Treuhandkonstruktion erlaubt, die kein Urkundserfordernis enthält. Bisher ist jedoch nicht bekannt, dass ein Fondsinitiator von dieser Möglichkeit der Tokenisierung Gebraucht gemacht hätte.

Die in der Praxis zu beobachtenden kreativen Bemühungen von Immobiliengesellschaften, den damit verbundenen zahlreichen Verpflichtungen zu entgehen, sind regelmäßig gescheitert. Auch wenn bei Inkrafttreten des KAGB die bestehenden bestandshaltenden börsennotierte Immobiliengesellschaften und -genossenschaften de facto Bestandsschutz erhielten, lässt die BaFin für neue Immobiliengesellschaften nur sehr wenige Ausnahmen gelten.[4] Wer also, wie es für Immobilieninvestment kennzeichnend ist, mehreren Investoren eine stabile Anlage für ein oder mehrere Immobilien bietet, kann nur unter sehr eingeschränkten Voraussetzungen der Qualifikation als Investmentvermögen entgehen.

### 2. Qualifizierter Rangrücktritt

Von einer dieser Ausnahmen wurde in der Vergangenheit reichlich Gebraucht gemacht. Nach BaFin-Auffassung liegt eine gemeinschaftliche Kapitalanlage nämlich dann nicht vor, wenn der Anleger mit dem Emittenten einen qualifizierten Rangrücktritt vereinbart. Beim qualifizierten Rangrücktritt wird der Anleger nicht generell am Verlust des Emittenten beteiligt, sondern er verpflichtet sich lediglich, das zur Verfügung gestellte Kapital nicht zurückzufordern (pactum de non petendo), wenn dadurch ein Grund für die Eröffnung des Insolvenzverfahrens herbeigeführt würde. Solange die

4 BaFin, Auslegungsschreiben zum Anwendungsbreich des KAGB und zum Begriff des »Investmentvermögens« v. 14.06.2013, geändert am 09.03.2015, Gz. Q 31-Wp 2137-2013/0006.

Erfüllung des Anspruches des Anlegers nicht die Insolvenz des Emittenten auslöst, hat der Anleger einen Anspruch auf die Rückzahlung seines zur Verfügung gestellten Kapitals in voller Höhe; und zwar unabhängig davon, ob der Emittent zwischendurch Verluste erlitten hat oder nicht.[5]

Mit diesem in Praxis regelmäßig verwendeten Ausweg aus der Anwendung des KAGB werden entsprechende Emissionen jedoch in die Graumarktecke gedrängt. Die BaFin selbst lässt an ihrer Bewertung von Angeboten mit qualifiziertem Nachrang wenig Zweifel.[6] Entsprechend verzichten professionelle Investoren noch immer weitgehend auf Immobilientokeninvestitionen auf dieser Grundlage.

### 3. Club-Emissionen

Eine weitere Gestaltungsmöglichkeit, die bisher weitgehend unbeachtet geblieben ist, eröffnet die ESMA-Leitlinie 2013/611 vom 13.08.2013 zu Schlüsselbegriffen der Richtlinie über die Verwalter alternativer Investmentfonds (AIFMD) zur Definitions des Begriffs Organismus für gemeinsame Anlage, im KAGB übersetzt als Investmentvermögen.

Nach der ESMA-Leitlinie setzt das Vorliegen eines Organismus für gemeinsame Anlagen voraus, dass die Anteilseigner des Organismus – als Gruppe – keine laufende Ermessens- bzw. Kontrollbefugnisse besitzen. Die Tatsache, dass einem oder mehreren, jedoch nicht allen Anteilseignern eine laufende Ermessens- bzw. Kontrollbefugnis gewährt wird, wird nicht als Nachweis dafür herangezogen, dass es sich bei dem Organismus nicht um einen Organismus für gemeinsame Anlagen handelt.[7]

Im Umkehrschluss kann daraus abgeleitet werden, dass in Fällen, in denen die Anteilseigener laufende Ermessens- und Kontrollbefugnisse besitzen, kein Organismus für gemeinsame Anlagen und damit keine Investmentvermögen vorliegt. Die BaFin hat ihrerseits bestätigt, dass »ein Organismus für gemeinsame Anlagen im Sinne des § 1 Abs. 1 Satz 1 KAGB nicht vorliege, wenn den Anlegern des Investitionsvehikels eine unmittelbare und kontinuierliche Entscheidungsgewalt über operative Fragen in Bezug auf das investierte Vermögen zukommt.«[8] In einem GmbH-Gesellschaftervertrag müsse dazu bspw. festgelegt sein, dass alle operativen Entscheidungen im Hinblick auf das Eingehen, Halten und Veräußern von Beteiligungen von der Gesellschafterversammlung und nicht originär von der Geschäftsführung getroffen werden. In einem solchen Fall bedürfe es keiner Erlaubnispflicht nach dem KAGB, da eine laufende Ermessens- und Kontrollbefugnis über das investierte Vermögen im Sinne der ESMA-Leitlinien durch die Gesellschafter hinreichend sichergestellt wäre.[9]

Allerdings scheint die entsprechende Gestaltung des Gesellschaftsvertrags (welcher Gesellschaftsform auch immer) zwar eine notwendige, aber keine hinreichende Bedingung zu sein. Die BaFin stellt lediglich klar, dass es um eine marktübliche Tätigkeit eines (erlaubnispflichtigen) Spezialfonds-Anbieters handelt, wenn den Investoren auf Anfrage ein zeichnungsfähiges maßgeschneidertes Produkt angeboten wird, dass den oben dargestellten Voraussetzungen entspricht. Zur Vermeidung der Gründung eines Investmentvermögens sei außerdem ein »eigeninitiatives Zusammenfinden« der Investoren notwendig. Hilfestellungen wie Musterverträge oder das Einschalten von Dienstleister zur Durchführung einer Bewertung schlössen ein eigeninitiatives Zusammenfinden nicht per se aus. Auf die Frage, ob es sich bei diesen Aktivitäten um private oder gewerbliche handele, kommt es aus Sicht der BaFin nicht an.

Die Beschreibung der Voraussetzungen für ein »eigeninitiatives Zusammenfinden« dürften vielen Investoren in Immobilienspezialfonds durchaus bekannt vorkommen. Tatsächlich geht die Initiative für die Aufsetzung von Spezialfonds sehr häufig von den Investoren aus, die ein geeignetes Objekt identifiziert haben und gemeinsam erwerben würden. Der Kreis der Beteiligten ist dabei regelmäßig klein, man kennt sich in der Branche. Die Kapitalverwaltungsgesellschaft wird zur Umsetzung des Konzepts und zur Verwaltung der Immobilie über die geplante Laufzeit angesprochen, wobei sich die (Spezial-) Investoren in unterschiedlichem und regulatorisch zulässigem Maße Entscheidungen über das Management der Immobilie vorbehalten.

Streng genommen erlaubt dies Investoren eines Spezialfonds zwar dem regulierten Bereich – einschließlich den Formvorschriften des KAGB – zu entkommen. Allerdings greifen dann, jedenfalls in Deutschland, die allgemeinen Formvorschriften für die Emission von Aktien, GmbH-Geschäftsanteilen oder Kommanditbeteiligungen. Immerhin gibt es bei eigeninitiativem Zusammenwirken auch keine Verpflichtung zur Direktbeteiligung mehr, so dass Treuhand- bzw. Nomineestrukturen ohne entsprechenden Formvorschriften die Tür geöffnet wird.

Die Vorteile einer Tokenemission mögen für viele Investoren nicht ohne Weiteres erkennbar sein, und häufig sind Immobilieninvestoren nicht bereit technische Infrastrukturen aufzubauen, die dem regelmäßig kleinen Kreis von Investoren eine Tokenemission ermöglichen. Für viele gewährleisten die regulierten Rahmenbedingungen des Spezialfonds auch ein Stück Sicherheit und – nicht zuletzt – ein Haftungssubjekt. Gleichwohl kann festgehalten werden, dass unter den geschilderten Voraussetzungen eine Tokenisierung von Immobiliengesellschaften (nicht Investmentvermögen) denkbar erscheint.

## C. Der Einfluss des eWpG auf Immobilientoken

Das geplante eWpG wird, so es denn zu keinen wesentlichen Änderungen mehr kommt, die Immobilien-Token-Emissionen in einigen Aspekten erleichtern.

Zunächst wird der Notwendigkeit zur Kautelarakrobatik bei Kryptowertpapieren ein Ende gesetzt. Durch die »Verdinglichung« von Token (sprich Code) gelingt es, elektronische Wertpapiere in den zivilrechtlichen und regulatorischen Rahmen des deutschen Wertpapierrechts einzubinden. Über die dogmatischen Grundlagen und Folgen dieses Kunstgriffs mögen sich die Gelehrten noch den Kopf zerbrechen; seine

5 A.a.O., Tz. 2.
6 BaFin, Thema Prospekte, Verbraucherschutz Qualifizierte Nachrangklauseln: Alles oder nichts – Risiken für Anleger im Grauen Kapitalmarkt, 01.08.2014.
7 ESMA, Leitlinien zu Schlüsselbegriffen der Richtlinie für Verwalter Alternativer Investmentfonds v. 13.08.2013, Berichtigte Fassung v. 30.01.2014 (ESMA/2013/611), ESMA/2013/611, S. 6.
8 BaFin-Stellungnahme v. 08.04.2016 zum Antrag des Business Angels Netzwerks Deutschland.
9 BaFin-Stellungnahme, a.a.O.

Vorteile liegen auf der Hand: Ein Sonderrecht für elektronische Wertpapiere wird vermieden.

Weiterer Vorzug des Gesetzentwurfs ist die Schaffung eines regulatorischen Rahmens für Dienstleistungen im Kontext von Tokenemissionen. Die Regeln für elektronische Wertpapierregister sind nach der Einführung der Erlaubnispflicht für Kryptoassetverwahrer ein wichtiger nächster Schritt, Tokenemisionen für institutionelle Investoren attraktiver zu machen. Bei aller Kritik aus der Kryptobranche, die gelegentlich immer noch glaubt, Verantwortlichkeiten (und damit Haftungsfragen) durch Algorithmisierung und Dezentralisierung vermeiden zu können: Die Schaffung von Haftungssubjekten wird der Entwicklung digitaler Wertpapiere schneller zum Durchbruch verhelfen als regulatorische Graubereiche dies vermögen.

Die Öffnung von offenen inländischen Sondervermögen für elektronische Wertpapiere ist grundsätzlich ebenfalls zu begrüßen. Allerdings hat der Gesetzgeber hier den letzten Schritt gescheut. Anteilsscheine dürften nicht als Kryptowertpapiere ausgegeben werden.[10] Der Regierungsentwurf erlaubt lediglich die Ausgabe elektronischer Anteilsscheine, d.h. deren Schaffung durch Registrierung in einem Wertpapierregister. Im Ergebnis entfällt also lediglich das Urkundenerfordernis. Das mag die Digitalisierung der Branche ein wenig fördern, ein großer Wurf ist es nicht. Jedenfalls hält der Regierungsentwurf eines seiner zentralen Versprechen, nämlich »technologieneutral« zu sein, nicht.[11] Im Gegenteil, die Befürchtung ist gerechtfertigt, dass ein Wechsel zu Kryptoanteilsscheinen, wenn er denn erlaubt werden sollte, zu spät kommt. Einmal eingeführt, dürften sich elektronische Anteilsscheine als zu langlebig erweisen, sofern die Vorteile von Kryptoanteilsscheinen sich nicht als deutlich größer und nachhaltiger erweisen sollten.

## D. Zusammenfassung

Der Gesetzentwurf zur Einführung elektronischer Wertpapiere in seiner aktuellen Fassung wird die Entwicklung elektronischer Wertpapiere fördern. Für Immobilienanlagen sind die Vorteile allerdings überschaubar. Emissionen außerhalb des Anwendungsbereichs des KAGB mit seinen strikten Formvorschriften sind nur in sehr eingeschränktem Maße zulässig. Genussrechte mit qualifiziertem Nachrang oder eigeninitiierte und selbstgemanagte Beteiligungen sind für professionelle Investoren wenig attraktiv. Blockchainbasierte Immobilien-Token werden ihr Nischendasein voraussichtlich noch eine Weile weiterführen müssen. Das Reich der regulierten und damit für einen Großteil der professionellen Investoren attraktiveren Anlageinstrumente bleibt ihnen verschlossen.

Für Sondervermögen hat der Gesetzgeber sich zu der – längst überfälligen – Öffnung für elektronische Wertpapiere mit Ausnahme von Kryptowertpapieren entschieden. Immerhin, möchte man sagen, aber zugleich zu wenig. Warum man die Wahl zwischen Zentralregisterwertpapieren und Kryptowertpapieren nicht den Anbietern überlassen hat, wäre eine interessante Frage. Ausnahmsweise scheint die Antwort nicht bei der Branchenlobby zu finden, die durchaus Anwendungsgebiete auch für blockchainbasierte Emissionen sieht.[12] So bleibt am Ende eines ambitionierten Unterfangens, der einen Aufbruch des Wertpapierwesens zu signalisieren schien, ein fader Beigeschmack.

10 Vgl. ausdrücklich Begründung Regierungsentwurf zu Art. 10 Nr. 2.
11 Regierungsentwurf, B. Lösung, S. 1.
12 Vergleiche die Stellungnahme des BVI zum Referententwurf zur Einführung elektronischer Wertpapiere vom 14.09.20202, S. 3, https://www.bvi.de/fileadmin/user_upload/200914_BVI_Stellungnahme_eWpG.pdf.

# Digital HR

## Beratung

# Der Mensch – Das vergessene Risiko für die Informations- und Datensicherheit

Sascha Kuhrau, Simmelsdorf*

**Betrachtet man die aktuelle Berichterstattung in den Medien, könnte man meinen, Datenpannen und (IT-)Sicherheitsvorfälle scheinen hauptsächlich das Ergebnis erfolgreichen Hackings und technischer Unzulänglichkeiten zu sein. Der vorliegende Aufsatz zeigt auf, dass – entgegen der Intuition – das größte Risiko in menschlichem Versagen liegt, und formuliert Handlungsempfehlungen, wie Unternehmen dieses Risiko minimieren können.**

## I. Aktuelle Sicherheitsvorfälle

Alleine in den letzten Monaten wurden zahlreiche Sicherheitsvorfälle in den Medien bekannt:

– In Finnland haben Hacker psychotherapeutische Krankenakten in großem Umfang entwendet.[1]
– Die Software AG wurde von Hackern angegriffen und Daten wurden von Servern, aber auch von Mitarbeiter-Geräten abgezogen. Selbst nach mehreren Tagen war das Problem noch nicht gelöst.[2]

* Der Autor ist zertifizierter Informationssicherheitsbeauftragter (OHT Regensburg), externe Datenschutzbeauftragter, Dozent an der Bayrischen Verwaltungsschule (BVS) und Gründer der a.s.k. Datenschutz mit Sitz im Nürnberger Land.

1 Ärzteblatt, Vertrauliche Psychotherapiedaten in Finnland gehackt, Artikel v. 27.10.2020, https://www.aerzteblatt.de/nachrichten/117742/Vertrauliche-Psychotherapiedaten-in-Finnland-gehackt [07.12.2020].
2 Hacker greifen Daten bei Darmstädter Software AG ab, Handelsblatt v. 08.10.2020, https://www.handelsblatt.com/technik/it-internet/sap-konkurrent-hacker-greifen-daten-bei-darmstaedter-software-ag-ab/26258192.html [07.12.2020].

– Die Webseite des Robert-Koch-Instituts (RKI) war Opfer eines Angriffs und für mehrere Stunden offline: gerade in der aktuellen Pandemie-Situation als häufig genutzte Informationsquelle durchaus eine brisante Angelegenheit.[3]
– Im Zusammenhang mit Corona stellt das Bundesamt für Sicherheit in der Informationstechnik (kurz BSI) in seinem aktuellen Lagebericht[4] vermehrt Angriffe auf medizinische Einrichtungen zumeist mit Verschlüsselungstrojanern fest. Hier besteht sogar Gefahr für Leib und Leben.
– Selbst das heimelige Home-Office steht im Fokus der Angreifer. So haben viele Organisationen im Frühjahr recht kurzfristig technische Lösungen für das Arbeiten von zu Hause geschaffen. In der Kürze der Zeit stand nicht unbedingt immer die Absicherung der technischen Infrastruktur im Vordergrund, so das BSI.[5] Es musste – nachvollziehbar –- schnell gehen und funktionieren.

