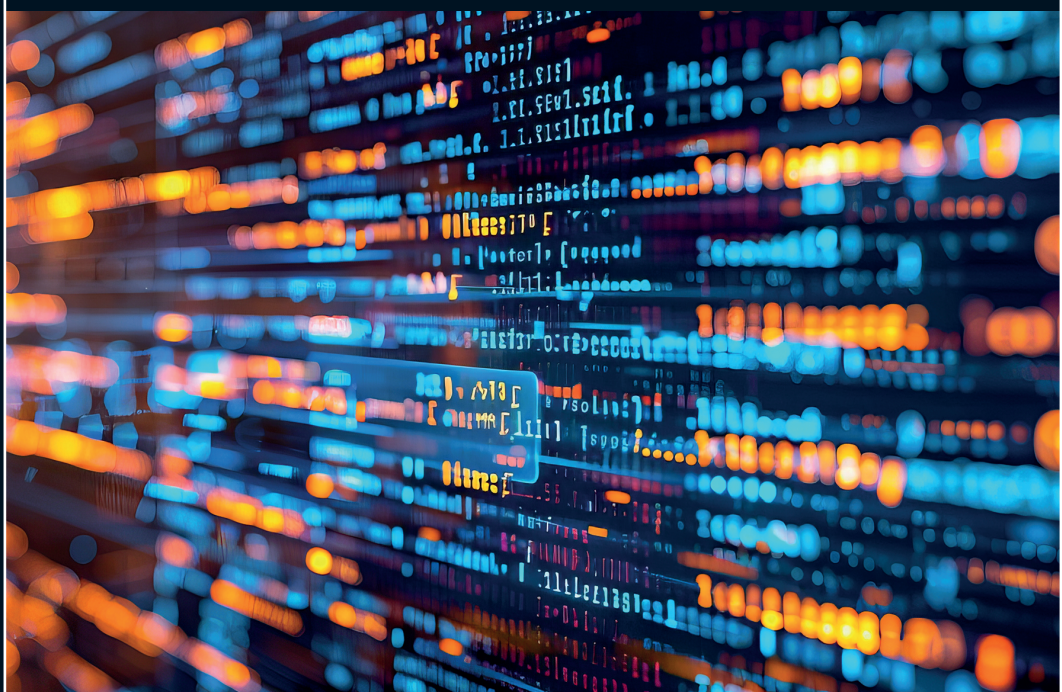
Schriften zum Digitalwirtschaftsrecht
Studies on Digital Business Law

1

Bösch | Laimer | Mittwoch | Müller (Hrsg.)

Daten, Plattformen, Smart Contracts

Aktuelle Rechtsfragen



Nomos DIKE facultas

https://doi.org/10.5771/9783748916475, am 17.09.2024, 05:11:31

Schriften zum Digitalwirtschaftsrecht
Studies on Digital Business Law

herausgegeben von
Univ.-Prof. Dr. Simon Laimer, LL.M.
Prof. Dr. Anne-Christin Mittwoch
Univ.-Prof. Dr. Thomas Müller, LL.M.
Dr. Lukas Staffler, LL.M.

Band 1

Fabian Bösch | Simon Laimer | Anne-Christin Mittwoch
Thomas Müller (Hrsg.)

Daten, Plattformen, Smart Contracts

Aktuelle Rechtsfragen

Nomos DIKE facultas

Gefördert durch:

GPK Pegger Kofler & Partner Rechtsanwälte

MCI – Management Center Innsbruck

Publikationsfonds der Martin-Luther-Universität Halle-Wittenberg

Universität Innsbruck

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

1. Auflage 2024

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN 978-3-7560-0901-5
(Nomos Verlagsgesellschaft mbH & Co. KG, Baden-Baden, Print)
ISBN 978-3-7489-1647-5
(Nomos Verlagsgesellschaft mbH & Co. KG, ePDF)

ISBN 978-3-03891-761-8 (Dike Verlag, Zürich/St. Gallen)

ISBN 978-3-7089-2518-9 (facultas Verlag, Wien)

DOI: https://doi.org/10.5771/9783748916475

Onlineversion
Nomos eLibrary

Vorwort

Sehr geehrte Leserin, sehr geehrter Leser!

Die Digitalisierung unserer Gesellschaft ist Jahrhundertthema. Informations- und Kommunikationstechnologien haben ein neues Zeitalter eingeläutet, das eine Fülle vernetzter Prozesse umfasst. Big-Data-Anwendungen haben die Art und Weise verändert, wie Menschen interagieren. Digitale Technologien bieten neue Möglichkeiten, Gesellschaft, Wissenschaft und Wirtschaft zu gestalten. Die zunehmende Verbreitung digitaler Technologien erfasst nahezu alle Lebensbereiche und wirkt damit auch auf das Recht in allen seinen Facetten ein. Eine herausragende Bedeutung kommt hier dem Wirtschaftsrecht zu. Denn es sind Wirtschaftsbeziehungen, oft gerade transnationale, die neue gesellschaftliche Entwicklungen früh aufgreifen, prägen und fortentwickeln – und damit auch Gesetzgeber und Rechtsanwender vor besondere Herausforderungen stellen. Die Digitalisierung der Wirtschaft erfordert eine geeignete rechtliche Infrastruktur, die Innovation fördert und gleichzeitig Rechtssicherheit bietet. Diese besondere transformative Bedeutung will die Reihe „Schriften zum Digitalwirtschaftsrecht" aufgreifen.

Ihr erster Band mit dem Titel „Daten, Plattformen, Smart Contracts. Aktuelle Rechtsfragen" zeigt bereits vieles, wofür die neue Reihe stehen soll. Dies betrifft zum einen die veröffentlichten Textsorten: Neben Monographien oder Konferenzbänden erscheinen, so wie in diesem Buch, auch Sammelbände mit hervorragenden Qualifikationsarbeiten aus Grund- oder Weiterbildungsstudien, womit der Zugang zu qualitativ hochwertigem Wissen, das jenseits klassischer Wissenschaftsformate entsteht, ermöglicht und der Diskurs zur Entwicklung und Entfaltung des Digitalwirtschaftsrechts bereichert werden soll. Zum anderen zeigt sich anhand der aufgenommenen Texte die inhaltliche Bandbreite, zumal es sich beim Digitalwirtschaftsrecht um eine Schnittstellenmaterie zwischen Privatrecht und Öffentlichem Recht handelt, welche die unterschiedlichsten Fragestellungen aus dem Zivil- und Unternehmensrecht ebenso wie aus dem öffentlichen Wirtschafts- und Verwaltungsrecht sowie dem Strafrecht erfasst. Im Sinne dieses umfassenden Blicks auf digitalwirtschaftsrechtliche Fragen findet sich in diesem Band eine Arbeit zum Vertragsschluss mit Programm- oder Maschinencode

(*Hartlieb*), eine Untersuchung der einseitigen Änderungsbefugnis des Unternehmers bei der Bereitstellung digitaler Inhalte (*Eitel*), eine Abhandlung zur Corporate Digital Responsibility im Kontext eines entstehenden Datenrechts (*Ruff*), eine Analyse datenschutzrechtlicher Aspekte bei der Umsetzung der Whistleblower-Richtlinie in Unternehmen (*Neumayer*) sowie eine Arbeit zur (un-)mittelbaren Grundrechtsbindung Privater im Digital Services Act (*Kapusta*).

Neben den Autor:innen, die das Werk mit ihrer qualitätsvollen Arbeit möglich machen, wollen wir an dieser Stelle dem NOMOS Verlag, insbesondere Herrn *Matthias Knopik*, für das Vertrauen und die Unterstützung bei der Umsetzung herzlich danken. Außerdem wollen wir uns beim MCI Management Center Innsbruck, bei GPK Pegger Kofler & Partner Rechtsanwälte, beim Publikationsfonds der Martin-Luther-Universität Halle-Wittenberg sowie bei der Universität Innsbruck für die finanzielle Unterstützung bestens bedanken.

Wir hoffen, dass die Leserinnen und Leser das Buch freundlich aufnehmen werden, und wir sind für inhaltliche Anregungen, Kritik und Verbesserungsvorschläge dankbar.

Innsbruck/Halle (Saale)
im Frühjahr 2024

Fabian Bösch
Simon Laimer
Anne-Christin Mittwoch
Thomas Müller

Inhaltsverzeichnis

Smart Contracts und das ABGB – zum Vertragsschluss mit Programm- oder Maschinencode

Marie-Therese Hartlieb

§ 1 Problemaufriss[1]

A. Forschungsfragen und Gang der Untersuchung

Smart Contracts sind ein Phänomen der Digitalisierung, das bestehende Institutionen wie das Vertragsrecht und traditionelle rechtsberatende Berufe berührt.[2] Ihnen wird enormes Potenzial zugeschrieben. Eine allgemein anerkannte Definition von Smart Contracts besteht indes nicht. Auch was sie genau können, ist unklar; was sie dürfen, ist Gegenstand vieler Diskussionen.[3] In diesen offenen Raum tritt die vorliegende Arbeit.

Sie will zunächst klären, was Smart Contracts sind. Die Bezeichnung „Smart Contract" taucht als unpräziser Sammelbegriff überall auf, wo auch nur ein Element des Vertragsschlusses oder der Vertragsdurchführung automatisiert ist.[4] Das fehlende Verständnis über Smart Contracts könnte daraus rühren, dass Techniker und Juristen wechselseitig zu wenig Rücksicht auf die jeweils fremde Disziplin nehmen. Der Versuch einer Begriffsschärfung muss daher in einem ersten Schritt die technische Basis erarbeiten, auf der Smart Contracts stehen (§ 2). Führt man die technischen Charakte-

1 Die vorliegende Arbeit wurde als Masterarbeit am 9.8.2022 zur Erlangung des akademischen Grades "Master of Laws " – "LL.M." im Masterprogramm LL.M. Digital Business & Tech Law Executive Education MCI – Die Unternehmerische Hochschule eingereicht. Für die Betreuung bedanke ich mich herzlich bei Univ.-Prof. Mag. Dr. Simon Laimer, LL.M. Die Arbeit befindet sich inhaltlich auf dem Stand der Einreichung. Die Verweise auf Kommentar-Literatur, Gesetzesentwürfe und anhängige Gerichtsentscheidungen sind zum Stichtag 9.1.2024 aktualisiert. Zu diesem Datum sind auch sämtliche Links zuletzt abgerufen. Bei Onlinequellen erfolgt ein Hinweis auf die Hauptseite der Onlinequelle. Der Direktlink zum zitierten Dokument sowie sämtliche Langzitate befinden sich im Literaturverzeichnis. Personenbezeichnungen und personenbezogene Wörter gelten für alle Geschlechter.

2 Braegelmann/Kaulartz Smart Contracts/Braegelmann/Kaulartz S. 1 (3 f.); Savelyev ICTL 26 (2017), 116.

3 Statt vieler Hoffmann JSSI 2021, 1 (12 f.).

4 Zu diskutierten Anwendungsgebieten s. Anhang III.

ristika danach mit dem rechtlichen Verständnis von Verträgen zusammen, könnte eine notwendige Präzisierung des Begriffsverständnisses gelingen (§ 3 B.).

Smart Contracts erheben begrifflich den Anspruch, Verträge zu sein. An dieser Einordnung lässt der Umstand zweifeln, dass sie aus Codes bestehen. Denn dies könnte zu Spannungen mit den Normen des ABGB führen, die sich mit Formvorgaben beschäftigen (§ 3 C.). Überdies gilt es zu untersuchen, ob der fein abgestimmte gesetzliche Vertragsabschlussmechanismus einen Vertragsabschluss in Code zulässt (§ 4).

Smart Contracts auf einer Blockchain (on-chain) sollen im Vergleich zu traditionellen Verträgen kostengünstiger sein (§ 5 A.). Sie sollen außerdem ohne Intermediäre auskommen, weil das in traditionellen Vertragsbeziehungen bestehende Vertrauensdefizit durch einen neutralen, fälschungssicheren Code verhindert werde (§ 5 B.). Ob diese Vorteile tatsächlich bestehen, gilt es zu überprüfen. Ein weiterer Vorteil liege in der Automatisierung des Vertragsabschlusses und der Vertragsdurchführung. Der Realisierung dieses Potenzials stehen derzeit aber sprachliche Barrieren entgegen. Zu untersuchen ist daher etwa, ob der Einsatz von Maschinen und autonomen Softwareagenten die Hürde der Kommunikation in Code bewältigen kann (§ 5 C.). Nach einem kurzen Ausblick auf die Vertragsdurchführung (§ 5 D.) schließt die Arbeit mit einer Zusammenfassung (§ 6).

B. Abgrenzung

Im Zusammenhang mit Smart Contracts stellen sich ganz unterschiedliche rechtliche Herausforderungen, deren Aufarbeitung über den Rahmen einer Masterarbeit weit hinausgeht. Im Folgenden wird daher umgrenzt, was die Arbeit zur Diskussion beitragen und fortführen will und was sie beiseitelassen muss. Die Anwendbarkeit österreichischen Sachrechts wird dabei vorausgesetzt; international-privatrechtliche Fragen bleiben ausgeklammert.[5]

Aus vertragsrechtlicher Sicht können Smart Contracts abstrakt zwei Hauptfunktionen übernehmen: Sie dienen zum einen dem Austausch der Willenserklärungen und damit dem Vertragsabschluss. Sie sollen zum an-

5 Insbesondere für on-chain Verträge stellen sich spannende Fragen des anwendbaren Rechts, weil der Vertrag im distribuierten Netzwerk überall auf der Welt abgelegt und durchgeführt werden kann. Zur Diskussion s. nur Braegelmann/Kaulartz Smart Contracts/Rühl S. 147.

deren in der Phase der Vertragsdurchführung den Leistungsaustausch automatisieren. Die vorliegende Arbeit legt den Fokus (nur) auf die erste Hauptfunktion. Das ist insofern unproblematisch, als es die klare Zweiteilung des ABGB in Titel und Modus erlaubt, die beiden Aspekte unabhängig voneinander zu bearbeiten. Diese Schwerpunktsetzung ist auch insofern nützlich, als eine wissenschaftliche Aufarbeitung für das „Ob" und „Wie" des Abschlusses eines Smart Contracts nach dem ABGB bis dato fehlt.[6]

Im Mittelpunkt steht daher die schuldrechtliche Frage, ob ein Smart Contract ein Titel sein kann. Die Arbeit geht grundsätzlich von fehlerfreien Codes aus.[7] Nicht behandelt werden daher etwaige Ansprüche aus fehlerhaften Codes. Ebenfalls ausgeklammert bleiben konsumentenschutzrechtliche Besonderheiten[8] und außervertragliche Fragen.[9] Rechtsfragen der Vertragsdurchführung werden in Form eines kurzen Ausblicks adressiert.

§ 2 Technische Grundlagen

Zum besseren Verständnis der rechtlichen Fragen sind in der gebotenen Kürze die notwendigsten technischen Grundlagen darzulegen. Das betrifft zunächst die Blockchain- und Distributed-Ledger-Technologie (Abschnitt A.), die für Smart Contracts fruchtbar gemacht werden kann (Abschnitt B.). Überdies betrifft das Codes, von denen Smart Contracts ihr Potential ableiten (Abschnitt C.).

A. Blockchain

Die meisten webbasierten Software-Applikationen (zB Google, Amazon, eBanking-Lösungen) sind zentral organisiert. Der Informationsfluss zentraler Systeme wird von einer Stelle gespeichert, verwaltet, kontrolliert, gesperrt und/oder gelöscht. Das setzt Vertrauen in die zentrale Stelle voraus.

6 Hanzl HdB Blockchain passim schneidet viele Fragen an. Meist erfolgt keine wissenschaftliche Aufarbeitung, was bei einem Handbuch aber auch nicht erforderlich ist.

7 Zu Fehlern und Irrtümern s. etwa Völkel ZFR 2021, 532.

8 Siehe dazu Wilhelm WM 2020, 1849 (1852 ff.).

9 Gedacht sei etwa daran, ob Software (zB Web Crawler) dafür eingesetzt werden darf, illegale, zB urheberrechtsverletzende, Inhalte im Internet zu finden und Verantwortliche auf Unterlassung, Beseitigung und/oder Schadenersatz zu klagen. Vgl. Wagner AcP 222 (2022), 56 (61).

Die Distributed-Ledger-Technologie (DLT) ermöglicht dezentrale Systeme. Dort verwalten und kontrollieren den Informationsfluss alle (oder viele) Teilnehmer[10] der „verteilten Datenbank". Für die Richtigkeit des Informationsflusses kann also auf das Netzwerk und nicht nur auf eine zentrale Drittpartei vertraut werden.[11] Das macht sich eine Blockchain zu nutze.

Eine Blockchain ist – vereinfacht dargestellt – eine Kette aus Blöcken, die auf die soeben gezeigte Art dezentral gespeichert wird.[12] Die Blöcke enthalten Informationen; zB alle Transaktionen von Assets[13] der Netzwerkteilnehmer.[14] Im Detail sind Blockchains zwar unterschiedlich ausgestaltet,[15] ihre Grundstruktur ähnelt sich aber.[16] Eine Information/Transaktion

10 Diese Arbeit spricht nur von solchen (Netzwerk-)Teilnehmern, die berechtigt sind, Smart Contracts auf einer Blockchain abzulegen. Es genügt daher, allgemein von (Netzwerk-)Teilnehmern zu sprechen. Je nach Blockchain und den Aufgaben, die Teilnehmer übernehmen, könnten sie kategorisiert werden. Siehe dazu Hanzl HdB Blockchain S. 10 ff., 35 mwN; Piska/Völkel Blockchain/Völkel Rn. 1.49; Rutz Blockchain S. 17.

11 Statt vieler Rutz Blockchain S. 9 f.; Bolesch/Mitschele ZfgK 2016, 1125 (1128); BaFin, DLT, 2016, https://www.bafin.de; Hancock/Vaizey, DLT, 2016, https://assets.publishing.service.gov.uk; Schulz c't 23 (2017), 108; Heckelmann NJW 2018, 504 (504 f.). Das wäre auch die Grundidee hinter der Bitcoin-Blockchain. Siehe nur Satoshi Nakamoto, Bitcoin White-Paper, 2008, https://bitcoin.org/bitcoin.pdf: „A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution."

12 Näher auch zum Folgenden Antonopoulos Bitcoin Blockchain passim; Piska/Völkel Blockchain passim; Finck Blockchain S. 1 ff.; Gupta Blockchain passim; Kaulartz CR 2016, 474; D. Tapscott/A. Tapscott Blockchain-Revolution passim; Savelyev ICTL 26 (2017), 116 (117 ff.); Schrey/Thalhofer NJW 2017, 1431; Forgó/Zöchling-Jud 20. ÖJT II/1/Forgó S. 285 (331 ff.); Achenbach/Baumgart/Rill DuD 2017, 673; Schulz c't 23 (2017), 103 ff.; Hoffmann-Riem Digitale Transformation S. 45 f.; Wright/De Filippi SSRN 2015, 1 (18 ff.).

13 Das sind etwa Kryptowährungen oder Token, die einen realen oder digitalen Gegenstand repräsentieren. Ein Token kann sich auf jede Sache iSd § 285 ABGB beziehen, s. Kogler JBl 2021, 685 (687); Kucsko/Pabst/Tipotsch/Tyrybon ecolex 2021/324, 496.

14 So etwa über Wallets – alphanummerische Adressen –, die einen bestimmten Ort auf der Blockchain bezeichnen, an den Assets gesendet, von dem sie versendet und auf dem sie gespeichert werden können. Soll der Smart Contract für die Parteien einen Treuhänder ersetzen, braucht er eine eigene Adresse. Kucsko/Pabst/Tipotsch/Tyrybon ecolex 2021, 495 (496). Asymmetrische Verschlüsselungsverfahren stellen letztlich sicher, dass der Sender einer Information/eines Assets dazu berechtigt ist. Vgl. Kaulartz CR 2016, 474 (475); Bolesch/Mitschele ZfgK 2016, 1125 (1127); Antonopoulos Bitcoin Blockchain S. 57 f.