Die Auswirkungen erfolgreicher Angriffe sind teuer, und das in vielerlei Hinsicht. Je nach Angriffsszenario und verwendetem Schadcode kann die komplette IT-Landschaft (Server und Endgeräte) befallen und zerstört sein. Ein Austausch – teilweise oder komplett – ist dann unvermeidlich. Sind kritische Geschäftsprozesse betroffen, drohen Umsatzausfälle bis hin zum Totalverlust der Organisation. Aber auch Lösegeldforderungen in Millionenhöhe sind nicht unüblich, um den Zugriff auf wichtige verschlüsselte Informationen der Organisation wiederzuerlangen. Ungemach droht aber auch von Seiten des Datenschutzes. Datenpannen mit personenbezogenen Daten können mit empfindlichen Bußgeldern belegt werden. Die Höhe eines Bußgelds orientiert sich an den Kriterien aus Art. 83 Abs. 1 DSGVO, darunter Art, Schwere und Dauer des Verstoßes, aber bspw. auch, wie mit der Aufsichtsbehörde zusammengearbeitet wurde. Ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, spielt für die Bemessung des Bußgelds ebenso eine Rolle wie die Frage, ob der Verstoß auf einem Organisationsverschulden oder auf einem unvorhersehbaren Fehlverhalten einer einzelnen Person beruht. Neben dem Bußgeld droht je nach öffentlicher Aufmerksamkeit mit ziemlicher Wahrscheinlichkeit noch ein nicht zu unterschätzender Image-Schaden.

Im Fokus sollte daher stehen, die Eintrittswahrscheinlichkeit solcher Risiken zu minimieren und das Schadensausmaß so gut wie möglich zu begrenzen. Sowohl in der Informationssicherheit[6] als auch im Datenschutz begegnet man diesen Risiken mit geeigneten technischen und organisatorischen Maßnahmen (kurz TOM).[7] Technische Schutzmaßnahmen[8] sind bspw. Firewall, Virenschutz oder auch Verschlüsselungslösungen. Zu den organisatorischen Schutzmaßnahmen[9] gehören das manuelle Sperren des PC, der Umgang mit Datei-Anhängen, aber auch das sichere Entsorgen von Papierdatenträgern.

Vor dem hier skizzierten Hintergrund werden Angriffe auf die IT-Sicherheit und damit verbundene Lösungen zuvörderst im Bereich der IT und in technischen Lösungen verortet. Es stellt sich allerdings die Frage, ob technische Fehler tatsächlich die (allein) maßgebliche Ursache darstellen. Daher gilt es, statt vorschnell konkrete Gegenmaßnahmen zu ergreifen, zunächst die Risikoursachen zu ermitteln.

## II. Die Data Breaches zeigen: Das größte Risiko ist der Mensch

Gem. Art. 33 Abs. 1 Satz 1 DSGVO sind Unternehmen seit Mai 2018 verpflichtet, die Verletzung des Schutzes personenbezogener Daten (auch Datenpannen, Data Breaches genannt) wie die eben dargestellten der Aufsichtsbehörde zu melden. Ein Nicht-Meldung ist ein Verstoß gegen die DSGVO, der wiederum mit Geldbußen sanktioniert werden kann. Die DSGVO hat den Rahmen deutlich angehoben. Verstöße gegen Art. 33 DSGVO werden gem. Art. 83 Abs. 4 Buchst. a) DSGVO mit Geldbußen von bis zu 10 Mio. € bzw. bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs sanktioniert, je nachdem, welcher der Beträge höher ist.

Seither nehmen die Meldungen nach Bekunden der Aufsichtsbehörden in hohem Maße zu. So vermeldete der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI BW) bereits im Juli 2019 eine Verzehnfachung der gemeldeten Datenpannen gegenüber Mai 2018.[10] Doch im Vergleich zur quantitativen Zunahme ist die Art der gemeldeten Datenpannen im vorliegenden Kontext viel interessanter. Dazu hat der LfDI BW in der zuvor genannten Pressemitteilung eine Übersicht der bis dato häufigsten Datenpannen vorgelegt, wobei die Reihenfolge der Häufigkeit entspricht:

1. Postfehlversand
2. Hackingangriffe/Malware/Trojaner
3. E-Mail-Fehlversand
4. Diebstahl eines Datenträgers
5. Versendung einer E-Mail mit offenem Adressverteiler
6. Verlust eines Datenträgers
7. Fax-Fehlversand.

Auf den ersten Blick scheint die Liste ein anderes Bild zu zeichnen. So stehen Hacking-Angriffe zwar auf Platz 2 des LfDI BW-Rankings. In Summe sind die gemeldeten und durch Menschen verursachten Datenpannen der Plätze 1 sowie 3 bis 7 jedoch häufiger vorgekommen. Das bedeutet nun nicht, dass Organisationen nicht versuchen sollten, Sicherheitsvorfälle rein technischer Natur mindestens so akribisch zu vermeiden wie durch Menschen ausgelöste Datenpannen. Festzuhalten bleibt aber, dass eine reine Fixierung auf technische Sicherheit als Vorsorge zu kurz greift.

3 DDoS-Angriff legte Website des Robert-Koch-Instituts lahm, Heise v. 28.10.2020, https://www.heise.de/news/DDoS-Angriff-legte-Website-des-Robert-Koch-Instituts-lahm-4941400.html [07.12.2020].
4 BSI, Die Lage der IT-Sicherheit in Deutschland, 2020, https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html [07.12.2020].
5 BSI, Die Lage der IT-Sicherheit in Deutschland, 2020, S. 33.
6 BSI, IT-Grundschutz Glossar, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html [07.12.2020].
7 Datenschutz Praxis, Technisch-organisatorische Maßnahmen: Das ändert sich, 29.05.2019, https://www.datenschutz-praxis.de/fachartikel/technisch-organisatorische-massnahmen-das-aendert-sich/ [07.12.2020].
8 Wikipedia, Technische und organisatorische Maßnahmen, 31.05.2020, https://de.wikipedia.org/wiki/Technische_und_organisatorische_Maßnahmen [07.12.2020].
9 Dr. Datenschutz, Technische und organisatorische Maßnahmen, 06.02.2019, https://www.dr-datenschutz.de/technische-und-organisatorische-massnahmen-nach-dem-zawas-prinzip/ [07.12.2020].
10 LfDI BW, Datenschutzverletzungen bereiten zunehmend Sorge, 30.07.2019, https://www.baden-wuerttemberg.datenschutz.de/datenschutzverletzungen-bereiten-zunehmend-sorge/ [07.12.2020].

Dieser Befund wird auch durch die Tätigkeitsberichte weiterer Landesdatenschutzaufsichten[11] untermauert, denen zu entnehmen ist, dass quantitativ die organisatorischen, also durch Menschen ausgelösten Datenpannen die häufigsten waren. Das bedeutet, dass der allgemeine Eindruck, technische Fehler seien der maßgebliche Grund für Sicherheitsvorfälle bzw. Datenpannen und die damit für Unternehmen verbundenen Konsequenzen, täuscht bzw. falsch ist. Die Mehrheit der Vorfälle ereignet sich aufgrund organisatorischer Fehler. Das bedeutet konkret, dass Menschen Fehler gemacht bzw. fehleranfällige Prozesse geschaffen haben.

## III. Was genau heißt Risikofaktor Mensch?

Risiken verwirklichen sich zuweilen schneller als verantwortliche Unternehmen glauben mögen. Das nachfolgende Beispiel passiert täglich: Mitarbeiter nutzen unverschlüsselte oder gar private USB-Sticks für den Datentransfer. Gehen diese mitsamt den darauf gespeicherten Daten verloren, ist die zu meldende Datenpanne in greifbarer Nähe. Bei Einsatz an externen, möglicherweise auch nicht ausreichend abgesicherten Geräten besteht zusätzlich das Risiko, bei einer späteren Nutzung Schadcode von außen in das interne Netz einzubringen.[12] Dadurch können etwa am eigenen Arbeitsplatz zahlreiche zentrale Schutzmaßnahmen wie Firewall oder der Virenschutz des E-Mail-Postfachs ausgehebelt werden und dann den ihnen ursprünglich zugedachten Schutzzweck nicht erfüllen.[13]

Warum handeln Mitarbeiter so leichtfertig? Das kann verschiedene Ursachen haben. Möglicherweise ist der Umgang mit USB-Sticks in der Organisation gar nicht geregelt. Woher sollen Mitarbeiter dann wissen, wie sie sich richtig zu verhalten haben und Sicherheitsrisiken vermeiden? Vielleicht gibt es zwar eine interne Vorgabe, diese wurde bzw. wird aber nie in angemessener Weise den Mitarbeitern bekannt gemacht. Die bloße Existenz einer Regelung auf dem Papier oder eine Veröffentlichung im Intranet alleine schaffen noch keine Sicherheit. Von daher sind Verantwortlichkeiten sowohl für das Erstellen und die Pflege solcher Anweisungen zu schaffen, als auch für die Schulung und Sensibilisierung der Mitarbeiter im Hinblick auf diese Anweisungen. Aber auch kontinuierliche Überlastung oder Überforderung von Mitarbeitern kann zu Sicherheitsvorfällen führen. Schnell schleicht sich Unachtsamkeit ein. Unsicher gestaltete Arbeitsplätze (wie Einsehbarkeit, fehlende Verschlussmöglichkeit für vertrauliche Unterlagen) oder Arbeitsprozesse (wie ein zentraler Posteingang mit unbeaufsichtigten und frei zugänglichen Ablagekörben) steigern das Risiko für Sicherheitsvorfälle weiter.[14]

Selbst bei technischen Datenpannen ist nicht immer die Technik am Eintritt des Risikos alleine ursächlich. So werden etwa Verschlüsselungstrojaner nach wie vor noch manuell mittels Mausklick am Arbeitsplatz durch Menschen gestartet. Mit Blick auf die Erhöhung technischer Risiken durch menschliches Verhalten kommt bspw. die von Solarwinds durchgeführte Studie[15] (durchgeführt durch IDC) aus März 2019 zu interessanten Ergebnissen:

- 62 % der Befragten nennen Fehler durch interne Benutzer als die größte Cybersicherheitsbedrohung, die das Unternehmen gefährdet und Sicherheitsvorfälle zur Folge hat.
- Mehr als 50 % der Befragten gaben an, dass nicht privilegierte Benutzer, sondern reguläre Angestellte das größte Risiko für internen Missbrauch oder Fehlanwendung darstellen. An nächster Stelle wurden externe Dienstleister mit 41 % und IT-Administratoren mit 31 % genannt, die aufgrund ihrer Aufgaben mit teilweise unbeschränkten Rechten ihrer Tätigkeit nachgehen.

Wenig überraschend ist, dass auch die aktuellere Studie von Drivelock »IT-Sicherheit im Mittelstand«[16] in 2020 im Kontext von Cyberattacken zu einem ähnlichen Befund kommt:

- »Das größte Risiko für die IT-Sicherheit ist der Faktor Mensch«
- In durchschnittlich 46 % der Fälle hat die Unachtsamkeit der Mitarbeiter den Sicherheitsvorfall ausgelöst, etwa durch schwache Passwörter, unbedachtes Öffnen von E-Mail-Anhängen oder die Nutzung öffentlicher Internetzugänge. Bei Großunternehmen verursachten gar in 68 % der Fälle die eigenen Mitarbeiter den Sicherheitsvorfall.

Über 200 Unternehmen mit maximal 999 Mitarbeitern aus verschiedenen Branchen wurden für die Studie befragt. Im Ergebnis hält die überwiegende Mehrheit (65 % der Befragten) mehr auf die Mitarbeiter ausgerichtete Maßnahmen für erforderlich, um das Sicherheitsbewusstsein der Belegschaft zu verbessern.

Einer KPMG Studie aus 08/2020[17] zum selben Thema zufolge sehen die befragten Unternehmen »Unachtsamkeit oder Nachlässigkeit mit 51 Prozent als den größten Faktor hinsichtlich wirtschaftskrimineller Vorfälle an. Ähnlich relevant seien fehlende oder mangelhafte Kontrollen (50 Prozent) sowie ein mangelndes Unrechtsbewusstsein (49 Prozent).« Klares Fazit war: »Darum sei es wichtig, durch gezielte, vorbeugende Maßnahmen wie Schulungen zur Sensibilisierung oder die klare Definition von Verhaltensgrundsätzen die Risiken zu minimieren.«

11 Sächsischer Datenschutzbeauftragter, Tätigkeitsbericht 01.04.2017–31.12.2018, 2019, https://www.saechsdsb.de/images/stories/sdb_inhalt/oeb/taetigkeitsberichte/Ttigkeitsbericht_2017_2018.pdf [07.12.2020].

12 BSI, Baustein SYS 4.5 Wechseldatenträger – Verbreitung von Schadprogrammen, 2020, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_4_5_Wechseldatentraeger.html?nn=10137184#doc10095886bodyText11 [07.12.2020].

13 Beide Technologien schützen den Datenfluss in ein Netzwerk am obersten elektronischen Zugangspunkt und verhindern z.B. die Verteilung von Schadcode an ein Endgerät. Wird ein mit Schadcode infizierter Speicherstick an ein Endgerät direkt angeschlossen, durchläuft der Datenfluss diese zentralen Schutzmöglichkeiten nicht. Bei unzureichender Absicherung direkt auf dem Endgerät z.B. mittels Virenscanner kann der somit eingebrachte Schadcode direkt aktiv werden und sich möglicherweise auch im internen Netzwerk an den zentralen Schutzmaßnahmen vorbei verbreiten. S.a. BSI, Der Virus kommt zu Fuß, 11.07.2018, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_095c.pdf?__blob=publicationFile&v=5 [07.12.2020].

14 BSI, Baustein INF.7 Büroarbeitsplatz – Beeinträchtigungen durch ungünstige Arbeitsbedingungen, 2020, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_7_Büroarbeitsplatz.html?nn=10137152#doc10095778bodyText7 [07.12.2020].

15 IDC-Whitepapers, Affordable Tools and Shared Responsibilities Define Midmarket IT Security Trends, 2019, https://www.solarwindsmsp.com/sites/solarwindsmsp/files/resources/SW-Core-MSP_WP_IDC-Cybersecurity-Study_2019.pdf [07.12.2020].

16 Drivelock, IT-Sicherheit im Mittelstand, 2019, https://www.drivelock.de/it-sicherheit-im-mittelstand?utm_campaign=2019%20Studie%20IT%20Sicherheit%20im%20Mittelstand&utm_source=HBI [07.12.2020].

17 Hacker-Angriffe auf jede dritte Firma, Tagesschau v. 17.08.2020, https://www.tagesschau.de/wirtschaft/hackerangriffe-wirtschaft-unternehmen-corona-101.html [07.12.2020].

## IV. Wie ist vorzugehen, wenn der Faktor Mensch als Risiko in der Informations- und Datensicherheit identifiziert ist?

Bekannte Informationssicherheitsmanagementsysteme wie die ISO 27001, der BSI IT-Grundschutz[18] oder auch ISIS12 nehmen sich auch dieses Themas an. Die Sicherheitskonzepte haben eins gemein: Sie wissen um den Risikofaktor Mensch und bieten mehr oder weniger umfangreich geeignete Empfehlungen zu technischen und organisatorischen Maßnahmen an, um diesem Risiko so gut wie möglich und angemessen Herr zu werden.

Im Baustein ORP.3 (Organisation und Personal) weist das BSI bspw. sehr deutlich auf die in den Studien zuvor erwähnten Problematiken hin:

- Unzureichende Kenntnis über Regelungen
- Unzureichende Sensibilisierung für Informationssicherheit
- Unwirksame Aktivitäten zur Sensibilisierung oder Schulung
- Unzureichende Schulung der Mitarbeiter zu Sicherheitsfunktionen
- Nicht erkannte Sicherheitsvorfälle
- Nichtbeachtung von Sicherheitsmaßnahmen
- Sorglosigkeit im Umgang mit Informationssicherheit
- Fehlende Akzeptanz von Informationssicherheitsvorgaben
- Social Engineering (Hacking des digitalen und menschlichen Betriebssystems)

Glücklicherweise bietet das BSI mit dem »IT-Grundschutz« in dessen Bausteinen zugleich konkrete und umfassende organisatorische Handlungsempfehlungen an, wie diesen genannten Risiken menschlichen Fehlverhaltens begegnet werden kann.