15 Statt vieler Achenbach/Baumgart/Rill DuD 2017, 673.

16 Diedrich Ethereum S. 38 f. Für die im Folgenden dargelegte Grundstruktur dient die Bitcoin-Blockchain als Basis, weil dazu die breiteste Information zugänglich ist.

wird (nur) dann in einen neuen Block der Blockchain geschrieben und durchgeführt, wenn diese berechtigt ist und der Block bestätigt wird (Mining).[17] Die Information/Transaktion wird dadurch ziemlich fälschungssicher in der Kette gespeichert,[18] weil jedermann (öffentliche Blockchain) oder die ausgewählten Netzwerkteilnehmer (private Blockchain) die Kette jederzeit einsehen und mit der bei sich gespeicherten Kopie abgleichen kann.[19] Die Sicherheit resultiert auch daraus, dass die Blöcke durch ein kryptografisches Rätsel und einen Hashwert aneinander gekettet sind.[20] Der Hashwert berechnet sich dabei aus allen Informationen/Transaktionen, die in dem Block gespeichert werden sollen. Die gleiche Information wird immer den exakt gleichen Hashwert ergeben.[21] Der Hashwert kann daher als ihr Fingerabdruck bezeichnet werden.[22] Je mehr Blöcke nach einem Block folgen, desto fälschungssicherer wird die Information in diesem Block. Denn bei einer Änderung einer Information in diesem Block ändert sich dessen Hashwert. Dieser Hashwert ist aber auch im Folgeblock abgelegt, wo er sich ebenso ändert. Es ändert sich also zugleich die Information im Folgeblock und damit dessen eigener Hashwert usw. Soll die

17 Mining bezeichnet daher nicht nur den Prozess der Erzeugung neuer Kryptoassets, sondern auch den Vorgang der Bestätigung einer Transaktion, s. Piska/Völkel Blockchain/Völkel Rn. 1.49. Neben proof-of-work gibt es weitere Ausprägungen von Konsensmechanismen (zB proof-of-stake, delegated-proof-of-stake). Sie alle dienen dazu, im Netzwerk einen Konsens zu erzielen und sich gemeinsam auf eine identische Wahrheit und Version der Blockchain zu einigen. Rutz Blockchain S. 15 f.; Bolesch/Mitschele ZfgK 2016, 1125 (1126 f.).

18 D. Tapscott/A. Tapscott Blockchain-Revolution passim; Saive DuD 2018, 764; Forgó/Zöchling-Jud 20. ÖJT II/1/Forgó S. 285 (331, 335).

19 Die Qualifikation als private oder öffentliche Blockchain hängt davon ab, wie neue Teilnehmer aufgenommen werden, sowie davon, ob die Blockchain öffentlich oder ausschließlich für zugelassene Nutzer einsehbar ist, s. etwa Thießen ZfgK 2020, 706; Martini/Weinzierl NVwZ 2017, 1251 (1252).

20 Rasch nachvollziehbar dargestellt auf https://andersbrownworth.com/blockchain und https://youtu.be/_160oMzblY8.

21 Grundsätzlich ist es möglich, dass verschiedene Informationen den gleichen Hashwert erhalten. Praktisch ist es aber unmöglich bzw. ineffizient, dies bewusst zu erwirken, s. dazu Kaulartz CR 2016, 474 (475).

22 Der SHA256-Hash der Information „Wenn die Zahlung am Konto des Veräußerers in Höhe von 2 ether einlangt, dann versende das NFT „MCI Fortbildung rocks“ an den Erwerber.“ lautet etwa „2eac8b6b47fa604e34c04ddb90045bb9c0e60698a248792ec9befb1bf4eab228“. Ändert man die Gegenleistung auf 3 ether ändert sich der Hashwert auf: „d95590257baea1596053aba6a37217400b34cfe44ba6b587a8947de8686e5c45“. Nachprüfbar unter: https://andersbrownworth.com/blockchain/hash.

Kette nicht zerstört werden, setzt das folglich voraus, dass auch für alle der Änderung folgenden Blöcke neue Hashwerte berechnet und gemined werden. Weil die Blockchain aber bei allen Netzwerkteilnehmern distribuiert gespeichert ist, müsste auch eine erforderliche Anzahl weiterer Netzwerkteilnehmer bestätigen, dass die Kette mit den geänderten Hashwerten und Informationen die wahre Blockchain ist. Die Netzwerkteilnehmer haben aber ein immanentes Interesse daran, möglichst korrekt zu arbeiten.[23] Denn nur, wenn weitgehend berechtigte Informationen/Transaktionen bestätigt werden, wird das Vertrauen in das Netzwerk nachhaltig aufrechtzuerhalten sein. Das ist für die Netzwerkteilnehmer wünschenswert, weil sie selbst Informationen oder Vermögen (Stakes) über das Netzwerk halten.

Demnach könnte ein böswilliger Einzeltäter eine Information nur dann fälschen, wenn er unter anderem alle Blöcke ab der Änderung neu mined.[24] Die Kosten[25] für diese Mining-Tätigkeit überträfen recht schnell den Wert der möglichen Beute. Insgesamt wäre die Verfälschung sehr zeit- und kostenintensiv und daher wirtschaftlich unattraktiv, aber nicht unmöglich.[26]

B. Smart Contracts

Smart Contracts müssen nicht auf einer Blockchain laufen. Bereits in den 1990er Jahren beschreibt der amerikanische Jurist *Nick Szabo* den Smart Contract als „computerized transaction protocol that executes the terms of a contract."[27] Er zeichnet das Bild einer Maschine, die mit Regeln programmiert ist, welche auch einem Vertrag entspringen können.[28] Die Maschine

23 Kritisch zu Fehlfunktionen Thießen ZfgK 2018, 606 (608).

24 Dafür bräuchte er so viel Rechenleistung, wie zumindest 51 % des Netzwerks halten. Zusätzliche Sicherheitsmerkmale (Zeitstempel/Timestamps) verhindern, dass mit besonders leistungsstarken PCs die gesamte Kette in Sekunden gefälscht und nachgebildet werden kann. Die Bitcoin-Blockchain sieht dafür etwa vor, dass nur alle zehn Minuten ein neuer Block gemined werden kann. Das Bitcoin Lightning-Netzwerk ist eine Skalierungslösung außerhalb des Bitcoin-Hauptnetzwerks, um schnellere Transaktionsprozesse zu günstigeren Gebühren zu ermöglichen.

25 Dazu auch § 5 A..

26 Die Behauptungen der absoluten Fälschungssicherheit haben sich rasch relativiert. Zur Diskussion C. Paulus/Matzke CR 2017, 769 (771 Fn. 17, 18).

27 Szabo, Smart Contracts, 1994, http://www.fon.hum.uva.nl.

28 Szabo, Smart Contracts: Building Blocks, 1996, http://www.fon.hum.uva.nl: „A set of promises, specified in digital form, including protocols within which the parties perform on these promises."; Szabo, Public Networks, 1997, https://nakamotoinstitute.org.

sorge auch für die Erfüllung bzw. für die Überwachung der Erfüllung des vertraglich Vereinbarten.[29] Der gemeine Warenautomat, der Ware und Kaufpreis definiert und deren ordnungsgemäßen Austausch sicherstellt, sei die jedermann geläufige Grundstruktur eines Smart Contracts.[30]

Erst ab dem Jahr 2014 führt die Verbindung der Idee *Szabos* mit der Blockchain und DLT zu der Aufmerksamkeit, die Smart Contracts heute haben.[31] *Buterin* integrierte Smart Contracts damals in die Ethereum-Blockchain.[32] Auf Blockchains sollen Smart Contracts dezentral, günstiger und ohne (zentrale) Intermediäre automatisch abgeschlossen und ausgeführt werden können.[33] Damit hätten sie gegenüber dem genannten Warenautomaten einen entscheidenden Vorteil: Der Eigentümer beherrscht den Warenautomaten. Er kann den Automaten ausschalten, vom Netz nehmen oder leeren und so den weiteren Abschluss sowie die weitere Durchführung von Verträgen verhindern.[34] Smart Contracts on-chain können von den Vertragsparteien demgegenüber nicht[35] geändert oder angehalten werden, indem sie ihren Computer vom Netz nehmen.[36]

C. Programm- und Maschinencode

Extrahiert man den technischen Teil der Beschreibung *Szabos*, ist ein Smart Contract ein „computerized [...] protocol that executes [...] terms [...]" also ein computergestütztes Protokoll, das Bedingungen ausführt. Um von Computern verarbeitet werden zu können, müssen solche Protokolle in

29 Szabo, Smart Contracts, 1994, http://www.fon.hum.uva.nl.

30 Szabo, Public Networks, 1997, https://nakamotoinstitute.org.

31 Möslein ZHR 183 (2019), 254 (261).

32 Buterin, Ethereum, 2014, https://bitcoinmagazine.com. Buterin versteht Smart Contract als „cryptographic "boxes" that contain value and only unlock it if certain conditions are met", s. Buterin, Ethereum White Paper, 2014, http://blockchainlab.com.

33 Siehe nur Heckelmann NJW 2018, 504 (504 f.); Möslein ZHR 183 (2019), 254 (263); Hoffmann-Riem Digitale Transformation S. 45 f., 245; Hoffmann JSSI 2021, 1 (5); Savelyev ICTL 26 (2017), 116 (119 f.); Hanzl/Rubey GesRZ 2018, 102 (102 f.); Bolesch/Mitschele ZfgK 2016, 1125 (1128); Forgó/Zöchling-Jud 20. ÖJT II/1/Forgó S. 285 (344); Fries/Paal Smart Contracts/Finck S. 1 (7 f.); Fraunhofer-Institut, Whitepaper, 2018, https://www.iml.fraunhofer.de; Fries/Paal Smart Contracts/Matzke S. 99 (107 ff.).

34 Savelyev ICTL 26 (2017), 116 (129).

35 Technisch wäre es unter meist unwirtschaftlichen Kosten möglich. Siehe § 2 A.

36 Die meisten Smart Contracts laufen derzeit aber noch off-chain. Dazu § 5 A. und B.

Maschinencode[37] übersetzt sein. Auf Ethereum[38] muss der Smart Contract aus einer Aneinanderreihung von Nullen und Einsen bestehen, um für die Ethereum Virtual Machine lesbar zu sein.[39] Aus der Perspektive von Menschen entsteht damit eine sprachliche Barriere: Denn Nullen und Einsen sind für sie grundsätzlich nicht les- und formulierbar.[40] Menschen bedienen sich daher einer Programmiersprache für ihre Eingaben. Der Computer kann die in der Programmiersprache erzeugten Programmcodes mit einem Compiler[41] in Maschinencode – seine „Muttersprache" – übersetzen.[42] Bei bestimmten Programmiersprachen werden überdies Zwischenstufen, sogenannter Zwischencode, erzeugt. Für die Zwecke dieser Arbeit genügt es, die verständlichste Form des „Codes"[43] – den Programmcode – dem auf unterster Ebene erzeugten Maschinencode gegenüberzustellen.

Für die menschlichen Eingaben gibt es verschiedene Programmiersprachen, wie Solidity.[44] Ihnen ist gemeinsam, dass sie Menschen wie eine Fremdsprache erlernen müssen. Das versuchen verschiedenste Program-

37 Fries/Paal Smart Contracts/Erbguth S. 25 (28 f.).

38 Das ist die bekannteste Blockchain, die Smart Contracts ermöglicht, Kiffer/Levin/Mislove IMC 2018, 494 (494 f.); Wright/De Filippi SSRN 2015, 1 (12).

39 Hupel c't 2021, 136 (137); Fries/Paal Smart Contracts/Erbguth S. 25 (28 f.).

40 Fries/Paal Smart Contracts/Erbguth S. 25 (29). Assemblersprachen können recht nahe an die Formulierung eines Maschinencodes kommen. Theoretisch bestünde die (fehleranfällige) Möglichkeit für Menschen, dem dualen Maschinencode aus Nullen und Einsen wieder Buchstaben und Zahlen zuzuweisen.

41 Ein Compiler ist ein Programm, das symbolische Programmiersprachen der zweiten bis vierten Generation in Maschinencode übersetzt. Auch Assembler oder Interpreter dienen zur Übersetzung. Ein Assembler übersetzt mnemonische Programmzeilen in Maschinencodes. Interpreter übersetzen im Unterschied zu Compilern nicht den kompletten Code, sondern arbeiten zeilenweise die Instruktionen ab.

42 Hupel c't 2021, 136 (137).

43 Spricht die Arbeit undifferenziert von Code, treffen die Aussagen sowohl für Programmcode als auch für Maschinencode zu. Allgemein ist ein Code eine Vorschrift für die eindeutige Zuordnung von Zeichen eines Zeichenvorrats zu denen eines anderen Zeichenvorrats, https://brockhaus.at/ecs/enzy/article/code-informatik.

44 Siehe nur https://solidity.readthedocs.io/en/develop/. Die Programmiersprache Solidity wurde von Gavin Wood zur Erstellung von Smart Contracts ausgearbeitet und unter der Leitung von Christian Reitwiessner für Ethereum weiterentwickelt. Mit Auszug aus einem Smart Contract Code auf Ethereum Savelyev ICTL 26 (2017), 116 (125).

mier-Tutorials[45] und -Tools[46] zu erleichtern. Die Tendenz geht dahin, dass die Übersetzung menschlicher Sprache in eine Programmiersprache künftig maschinell übernommen werden wird. Diese Einschätzung lässt sich etwa mit dem EtherScripter[47] demonstrieren. Er erlaubt es, vorformulierte Codezeilen wie in einem Baukasten zusammenzufügen und mit Inhalten zu ergänzen. Während diese Codezeilen aufgrund ihrer Länge als Anhang zu dieser Arbeit abgedruckt sind, ist der Baukasten für einen ganz reduzierten Vertrag kurz darstellbar:

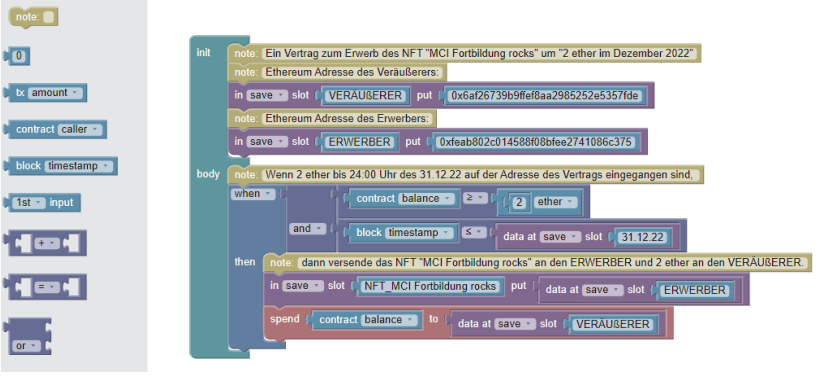


Abbildung eines Vertrags im EtherScripter; Eigenarbeit

Der „Code" hat gegenüber der menschlichen Sprache allerdings eine semantische Limitierung. Codierte Protokolle verlangen klare Wenn-Dann-Bedingungen.[48] Der Hauptteil des im Baukasten dargestellten Vertrags folgt daher auch einer „When-Then"-Logik: *Wenn* die Zahlung in Höhe von 2

45 Vgl. https://www.freecodecamp.org/; https://youtu.be/M576WGiDBdQ; https://codeburst.io/build-your-first-ethereum-smart-contract-with-solidity-tutorial-94171d6b1c4b.

46 Ethereum nutzt etwa nicht nur ein standardisiertes Application Binary Interface, das die Funktionen des Vertrags festlegt und bestimmt, wie Datenfelder der Transaktion codiert werden können. Es gibt auch DApps, die Codier-Aufgaben erledigen, ohne dass die Nutzer die Schwierigkeit dahinter bemerken. Siehe zu all dem Hupel c't 2021, 136 (137).

47 https://etherscripter.com/0-5-1/.

48 Etwa Linardatos Autonome Aktanten S. 39; Wilhelm WM 2020, 1807 (1810); Hanzl in Hanzl/Pelzmann/Schragl 263 (264); Hanzl/Rubey GesRZ 2018, 102 (103); Wilkens/Falk Smart Contracts S. 4; aA wohl Reusch Future Law Rn. 380 (Stand 1.7.2022, rdb.at).

Ether am 31.12.2022 am Konto des Vertrags ist, *dann* versende das dort abgelegte NFT[49] „MCI Fortbildung rocks" an den Erwerber. Der Eintritt oder Nichteintritt des Ereignisses muss überdies digital prüfbar (gemacht) sein. Soll die Ausführung eines Vertrags an analoge Ereignisse anknüpfen, braucht es daher zusätzliche Informationsschnittstellen (zB Sensoren eines IoT-Geräts).[50]

Eine weitere Limitierung liegt in der mangelnden Rückübersetzbarkeit: Decompiler können Maschinencode zwar grundsätzlich wieder in einen für Menschen lesbaren Programmcode bringen. Bereits beim Compiling werden aber Zusatzinformationen, die den Programmcode leichter verständlich machen, gestrichen, wenn sie die Maschine für die Ausführung der Wenn-Dann-Bedingung nicht braucht. Der Maschinencode ist daher auf das Nötigste reduziert. Die Rückübersetzung in einen Programmcode funktioniert also nur bedingt, weil sinngebende Zusatzinformationen verloren gegangen sind.[51] Offen ist, ob der technische Fortschritt auch diese Limitierungen in Zukunft beseitigen wird.

§ 3 Vertragsbegriff und Formfreiheit

§ 2 hat die technischen Grundlagen für Smart Contracts bereitet. Im Folgenden liegt der Fokus auf rechtlichen Aspekten. Ausgangspunkt ist dabei

49 Ein NFT (Non Fungible Token) ist ein auf einer Blockchain unter einer bestimmten Adresse gespeicherter Hashwert oder sonstiger Datensatz, der ein extern gespeichertes digitales Bild, ein Video oder jede andere Sache repräsentieren kann. Der Token ist einmalig und eindeutig identifizierbar (non fungible). Siehe dazu Kogler JBl 2021, 685 (687); Kucsko/Pabst/Tipotsch/Tyrybon ecolex 2021, 495 (496 f.); Fasching/Bernsteiner RdW 2022, 234; Kodek Zak 2022, 24. Traditionshäuser sind mittlerweile Akteure auf den Märkten für NFT. Zum Valentinstag im Jahr 2022 verkaufte das Belvedere 10.000 NFT aus einer hochaufgelösten digitalen Kopie von Gustav Klimts „Kuss", https://www.belvedere.at/digitale-liebeserklaerung; Stadler/Bichler, 2022, https://www.derstandard.at/.

50 Das Internet der Dinge (IoT) ist die Vernetzung verschiedener Geräte über das Internet. So können die Geräte bzw. deren Software angesprochen und etwa mit Befehlen wie „Entriegeln" oder „nicht starten" versorgt werden. Gemeinsam mit Smart Contracts erlaubt dies die Verzahnung von digitaler und analoger Welt. Siehe Forgó/Zöchling-Jud 20. ÖJT II/1/Zöchling-Jud S. 273; Mandl immolex 2019, 200; vgl. auch Heckelmann NJW 2018, 504 (504); Wilhelm WM 2020, 1807 (1809). Die USA haben für die Erhöhung der Sicherheit dieser Anwendungen einen eigenen Act in Kraft gesetzt, s. IoT Cybersecurity Improvement Act of 2020, Public Law No: 116–207 (12/04/2020), https://www.congress.gov/bill/116th-congress/house-bill/1668.

51 Fries/Paal Smart Contracts/Erbguth S. 25 (29).

ein Anwendungsbeispiel, auf das im weiteren Verlauf der Arbeit zurückzukommen sein wird (Abschnitt A.). Sodann wird ein Blick auf den Begriff „Smart Contract" geworfen. Zu prüfen ist, ob es einer begrifflichen Konkretisierung bedarf (Abschnitt B.). Abschnitt C. beschäftigt sich mit der Frage, wie sich Smart Contracts zum Grundsatz der Formfreiheit verhalten.

A. Anwendungsbeispiel

Ein Künstler verkauft seine NFT laut Angabe auf seiner Webseite nur an unternehmerische Käufer. Er veröffentlicht dafür auf seiner Webseite Programmcodes, mit denen er jeweils derjenigen Bieterin ein verbindliches Verkaufsangebot macht, die bis zum Tag X das höchste Annahmegebot in EUR abgibt.[52]

Die Eingabemaske für Gebote verlangt neben der Höhe des Gebots auch eine Mail-Adresse, eine UID und eine qualifizierte elektronische Signatur der berechtigten Person. Der Code gleicht die Daten aus der Signatur mit öffentlich zugänglichen Informationen über die geschäftsführungsbefugte Person ab[53] und überprüft die Validität der UID.[54] Das aktuelle Höchstgebot einer zugelassenen Bieterin wird laufend angezeigt. Am Tag X sendet der Code an die Höchstbieterin eine Information über den Abschluss des Kaufvertrags samt Aufforderung zur Zahlung binnen sieben Tagen an die angegebene IBAN.