Aber auch in anderen Bausteinen finden sich Hinweise auf organisatorische Risiken, denen mittels der Handlungsempfehlungen Einhalt geboten bzw. zumindest das Risiko beschränkt werden kann. Hier werden u.a. Punkte behandelt wie der Einsteuerungsprozess neuer Mitarbeiter, die Rechtevergabe, der Umgang mit mobilen Datenträgern wie USB-Sticks, aber auch die Bedeutung der Zurverfügungstellung sicherer Betriebsmittel oder der sicheren Arbeitsplatzgestaltung (Einsehbarkeit, verschließbare Schränke etc.) hervorgehoben.

Gerade in der aktuellen Pandemie-Situation stehen Organisationen vor der Herausforderung, Mitarbeiter vermehrt im Home-Office einzusetzen. Nicht immer steht hierfür ausreichend organisationseigene Hardware zur Verfügung. In diesem Fall wird gerne auf die Nutzung privater Geräte der Mitarbeiter für geschäftliche Zwecke zurückgegriffen (»Bring your own device« oder kurz BYOD). Dies stellt je nach Umsetzung und Tätigkeit hohe Anforderungen an die technische Absicherung, sofern über die private Hardware auf das organisationsinterne Netzwerk zugegriffen werden muss. Aber auch die »Spielregeln« für die Nutzung und Handhabung müssen mit den Mitarbeitern klar geregelt sein, um Sicherheitsvorfälle möglichst zu vermeiden.[19] Dies gilt im Übrigen nicht nur im Falle von BYOD, sondern auch für die damit zusammenhängenden Aspekte Heimarbeitsplatz[20] bzw. Mobiles Arbeiten.[21]

## V. Prozesse und regelmäßige Sensibilisierungen liegen in der Verantwortung des Personalbereichs

Doch Technik allein (»die IT«) wird diese Probleme und Risiken nicht bewältigen können. Hier ist der nicht-technische Bereich einer Organisation stark gefordert. Bereits im Einstellungsprozess sollten Mitarbeiter mit den grundlegenden Sicherheits- und Datenschutzanforderungen vertraut gemacht werden. Dazu gehört mehr als das Aushändigen der einschlägigen Anweisungen und Richtlinien, die selbstverständlich auf dem aktuellen Stand und zielgruppengerecht formuliert (»Bitte denken Sie daran, Ihren PC beim Verlassen des Arbeitsplatzes zu sperren. Dies geht am einfachsten mittels der Tastenkombination Win+L«) sein müssen, nämlich das persönliche Gespräch samt Erläuterungen und Hilfestellungen. Aber auch erste Grundlagenschulungen leisten gute Dienste. Diese können durchaus auch virtuell in Form von Webinaren stattfinden. Dies als festen Prozess zu etablieren, ist Aufgabe des Personalbereichs. Hier wäre üblicherweise auch die Sicherstellung regelmäßiger Sensibilisierungen und Schulungen für bestehende Mitarbeiter zu verorten, selbstverständlich in enger Abstimmung mit den Ansprechpartnern für Datenschutz und Informationssicherheit. Empfehlenswert ist die gemeinsame Entwicklung eines Schulungskonzepts, in dem Intervalle, Methoden und Inhalte für die nächsten zwölf bis 24 Monate festgelegt werden.[22] Dabei kann und darf man sich durchaus von klassischen Schulungskonzepten lösen. Ein auffälliges Plakat in den Sanitär-Räumen mit der Aufschrift »Na, PC gesperrt?« kann nachhaltiger beeindrucken als eine vierstündige Präsenzveranstaltung zum Thema »Sicherheit am Arbeitsplatz«.[23]

## VI. Handlungsempfehlung

Die Vermeidung von Sicherheitsvorfällen und Datenpannen setzt eine kontinuierliche Beschäftigung mit den Themen Informationssicherheit und Datenschutz sowie die Weiterentwicklung und Verbesserung von deren Umsetzung in der Organisation voraus. Von daher empfiehlt es sich, systematisch vorzugehen. Wer sich nicht gleich mit den »big playern« der Informationssicherheit wie der ISO27001 oder dem BSI IT-Grundschutz auseinandersetzen möchte, kann auf kleinere Standards wie bspw. ISIS12 (Informationssicherheit in 12 Schritten) des Sicherheitsclusters mit Sitz in Regensburg ausweichen.[24] Unabhängig davon gilt es

18 BSI, IT-Grundschutz Kompendium, 2020, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html [07.12.2020].

19 BSI, Consumerisation und BYOD, 2019, S. 106 ff., https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/Diplomarbeiten/Berrendorf_BYOD.pdf?__blob=publicationFile&v=2 [14.12.2020].

20 BSI, INF.8 Häuslicher Arbeitsplatz, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_8_Häuslicher_Arbeitsplatz.html [14.12.2020].

21 BSI, INF.9 Mobiler Arbeitsplatz, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_9_Mobiler_Arbeitsplatz.html [14.12.2020].

22 BSI, Baustein ORP.3 Sensibilisierung und Schulung – Standard-Anforderungen, 2020, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_3_Sensibilisierung_und_Schulung.html?nn=10137172#doc10095888bodyText17 [07.12.2020].

23 IT-Administrator, Gefahren-Sensibilisierung von Mitarbeitern, https://www.it-administrator.de/themen/sicherheit/grundlagen/166738.html [07.12.2020].

24 Sicherheitscluster e.V., Informationssicherheit in 12 Schritten (ISIS12), https://www.isis12.de [07.12.2020].

- Verantwortlichkeiten und Zuständigkeiten festzulegen,
- Richtlinien, Anweisungen und Betriebsvereinbarungen aktuell zu halten bzw. fehlende zu ergänzen,
- Mitarbeiter frühzeitig für das Thema Sicherheit zu sensibilisieren,
- bestehende Prozesse auf mögliche Schwachstellen abzuklopfen und diese zu beseitigen,
- ein sicheres Arbeitsumfeld für die Mitarbeiter zu schaffen (z.B. Schredder, Nicht-Einsehbarkeit der Arbeitsplätze/ Bildschirme etc.),
- bestehende und neue technische und organisatorische Maßnahmen regelmäßig auf deren Wirksamkeit hin zu prüfen (Erfolgskontrolle) und
- für das Thema Sicherheit ausreichend Zeit und finanzielle Mittel einzuplanen.

Damit wäre jedenfalls ein guter Anfang für ein gutes Ende geschaffen.

## Beratung

# Organisatorische Maßnahmen i.S.v. Art. 32 DSGVO – Das unterschätzte »Must-Have« eines jeden Unternehmens zur datenschutzrechtlichen Haftungsminimierung

Rechtsanwältin Nina Diercks,M.Litt. (University of Aberdeen), Hamburg*

**Wie Sascha Kuhrau in seinem Beitrag »Der Mensch – Das vergessene Risiko für die Informations- und Datensicherheit« (in diesem Heft) plastisch erläutert, sind die Beschäftigten eines jeden Unternehmens die größte Schwachstelle im Hinblick auf die IT- und Datensicherheit der Organisation. Diese Risiken können durch die im vorgenannten Aufsatz skizzierten Maßnahmen erheblich gesenkt werden. Eine hundertprozentige Sicherheit schaffen jedoch auch die besten Maßnahmen nicht. Daraus abzuleiten, dass auf organisatorische Maßnahmen wie Schulungen, IT-Richtlinien und/ oder Betriebsvereinbarungen keine oder nur entsprechend geringe Ressourcen verwendet werden sollten, wäre indes ein gravierender Fehlschluss. Nachfolgend wird gezeigt, warum eine solche Haltung nicht nur die Verwirklichung von IT-Sicherheitsrisiken befördert, sondern auch datenschutzrechtliche Risiken und damit verbunden eine mögliche Haftung des verantwortlichen Unternehmens nach der DSGVO begründet.**

### I. Pflicht zur Ergreifung von technischen und organisatorischen Maßnahmen nach Art. 24, 32 DSGVO

Nach Art. 24 Abs. 1 Satz 1 DSGVO muss der Verantwortliche, d.h. das datenverarbeitende Unternehmen,[1] »geeignete technische und organisatorische Maßnahmen um[setzen], um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.« Art. 24 DSGVO konkretisiert damit die Umsetzung der Grundsätze des Art. 5 DSGVO für den Verantwortlichen.

Art. 32 DSGVO spezifiziert diese Verpflichtung noch weiter im Hinblick auf die Einhaltung der Datensicherheit. Denn nach Art. 32 Abs. 1, Halbs. 1 DSGVO ist der Verantwortliche, d.h. das datenverarbeitende Unternehmen, verpflichtet, »[u]nter 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 […] geeignete technische und organisatorische Maßnahmen [zu treffen], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten«.

Diese Vorschrift verpflichtet also den Verantwortlichen unmittelbar zur Gewährleistung der Sicherheit der Datenverarbeitung mittels technischer und organisatorischer Maßnahmen.[2] Technische und organisatorische Maßnahmen sind zunächst alle notwendigen sowie geeigneten Maßnahmen, um die Beachtung des Datenschutzes und der Datensicherheit bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten und den dazu betriebenen Verfahren sicherzustellen.[3]

Während sich technische Maßnahmen regelmäßig auf alle Hard-, Software- und Netzwerkkomponenten beziehen, etwa Maßnahmen der Zugriffskontrolle wie technische Berechtigungskonzepte und Passwortsicherungen,[4] beziehen sich die organisatorischen Maßnahmen insbesondere auf den Ablauf, die Umstände und die durchführenden Personen, wie etwa die Verpflichtungen zur Befolgung von technischen Prozessen, die Protokollierungen von Tätigkeiten oder Schulungen zur Sensibilisierung von Beschäftigen für datenschutzrechtliche und -technische Belange.[5]

Als ein Beispiel für eine technische wie auch eine organisatorische Maßnahme seien die Maßnahmen für sichere Passwörter bzw. die Sicherung der hinter diesen passwortgeschützten Accounts liegenden Daten genannt. Technisch können entsprechende Einstellungen vorgenommen werden, dass nur hinreichend sichere Passwörter (Mindestlänge, Buchstaben,

* Die Autorin ist seit 2010 als Rechtsanwältin tätig und führt die Anwaltskanzlei Diercks in Hamburg. Sie arbeitet bundesweit ausschließlich in den Bereichen des IT-| Medien-| Datenschutz- und des angrenzenden Arbeitsrechts.

1 Verantwortlicher i.S.v. Art. 4 Nr. 7 DSGVO.

2 Vgl. Kühling/Buchner/*Jandt*, DS-GVO/BDSG, 3. Aufl. 2020, DS-GVO Art. 32 Rn. 4.

3 BeckOK DatenschutzR/*Schmidt/Brink*, 34. Ed. 01.11.2019, DS-GVO Art. 24 Rn. 13.

4 Vgl. u.a. Kühling/Buchner/*Jandt* (s. Fn. 2), DS-GVO Art. 32 Rn. 5; Paal/Pauly/*Martini*, DS-GVO, 2. Aufl. 2018, Art. 24 Rn. 21; BeckOK DatenschutzR/*Schmidt/Brink* (s. Fn. 3), DS-GVO Art. 24 Rn. 11–21; Taeger/Gabel/*Lang*, DSGVO/BDSG, 3. Aufl. 2019, DSGVO Art. 24 Rn. 23.

5 Vgl. u.a. Kühling/Buchner/*Jandt* (s. Fn. 2), DS-GVO Art. 32 Rn. 5; Paal/Pauly/*Martini* (s. Fn. 4), Art. 24 Rn. 22; BeckOK DatenschutzR/*Schmidt/Brink* (s. Fn. 3), DS-GVO Art. 24 Rn. 11–21; Taeger/Gabel/*Lang* (s. Fn. 4), DS-GVO Art. 24 Rn. 23.

Zahlen, Sonderzeichen) vergeben werden können. Daneben muss jedoch auch sichergestellt werden, dass Beschäftigte nicht für alle Accounts im Rahmen ihrer beruflichen Tätigkeit dasselbe Passwort verwenden. Dies erfolgt durch eine Passwort-Richtlinie oder eine Klausel in einer IT-Richtlinie bzw. einer Betriebsvereinbarung, nach der die Beschäftigten verpflichtet werden, unterschiedliche Passwörter und zur Verwaltung der nicht selten weniger als 20 notwendigen Passwörter einen Passwortmanager sowie – soweit möglich – eine Zwei-Faktor-Authentifizierung zu verwenden. Regelmäßig entstehen so erst im Zusammenwirken von technischen und organisatorischen Maßnahmen i.S.v. Art. 24 und 32 DSGVO geeignete Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit, da sie erst zusammen für ein geeignetes Schutzniveau sorgen können. So hilft etwa die hinreichende Komplexität eines Passworts nur bedingt, wenn dieses Passwort für mehrere Accounts verwendet wird. Denn im Falle eines Accountbruchs durch Passwort-Erlangung wären so gleich alle weiteren Accounts in der dringenden Gefahr kompromittiert zu werden.[6]

Organisatorische Maßnahmen wie IT-Richtlinien und Betriebsvereinbarungen sind also schon deswegen notwendig, um der allgemeinen Nachweispflicht aus Art. 5 Abs. 2 DSGVO sowie der konkretisierten aus Art. 24 DSGVO nachkommen zu können.[7] Mit ihnen kann ein Verantwortlicher leichter nachweisen, dass organisatorische Maßnahmen – wie etwa die Verpflichtung zur Verwendung unterschiedlicher Passwörter und eines Passwortmanagers – im Unternehmen i.S.v. Art. 24 Abs. 1 Satz 1 und Art. 32 Abs. 1 DSGVO getroffen wurden.

Darüber hinaus begründet Art. 32 Abs. 4 DSGVO eine weitere Verpflichtung zur Erstellung von IT-Richtlinien bzw. Betriebsvereinbarungen für Arbeitgeber. Davon ausgehend, dass mit arbeitsteiligen Prozessen und damit mit jedem Beschäftigten, der über Zugriffsberechtigungen verfügt, ein weiteres Missbrauchs- und Fehlerrisiko einhergeht, verpflichtet Art. 32 Abs. 4 DSGVO den Verantwortlichen noch einmal gesondert »Schritte« zu unternehmen, »um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten«[8] – ergo organisatorische Maßnahmen zu ergreifen.

## II. Rechtsfolgen

Verstößt der Verantwortliche gegen die Verpflichtung aus Art. 24 und 32 DSGVO, organisatorische Maßnahmen zu ergreifen, und/oder kann er die Einhaltung nicht nachweisen, so können nach Art. 83 Abs. 4 Buchst. a) DSGVO Bußgelder in einer Höhe von bis zu 10 Mio. € bzw. bis zu 2 % des weltweiten Jahresumsatzes verhängt werden.

Ein solcher Verstoß eines verantwortlichen Unternehmens entsteht regelmäßig durch ein Verhalten eines Beschäftigten innerhalb des Unternehmens – und nicht durch einen natürlichen Organvertreter. Dieses Verhalten oder ein sonstiger Umstand bedingen den Datenschutzverstoß sowie den gegebenenfalls daraus entstandenen Schaden materieller oder immaterieller Art. Hat der Verantwortliche keine organisatorischen Maßnahmen wie vorstehend skizziert ergriffen, kann er im Zweifel nicht den Nachweis erbringen, dass er für den Umstand, der den Verstoß und den Schaden verursachte, aufgrund von organisatorischer Maßnahmen nicht verantwortlich ist. Der Verantwortliche kann sich aus einem Organisationsverschulden nicht exkulpieren. Damit kann das verantwortliche Unternehmen sowohl nach Art. 82 DSGVO für etwaige Schäden haften als auch wegen dieser Verstöße mit einem (weiteren) Bußgeld nach Art. 84 Abs. 4 Buchst. a) DSGVO belegt werden.[9]

## III. Haftung für Datenschutzverstöße durch das verantwortliche Unternehmen

Auch wenn das Thema »Haftung des verantwortlichen Unternehmens« in diesem Rahmen nicht hinreichend behandelt werden kann, sollen doch die Grundzüge der Problematik kurz beleuchtet werden, um darauf aufbauend die Relevanz von organisatorischen Maßnahmen wie IT-Richtlinien und Betriebsvereinbarungen zur Risikominimierung im Hinblick auf die Haftung für Bußgelder und Schadensersatz zu erörtern.