Der Leistungsaustausch kann unterschiedlich geregelt sein, ist für die Frage, ob ein Vertrag zustande kommt, aber grundsätzlich nicht relevant.

52 Allgemein zum Verkaufsangebot auf Plattformen wie eBay OGH 4 Ob 135/07t, ecolex 2007/388 (Anderl); Pfeffer/Rauter HdB Kunstrecht/Leopold Rn. 16.10 f. (Stand 15.1.2020).

53 Mit einem Web Crawler können Inhalten im Internet gesucht werden.

54 Nach dem Unternehmerbegriff des § 2 UStG und dessen Auslegung in den UStR 2000 Rn. 181 ist ein Unternehmer „jede natürliche Person und jedes Wirtschaftsgebilde…, das nachhaltig, selbstständig gegen Entgelt Leistungen erbringt und nach außen hin in Erscheinung tritt". Wer unter Angabe einer UID ein Geschäft abschließt, den darf der Erklärungsempfänger grundsätzlich auch zivilrechtlich als Unternehmer einstufen. Handelte tatsächlich ein Verbraucher, der unter Nutzung einer fremden UID nur vorgibt, Unternehmer zu sein, kommt das KSchG zur Anwendung, aber der Unternehmer kann den Vertrag anfechten oder den Verbraucher wegen culpa in contrahendo belangen (Schwimann/Kodek/Apathy/Frössel ABGB § 1 KSchG Rn. 2; Rummel/Krejci ABGB §1 KSchG Rn. 27 (Stand 1.1.2002, rdb.at)). Die Software kann den Namen der Bieterin auf Übereinstimmung mit einer validen UID digital abgleichen, s. etwa https://finanzrechner.at/uid-nummer-pruefen; https://ec.europa.eu/taxation_customs/vies/#/vat-validation.

Es kann etwa vorgesehen sein, dass der Code den Downloadlink für NFT und Berechtigungszertifikat ab Tag X nur unter Setzen der Signatur der Höchstbieterin entsperrt, wenn er überdies die Information erhält, dass das Höchstgebot am Konto des Künstlers eingezahlt ist. Ist der Zahlungseingang vierzehn Tage nach Tag X noch immer nicht bestätigt, kann der Code vorsehen, dass der Künstler das NFT unter Setzung seiner Signatur wieder in seine Galerie aufnehmen kann.

Der Künstler verkauft auch über eine Plattform. Dort wird aber nicht der Programmcode veröffentlicht. Dieser bleibt im Hintergrund. Auf der Plattform erfolgt die Verkaufsmitteilung: „Heute für [NFT-Abbildung] *hier* mitbieten." Mit dem Klick auf *hier* gelangt man zu einer Eingabemaske, die alle Abfragen (Höchstgebot, Mail-Adresse, UID, Signatur) in deutscher Sprache macht.

B. Begriffskonkretisierung

Es gibt für Smart Contracts kein einheitliches oder gar anerkanntes Begriffsverständnis.[55] Die Rechtsliteratur stößt sich aber beinahe ausnahmslos an der Begriffswahl.[56]

Die Kritik am Begriffsteil „Smart" ist insofern vernachlässigbar, als nur klarzustellen ist, dass kein zwingender Konnex zu KI besteht.[57] Ansonsten sind Smart Contracts „nur" so smart wie ihre Nutzer. Das betrifft nicht nur ihre Ausgestaltung, sondern bereits die Entscheidung, ob der Einsatz eines

55 Mit einem eigenen Kapitel zu Definitionsversuchen etwa Braegelmann/Kaulartz Smart Contracts/Braegelmann/Kaulartz S. 1 (4 ff.); Kaulartz/Heckmann CR 2016, 618 (618 f.); Smets/Kapeller ÖJZ 2018, 293; Thiele 20. ÖJT II/2 201 (202); Müller/Seiler AJP/PJA 2017, 317 (318); Linardatos Autonome Aktanten S. 38 f.; Diedrich Ethereum S. 166 ff.

56 Buchleitner/Th. Rabl ecolex 2017, 4 (6); Th. Rabl ecolex 2019, 214 bezeichnet sie als „äußerst stupide (und gar nicht smart)"; Fries/Paal Smart Contracts/Finck S. 1 (7 f.); Thiele 20. ÖJT II/2 201 (202); Levy ESTS 2017, 1; Kaulartz/Heckmann CR 2016, 618 (618 ff.); Forgó/Zöchling-Jud 20. ÖJT II/1/Forgó S. 285 (342).

57 Forgó/Zöchling-Jud 20. ÖJT II/1/Forgó S. 285 (342); Kaulartz/Heckmann CR 2016, 618 (618 f.). Es ist mE naheliegend, dass die derzeit zur Programmierung von Smart Contracts eingesetzten Tools und Smart Contracts selbst künftig mit KI-Anwendungen verbunden werden; vgl. auch Möslein ZHR 183 (2019), 254 (273). Es gibt derzeit mehrere Ansätze, KI zu definieren, s. Linardatos Autonome Aktanten S. 48 ff. Der Vorschlag für eine Verordnung zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) COM(2021) 206 final, ist seit April 2021 veröffentlicht. Der Vorschlag enthält in Art. 3 eine auffallend allgemein und weit gefasste, also zukunftsoffene Legaldefinition für KI.

Smart Contracts überhaupt vorteilhaft ist. In bestimmten Bereichen ist das leichter zu bejahen als in anderen. Denn Smart Contracts unterscheiden sich in verschiedenen Bereichen von „herkömmlichen" Verträgen, etwa im Hinblick auf die Flexibilität: Vertragliche Beziehungen sind oft (notwendigerweise) unvollständig. Für diese Fälle enthält das ABGB mit den §§ 914 ff. ABGB eigene Instrumente der Auslegung und Lückenfüllung. Smart Contracts führen demgegenüber ungeachtet dessen, welche Ergebnisse die Auslegung hervorbringt, die codierte Wenn-Dann-Bedingung durch. Der Einsatz eines Smart Contracts kann also smart sein, muss es aber nicht, wenn die gewünschte Flexibilität im Code nicht abgebildet werden kann.

Spannender ist die Auseinandersetzung mit dem Begriffsteil „Contract". Manche bezeichnen jedes computergestützte Protokoll, das bestimmte Bedingungen festhält und gegebenenfalls bei Bedingungseintritt durchführt,[58] als Smart Contract. Andere lehnen die Möglichkeit eines Vertrags ganz ab.[59] Ein Grund für den fehlenden Konsens über den Begriffsinhalt von Smart Contracts liegt wohl darin, dass die verschiedenen Akteure in der Diskussion unterschiedliches wollen: Die technischen und innovationsgeleiteten Akteure wollen dem Begriff möglichst viele Ideen und Anwendungsfelder subsumieren. Demgegenüber sind die rechtlichen Akteure zugunsten einer korrekten rechtlichen Einordnung daran interessiert, möglichst präzise festzuhalten, um was es geht. Die vorliegende Arbeit geht davon aus, dass etwas entweder ein Vertrag ist oder nicht. Ein „bisschen" Vertrag oder einen „unechten"[60] Vertrag gibt es als rechtliche Kategorie nicht.[61] Auch die Technik sollte sich des Begriffs „Vertrag" daher nur dann bedienen, wenn von einem Vertrag im Rechtssinne gesprochen wird. In der Überzeugung, dass Präzision mehr Rechtssicherheit bringt, wird hier eine Zweiteilung

58 Etwa Diedrich Ethereum S. 3.

59 Pauschal dazu, dass Smart Contracts keine Verträge sind, etwa Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 861 Rn. 16/1 (Stand 2.1.2022); vgl. auch D. Paulus/Matzke ZfPW 2018, 431 (464 f.); Lindner NZM 2021, 665 (667); Djazayeri jurisPR-BKR 12/2016 Anm. 1 bei Fn. 21; Mann NZG 2017, 1014 (1016).

60 Ein unechter Vertrag zugunsten Dritter ist im ABGB nicht vorgesehen. Die obige Begriffswahl damit zu rechtfertigen, wäre also ein Zirkelschluss. Außerdem ist er ein Vertrag. Das „unecht" bezieht sich auf die Qualität der Rechtsstellung des Dritten.

61 Siehe demgegenüber die Begriffe wie „unsmarte", „echte", „unechte", „transacting" oder „selfacting" Smart Contracts, Smart „legal" Contract oder „Smartest Contract", etwa bei Hanzl HdB Blockchain S. 43 ff.; Anderl Blockchain Rechtspraxis/Anderl/Aigner/Schelling S. 78 (79); Smets/Kapeller ÖJZ 2018, 293 (294); Hanzl ÖJZ 2019, 293 (293); Hanzl/Rubey Zak 2018, 184 (184); Hanzl/Rubey Zak 2018, 127 (127); Buchleitner/Th. Rabl ecolex 2017, 4 (7); Pittl/Gottardis immolex 2019, 194 (195 ff.).

vorgeschlagen: Es sollte zwischen Smart Contracts und Smart Forms unterschieden werden.

Das computergestützte Protokoll – also der Code – dient wie die herkömmliche Schrift dazu, etwas festzuhalten. Sowohl in herkömmlicher als auch in smarter Form kann das Festgehaltene zu einem Vertrag verbunden sein oder eben nicht. Der enge Begriff Smart Contract sollte nur für ersteren Fall eingesetzt werden. Ein Smart Contract liegt folglich nur vor, wenn die Parteien ihren Vertrag in Maschinen- oder Programmcode verfassen. Die These, dass dies de lege lata möglich ist, gilt es zu prüfen.[62]

Um darüber hinaus gehende vertragsrechtliche Anwendungsfelder für Codes erfassen zu können, scheint der Sammelbegriff „Smart Form" besser geeignet. Er ist insofern ein Kompromiss, als es möglich wäre, das jeweils Gemeinte genau(er) zu bezeichnen. Er vermeidet aber eine unnötige Begriffsflut und weist zugleich präzise auf die Neuerung hin: Neu ist nicht die Willenserklärung, die Vertragsklausel, die Bedingung, die Möglichkeit, sich für den Vertragsabschluss eines Musters oder Formulars zu bedienen. Neu ist, dass diese in Gestalt – der „Form" – von Maschinen- und Programmcodes verfasst oder übersetzt sein können. Die Codes sollen rechtliche Inhalte nicht nur darstellen, sondern ihren Inhalt überdies bewirken können. Dieser Inhalt kann von der Abgabe einer Erklärung zum Vertragsabschluss bis zum (teilweisen) Leistungsaustausch reichen.

Abstrakt führt das zu folgendem Begriffsverständnis: Ein Smart Contract ist ein Vertrag, der in Maschinen- oder Programmcode verfasst ist. Demgegenüber liegt eine Smart Form bereits dann vor, wenn Maschinen- oder Programmcodes irgendwie beim Abschluss oder der Durchführung eines Vertrags (ungeachtet dessen traditioneller oder codebasierter Form) unterstützen sollen. Die Codes können in beiden Fällen die codierten Vorgaben kontrollieren (*wenn*) und durchführen (*dann*), sie können da wie dort mit einer Blockchain verbunden sein oder nicht. Nicht jede Smart Form ist daher ein Vertrag, also ein Smart Contract. Umgekehrt ist ein Smart Contract immer eine Smart Form, weil seine Teilelemente Smart Forms sind.

In dem Anwendungsbeispiel werden über die Webseite des Künstlers folglich Smart Contracts abgeschlossen, weil die Vertragsgrundlage in Programmcode besteht.[63] Für die Erwerber über die Plattform mag die Ver-

62 Siehe dazu § 4.

63 Im Folgenden ist erst zu prüfen, ob das rechtlich möglich ist.

kaufsmitteilung, die Abbildung und danach die Freischaltung des Downloads im Hintergrund über Smart Forms gesteuert sein. Zur Vertragsgrundlage werden sie aber nicht.[64]

C. Grundsatz der Formfreiheit

Rechtssubjekte können im Rahmen ihrer verfassungsrechtlich geschützten[65] Privatautonomie selbstbestimmt und selbstverantwortlich Verträge schließen.[66] Teil dieser Vertragsfreiheit ist die Formfreiheit: Die Vertragsparteien können frei wählen, welche Form ihr Vertrag aufweisen soll. Das legt die Vermutung nahe, dass Verträge auch in Programm- und Maschinencode geschlossen werden können. Zweifeln lässt aber ein Blick auf § 883 ABGB: Diese Norm, die als Grundlage der Formfreiheit gesehen wird,[67] ist nämlich taxativ formuliert. Es gilt daher die Bedeutung dieser Regelung zu prüfen (Abschnitt I.) und ihre Rolle für den Vertragsschluss in Programm- und Maschinencode auszuloten (Abschnitt II.). Bestehen gesetzliche oder vertragliche Formpflichten, interessiert überdies, ob Smart Contracts diesen Anforderungen gerecht werden (Abschnitt III.).

I. Die Bedeutung des § 883 ABGB

1. Einfache Auslegung

§ 883 ABGB lautet seit der Urfassung wie folgt: „Ein Vertrag kann mündlich oder schriftlich; vor Gerichte oder außerhalb desselben; mit oder ohne Zeugen errichtet werden. Diese Verschiedenheit der Form macht, außer den im Gesetze bestimmten Fällen, in Ansehung der Verbindlichkeit keinen Unterschied." Mit Blick auf diesen Wortlaut ist unklar, ob die Norm auch in Programm- bzw. Maschinencode verfasste Smart Contracts erfasst.[68]

64 Näher dazu bei § 5 C. I.

65 Siehe etwa VfGH G 1395/95, VfSlg 14.503; VfGH G 139/88, VfSlg 12.227; Griller ZfV 1983, 109 (115).

66 F. Bydlinski Privatautonomie S. 114 ff.; F. Bydlinski System und Prinzipien S. 147 ff.; Möslein Dispositives Recht S. 47.

67 III. TN 78 BlgHH 144; OGH 2 Ob 535/93, ecolex 1994, 27; KBB/P. Bydlinski § 883 Rn. 1; Kletečka/Schauer/Kalss ABGB-ON[1.06] § 883 Rn. 1 (Stand 1.8.2022).

68 So ohne weiteres Smets/Kapeller ÖJZ 2018, 293 (294); Hanzl/Rubey Zak 2018, 184 (184); Anderl Blockchain Rechtspraxis/Anderl/Aigner/Schelling S. 78 (80). Hingegen

Denn sie nennt (nur) die Schriftlichkeit und die Mündlichkeit, sowie die Errichtung vor Gericht und vor Zeugen. Satz 2 bezieht sich wörtlich nur auf „diese" in Satz 1 genannten Formen.[69]

„Vor Gericht" oder „vor Zeugen" können jeweils zugleich die Kriterien der Mündlichkeit oder der Schriftlichkeit erfüllt sein.[70] Es wäre daher denkbar, dass der Gesetzgeber alle weiteren erdenklichen Formen immer (zumindest auch) entweder als mündliche oder schriftliche Form verstanden wissen will. Dafür ist ein Blick auf den Sprachgebrauch rund um 1800 aufschlussreich: § 884 ABGB hält in der Stammfassung[71] fest, dass Parteien, die sich zu einem schriftlichen Vertrag verabredet haben, vor der Unterschrift noch keinen Vertrag geschlossen haben. Dieses Verständnis der Schriftlichkeit im Sinne von Unterschriftlichkeit hat das ABGB beibehalten.[72] Die in diesem Zeitraum jedenfalls bereits tatsächlich bestehende und dem Gesetzgeber des ABGB bekannte Errichtung einer schriftlichen Urkunde ohne Unterschrift (Textform), ist damit weder schriftlich noch mündlich im Sinne des § 883 ABGB. Nach § 863 ABGB[73] kann der Wille nicht nur ausdrücklich durch Worte und allgemein angenommene Zeichen, sondern auch stillschweigend durch solche Handlungen erklärt werden, welche mit Überlegung aller Umstände keinen vernünftigen Grund, daran zu zweifeln, übrig lassen. Die Konkludenz[74] ist jedenfalls weniger als die Mündlichkeit iSd § 883 ABGB. Zwar liegen manche allgemein angenommenen Zeichen nahe an der Mündlichkeit. Nach dem Sprachgebrauch sind aber auch sie nicht mündlich. Das belegen für die Zeit um 1800 die Ausfüh-

unter Berufung auf die (weitere) Vertragsfreiheit Forgó/Zöchling-Jud 20. ÖJT II/1/Forgó S. 285 (343); Knoll ZIIR 2016, 406 (409). § 125 BGB ist seinem Wortlaut nach nicht mit § 883 ABGB zu vergleichen. Zum BGB vgl. Möslein ZHR 183 (2019), 254 (267 mwN); Kaulartz DSRITB 2016, 1023 (1029).

69 Arg: „*Diese* Verschiedenheit der Form…" (Hervorhebung durch die Verfasserin).

70 So muss etwa das gerichtliche Protokoll nach Maßgabe des § 209 Abs. 3 ZPO (auch) von den Parteien unterschrieben werden. Vergleiche auch § 581 ABGB.

71 JGS 1811/946.

72 Siehe § 886 Satz 1 ABGB idgF. Zu Abweichungen in Sondergesetzen vgl. etwa Schwimann/Kodek/Riedler ABGB § 886 Rn. 1.

73 JGS 1811/946 zuletzt geändert durch RGBl. 1916/69; Ofner Ur-Entwurf II S. 8 § 7.

74 Die Konkludenz unterscheidet sich von den allgemein angenommenen Zeichen insbesondere dadurch, dass bei letzteren typische Erklärungszeichen verwendet werden. Diese haben „an und für sich (ohne Bedachtnehmung auf die besonderen Umstände) ihre bestimmte Bedeutung", v. Zeiller Commentar III/1 § 863 Anm. 1. Bei der Konkludenz sind die Zeichen demgegenüber weniger allgemein angenommen und daher die Begleitumstände der Handlung bedeutsamer, v. Zeiller Commentar III/1 § 863 Anm. 2.

rungen *v. Zeillers*:[75] „Man erklärt seinen Willen ausdrücklich durch Worte (mündlich oder schriftlich), oder durch andere allgemein angenommene Zeichen". § 863 ABGB kennt daher mit den allgemein angenommenen Zeichen und der Konkludenz gleich zwei weitere Formen, die weder schriftlich noch mündlich sind.

Damit waren zum Zeitpunkt der Schaffung des § 883 ABGB jedenfalls allgemein angenommene Zeichen, die konkludente Erklärung sowie die Textform bekannt. Dennoch nennt sie die Norm nicht. Dasselbe gilt im Hinblick auf die im Jahr 1871 mit dem NotAktsG eingeführte und damit zum Zeitpunkt der III. Teilnovelle des ABGB, mit der unter anderem das Rechtsgeschäftsrecht überarbeitet wurde, bereits bekannte Notariatsaktform.[76] Die Gesetzessystematik zeigt daher, dass die Aufzählung des § 883 ABGB entgegen dem Wortlaut[77] nicht abschließend hätte sein sollen.

Dagegen könnte eingewendet werden, dass Zeichen und die Konkludenz nicht genannt seien, weil sie von weiteren Umständen abhängig sind und sich insofern in ihrer Verbindlichkeit von der Mündlichkeit und Schriftlichkeit unterscheiden: Eine Erklärung kann nur mit *allgemein angenommenen* Zeichen, wie dem Kopfnicken,[78] abgegeben werden. Die Konkludenz genügt nur dort, wo *kein vernünftiger Grund, daran zu zweifeln, übrig* bleibt.[79] Dieser Einwand trägt aber schon deshalb nicht, weil er die Nichtnennung der Textform nicht erklären kann. Überdies ist es jeglicher Form inhärent, dass sie nicht erfüllt ist, wenn ihre vom Gesetz bestimmten Tatbestandsmerkmale nicht erreicht sind. Aus § 883 ABGB folgt also nicht e contrario, dass die Konkludenz in Ansehung ihrer Verbindlichkeit einen Unterschied mache. Vielmehr bestimmt der Gesetzgeber mit § 863 ABGB

75 Siehe v. Zeiller Commentar III/1 § 863 Anm. 1.

76 Bereits § 4 Notariatsordnung, RGBl. 1850/366 legte transitorisch (vom 1.8.1851 bis 16.12.1852) und territorial beschränkt notariatsaktspflichtige Geschäfte fest. Der Notariatsakt wäre zumindest insofern eine neue Form gewesen, als er nicht nur außergerichtliche und schriftliche Form, sondern öffentliche Urkunde mit besonderer Aufklärung ist (§§ 1 f. NO). Wo das Gesetz einen Notariatsakt verlangt, genügt die bloße Schriftform jedenfalls nicht. Dennoch scheint der Gesetzgeber den Notariatsakt als außergerichtliche und/oder schriftliche Form grundsätzlich miterfasst zu sehen. Vergleiche dazu auch § 577 ABGB iVm § 583 ABGB.