Die DSGVO trifft keine Regelungen dazu, inwieweit ein Unternehmen als Verantwortlicher im Sinne der DSGVO für Fehlverhalten von natürlichen Personen wie etwa Beschäftigten haftet. Es gelten hier die nationalen Regelungen. Nach § 41 BDSG findet das Ordnungswidrigkeitengesetz (OWiG) Anwendung. Das OWiG kennt wiederum zwei Fälle, in denen ein Unternehmen strafrechtlich sanktioniert werden kann. Nach § 30 OWiG kann (sehr verkürzt dargestellt) eine Geldbuße gegen ein Unternehmen verhängt werden, wenn ein Mitglied des vertretungsberechtigten Organs oder Mitarbeiter in leitender Position eine Straftat oder Ordnungswidrigkeit begangen hat und hierdurch die Pflichten, die das Unternehmen betreffen, verletzt worden sind. Gerade im Bereich des Datenschutzes sind es jedoch wie ausgeführt weniger die Organe oder Mitarbeiter in leitender Funktion, die unmittelbar Straftaten bzw. Ordnungswidrigkeiten i.S.d. § 30 OWiG begehen.

Nahezu klassisch ist das folgende Beispiel: Ein System-Administrator verwendet stets für alle seine Unternehmens-Accounts und -Zugänge das Passwort »Unternehmen2020« und verschickte dieses Passwort einmal in einer unverschlüsselten E-Mail an einen externen Dienstleister. Eines Tages dringen Skript-Kiddies[10] in die Datensysteme ein, löschen einige personenbezogene Daten, transferieren andere und stellen über die Firmenserver Kreditkartendaten von Kunden frei zugänglich ins Netz.

Hier ist durch ein Fehlverhalten eines einzelnen Beschäftigten ein massiver Data Breach des Unternehmens entstanden, welcher zu Schadensersatz von Betroffenen nach Art. 82 DSGVO, aber auch zu Bußgeldern nach Art. 84 DSGVO führen kann. Für dieses Fehlverhalten kann das Unternehmen im Rahmen von § 130 OWiG haften. Voraussetzung ist – wieder verkürzt dargestellt –, dass der Inhaber oder ein Organ des Unternehmens vorsätzlich oder fahrlässig eine

6 Zur Wesentlichkeit der Eignung der Maßnahmen Taeger/Gabel/*Lang* (s. Fn. 4), DS-GVO Art. 24 Rn. 24.
7 Vgl. BeckOK DatenschutzR/*Schmidt/Brink* (s. Fn. 3), DS-GVO Art. 24 Rn. 13.
8 Vgl. Paal/Pauly/*Martini* (s. Fn. 4), Art. 32 Rn. 64; Gola/*Piltz*, DS-GVO, 2. Aufl. 2018, Art. 32 Rn. 50.
9 So auch Paal/Pauly/*Martini* (s. Fn. 4), Art. 32 Rn. 72.
10 Jugendliche und junge Erwachsene, die aus Spaß an der Freude probieren, in fremde Systeme einzudringen.

Aufsichtsmaßnahme unterlassen hat, die erforderlich gewesen wäre, um Zuwiderhandlungen gegen Bußgeldnormen zu verhindern, und wenn hierdurch Pflichten des Unternehmens verletzt worden sind. Im genannten Beispielsfall sind offensichtlich Pflichten aus Art. 32 DSGVO verletzt worden. Die Verwendung eines derart einfachen Passworts in allen Accounts stellt keine geeignete Maßnahme zur Datensicherheit dar. Die Frage ist folglich nur noch, ob eine Aufsichtsmaßnahme unterlassen wurde, also ob ein Organisationsverschulden vorliegt. Wie dargelegt besteht die Verpflichtung nach Art. 24 und Art. 32 DSGVO, entsprechende geeignete organisatorische Maßnahmen zu ergreifen, und diese auch nachweisen zu können.[11] Der Nachweis scheitert jedenfalls, wenn der Verantwortliche schon keinerlei rechtsverbindliche organisatorische Maßnahmen ergriffen hat.[12]

Es ist in diesem Zusammenhang festzuhalten, dass die Wirkung der Nachweispflicht i.S.v. Art. 5 Abs. 2 und Art. 24 DSGVO im Rahmen des Straf- bzw. Ordnungswidrigkeitsverfahren strittig ist. Nach einer Auffassung stellt die Nachweispflicht nur eine materiell-rechtliche Verpflichtung dar, die nicht dazu führen dürfe und könne, dass faktisch die Befugnisse der Behörden nach Art. 58 DSGVO und damit die Position der Behörden in strafrechtlichen Verfahren verbessert würde. Vielmehr diene die Nachweispflicht nur dem Schutz der Betroffenen.[13] Nach anderer – vorzugswürdiger – Auffassung ist die Nachweispflicht verfahrensrechtlich bedeutsam. Art. 58 DSGVO gewährt den Behörden entsprechende Befugnisse zur Erfüllung ihrer Aufgaben, darunter nach Art. 57 Abs. 1 DSGVO die Überwachung und Durchsetzung der DSGVO. Hierzu gehören auch anlasslose und präventive Untersuchungen von Amts wegen.[14] In diesem Zusammenhang kann die Behörde nach Art. 58 Abs. 1 Buchst. a) DSGVO[15] den Verantwortlichen anweisen, alle Informationen bereitzustellen, die zur Erfüllung der Aufgabe erforderlich sind. Die Anweisung zur Bereitstellung von Informationen beinhaltet auch eine Auskunftsverpflichtung des Verantwortlichen; vgl. auch § 40 Abs. 3 S. 1 BDSG.[16] Die Auskunftspflicht betrifft umfassend »alle Informationen«, was auch die Auskunft über technische Abläufe und organisatorische Zusammenhänge bei der Verarbeitung personenbezogener Daten einschließt.[17] Das heißt, es sind auch Verfahrensdokumentationen einschließlich vorhandener Datenschutz- und Sicherheitskonzepte, die Beschreibung technisch-organisatorischer Maßnahmen sowie interne Handlungsanweisungen und Richtlinien vorzulegen.[18]

Es ist nicht ersichtlich, dass und woraus eine grundsätzliche Sperrwirkung hinsichtlich eines Bußgeldverfahrens erwachsen sollte.[19] Allerdings kann sich der Verantwortliche bzw. Auftragsverarbeiter aufgrund der Rechtsstaatlichkeitsklausel in Art. 58 Abs. 4 und insbesondere wegen des Grundsatzes »nemo tenetur se ipsum accusare« auf ein Auskunftsverweigerungsrecht berufen, soweit er sich durch die Bereitstellung der Informationen selbst belasten würde.[20] Hierauf ist der Auskunftsverpflichtete auch nach § 40 Abs. 3 BDSG hinzuweisen.

Von all dem abgesehen, stellt sich in der unternehmerischen Praxis die Frage, warum sich ein Verantwortlicher überhaupt diesen dogmatischen Fragestellungen mit für ihn ungewissem prozessualen Ausgang stellen sollte, anstatt unmittelbar – nicht nur aus datenschutz- und haftungsrechtlicher Sicht, sondern auch aus Gründen der IT-Sicherheit und des reibungslosen Betriebsablaufes – organisatorische Maßnahmen i.S.d. Art. 32 DSGVO in Form von Richtlinien bzw. Betriebsvereinbarungen zu schaffen.

## IV. Implementierung von organisatorischen Maßnahmen

Organisatorische Maßnahmen können in vielfältiger Weise ergriffen werden. Es kann sich um Schulungen, leicht verständliche und gut aufbereitete Hinweise im Intranet, Dienstanweisungen oder verbindliche Richtlinien bzw. Betriebsvereinbarungen handeln. So wichtig Schulungen und leicht verständliche Hinweise zur praktischen Umsetzung im unternehmerischen Alltag sind, so problematisch sind diese in Bezug auf Nachweispflichten, die Durchsetzbarkeit im Innenverhältnis sowie im Hinblick auf etwaige Regressmöglichkeiten gegenüber Mitarbeitern im Rahmen der Grundsätze zur Arbeitnehmerhaftung bzw. des innerbetrieblichen Schadensausgleichs.[21] Deswegen sollte die arbeitsrechtliche Dimension bei der Gestaltung von organisatorischen Maßnahmen so gleich mitgedacht und auch eine rechtsverbindliche Implementierung im Rahmen von IT-Richtlinien bzw. Betriebsvereinbarungen erfolgen, die eine Durchsetzung der Weisungen auch durch die arbeitsrechtlichen zulässigen Sanktionsmittel ermöglichen.[22] In der unternehmerischen Praxis sollte es sich bei den organisatorischen Maßnahmen stets um ein sich jeweils ergänzendes Maßnahmenbündel aus leicht verständlichen Hinweisen, Schulungen sowie rechtsverbindlichen Dokumenten handeln.

## V. Beispielhafte Inhalte einer IT-Richtlinie oder IT-Betriebsvereinbarung

IT-Richtlinien verpflichten die Beschäftigen eines Verantwortlichen verbindlich, bestimmte IT-Sicherheits-Standards und technische wie organisatorische Prozesse einzuhalten. Sie stellen eine geeignete organisatorische Maßnahme i.S.d. Art. 24 und 32 DSGVO dar. Eine derartige Richtlinie enthält unter anderem Regelungen:

- zu Konfigurationsrechten an Hard- und Software
- zu IT- und Datensicherheit am Arbeitsplatz wie

11 Vgl. BeckOK DatenschutzR/*Schmidt/Brink* (s. Fn. 3), DS-GVO Art. 24 Rn. 13.
12 Siehe dazu unter IV.
13 *Haerting/Konrad,* DSGVO im Praxistest, 2020, Rn. 355 ff.
14 Ehmann/Selmayr/*Selmayr*, DS-GVO, 2. Aufl. 2018, Art. 58 Rn. 11.
15 Und normwiederholend nach § 40 Abs. 4 Satz 1 BDSG.
16 Simitis/Hornung/Spiecker gen. Döhmann/*Polenz*, Datenschutzrecht, 2019, Art. 58 Rn. 13.
17 Ehmann/Selmayr/*Selmayr* (s. Fn. 14), Art. 58 Rn. 12.
18 Simitis/Hornung/Spiecker gen. Döhmann/*Polenz* (s. Fn. 16), Art. 58 Rn. 12.
19 Im Ergebnis ebenso Kühling/Buchner/*Bergt*, DS-GVO/BDSG, 3. Aufl. 2020, DSGVO Art. 83 Rn. 11; Paal/Pauly/*Martini* (s. Fn. 4), Art. 32 Rn. 72; speziell im Hinblick auf mobiles Arbeiten im Home Office so auch *Suwelack* ZD 2020, 561, 562.
20 Kühling/Buchner/*Boehm*, DS-GVO/BDSG, 3. Aufl. 2020, DS-GVO Art. 58 Rn. 14; Paal/Pauly/*Körffer*, DS-GVO, 2. Aufl. 2018, Art. 58 Rn. 8; Ehmann/Selmayr/*Selmayr* (s. Fn. 14), Art. 58 Rn. 12.
21 Zur Haftung des Arbeitnehmers Auer-Reinsdorff/Conrad/*Conrad*, Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, § 37 Rn. 328; ob die Durchsetzung eines Regressanspruches gegenüber einem Mitarbeiter tatsächlich sinnvoll ist, ist eine zweite Frage.
22 Paal/Pauly/*Martini* (s. Fn. 4), Art. 32 Rn. 66.; Schwartmann/Jaspers/Thüsing/Kugelmann/*Ritter*, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 Rn. 116.

- Passwortmanagement, Sperren des Arbeitsplatzes, Verschlüsselung von Daten
- Datensicherungen, Down- und Upload von Dateien
- Arbeiten im öffentlichen Raum, Arbeiten im Home Office (mobiles Arbeiten)
- zur Klassifikation zur Vertraulichkeit von Daten und zum Umgang mit den Daten der jeweiligen Vertraulichkeitsklassen
- zur dienstlichen und privaten Nutzung der IT-Infrastruktur[23]
- zur Analyse von personenbezogenen Daten im Fall des Missbrauchsverdachts
- zu Meldepflichten i.S.d. Art. 33 DSGVO[24]
- zu Sanktionen

Auch wenn die Grundstruktur von IT-Richtlinien bzw. Betriebsvereinbarungen[25] stets gleich ist, so sind die konkreten Regelungen im Detail so individuell wie jedes Unternehmen, seine eingesetzten Systeme sowie die Unternehmenskultur.

### VI. Fazit – Wirkung von organisatorischen Maßnahmen

IT-Richtlinien bzw. IT-Betriebsvereinbarungen enthalten essentielle Regelungen, die – bei guter Um- und Durchsetzung im Unternehmen – zum einen das Risiko für den Eintritt eines Datenschutzvorfalls erheblich minimieren und zum anderen aus den oben aufgezeigten Gründen das Haftungsrisiko für den Verantwortlichen im Falle eines bereits verwirklichten Risikos, d.h. eines Datenschutzvorfalls, beträchtlich senken.

Mit IT-Richtlinien bzw. IT-Betriebsvereinbarungen werden organisatorische Maßnahmen i.S.d. Art. 24 und 32 DSGVO zur Gewährleistung der Datensicherheit und des Datenschutzes ergriffen. Zugleich können Nachweispflichten nach Art. 5 Abs. 2 sowie Art. 24 DSGVO erfüllt werden. Das bedeutet auch, dass dem Vorwurf eines Organisationsverschuldens unmittelbar entgegengetreten und das Haftungsrisiko für Datenschutzverletzung erheblich minimiert werden kann. Organisatorische Maßnahmen in Form von IT-Richtlinien bzw. IT-Betriebsvereinbarungen sind insoweit ein »Must-Have« eines jeden verantwortlichen Unternehmens.

23 *Diercks* K&R 2014, 1.
24 Siehe dazu *Kuhrau* (in diesem Heft).
25 Im Fall einer Betriebsvereinbarung müssen neben dem Betriebsverfassungsgesetz die Anforderungen des Art. 88 DSGVO beachtet werden.

**M&A/Corporate digital**

## Überblick

# Technologische Souveränität und deutsche Investitionsprüfung

Dr. Jan D. Bonhage, LL.M. (NYU)/Erasmus Hoffmann, LL.M. (Cambridge), Hengeler Mueller, Berlin*

**Kritische (IT-)Infrastruktur und Software für deren Betrieb gehören schon aktuell zu den besonders sensitiven Bereichen der außenwirtschaftsrechtlichen Investitionsprüfung. Die Bundesregierung beabsichtigt, künftig auch kritische Technologien als besonders sicherheitssensitiv einzustufen. Gesetzgebungsverfahren zur weiteren Verschärfung der Investitionsprüfung laufen. Die Novellen sollten mit Augenmaß erfolgen und die Investitionsprüfung am Maßstab öffentlicher Ordnung und Sicherheit nicht mit Aspekten technologischer Souveränität industriepolitisch aufladen.**

Das Konzept technologischer Souveränität hat in Europa und Deutschland angesichts der Veröffentlichung geheimer Informationen im Sommer 2013, der Dominanz von US-Plattformanbietern bei vielen digitalen Diensten und der Ausbreitung industriepolitischer Erwerbsstrategien bestimmter asiatischer Staaten einen Popularitätsschub erfahren.[1] Im Fokus der europäischen Diskussion um die digitale und technologische Souveränität standen zuletzt z.B. das Mitte Dezember 2020 vorgelegte Legislativpaket der Europäischen Kommission über digitale Dienste einschließlich Ex-ante-Regulierung digitaler Plattformen und *New Competition Tools*[2] sowie der Infrastruktur- und Datenschutz beim 5G-Netzausbau. Aspekte der technologischen Souveränität und des Schutzes kritischer Infrastrukturen und deren Software kommen auch bei der deutschen Investitionsprüfung von ausländischen Investitionen in deutsche Unternehmen zum Tragen. Gesetzgebungsverfahren mit dem Ziel des verstärkten Schutzes kritischer Technologien in der Investitionsprüfung laufen.