77 Zur Grenze des äußerst möglichen Wortsinns s. Fenyves/Kerschner/Vonkilch/Kerschner/Kehrer ABGB §§ 6, 7 Rn. 23 mwN; Kramer Methodenlehre, Aufl. 5, S. 65 f.; Kletečka/Schauer/Schauer ABGB-ON[1.02] § 6 Rn. 4, 25 (Stand 1.3.2017); KBB/P. Bydlinski § 6 Rn. 3.

78 Siehe v. Zeiller Commentar III/1 § 863 Anm. 1 f.

79 Kletečka/Schauer/Wiebe ABGB-ON[1.05] § 863 Rn. 17 ff. (Stand 2.1.2022).

lediglich, dass diese Form eine gewisse Qualität haben muss. Ist diese Qualität erreicht, bindet sie.

Für das Verständnis des § 883 ABGB kann ein Größenschluss fruchtbar gemacht werden:[80] Wenn schon die Mündlichkeit der Form eines Vertrags genügt,[81] dann muss ihr erst recht eine strengere Form genügen. Die handschriftliche Textform, also die Errichtung einer handschriftlichen Urkunde ohne Unterschrift, ist daher von § 883 ABGB erfasst: Sie ist zwar weder unterschriftlich noch mündlich, sie ist aber im Hinblick auf die Form zumindest ebenso viel wie mündlich. Denn die Graphologie ermöglicht Rückschlüsse von der Handschrift auf die Person des Verfassers. Lässt das Gesetz also die Mündlichkeit ausreichen, genügt erst recht die handschriftliche Textform. Die Richtigkeit dieses Größenschlusses bestätigt ein Blick auf § 886 Satz 2 ABGB, nach dem die Schriftform durch die strengere gerichtliche oder notarielle Beurkundung ersetzt werden kann.[82] Demgegenüber ist die elektronische Textform heute kaum mehr als die Mündlichkeit, weil jedermann einen Text tippen und danach behaupten kann, er stamme von einer anderen Person.

2. Rechtsfortbildung

Formen, die nur gleichwertig schützen wie die Mündlichkeit, können § 883 ABGB durch einfache Auslegung nicht subsumiert werden. § 883 ABGB könnte für solche Formen daher allenfalls im Wege der Rechtsfortbildung[83] gelten.

Die Materialien zum Ur-Entwurf von § 883 und § 863 ABGB sind im Hinblick auf die Form kurz und wenig aussagekräftig.[84] Nach der authentischen Interpretation *v. Zeillers* sollte den Bürgern volle Freiheit bei der

80 Der Größenschluss wird zurecht unter bestimmten Umständen als eine Methode der einfachen Auslegung verstanden, s. Fenyves/Kerschner/Vonkilch/Kerschner/Kehrer ABGB §§ 6, 7 Rn. 85.

81 Für Normen, die eine bestimmte Form verlangen, ist überdies der Zweck der Formpflicht zu berücksichtigen.

82 Zutreffend wurde daraus für Formpflichten der allgemeine Grundsatz abgeleitet, dass die strengere Form die einfachere ersetzen kann. Siehe Kletečka/Schauer/Kalss ABGB-ON[1.06] § 883 Rn. 9 (Stand 1.8.2022); Rummel/Lukas/Dullinger ABGB § 886 Rn. 11 (Stand 1.11.2014).

83 Fenyves/Kerschner/Vonkilch/Kerschner/Kehrer ABGB §§ 6, 7 Rn. 40 ff.

84 Ofner Ur-Entwurf II S. 8 § 7 sowie 17 § 26. In der Revision und Superrevision des Gesetzbuches wurden die beiden Bestimmungen nicht mehr gesondert behandelt.

Frage belassen werden, in welcher Form sie ihre Verträge schließen.[85] Das indiziert, dass § 883 ABGB planwidrig zu eng geraten ist. Auch die III. Teilnovelle bestätigt dieses Verständnis: Der Gesetzgeber betont, dass trotz der Neigung, für gewisse wichtige Geschäfte Formpflichten vorzugeben, der Grundsatz der Formfreiheit gewahrt bleibe.[86] Dieses Anliegen zeigt er auch dadurch, dass er § 884 ABGB weiter gefasst hat:[87] Dort ist fortan nicht mehr von „Schriftlichkeit",[88] sondern allgemein von „einer bestimmten Form" die Rede, da die Schriftlichkeit nicht die einzige gewillkürte Form sei.[89] Die Änderung des Wortlauts beruht damit auf dem Umstand, dass der Gesetzgeber diesen selbst als zu eng auffasste. § 884 ABGB sollte möglichst weit gefasst werden.[90]

Diese Äußerungen des Gesetzgebers sowie die gesetzlichen Anpassungen zeigen, dass (der durch die III. Teilnovelle unveränderte) § 883 ABGB planwidrig formuliert ist. Vor dem Hintergrund, dass die Norm einen Freiheitsgrundsatz festhalten will, ihrem Wortlaut nach aber zum Gegenteil – dessen Eingrenzung – führt, ist sie rechtsfortbildend zu korrigieren. Methodisch erfolgt dies nicht im Wege der Analogie, sondern im Wege der teleologischen Reduktion.[91] Der Gesetzgeber hat mehr geregelt, als er regeln wollte. Die Aufzählung der Formen in Satz 1 ist missglückt. Satz 2 ist nicht als „Diese Verschiedenheit der Form", sondern als „Die Verschiedenheit der Form" zu lesen. So verhilft die Rechtsfortbildung auch zu einem verfassungskonformen Ergebnis. Denn der enge Wortlaut des § 883 ABGB beschränkt die verfassungsrechtlich gewährleistete Privatautonomie, ohne ein Ziel im öffentlichen Interesse auf geeignete, erforderliche und adäquate Art zu verfolgen. Der Vertragsfreiheit steht im hier interessierenden Fall

85 Siehe v. Zeiller Commentar III/1 § 883 Anm. 4.
86 III. TN 78 BlgHH 144.
87 JGS 1811/946 zuletzt geändert durch RGBl. 1916/69.
88 Satz 1 lautete in der Fassung JGS 1811/946 „Haben sich die Parteien ausdrücklich zu einem schriftlichen Vertrage verabredet, so wird er vor der Unterschrift der Parteien nicht für geschlossen angesehen."
89 III. TN 78 BlgHH 144.
90 III. TN 3 BlgHH 130.
91 Die teleologische Reduktion hilft dem Freiheitsgrundsatz gegen einen überschießend weiten Gesetzeswortlaut zum Durchbruch. Vgl. dazu Kramer Methodenlehre, Aufl. 5, S. 233; Fenyves/Kerschner/Vonkilch/Kerschner/Kehrer ABGB §§ 6, 7 Rn. 69. Es fehlt aber nicht wie üblich eine Ausnahmeregelung (RIS-Justiz RS0008979). Methodisch wäre die Rolle der Analogie und der teleologischen Reduktion für Normen, die Freiheitsgrundsätze festhalten, zu untersuchen. Dafür ist im Rahmen dieser Arbeit kein Raum.

auch kein anderes vertragsrechtliches Rechtsprinzip[92] (insbesondere der Vertrauens- und Verkehrsschutz) gegenüber, das eine Einschränkung rechtfertigen würde. Völlig zu Recht wird der Grundsatz der Formfreiheit daher unstrittig weit verstanden.[93] De lege ferenda sollte der Gesetzgeber den ersten Satz des § 883 ABGB streichen und im zweiten Satz „Diese Verschiedenheit der Form" durch „Die Verschiedenheit der Form" ersetzen.

II. Smart Contracts bei Formfreiheit

Programm- und Maschinencodes sind als solche (also ohne Zusätze) weder mündlich noch unterschriftlich. Mit den vorherigen Abschnitten ist aber die Grundlage für die Aussage gelegt, dass ihr Einsatz aus Gründen der Form jedenfalls dann unproblematisch ist, wenn keine gesetzlichen oder vertraglichen Formpflichten bestehen.[94]

Für den Maschinencode ist zu ergänzen, dass das Abgefasste aus Formgesichtspunkten nicht lesbar sein muss. Denn zum einen ist es für Formfragen irrelevant, ob die Erklärungen unwiederbringlich sind. Das zeigt gerade der gesetzlich geregelte Fall der mündlichen Erklärung. Zum anderen werden keine Formfragen berührt, wenn die Parteien ihre Eingaben machen und aus der Hand geben, um sie von einem Compiler übersetzen zu lassen. Passieren „Übersetzungsfehler", geht es nicht um Formfragen, sondern vielmehr um das Willenselement.[95] Für ein Verständnis des Maschinencodes als Form reicht es im Ergebnis bereits aus, dass dieser nicht formlos ist. Das wäre nur der Fall, wenn sich ein im Maschinencode geäußerter Wille gar nicht nach außen manifestiert. Da die Erklärung in Nullen und Einsen Reaktionen im Computer auslöst, liegt eine solche Manifestation aber vor.

92 Zu den Rechtsprinzipien des Vertragsrechts s. F. Hartlieb Verbandsvertragsrecht S. 48.

93 Siehe § 17 ABGB; statt aller Klang/Gschnitzer ABGB IV/1² § 883 S. 246. Siehe auch die zutreffende Rechtsprechung, wonach bei Zweifeln über das Bestehen einer Formvorschrift zugunsten der Formfreiheit zu entscheiden ist, OGH 5 Ob 124/92, JBl 1993, 312; OGH 2 Ob 535/93, ecolex 1994, 27.

94 Im Ergebnis für Programmiersprachen ebenso Hanzl/Rubey Zak 2018, 184 (184); Smets/Kapeller ÖJZ 2018, 293 (294); Anderl Blockchain Rechtspraxis Anderl/Aigner/Schelling S. 78 (80); Knoll ZIIR 2016, 406 (409); vgl. auch Heckelmann NJW 2018, 504 (506 f.).