### I. Die deutsche Investitionsprüfung

Seit über einem Jahrzehnt kann das Bundesministerium für Wirtschaft und Energie (BMWi) den Erwerb von sowie die Beteiligung an deutschen Unternehmen durch unionsfremde Investoren prüfen (vgl. §§ 55 ff. Außenwirtschaftsverordnung (AWV)). Dies gilt unabhängig von den Industriesektoren, in denen das Zielunternehmen und der Investor tätig sind (sektorübergreifende Prüfung). Die Investitionsprüfung erfasst insbesondere alle Erwerbsvorgänge, durch die ein Unionsfremder unmittelbar oder mittelbar Stimmrechte an einem inländischen Unternehmen oberhalb bestimmter Aufgreifschwellen erwirbt. Die Aufgreifschwelle von 25 % der Stimmrechtsanteile wurde Ende 2018 für bestimmte, besonders sicherheitsrelevante Bereiche auf 10 % abgesenkt. Für nicht-deutsche Erwerbe im Verteidigungsbereich und dem

* *Dr. Jan D. Bonhage* ist Partner bei Hengeler Mueller, *Erasmus Hoffmann* ist dort Senior Associate.
1 Vgl. zum ersten Punkt *Hohmann/Maurer/Morgus/Skierka*, Technological Sovereignty: Missing the Point?, https://www.gppi.net/media/Maurer-et-al_2014_Tech-Sovereignty-Europe.pdf.
2 Vgl. hierzu *Bischke/Brack* NZG 2020, 1260.

mit zertifizierten IT-Produkten für staatliche Verschlusssachen befassten IT-Bereich besteht eine sektorspezifische Prüfung mit einer Aufgreifschwelle von ebenfalls 10 %.[3] Gefährdet eine Transaktion voraussichtlich die öffentliche Ordnung oder Sicherheit, kann das BMWi eine solche Transaktion beschränken oder untersagen. Eine Überprüfung jeder ausländischen Investition von Amts wegen erfolgt nicht.

Nach Eingang eines Investitionsprüfungs-Filings des unmittelbaren Erwerbers kann das BMWi binnen zwei Monaten (Phase 1) ein förmliches Prüfverfahren (Phase 2) eröffnen. Die Phase 2 dauert grundsätzlich bis zu vier Monate nach Einreichung der eingangs der Phase 2 vom BMWi angefragten Informationen, die Frist kann um bis zu vier Monate verlängert werden.[4] Das BMWi konsultiert im Prüfverfahren andere Ministerien und Behörden. Bestehen keine Sicherheitsbedenken oder können diese durch öffentlich-rechtlichen Vertrag ausgeräumt werden, bestätigt das BMWi die investitionsschutzrechtliche Unbedenklichkeit des Erwerbs durch Unbedenklichkeitsbescheinigung (nicht meldepflichtiger Bereich) oder Freigabe (meldepflichtiger Bereich).[5]

## 1. Verschärfungen der Investitionsprüfung in 2020

Eine AWG-Novelle und zwei AWV-Novellen haben die Investitionsprüfung in 2020 deutlich verschärft.[6]

### a) Ausweitung des Melde- und Freigabeerfordernisses

Ein Kernpfeiler der verschärften Prüfung ist, dass künftig alle meldepflichtigen Erwerbe im sektorübergreifenden Bereich bis zur Freigabe durch das BMWi einem gesetzlichen Vollzugsverbot unterliegen. Bis zur Freigabe ist der Erwerb schwebend unwirksam.[7] Das Melde- und Freigabeerfordernis erfasst einen abschließenden Katalog besonders sensitiver Unternehmenserwerbe (§ 55 Abs. 1 Satz 2 AWV). Besonders sensitiv sind u.a. die Bereiche kritische Infrastruktur und branchenspezifische Software für den Betrieb kritischer Infrastruktur (dazu nachfolgend II.), breitenwirksame Medienhäuser, Cloud-Computing-Dienstleister sowie bestimmte Dienstleister für Telekommunikations-, Telematik- und staatliche Kommunikationsinfrastrukturen.

Im Zusammenhang mit der COVID-19-Pandemie hat die Bundesregierung mit der 15. AWV-Novelle die melde- und freigabepflichtigen Bereiche im Gesundheitssektor ausgedehnt. Dies betrifft insbesondere Entwicklung und Herstellung von für die Gesundheitsversorgung »wesentlichen Arzneimitteln« einschließlich deren Ausgangs- und Wirkstoffe, Medizinprodukten und In-vitro-Diagnostika zur Nutzung im Zusammenhang mit lebensbedrohlichen und hochansteckenden Infektionskrankheiten sowie persönlicher Schutzausrüstung (§ 55 Abs. 1 Satz 2 Nr. 8–11 AWV).[8]

### b) Neue Vollzugsverbote

Die Novelle des AWG im Sommer 2020 hat für alle meldepflichtigen Erwerbe straf- und bußgeldbewehrte[9] Vollzugsverbote eingeführt (sogenannte *Gun-Jumping*-Verbote, vgl. § 15 Abs. 4 AWG). Bis zur Freigabe des Erwerbs durch das BMWi[10] ist es insbesondere verboten, dem Erwerber eine Stimmrechtsausübung oder Gewinnzuteilung zu ermöglichen. In der Transaktionspraxis herausfordernd ist das Verbot, dem Erwerber solche Informationen zu überlassen oder anderweitig offenzulegen, die sich auf die besonders sicherheitsrelevanten Unternehmensbereiche oder -gegenstände der Zielgesellschaft beziehen.

Bisher bestand ein Vollzugsverbot lediglich im sektorspezifischen Prüfbereich, also insbesondere für Herstellung und Entwicklung von Rüstungsgütern und bestimmten durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierten IT-Produkten für staatliche Verschlusssachen. Die AWG-Novelle hat den Anwendungsbereich der sektorspezifischen Prüfung auf Unternehmen erweitert, die Rüstungsgüter »modifizieren« oder die »tatsächliche Gewalt« über solche Güter haben. Erfasst sind auch Unternehmen, die solche Tätigkeiten in der Vergangenheit vorgenommen haben und noch über entsprechende Kenntnisse verfügen.[11]

## 2. Prüfbereich

Die sektorübergreifende Prüfung erfasst allein außereuropäische Investoren. Investoren mit Sitz in der EU oder der EFTA stehen unter dem Schutz der unionsrechtlichen Freiheiten und werden von der sektorübergreifenden Prüfung nicht unmittelbar erfasst.[12] Im Prüfbereich liegt allerdings auch der mittelbare Erwerb inländischer Unternehmen. Dem außereuropäischen Eigner wird der Erwerb der Stimmrechte an dem inländischen Unternehmen durch unionsansässige – auch deutsche – Töchter wie ein eigener Erwerb zugerechnet (§ 56 AWV). Die Investitionsprüfung prüft mithin in den Beteiligungsstrukturen der Erwerberseite bis zum obersten Gesellschafter. Auf jeder Ebene genügt aus Sicht des BMWi das Erreichen oder Überschreiten der anwendbaren Aufgreifschwelle, eine anteilsverwässernde Durchrechnung der Anteile ist nicht vorgesehen. Unter bestimmten Umständen muss sich ein Investor auch Stimmrechte Dritter außerhalb der Erwerbsstruktur/des Konzerns zurechnen lassen, insbesondere dann, wenn der mittelbare Inverstor seinerseits mindestens die erforderlichen 10 % bzw. 25 % der Stimmrechte an dem Dritten hält oder der Investor und der Dritte eine gemeinsame Ausübung der Stimmrechte an der deutschen Zielgesellschaft vereinbart haben.[13]

Neben Anteilserwerben an deutschen Unternehmen oberhalb der anwendbaren Aufgreifschwelle kann das BMWi auch den Erwerb der das Unternehmen konstituierenden Wirtschaftsgüter (*Asset Deal*) prüfen. Eine Prüfbefugnis des BMWi besteht beim Erwerb des gesamten Unternehmens, beim Erwerb eines abgrenzbaren Betriebsteils eines inländischen Unternehmens sowie beim Erwerb aller wesentlichen Betriebsmittel eines inländischen Unternehmens.[14]

3 Siehe §§ 60, 60a AWV.
4 Vgl. im Einzelnen, auch zur Hemmung des Fristenlaufs, § 14a AWG.
5 Siehe § 58 Abs. 1 Satz 1, § 61 Satz 1 AWV.
6 Erstes Gesetz zur Änderung des Außenwirtschaftsgesetzes und anderer Gesetze v. 10.07.2020, BGBl. I S. 1637; 15. Verordnung zur Änderung der Außenwirtschaftsverordnung v. 25.05.2020, BAnz AT 02.06.2020; 16. Verordnung zur Änderung der Außenwirtschaftsverordnung v. 26.10.2020, BAnz AT 28.10.2020.
7 Vgl. § 15 Abs. 3 AWG.
8 Auch der Schutz bestimmter staatlicher Kommunikationsinfrastrukturen nach § 55 Abs. 1 Satz 2 Nr. 7 AWV wurde in 2020 eingeführt.
9 Siehe § 18 Abs. 1b, § 19 Abs. 1 Nr. 2 AWG.
10 Bzw. bis zum Ablauf der jeweiligen Freigabefiktionsfristen, siehe § 14a Abs. 1 AWG.
11 Vgl. § 5 Abs. 3 AWG, in der AWV ist die Erweiterung bisher nicht abgebildet.
12 Siehe aber den Umgehungstatbestand des § 55 Abs. 2 Satz 1 und 2 AWV.
13 Siehe § 56 Abs. 2 und 3 AWV.
14 Vgl. §§ 55 Abs. 1a, 60 Abs. 1a AWV.

### 3. Prüfmaßstab öffentliche Ordnung oder Sicherheit

Eine Untersagung des Erwerbs bzw. Anordnungen durch das BMWi setzen in der sektorübergreifenden Prüfung voraus, dass der Erwerb die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland oder eines anderen EU-Mitgliedstaates oder in Bezug auf Projekte oder Programme von Unionsinteresse voraussichtlich beeinträchtigt (§ 55 Abs. 1 Satz 1 AWV).[15] Vor den diesjährigen Novellen musste eine gegenwärtig und hinreichend gewichtige Gefährdung für wesentliche (deutsche) öffentliche Interessen bestehen. Allgemeine wirtschaftspolitische Ziele rechtfertigen weiterhin keine Beschränkung oder Untersagung eines Erwerbs.

### 4. Kooperationsmechanismus der EU-Screening-VO

Auf EU-Ebene stellt die am 11.10.2020 voll in Kraft getretene EU-Screening-VO[16] einen Rahmen für die Überprüfung ausländischer Direktinvestitionen auf. Sie schafft kein eigenständiges EU-Investitionsprüfverfahren, sondern überlässt es den EU-Mitgliedstaaten, ob diese ausländische Investitionen überprüfen. Führen Mitgliedstaaten Prüfverfahren durch, müssen sie die prozeduralen und materiellen Mindeststandards der EU-Screening-VO einhalten.[17] Die EU-Screening-VO etabliert einen Kooperationsmechanismus zum Informationsaustausch zwischen Mitgliedstaaten und Europäischer Kommission samt Recht zur Stellungnahme.[18]

## II. Kritische Infrastrukturen und Software zu deren Betrieb

Die Melde- und Freigabeerfordernisse nebst den Vollzugsverboten gelten für alle Transaktionen im Anwendungsbereich der Investitionsprüfung, die kritische Infrastruktur oder branchenspezifische Software für den Betrieb kritischer Infrastruktur betreffen (§ 55 Abs. 1 Satz 2 Nr. 1 und 2 AWV).

### 1. Kritische Infrastruktur

Kritische Infrastrukturen sind im BSI-Gesetz und der BSI-Kritisverordnung (BSI-KritisV) definiert. Diese benennen bestimmte Einrichtungen, Anlagen und Systeme in den Sektoren Energie, Wasser, IT, Finanz- und Versicherungswesen, Gesundheit sowie Transport und Verkehr. Als »kritisch« werden diese Einrichtungen, Anlagen und Systeme nur dann eingestuft, wenn sie definierte Schwellenwerte überschreiten.[19] Die Schwellenwerte orientieren sich grundsätzlich an dem Durchschnittsverbrauch von 500.000 versorgten Personen. Systemausfälle in dieser Größenordnung können typischerweise nicht mehr über Notfallmechanismen und -kapazitäten ersetzt werden.

Im IT-Bereich sind die Schwellenwerte tendenziell durchaus hoch. Bei Rechenzentren ist eine vertraglich vereinbarte Leistung von 5 MW die Kritikalitätsgrenze, Serverfarmen sind ab einem Jahresdurchschnitt von 25.000 laufenden Instanzen erfasst, und bei Content Delivery Netzwerken liegt die Schwelle bei einem ausgelieferten jährlichen Datenvolumen von 75.000 Terrabyte.[20] Die Behörden gingen dementsprechend bei der Einführung der BSI-KritisV davon aus, dass im Bereich Datenspeicherung und -verarbeitung deutschlandweit insgesamt lediglich etwa 30 Rechenzentren, Serverfarmen und Content Delivery Netzwerke kritische Infrastruktur darstellen.[21]

Die Betreiber kritischer Infrastruktur müssen grundsätzlich[22] angemessene organisatorische und technische Vorkehrungen nach dem Stand der Technik zur Vermeidung von Störungen treffen und dies dem BSI nachweisen (§ 8a BSI-Gesetz). Zielgesellschaft und Verkäuferseite haben vor diesem Hintergrund typischerweise Kenntnis davon, wenn die Zielgesellschaft kritische Infrastruktur betreibt.

### 2. Software für den Betrieb kritischer Infrastruktur

Neben der kritischen Infrastruktur erachtet die AWV auch Software für deren Betrieb als besonders kritisch (§ 55 Abs. 1 Satz 2 Nr. 2 AWV). Unternehmen, die branchenspezifische Software für den Betrieb kritischer Infrastruktur besonders entwickeln oder ändern, unterfallen daher ebenfalls dem Melde- und Freigabeerfordernis.

Die Außenwirtschaftsverordnung bestimmt die erfasste branchenspezifische Software der Sektoren Energie, Wasser, IT, Finanz- und Versicherungswesen, Gesundheit sowie Transport und Verkehr abschließend (§ 55 Abs. 1 Satz 3 AWV). Allerdings sind die Definitionen teilweise recht generisch, so ist bspw. im IT-Bereich Software »zum Betrieb von Anlagen oder Systemen zur Sprach- und Datenübertragung oder zur Datenspeicherung und -verarbeitung« kritisch.[23]

Im Gegensatz zu Betreibern kritischer Infrastruktur müssen deren Softwaredienstleister für branchenspezifische Software nach der BSI-KritisV diese Tätigkeit nicht dem BSI melden. Anders als im Bereich kritischer Infrastrukturen kann die Bewertung der (möglichen) branchenspezifischen Softwaretätigkeit daher regelmäßig nicht an den fachlichen Austausch der Zielgesellschaft mit dem BSI anknüpfen.

## III. Technologische Souveränität und kritische Technologien

Aktuell wird intensiv diskutiert, ob und inwieweit die deutsche Investitionsprüfung auch auf den Schutz kritischer Technologien und der digitalen und technologischen Souveränität Deutschlands zielen soll. Digitale Souveränität war ein politisches Leitmotiv der deutschen EU-Ratspräsidentschaft im zweiten Halbjahr 2020. Ein ähnliches Konzept der technologischen Souveränität ist einer der drei Pfeiler der deutschen Industriestrategie gemäß der Industriestrategie 2030 des BMWi vom November 2019.[24] Der Schutz kritischer Infrastrukturen und technologischer Souveränität ist ferner als einer der Zwecke des neuen deutschen Wirtschaftsstabilisierungsfonds, d.h. im Zusammenhang mit staatlichen Beteiligungen an Unternehmen, gesetzlich verankert.[25] Gemäß dem ersten Referentenentwurf des BMWi zur AWG-Novelle vom 30.01.2020 soll das Schutzkonzept der deutschen technologischen Souveränität und der Schutz kritischer Technologien

15 In der sektorspezifischen Prüfung ist die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland Prüfmaßstab (§ 59 Abs. 1 AWV).
16 Verordnung (EU) 2019/452 zur Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen in der Union.
17 Vgl. Art. 3 EU-Screening-VO.
18 Vgl. Art. 6 und 7 EU-Screening-VO.
19 Siehe die Anhänge der BSI-KritisV.
20 Siehe Anhang 4 Teil 3 Nr. 2 BSI-KritisV, auch zu den Schwellenwerten für Vertrauensdienste.
21 Referentenentwurf der BSI-KritisV v. 13.01.2016, S. 4.
22 Zu Ausnahmen siehe § 8d Abs. 1 und 2 BSI-Gesetz.
23 Vgl. § 55 Abs. 1 Satz 3 Nr. 3 AWV.
24 BMWi, Industriestrategie 2030, November 2019, S. 27 ff., https://www.bmwi.de/Redaktion/DE/Publikationen/Industrie/industriestrategie-2030.pdf?__blob=publicationFile&v=20 [17.12.2020].
25 Vgl. § 16 Abs. 1 Wirtschaftsstabilisierungsfondsgesetz.

über althergebrachte Schutzbereiche der Investitionsprüfung wie Verteidigung, Sicherheit, öffentliche Versorgung und kritische Infrastrukturen hinausgehen.[26] In der Tat verweist die EU-Screening-VO auf kritische Technologien als einen relevanten Faktor, der beim Screening ausländischer Investitionen berücksichtigt werden kann.[27] Auch die Mitte Dezember 2020 vorgelegte Cybersecurity-Strategie der Europäischen Kommission zielt auf den Schutz kritischer Infrastrukturen und Technologien.[28]

Der deutsche Spielraum zum Schutz der technologischen Souveränität im Rahmen der Investitionsprüfung hat Grenzen. Das EU-Recht einschließlich der Grundfreiheiten setzt Schranken für die mitgliedstaatlichen Investitionsprüfregime.[29] Das EU-Recht wird seinerseits durch internationales Recht wie die im Rahmen der Welthandelsorganisation (WTO) eingegangenen Verpflichtungen bestimmt und begrenzt.[30] Die EU-Screening-VO macht Vorgaben für die Investitionsprüfung in der EU im Rahmen und in den Grenzen der internationalen Verpflichtungen der EU und der Mitgliedstaaten im Rahmen der Welthandelsorganisation (WTO), der OECD sowie der bestehenden Handels- und Investitionsabkommen.[31] Dies gilt insbesondere auch für den Prüfmaßstab der Sicherheit und öffentlichen Ordnung.[32]

Das geltende deutsche Investitionsprüfrecht enthält jedenfalls keinen expliziten Schutzauftrag für kritische Technologien oder die technologische Souveränität Deutschlands. Schon jetzt ist allerdings absehbar, dass die Bundesregierung jedenfalls bestimmte High-Tech-Bereiche im Investitionsprüfverfahren besonders schützen will. Der Kabinettsentwurf des IT-Sicherheitsgesetzes 2.0 vom 16.12.2020[33] sieht vor, dass auch Herstellung und Entwicklung von kritischen Komponenten dem investitionsschutzrechtlichen Freigabeerfordernis unterliegen.[34] Der Begriff kritische Komponente erfasst insbesondere Kommunikationsinfrastruktur für 5G-Netze. Gemäß dem Entwurf dürfen kritische Komponenten nur eingesetzt werden, wenn der Hersteller eine Erklärung über seine Vertrauenswürdigkeit gegenüber dem Betreiber der kritischen Infrastruktur abgeben hat (Garantieerklärung). Die Garantieerklärung muss sich auf die gesamte Lieferkette des Herstellers beziehen und angeben, wie der Hersteller sicherstellt, dass die kritische Komponente über keine technischen Eigenschaften verfügt, die zu missbräuchlichen Zwecken wie Sabotage, Spionage oder Terrorismus eingesetzt werden können. Diese Regeln dürften bei der Vergabe von 5G-Infrastrukturleistungen z.B. an asiatische Bieter relevant werden.

Die Bundesregierung hat ferner angekündigt, dass weitere High-Tech-Bereiche im Rahmen der deutschen Investitionsprüfung speziell geschützt werden sollen. Dazu könnten u.a. Halbleiter, Robotik, künstliche Intelligenz sowie Bio- und Quantentechnologien gehören.[35] Der Regelungsentwurf der 17. AWV-Novelle ist seit längerem in der Ressortabstimmung. Die Novelle wird für das erste Halbjahr 2021 erwartet.

## IV. Fazit und Ausblick

Der Schutz der technologischen Souveränität steht (auch) im Bereich der deutschen Investitionsprüfung im Fokus. Kritische (IT-)Infrastruktur sowie Software für deren Betrieb wird schon heute besonders geschützt. Die Aktualisierung und ggf. erweiternde Nachjustierung dieses Schutzes verwirklicht deutsche Sicherheitsinteressen und damit den Zweck der Investitionsprüfung.

Im Fokus der laufenden Gesetzgebungsverfahren wird insbesondere die Balance zwischen staatlichen Sicherheitsbelangen und den Entwicklungs- und Wachstumschancen der (insbesondere jungen) digitalen Wirtschaft stehen. Das BMWi erkennt z.B. eine Kapitalangebotslücke in der Start-up- und Wachstumsphase für technologieorientierte Start-ups in Deutschland. Ein Freigabeerfordernis für die Beteiligung von US- und anderen nicht-europäischen Venture-Capital-Fonds und Investoren in frühen Finanzierungsrunden würde das Investitions- und Wachstumsklima für Start-ups wesentlich verschlechtern, insbesondere aufgrund der mit der Investitionsprüfung verknüpften Verzögerungsrisiken für die Finanzierung. Ein finanzieller Schwellenwert für kleine Unternehmen ist dem deutschen Investitionsprüfregime bisher fremd. Dagegen hat z.B. Österreich bei der Einführung des Investitionsprüfregimes 2020 Start-up-Unternehmen und andere Kleinstunternehmen mit weniger als zehn Beschäftigten und einem Jahresumsatz oder einer Jahresbilanzsumme von unter zwei Millionen Euro von der Prüfung ausgenommen.[36]

Staatliche Industriestrategien, Spannungen in den Handelsbeziehungen und die mit der COVID-19-Pandemie verknüpften Bewertungsschwankungen haben weltweit zu einer erhöhten Aufmerksamkeit für ausländische Investitionen und der Einführung oder Verschärfung von Investitionsprüfregimen geführt.[37] Die Exportnation Deutschland sollte Sorge dafür tragen, die Investitionsprüfung nicht mit einem allzu abstrakten und letztlich industriepolitischen Konzept der technologischen Souveränität aufzuladen.

26 S. 13.
27 Siehe Art. 4 Abs. 1 Buchstabe b) EU-Screening-VO.
28 Vgl. zu dieser Strategie https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade [17.12.2020].
29 *Hindelang/Hagemeyer* EuZW 2017, 882; *Nettesheim* ZHR 172 (2008), 729. Die EU-Screening-VO soll auch vor diesem Hintergrund Rechtssicherheit für die EU-Mitgliedstaaten mit Investitionsprüfregeln schaffen, vgl. *Schuelken* EuR 2018, 577, 584.
30 Schulze/Janssen/Kadelbach/*Boysen*, Europarecht, 4. Aufl. 2020, § 33 Rn. 26 ff.
31 Vgl. Erwägungsgrund 3 EU-Screening-VO.
32 Vgl. Erwägungsgrund 35 EU-Screening-VO.
33 Https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/it-sicherheitsgesetz.pdf;jsessionid=A314CF960C180AE47E6847ABC318AD85.1_cid373?__blob=publicationFile&v=2 [17.12.2020].
34 Einfügung in den Katalog des § 55 Abs. 1 Satz 2 AWV.
35 Vgl. BMWi, Kerninhalte des ersten Teils der Novelle des Außenwirtschaftsrechts, 30.01.2020, https://www.bmwi.de/Redaktion/DE/Downloads/J-L/kerninhalte-des-ersten-teils-der-novelle-des-aussenwirtschaftsrechts.pdf?__blob=publicationFile&v=4 [17.12.2020].
36 Vgl. § 2 Abs. 2 Investitionskontrollgesetz.
37 Vgl. OECD, Acquisition- and ownership-related policies to safeguard essential security interests, Mai 2020, http://www.oecd.org/Investment/OECD-Acquisition-ownership-policies-security-May2020.pdf [17.12.2020].

Querschnitt

Überblick

# Geldbußen bei unternehmensbezogenen Datenschutzverstößen: Was bleibt von der datenschutzrechtlichen Verantwortlichkeit auf der Haftungsseite?

Dr. Arne Klaas, Berlin*

Im Geschäftsbericht müssen keine »fancy buzzwords« wie »AI«, »IoT« oder »digital value chain« fallen. Auch abseits der Tech-Branche setzen mit Blick auf Kunden- und Mitarbeiterdaten sowie Internetpräsenz nahezu alle Geschäftsmodelle die Verarbeitung von personenbezogenen Informationen voraus. Dem Thema Datenschutz kann sich im Jahr 2021 kein Unternehmen entziehen. Mit einem vornehmlich digitalisierten Leistungsangebot steigt jedoch die Komplexität der Datenschutz-Compliance und damit zwangsläufig das Risiko einer Geldbuße. Doch auch bald drei Jahre nach dem Startschuss für die DSGVO sorgen die Zusammenhänge zwischen europäischem und nationalem Recht für Unsicherheiten bei der Frage nach der Haftungsverantwortung von Gesellschaften. Folgt aus dem funktionalen Unternehmensbegriff eine rechtsformübergreifende Haftung der gesamten wirtschaftlichen Einheit oder haftet ausschließlich der individuelle datenschutzrechtlich Verantwortliche – möglicherweise unter Heranziehung der zurechnungseinschränkenden Regeln der §§ 130, 30 OWiG? Aktualität gewinnt die Thematik nicht nur durch das Positionspapier der Datenschutzkonferenz (DSK), sondern insbesondere mit dem kürzlich ergangenen Urteil des LG Bonn gegen den Telekommunikationsdienstleister 1&1 (11.11.2020 – 29 OWi 1/20 LG).[1]

## I. Geldbußen als finanzielles Schreckgespenst

Das datenschutzrechtliche Haftungsregime gliedert sich grob in drei Blöcke: zivilrechtliche Schadensersatzansprüche der Betroffenen (Art. 82 DSGVO), sowie Bußgeld- (Art. 83 DSGVO, § 43 BDSG) und Straftatbestände (u.a. § 42 BDSG).

Für Unternehmen dürften die größten finanziellen Risiken von den Bußgeldtatbeständen der DSGVO ausgehen. Art. 83 DSGVO normiert in seinen Abs. 4 bis 6 für nahezu jede Zuwiderhandlung gegen die Vorgaben der Verordnung einen Bußgeldtatbestand. Soll die Geldbuße ein Unternehmen treffen, sieht die Verordnung zwei Sanktionsobergrenzen vor, die ihrem Anspruch »abschreckend« zu sein gerecht werden: Verstöße gegen Abs. 4 können mit Geldbußen bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs geahndet werden. Bei Verstößen gegen die in Abs. 5 und 6 festgelegten Pflichten sind es sogar 4 %.

### 1. Verpflichteter: der datenschutzrechtlich Verantwortliche

Die meisten der in Art. 83 Abs. 4–6 DSGVO mit einer Geldbuße bewehrten Pflichten treffen den datenschutzrechtlich Verantwortlichen.[2] Das ist gem. Art. 4 Nr. 7 DSGVO die Stelle, die (allein oder gemeinsam mit anderen) über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Innerhalb von Organisationen ist nach zivilrechtlichen Regeln zu ermitteln, wem die Zweck- und Mittelbestimmung zuzurechnen ist.[3] Treffen Mitarbeiter in ihrem Aufgabenbereich Verarbeitungsentscheidungen, die dem Unternehmenszweck dienen, ist gem. § 278 Satz 1 BGB analog bzw. § 166 Abs. 1 BGB analog[4] grundsätzlich die Gesellschaft als verantwortlich anzusehen.[5] Verfolgen die tatsächlich handelnden Mitarbeiter dagegen persönliche Zwecke, sind sie vielmehr selbst als Verantwortliche anzusehen.[6]

### 2. Abweichende Anforderungen an die Haftungsverantwortung einer Gesellschaft?

Streit entzündet sich nun an der Frage, ob die datenschutzrechtliche Verantwortlichkeit einer Gesellschaft bereits für sich genommen ausreicht, um bei Verstößen gegen die diese treffenden Vorschriften eine *haftungsrechtliche* Einstandspflicht nach Art. 83 Abs. 4–6 DSGVO zu begründen.[7]

Abweichend von dem isolierten Anknüpfungspunkt der datenschutzrechtlichen Verantwortlichkeit wird vertreten, dass die zurechnungseinschränkenden Vorgaben der §§ 130, 30 OWiG ergänzend herangezogen werden müssen.[8] Die

* Der Autor ist Rechtsanwalt bei der auf Wirtschaftsstrafrecht spezialisierten Kanzlei Krause & Kollegen Rechtsanwälte in Berlin.

1 Online verfügbar über die Rechtsprechungsdatenbank NRWE, www.nrwe.de, unter https://www.justiz.nrw.de/nrwe/lgs/bonn/lg_bonn/j2020/29_OWi_1_20_Urteil_20201111.html [22.12.2020]; s.a. ZD-Aktuell 2020, 7401.

2 Simitis/Hornung/Spiecker gen. Döhmann/*Boehm*, Datenschutzrecht, 2019, DSGVO Art. 83 Rn. 37; vgl. Forgó/Helfrich/Schneider/*Cornelius*, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil XIV Rn. 95.

3 Kühling/Buchner/*Hartung*, DS-GVO/BDSG, 3. Aufl. 2020, DS-GVO Art. 4 Nr. 7 Rn. 9.

4 *Klaas* CCZ 2020, 256 (257 Fn. 12.).

5 Kühling/Buchner/*Hartung* (s. Fn. 3), DS-GVO Art. 4 Nr. 7 Rn. 9; Sydow/*Raschauer*, DSGVO, 2. Aufl. 2018, Art. 4 Rn. 129.

6 Kühling/Buchner/*Hartung* (s. Fn. 3), DS-GVO Art. 4 Nr. 7 Rn. 10.

7 So: Spindler/Schuster/*Eckhardt*, Recht der elektronischen Medien, 4. Aufl. 2019, DS-GVO Art. 83 Rn. 77, 65, 62; Taeger/Gabel/*Moos/Schefzig*, DSGVO/BDSG, 3. Aufl. 2019, DS-GVO Art. 83 Rn. 89; vgl. Sydow/*Popp* (s. Fn. 5), Art. 83 Rn. 7.

8 Gola/*Gola*, DS-GVO, 2. Aufl. 2018, Art. 83 Rn. 11, 16 f.; Schantz/Wolff/*Wolff*, Das neue Datenschutzrecht, 2017, Rn. 1132 ff. *Konrad*, Bußgelder aufgrund von Datenschutzverstößen (Teil 1), 08.06.2020, https://www.cr-online.de/blog/2020/06/08/teil-1-bussgelder-aufgrund-von-datenschutzverstoessen/ [13.12.2020].

Aufsichtsbehörden[9] – und mit ihnen das LG Bonn[10] – gehen dagegen ihren eigenen Weg und rechnen schuldhafte Datenschutzverstöße von Beschäftigten der sog. »wirtschaftlichen Einheit« über den funktionalen Unternehmensbegriff zu.[11]

#### a) Kritik: keine Haftungs*begründung* über den funktionalen Unternehmensbegriff

Die DSK stellt sich (gegen die Stimmen der Landesdatenschutzbehörden von Bayern und Baden-Württemberg) auf den Standpunkt, dass »Unternehmen […] im Rahmen von Art. 83 [DSGVO] für schuldhafte Datenschutzverstöße ihrer Beschäftigten [haften], sofern es sich nicht um einen Exzess handelt«.[12] Sie geht hierbei nicht auf die Notwendigkeit der datenschutzrechtlichen Verantwortlichkeit ein, sondern begründet ihren Ansatz ausschließlich mit dem funktionalen Unternehmensbegriff des europäischen Primärrechts.

Auf den ersten Blick stützt EG 150 S. 3 DSGVO diese Vorgehensweise. Danach soll bei der Bebußung von Unternehmen der Begriff eines »Unternehmen« i.S.d.. Art. 101 und 102 AEUV verstanden werden. Der dort verankerte sog. »funktionale Unternehmensbegriff« knüpft nicht an den hinter einem Unternehmen stehenden individuellen Rechtsträger an, sondern bezieht sich auf die »wirtschaftliche Einheit«.[13] Diese umfasst alle rechtlich selbstständigen natürlichen und juristischen Personen, die weisungsgebunden und dauerhaft einen gemeinsamen wirtschaftlichen Zweck verfolgen.[14] Sollte der funktionale Unternehmensbegriff bereits auf Ebene der Haftungsbegründung Anwendung finden,[15] könnte das Verhalten eines einzelnen Mitarbeiters – der zusammen mit der weiteren Belegschaft und den verbundenen Unternehmen die wirtschaftliche Einheit bildet – derselbigen als eigene Handlung zugerechnet werden.[16] Der Verstoß des Einzelnen würde also den Anknüpfungspunkt für die originäre eigene Haftung der wirtschaftlichen Einheit bilden.[17]

Auf den zweiten Blick verliert der Verweis auf den funktionalen Unternehmensbegriff erheblich an Überzeugungskraft. Zum einen dürfte EG 150 S. 3 DSGVO seiner Intention nach nicht auf die Haftungsbegründung, sondern lediglich auf die sich anschließende Bußgeldbemessung abzielen.[18] Der Erwägungsgrund präzisiert den in Art. 83 Abs. 4–6 DSGVO verwendeten Begriff des »Unternehmens«, der sich jedoch alleine auf den Sanktionsrahmen bezieht.[19] Systematischer Bezugspunkt des Merkmals »Unternehmens« ist die Rechtsfolgen- und nicht die Tatbestandsseite. Die Erläuterungsfunktion von EG 150 S. 3 DSGVO erschöpft sich im Versuch[20] klarzustellen, dass es bei der Ermittlung des Sanktionshöchstmaßes beim »weltweit erzielten Jahresumsatz« auf den der gesamten wirtschaftlichen Einheit ankommen soll. Hierfür spricht auch die einleitende Formulierung des Erwägungsgrunds selbst: Diese geht davon aus, dass die der Sanktionsbemessung vorgelagerte – und hier alleine interessierende – Frage der Haftungsbegründung bereits geklärt ist (»werden Geldbußen Unternehmen auferlegt, […]«).

Zum anderen aber – und das ist ein noch gewichtigeres Argument – beißt sich der alles umspannende Begriff der wirtschaftlichen Einheit mit dem ausdifferenzierten System der datenschutzrechtlichen Verantwortlichkeit.[21] Selbst wenn man davon ausgehen würde, dass sich EG 150 S. 3 DSGVO nicht nur auf die Sanktionshöhe, sondern auch auf die Haftungsbegründung bezieht, müsste dem Prinzip der datenschutzrechtlichen Verantwortlichkeit der Vorrang eingeräumt werden. Diese ist in Art. 83 Abs. 4 Buchst. a) und – wie im nächsten Abschnitt dargelegt wird – in Abs. 5 DSGVO als maßgeblicher Anknüpfungspunkt für die bußgeldrechtliche Haftung gesetzlich verankert und wirkt normativ. Normative Wirkung kommt auch der gesetzlichen Definition des Verantwortlichen in Art. 4 Nr. 7 DSGVO zu. Erwägungsgründe dienen dagegen lediglich als Auslegungshilfe, können entgegenstehende gesetzliche Aussagen aber nicht in ihr Gegenteil verkehren.[22]

#### b) Überzeugender: Gleichlauf von datenschutz- und haftungsrechtlicher Verantwortlichkeit

Dogmatisch überzeugender ist es, die haftungsrechtliche Einstandspflicht für Verstöße unmittelbar aus der datenschutzrechtlichen Verantwortlichkeit zu folgern.[23] Dafür spricht die Systematik der DSGVO. Der datenschutzrechtlich Verantwortliche ist auf der Tatbestandsseite materiell zur Einhaltung der meisten bußgeldbewehrten Vorgaben verpflichtet.[24] Wer – wenn nicht er – sollte damit spiegelbildlich auf der Rechtsfolgenseite auch für die Verletzungen seiner Pflicht zur

9 DSK-Positionspapier v. 03.04.2019, S. 1, https://www.datenschutzkonferenz-online.de/media/en/20190405_Entschliessung_Unternehmenshaftung.pdf [13.12.2020].
10 LG Bonn, 11.11.2020 – 29 OWi 1/20 LG – 1&1, Rn. 57.
11 So auch BeckOK DatenschutzR/*Holländer*, 34. Ed. 01.08.2020, DS-GVO Art. 83 Rn. 14 f.; Kühling/Buchner/*Bergt* (s. Fn. 3), DS-GVO Art. 83 Rn. 20, 28, 39; Ehmann/Selmayr/*Nemitz*, DS-GVO, 2. Aufl. 2018, Art. 83 Rn. 42; Simitis/Hornung/Spiecker gen. Döhmann/Boehm (s. Fn. 2), DSGVO Art. 83 Rn. 43; *Uebele* EuZW 2018, 440, 445 f.
12 DSK Positionspapier v. 03.04.2019, S. 1.
13 EuGH 10.04.2014, C-231/11 P, C-232/11 P, C-233/11 P – Kommission/Siemens AG Österreich u.a., Rn. 43.
14 Forgó/Helfrich/Schneider/*Cornelius* (s. Fn. 2), Teil XIV Rn. 90 f.; *Faust/Spittka/Wybitul* ZD 2016, 120, 121.
15 So Ehmann/Selmayr/*Nemitz* (s. Fn. 11), Art. 83 Rn. 42; BeckOK DatenschutzR/*Holländer* (s. Fn. 11), DS-GVO Art. 83 Rn. 11; Kühling/Buchner/*Bergt* (s. Fn. 3), DS-GVO Art. 83 Rn. 20, 28, 39; *Uebele* EuZW 2018, 440, 445 f.
16 *Faust/Spittka/Wybitul* ZD 2016, 120, 121, 124; Kühling/Buchner/*Bergt* (s. Fn. 3), DS-GVO Art. 83 Rn. 20, 28, 39.
17 Vgl. *Fiedler/Klaas* NZKart 2018, 517, 518; vgl. *Dannecker/Dannecker* NZWiSt 2016, 162, 168.
18 Spindler/Schuster/*Eckhardt* (s. Fn. 7), DS-GVO Art. 83 Rn. 70, 77.
19 Spindler/Schuster/*Eckhardt* (s. Fn. 7), DS-GVO Art. 83 Rn. 70, 77.
20 Zur inkohärenten Bestimmung des Unternehmensbegriffs in Art. 4 Nr. 18 und EG 150 S. 3 DSGVO, die m.E. gerade mit Blick auf die Bestimmtheit des Tatbestands (Art. 49 GrCh) auch auf Seiten der Bußgeldbemessung dieselben auslegungstechnischen Konsequenzen nach sich ziehen kann, siehe Forgó/Helfrich/Schneider/*Cornelius* (s. Fn. 2), Teil XIV Rn. 96 f., 102, 105; *ders.* NZWiSt 2016, 421, 423 f.; *Faust/Spittka/Wybitul* ZD 2016, 120, 123 f.; Gola/*Gola* (s. Fn. 8), Art. 83 Rn. 20.
21 Taeger/Gabel/*Moos/Schefzig* (s. Fn. 7), DS-GVO Art. 83 Rn. 89; vgl. Spindler/Schuster/*Eckhardt* (s. Fn. 7), DS-GVO Art. 83 Rn. 68; BeckOK DatenschutzR/*Schild* (s. Fn. 11), DS-GVO Art. 4 Rn. 88; Forgó/Helfrich/Schneider/*Cornelius* (s. Fn. 2), Teil XIV Rn. 95; *Faust/Spittka/Wybitul* ZD 2016, 120, 123. A.A. BeckOK DatenschutzR/*Holländer* (s. Fn. 11), DS-GVO Art. 83 Rn. 14 f.
22 S.a. *Faust/Spittka/Wybitul* ZD 2016, 120, 124; Sydow/*Popp* (s. Fn. 5), Art. 83 Rn. 7; Taeger/Gabel/*Moos/Schefzig* (s. Fn. 7), DS-GVO Art. 83 Rn. 89; vgl. Paal/Pauly/*Frenzel*, DSGVO/BDSG, 2. Aufl. 2018, DS-GVO Art. 83 Rn. 20 (»die unzureichende Gesetzgebungstechnik [steht] der Anwendung des weiten Unternehmensbegriffs (noch) entgegen«); vgl. Spindler/Schuster/*Eckhardt* (s. Fn. 7), DS-GVO Art. 83 Rn. 71; *Cornelius* NZWiSt 2016, 421, 423.
23 Spindler/Schuster/*Eckhardt* (s. Fn. 7), DS-GVO Art. 83 Rn. 77, 65, 62; Taeger/Gabel/*Moos/Schefzig* (s. Fn. 7), DS-GVO Art. 83 Rn. 89; vgl. Sydow/*Popp* (s. Fn. 5), Art. 83 Rn. 7; *Cornelius* NZWiSt 2016, 421, 424 f.
24 BeckOK DatenschutzR/*Schild* (s. Fn. 11), DS-GVO Art. 4 Rn. 88; *Faust/Spittka/Wybitul* ZD 2016, 120, 123; *Cornelius* NZWiSt 2016, 421, 424.

Verantwortung gezogen werden?[25] Insoweit ist es nicht weiter verwunderlich, dass der Wortlaut in Art. 83 Abs. 5 und 6 DSGVO zum konkreten Haftungsadressaten schweigt. Die Verordnung setzt schlichtweg voraus, dass dieser dem Normadressaten der verletzten materiellen Pflicht entspricht.[26]

#### c) Anwendbarkeit der zurechnungseinschränkenden Regeln der §§ 130, 30 OWiG?

Von großer praktischer Bedeutung ist die Frage, ob die aus der datenschutzrechtlichen Verantwortlichkeit folgende haftungsrechtliche Einstandspflicht durch § 41 Abs. 1 Satz 1 BDSG iVm. §§ 130, 30 OWiG eingeschränkt wird.

Bei einer rein nationalen Betrachtung müsste dies bejaht werden.[27] § 41 Abs. 1 Satz 1 BDSG erklärt die Regeln des OWiG für Verstöße gegen Art. 83 Abs. 4–6 DSGVO für sinngemäß anwendbar. In Satz 2 werden einzelne, ausgewählte Vorschriften des OWiG von diesem Pauschalverweis wieder ausgenommen – die §§ 130, 30 OWiG werden hierbei jedoch gerade nicht genannt. Der Gesetzgeber hat sich bei seinem Streifzug durch das OWiG ganz bewusst dazu entschieden, die Zurechnungsregeln für eine bußgeldrechtliche Verantwortlichkeit einer juristischen Person für Verstöße gegen Art. 83 Abs. 4–6 DSGVO für anwendbar zu erklären. Ein bloßes gesetzgeberisches Versehen ist aufgrund der dezidierten Auswahl einzelner, für nicht kompatibel gehaltener Vorschriften nahezu auszuschließen. Dieser Eindruck wird durch das »Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz« vom 20.11.2019 unterstrichen. Der Gesetzgeber ist der nochmals bekräftigten Aufforderung der DSK, §§ 130, 30 OWiG aus der Verweisnorm des § 41 Abs. 1 Satz 1 BDSG auszunehmen, abermals nicht gefolgt.[28]

Allerdings ist zu bezweifeln, ob die Einschränkung der materiellen Bußgeldhaftung unionsrechtskonform ist.[29] Zwar gilt für die prozessuale Ausgestaltung des Bußgeldverfahrens das nationale Recht der Mitgliedsstaaten, vgl. Art. 83 Abs. 8 DSGVO.[30] Dieser Aufgabe widmet sich jedoch allein § 41 Abs. 2 BDSG. Abs. 1 erklärt dagegen (weitestgehend) die *materiellen* Regelungen des OWiG für anwendbar.[31] Die §§ 130, 30 OWiG bewirken durch das (Mindest-)Erfordernis einer Aufsichtspflichtverletzung einer Leitungsperson eine die Art. 83 Abs. 4–6 DSGVO modifizierende Einstandspflicht datenschutzrechtlich verantwortlicher Gesellschaften. Das Absenken der unionsrechtlichen materiellen Haftungsverantwortung durch eine nationale Regelung kann sich allerdings nicht auf die Öffnungsklausel in Art. 84 Abs. 1 Satz 1 DSGVO stützen, die sich gerade auf »andere Sanktionen«, als die in der Verordnung bereits vorhandenen (insbesondere Art. 83 Abs. 4–6 DSGVO) bezieht.[32] Die Anwendbarkeit der §§ 130, 30 OWiG steht vielmehr im Widerspruch zu der in EG 152 S. 1 DSGVO vorausgesetzten Absicht harmonisierter verwaltungsrechtlicher Sanktionen.[33] Aus dem Anwendungsvorrang des Unionsrechts folgt daher, dass es auch bei der Haftung einer Gesellschaft gem. Art. 83 Abs. 4–6 DSGVO bei der datenschutzrechtlichen Verantwortlichkeit als ausreichendem Anknüpfungspunkt bleibt.[34]

## II. Zusammenfassung und Ausblick

Ahndungssubjekt der Art. 83 Abs. 4–6 DSGVO ist ausschließlich der Normadressat der verletzten Verarbeitungsvorschriften. Das wird in der Regel der datenschutzrechtlich Verantwortliche sein und damit im Unternehmenskontext die Gesellschaft als Rechtsträger selbst. Da der nationale Gesetzgeber die Bußgeldtatbestände der Verordnung nicht abändern kann, steht einer Einschränkung der Einstandspflicht von datenschutzrechtlich verantwortlichen juristischen Personen und Personenvereinigungen gem. §§ 41 Abs. 1 Satz 1 BDSG, §§ 130, 30 OWiG der unionsrechtliche Anwendungsvorrang entgegen.

Jedenfalls zur Begründung der Haftung kann es nicht auf die Figur der wirtschaftlichen Einheit ankommen. Verstöße einzelner Beschäftigter anderer Rechtsträger im Unternehmensverbund führen nicht »automatisch« zur Haftung der Mutter-, Tochter- oder Schwestergesellschaft. Der systematische Streit, ob es bei der sich anschließenden Sanktionsbemessung auf den Unternehmensbegriff der Art. 101, 102 AEUV ankommt, ist hiermit nicht entschieden.

Für die (beratende) Praxis ist die gegenteilige Auffassung der Datenschutzbehörden jedoch ernst zu nehmen. Mit dem LG Bonn hat sich nun erstmals auch ein deutsches Gericht dieser Ansicht angeschlossen – abzuwarten bleibt, ob dieser systemwidrige Ansatz in Zukunft auch andere Gerichte überzeugen wird.

25 Spindler/Schuster/*Eckhardt* (s. Fn. 7), DS-GVO Art. 83 Rn. 68; Taeger/Gabel/*Moos/Schefzig* (s. Fn. 7), DS-GVO Art. 83 Rn. 89; Forgó/Helfrich/Schneider/*Cornelius* (s. Fn. 2), Teil XIV Rn. 95, 101. A.A. BeckOK DatenschutzR/*Holländer* (s. Fn. 11), DS-GVO Art. 83 Rn. 14.1: Eine »nach deutschem Verständnis folgende Trennung zwischen Verstoß und Haftungsadressat« werde europarechtlich nicht vorausgesetzt.

26 Kühling/Buchner/*Bergt* (s. Fn. 3), DS-GVO Art. 83 Rn. 22 f.; Simitis/Hornung/Spiecker gen. Döhmann/*Boehm* (s. Fn. 2), DSGVO Art. 83 Rn. 43; Spindler/Schuster/*Eckhardt* (s. Fn. 7), DS-GVO Art. 83 Rn. 65.

27 So Schantz/Wolff/*Wolff* (s. Fn. 8), Rn. 1132 ff.; Gola/*Gola* (s. Fn. 8), Art. 83 Rn. 11, 16 f.; *Konrad* (s. Fn. 8).

28 *Wybitul* Der Criminal Compliance Podcast – Das Bußgeldverfahren im Datenschutzrecht, Minute 22.10 – 22.46, https://criminal-compliance.podigee.io/23-rosinusonair [14.12.2020]; vgl. auch: LG Bonn, 11.11.2020 – 29 OWi 1/20 LG – 1&1, Rn. 52.

29 So auch: Gola/Heckmann/*Ehmann*, BDSG, 13. Aufl. 2019, § 41 Rn. 19 ff.; BeckOK DatenschutzR/*Brodowski/Nowak* (s. Fn. 11), BDSG § 41 Rn. 11, 11.3. Verhaltener Sydow/*Popp* (s. Fn. 5), Art. 83 Rn. 5; Kühling/Buchner/*Bergt* (s. Fn. 3), BDSG § 41 Rn. 7; Taeger/Gabel/*Nolde* (s. Fn. 7), BDSG § 41 Rn. 11; LG Bonn, 11.11.2020 – 29 OWi 1/20 LG – 1&1, Rn. 58 ff..

30 BeckOK DatenschutzR/*Brodowski/Nowak* (s. Fn. 11), BDSG § 41 Rn. 3.2; Gola/Heckmann/*Ehmann* (s. Fn. 29), § 41 Rn. 2 f., 6.

31 BeckOK DatenschutzR/*Brodowski/Nowak* (s. Fn. 11), BDSG § 41 Rn. 3.

32 Allgemein *Bergt* DuD 2017, 555, 559; Kühling/Buchner/*Bergt* (s. Fn. 3), BDSG § 41 Rn. 4; *Ehmann* ZD 2017, 201, 201 f.; BeckOK DatenschutzR/*Holländer* (s. Fn. 11), DS-GVO Art. 83 Rn. 90.1.

33 Gola/Heckmann/*Ehmann* (s. Fn. 29), § 41 Rn. 19; LG Bonn, 11.11.2020 – 29 OWi 1/20 LG – 1&1, Rn. 58 ff.

34 Vgl. allgemein BeckOK DatenschutzR/*Brodowski/Nowak* (s. Fn. 11), BDSG § 41 Rn. 5.

Souveränität, Datenverfügbarkeit, Interoperabilität, Offenheit und Transparenz verpflichten. Sobald der formale Gründungsprozess abgeschlossen ist, werden weitere Mitglieder, insbesondere aus anderen europäischen Mitgliedsstaaten, aufgenommen. Der gesamte Gründungsprozess wurde im Auftrag des BMWi durch die europäische Wirtschaftskanzlei Fieldfisher beraten.

### ■ BaFin und Bundesbank formulieren strategische Ziele in einer gemeinsamen Digitalen Agenda

BaFin und Bundesbank haben eine gemeinsame Digitale Agenda vorgestellt, die drei Innovationsfelder abdeckt: (1) Schnellere und einfachere Erhebung sowie Aufbereitung von Daten. Hierdurch wird auf die Komplexität des bankaufsichtlichen Meldewesens reagiert und die Aufsicht soll aktuellere und passgenauere Informationen erhalten können, ohne die Banken zu überlasten. (2) Ausbau der Qualität der Analysen mit dem Ziel, dass die Aufseher sämtliche vorliegenden Daten und Informationen zu einer Bank leicht abrufen, miteinander verknüpfen und analysieren können. Unter Einsatz von KI sollen Warnfunktionen für die Aufseher generiert werden mit Analysetools, die u.a. auf Advanced-Analytics-Methoden, Machine Learning und Text Mining basieren sollen. (3) Die internen Arbeitsabläufe, auch zwischen BaFin und Bundesbank sollen optimiert werden. Vorgesehen ist die Implementierung eines Dashboards, um sicherzustellen, dass zu jeder Zeit eine gemeinsame Sicht auf die Daten und Informationen besteht und alle bankaufsichtlich relevanten Daten für ein Institut über diese Arbeitsoberfläche verfügbar sind.

### ■ US Börsenaufsicht SEC erhebt Anklage gegen Ripple

Die Security Exchange Commission (SEC) hat am 23.12.2020 eine Klage gegen das Blockchain-Unternehmen Ripple eingereicht. Der Vorwurf lautet, dass Ripple durch ein sog. »unregistriertes Wertpapierangebot« rechtswidrig 1,3 Mrd. Dollar eingenommen haben soll. Zudem wurden zwei Führungskräfte von Ripple wegen der Erzielung persönlicher Gewinne angeklagt, die sie infolge des unerlaubten Angebots erhalten haben sollen. Ripple ist mit der Kryptowährung XRP verbunden, die nach Marktkapitalisierung derzeit die drittgrößte Kryptowährung weltweit ist.

## Aus der Gesetzgebung

### ■ Änderungen zur virtuellen Hauptversammlung für die Saison 2021 im BGBl

Die im Rahmen des Gesetzes zur Verkürzung der Restschuldbefreiung in Art. 12 vorgesehen Änderungen des COVID19-Maßnahmengesetzes vorgesehenen Modifikationen für die virtuelle Hauptversammlung sind nunmehr im BGBl (Teil I Nr. 67, S. 3332 vom 30.12.2020) veröffentlicht. Zu beachten sind insb. die folgenden Key Points: (1) Ab 2021 steht Aktionären ein Fragerecht zu, nachdem ihnen in 2020 lediglich eine Fragemöglichkeit bei virtuellen Hauptversammlung eingeräumt war. Damit geht eine grundsätzliche Pflicht der Verwaltung einher, fristgemäß eingegangene Fragen zu beantworten. (2) Im Vorfeld der Hauptversammlung ordnungsgemäß gestellte Gegenanträge und Wahlvorschläge gelten künftig als in der Versammlung gestellt, sofern der Antragsteller ordnungsgemäß legitimiert und zur Hauptversammlung angemeldet ist. (3) Künftig können Fragen zwingend bis mindestens einen Tag vor der Hauptversammlung eingereicht werden. Zahlreiche Gesellschaften haben diese Möglichkeit bereits in diesem Jahr eröffnet.

## Aus der Wissenschaft

### ■ Ehrung für die Juristische Fakultät der Universität Passau

Im Rahmen der Digital Study 2020 ist der Juristischen Fakultät der Universität Passau eine doppelte Ehre zuteil geworden: Sie wurde sowohl in der Kategorie »Bestes E-Learning« als auch in der Kategorie »Digitaler Vorreiter« ausgezeichnet.[1]

Die **Passauer Angebote zur Examensvorbereitung** (Examenskurs, Examensklausurenkurs, Ferienklausurenkurs, Einzelcoaching und simulierte mündliche Prüfungen) wurden als »Digital Award Bestes E-Learning 2020« prämiert. Das **Institut für Rechtsdidaktik** hat hier auf die Pandemiesituation reagiert und ein interaktives Angebot aufgesetzt, das der Qualität der bewährten Präsenzveranstaltungen zumindest nahekommt. Zudem wurde die Fakultät für die Einführung des neuen Bachelorstudiengangs **LL.B. Legal Tech** als »Digitaler Vorreiter 2020« ausgezeichnet. Der Studiengang ermöglicht deutschlandweit einen interdisziplinären Einstieg in den Einsatz der Technik zur Unterstützung bei rechtlichen Aufgaben – auch und gerade parallel zum Staatsexamen.

## Veranstaltungen

### ■ 04.02.2021: WM Online-Seminar »Digitalisierung des Gesellschaftsrechts«

Virtuelle Hauptversammlung, Cyber-Risiken und Unternehmensorganisation, Online-Gründung von Kapitalgesellschaften

1 Die Digital Study ist nach eigenen Angaben Deutschlands umfassendste Studie zur Digitalisierung in der juristischen Ausbildung und verfolgt das Ziel, die digitale Transformation der juristischen Ausbildung als Informationsmedium, Gradmesser und Impulsgeber kontinuierlich zu begleiten. Sie ist als Langzeitstudie konzipiert, welche im Jahresrhythmus den Status quo der Digitalisierung in der Juristenausbildung erhebt und den Auffassungen und Wünschen der Studierenden und Referendare Ausdruck verleiht.

■ **09.02.2021, 11:00 – 12:30: eco Akademie: Data Centers 2030 – Trends, Technologien & Strategien für die Zukunft**
Die digitale Welt befindet sich in einem Umbruch – nicht erst seit Corona ist eine deutlich wachsende Akzeptanz gegenüber Technologien wie Cloud Computing, Video-Conferencing, Smart Home & Smartphone sowie immer mehr KI-basierten Anwendungen erkennbar. Gleichwohl gewinnen all diese Technologien durch die anhaltende COVID-19 Pandemie massiv an Bedeutung – ob für das Funktionieren der Wirtschaft oder für das Alltagsleben eines jeden einzelnen von uns.

■ **10.02.2021, 12:00 – 18:00: eco Akademie – Optimieren zwischen Gitabit-Hype und Narrowband-Ökonomie?**
Seit vielen Jahren wird über das Internet-der Dinge geredet. Nachdem der Hype in den letzten Jahren unter der Überschrift »everything that can be connected will be connected« richtig Fahrt aufnahm, sind die euphorischen Prognosen inzwischen deutlich reduziert worden, und die Ist-Entwicklung hinkt hinter den Prognosen her. Aber: Das, was vernetzt wird, ist häufig stabiler und mehrwertiger als viele der frühen Anwendungs-Prognosen – Grund genug, auch 2021 wieder intensiv über das IoT zu diskutieren.

■ **25.02.2021: Global DIGITAL-FUTURE congress virtual**
Die Online-Kongressmesse zum Thema »German Mittelstand« meets International Business Development and Digitalization (Themen wie: Online Marketing & Vertriebsoptimierung, Prozessoptimierung & IT-Infrastruktur, Arbeit 4.0 & IT-Future Thinking, Cyber Security & Datensicherheit, Digitalisierung & Transformation)

■ **26.02.2021, 09:00 – 18:15: IRDi – Tagung »Elektronische Wertpapiere«**
Den inhaltlichen Mittelpunkt der Tagung bildet der eWpG-Entwurf von BMJV und BMF – Online-Event (via ZOOM)

# Impressum

**Herausgeberinnen und Herausgeber:**
RA Dr. Jan D. Bonhage, LL.M. (NYU) • RA Dr. Kuuya J. Chibanguza • RAin Nina Diercks, M.Litt (Aberdeen) • Prof. Dr. Bernd J. Hartmann, LL.M. (Virginia) • RA Prof. Dr. Markus Köhler • Prof. Dr. Mary-Rose McGuire, M.Jur. (Göttingen) • RAin Marlene Schreiber • RA Alireza Siadat, M.J.I. • RAin Dr. Nina-Luisa Siedler • Hans Steege • RA Oliver Süme • RA Dr. Thorsten Voß

**Schriftleitung:**
Prof. Dr. Bernd J. Hartmann, LL.M. (Virginia),
Prof. Dr. Mary-Rose McGuire, M. Jur. (Göttingen)
Manuskripte erbeten an ZdiW-redaktion@wolterskluwer.com



**Verlag:**
Wolters Kluwer Deutschland GmbH
Wolters-Kluwer-Str. 1, 50354 Hürth
http://www.wolterskluwer-online.de
Kundenservice: Telefon 0 26 31/ 8 01-22 22
e-mail: info@-wolterskluwer.de

**Redaktion:**
RAin Leah Ngabi
Wolters-Kluwer-Str. 1, 50354 Hürth
Tel.: 02233/3760-7190
ZdiW-redaktion@wolterskluwer.com

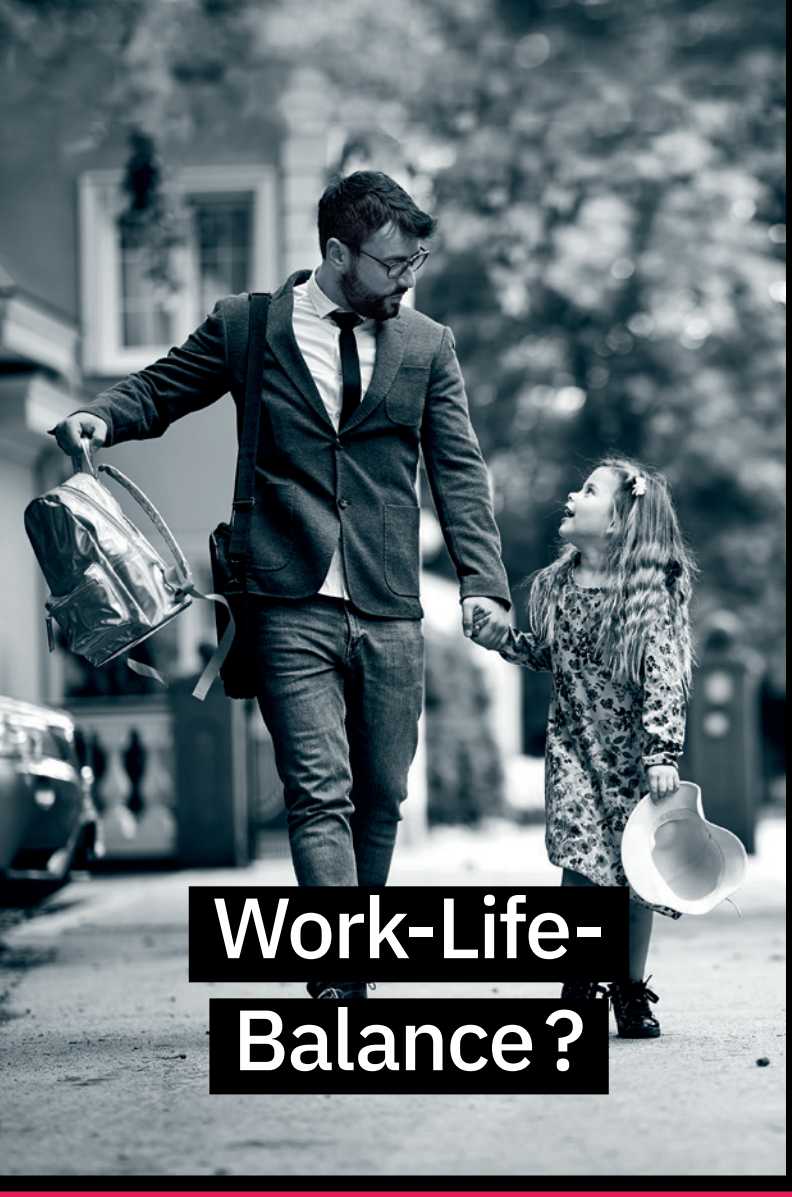
**Anzeigen:**
Anzeigenverkauf: Janosch Kleibrink, Tel. (02233) 3760 - 7719
E-Mail: Janosch.Kleibrink@wolterskluwer.com
Anzeigendisposition: Karin Odening, Tel. (02233) 3760 - 7760
E-Mail: anzeigen@wolterskluwer.com
Die Anzeigen werden nach der Preisliste Nr. 1 vom 1.1.2021 berechnet.

**Bezugspreis zzgl. Versandkosten**
Jahresabonnement: € 299,00
Einzelheft: € 32,00
Erscheinungsweise: monatlich
Kündigungsfrist: 6 Wochen zum Ende des Bezugsjahres

**Satz:**
Newgen Knowledge Works (P) Ltd., Chennai

**Druck:**
Lotos Druck GmbH, Dippoldiswalde

ISSN 2702-4040





# Deine Entscheidung!

Egal, was dir wichtig ist, du findest deinen Traumjob bei LTO Karriere, deinem neuen Karriereportal von LTO.

www.lto-karriere.de

LTO karriere

Weil du den besten Job verdienst.

Wolters Kluwer

# Fundiertes Fachwissen für richtige Entscheidungen

**Mit dem Modul Handels- und Gesellschaftsrecht Plus auf dem neuesten Stand:**

- Basiswissen für die alltägliche Praxis und zusätzliche Inhalte zu spezifischen Fragestellungen
- Mit *Karsten Schmidt*, Handelsrecht, *Happ*, Aktienrecht, *Mehrbrey*, Handbuch Gesellschaftsrechtliche Streitigkeiten
- Inkl. der renommierten Reihe der Kölner Kommentare zum Aktienrecht, Kartellrecht, Umwandlungsgesetz

**Jetzt abonnieren**
**ab 129 € mtl.**
zzgl. MwSt.


Profitieren Sie von den Vorteilen eines Abonnements: stets aktuelle Inhalte und komfortable Tools, die Ihre Recherche erleichtern.
Mit Wolters Kluwer Recherche haben Sie außerdem Zugriff auf unsere kostenlose Rechtsprechungs- und Gesetzesdatenbank.

**wolterskluwer-online.de**

ALLES, WAS EXPERTEN BEWEGT.