95 Näher zum Maschinencode § 2 C. Zum Willen § 4 A. III.

III. Smart Contracts bei Formpflicht

Zu untersuchen ist überdies, ob Programmcode (Abschnitt 1.) oder Maschinencode (Abschnitt 2.) gesetzlichen oder vertraglichen Formpflichten entsprechen kann. Das hängt von der Erfüllung zweier Kriterien ab: Einerseits müssen sie die objektiven Merkmale der Form aufweisen (i), andererseits müssen sie dem Zweck der Formpflicht nachkommen können (ii).[96]

1. Programmcode

Programmcode kann die objektiven Merkmale der Textform iSd § 13 Abs. 2 AktG aufweisen (i): Denn er besteht aus Schriftzeichen, er kann die Person des Erklärenden nennen, am Ende die Namensunterschrift nachbilden bzw. erkennbar machen und auf eine Weise abgelegt werden, die zur dauerhaften Wiedergabe geeignet ist. Programmcode genügt im AktG[97] folglich der Textform, sofern der Zweck der Formanordnung nicht dagegen spricht (ii). Die Textform etwa in § 10a AktG[98] oder in § 61 Abs. 2 AktG[99] soll die dort geschilderten Akte nachweislich bestätigen. Diesen Zweck kann auch Programmcode erfüllen. An anderen Stellen bedarf es der Textform, weil Informationspflichten erfüllt werden müssen.[100] So sind etwa Führungskräfte bestimmter börsenotierter Gesellschaften über das in Art. 19 Abs. 11 MAR geregelte Handelsverbot schriftlich aufzuklären.[101] Diesem Formzweck wird

96 Zur Unentbehrlichkeit der Berücksichtigung des Formzwecks OGH 2 Ob 535/93, ecolex 1994, 27.

97 Nach den Materialien soll der Anwendungsbereich des § 13 Abs. 2 AktG auf das AktG beschränkt bleiben. Die Definition ist damit zumindest nicht im Analogieweg verallgemeinerbar. Siehe ErläutRV 208 BlgNR 24. GP 9. Liegen die genannten Kriterien vor, wird die Textform, soweit überblickbar, aber häufig erreicht sein. Siehe etwa § 1b Abs. 1 Satz 2 VersVG: „Soweit dieses Bundesgesetz die geschriebene Form verlangt, ist keine Unterschrift oder qualifizierte elektronische Signatur erforderlich, wenn aus der Erklärung die Person des Erklärenden hervorgeht." Für § 126b BGB die Lesbarkeit und Möglichkeit der Nennung des Erklärenden bejahend Braegelmann/Kaulartz Smart Contracts/Möslein S. 81 (88 f.).

98 Für Depotbestätigungen mit entsprechender Satzungsbestimmung.

99 Im Fall des § 61 Abs. 2 AktG soll gegenüber der AG bestätigt werden, dass ein Kreditinstitut zur Ausübung des Stimmrechts ermächtigt ist.

100 Siehe etwa §§ 40, 47, 49 ZaDiG, §§ 6, 9, 11, 14, 19, 21 f., 24 VKrG, §§ 5 f., 15 TNG.

101 In autonomer Auslegung verlangt dies die lesbare, für die Führungskraft aufbewahrungsfähige, stets abrufbare und verfügbare Belehrung in Textform, s. Gruber/F. Hartlieb BörseG 2018 Art. 19 MAR Rn. 1 ff., 119 (Stand 1.7.2020).

Programmcode (noch)[102] nicht gerecht. Denn da ihm Informationen nur mit Sonderwissen (nämlich der Kenntnis der Programmiersprache) zu entnehmen sind, ist die Belehrung nicht leicht zugänglich bzw. lesbar. Die Informationspflicht ist daher nicht erfüllt, wenn die Information nur in Programmcode erfolgt.

Auch für die Frage, ob Programmcode die Schwelle der Schriftlichkeit erreichen kann, sind die objektiven Merkmale der Schriftform (i) und der Zweck der jeweiligen Formpflicht (ii) zu prüfen. Auf objektiver Seite meint Schriftlichkeit im ABGB eigenhändige Unterschriftlichkeit (§ 886 ABGB).[103] Zwar darf der Text eigen-, fremdhändig oder auch gedruckt verfasst sein, die Unterschrift am Textende[104] muss aber eigenhändig erfolgen.[105] Diese eigenhändige Unterschrift kann als Stenogramm oder in ausländischer Schrift erfolgen, nicht aber in Geheimschrift oder anderen Zeichen.[106] Eine eigenhändige Unterschrift in diesem Sinn kann in Programmcode nicht erfolgen. Ist für ein Rechtsgeschäft nur diese Unterschrift möglich, wie für das fremdhändige Testament (§ 579 Abs. 1 ABGB iVm § 4 Abs. 2 SVG), scheidet der Einsatz von Programmcodes aus. Muss auch der Text eigenhändig geschrieben sein, etwa bei dem eigenhändigen Testament (§ 578 ABGB), gilt dasselbe. Auch die handschriftliche Abfassung des Programmcodes, die ohnehin wenig sinnvoll erscheint, würde nichts an der Formfehlerhaftigkeit des Testaments ändern. Denn der handschriftliche Programmcode ließe meist allenfalls teilweise Rückschlüsse auf das individuelle Schriftbild des letztwillig Verfügenden zu. Das individuelle Schriftbild ist aber entscheidend, um die Fälschungssicherheit zu gewährleisten.[107]

---

102 Offen ist, ob das Erlernen einer (der vielen?) Programmiersprachen so in das Schulsystem integriert werden kann, dass diese in Zukunft kein „Sonderwissen" mehr sind oder die Übersetzungs-Tools so gut werden, dass ohnedies keine Sprachbarriere mehr besteht.

103 Ebenso nach § 126 BGB vgl. D. Paulus/Matzke ZfPW 2018, 431 (457).

104 Vgl. OGH 2 Ob 538/78, SZ 51/85; Rummel/Lukas/Dullinger ABGB § 886 Rn. 8 (Stand 1.11.2014).

105 Rummel/Lukas/Dullinger ABGB § 886 Rn. 2 (Stand 1.11.2014).

106 Rummel/Lukas/Dullinger ABGB § 886 Rn. 2 (Stand 1.11.2014).

107 Umstritten ist daher, ob die eigenhändige Blindenschrift (zB Brailleschrift oder das Moonalphabet) für ein eigenhändiges Testament genügt. Schwimann/Kodek/Nemeth ABGB § 578 Rn. 2 mwN; Fenyves/Kerschner/Vonkilch/Tschugguel ABGB § 578 aF, § 578 nF ABGB Rn. 5. Die bloß teilweisen Rückschlüsse können dem Erfordernis einer einheitlichen Urkunde aber nicht entsprechen. Zur einheitlichen Urkunde s. Schwimann/Kodek/Nemeth ABGB § 578 Rn. 5. Ansonsten wäre die Fälschungsgefahr zu groß. Auch sonst genügt es nicht, wenn nur unzusammenhängende Worte lesbar sind, OGH 7 Ob 185/05i, NZ 2007/13.

Seit der III. Teilnovelle kann die eigenhändige Unterschrift durch eine mechanische Nachbildung ersetzt werden, wo das im Geschäftsverkehr üblich ist (§ 886 ABGB).[108] Das soll der Erleichterung und Beschleunigung des Geschäftsverkehrs dienen.[109] Auch das hilft beim Einsatz von Programmiersprachen aber nicht weiter. Denn die Berufung auf die Ersetzbarkeit eigenhändiger Unterschriften scheitert daran, dass die Norm nur mechanische Nachbildungen, nicht aber elektronische Stempel vor Augen hat.[110] Darin liegt auch keine (nachträgliche) Unvollständigkeit des Rechts, weil der Gesetzgeber mit der Einführung der qualifizierten elektronischen Signatur genau festgelegt hat, unter welchen Voraussetzungen er die elektronische Nachbildung akzeptiert: Nur eine qualifizierte elektronische Signatur entfaltet (weitgehend)[111] die gleiche Rechtswirkung wie eine handschriftliche Unterschrift (Art 3 Nr. 12 iVm Art. 25 Abs. 2 eIDAS-VO (EU) Nr. 910/2014[112] bzw. § 4 Abs. 1 SVG). Nur wenn eine solche qualifizierte elektronische Signatur im Programmcode eingebunden wird,[113] wäre die objektive Schwelle (i) der Schriftlichkeit iSd § 883 ABGB erfüllt. Darüber hinaus muss der Programmcode auch dem Formzweck gerecht werden (ii): Liegt dieser in der bloßen Beweisbarkeit[114] oder im Gläubigerschutz,[115]

---

108 JGS 1811/946 zuletzt geändert durch RGBl. 1916/69. Die deutsche Parallelregelung, die die mechanische Nachbildung nur ausreichen ließ, wenn das Gesetz dies ausdrücklich ermöglichte, wurde als zu eng befunden. Siehe III. TN 78 BlgHH 145.

109 III. TN 78 BlgHH 145; Kletečka/Schauer/Kalss ABGB-ON[1.06] § 886 Rn. 7 (Stand 1.8.2022).

110 An (mechanische) Stempel wurde jedenfalls schon gedacht, s. III. TN 78 BlgHH 145.

111 Anderes gilt für bestimmte Rechtsgeschäfte, s. § 4 Abs. 2 SVG.

112 Eine qualifizierte elektronische Signatur ist eine fortgeschrittene elektronische Signatur, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht.

113 Zur technischen Möglichkeit auf einer Blockchain s. https://digiexpo.e-estonia.com/Solutions/guardtime-ksi-blockchain-stack/; Möslein ZHR 183 (2019), 254 (279); Braegelmann/Kaulartz Smart Contracts/Möslein S. 81 (89 f.); D. Paulus/Matzke ZfPW 2018, 431 (457).

114 Schwimann/Kodek/Riedler ABGB § 883 Rn. 4. Generell gegen die Möglichkeit, das Schriftformerfordernis erfüllen zu können, Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 861 Rn. 16/2 (Stand 2.1.2022); Heckelmann NJW 2018, 504 (507); s. auch D. Paulus/Matzke ZfPW 2018, 431 (457): nach derzeitigem Stand.

115 Rechtspolitisch ist zu bezweifeln, ob die Unterschriftlichkeit aus Gründen des Gläubigerschutzes angeordnet werden sollte. Der Gläubigerschutz ist durch Schriftformerfordernisse kaum zu wahren. Denn weder Schriftlichkeit noch Programmcode – mag er auch auf einer öffentlichen Blockchain abgelegt sein – schützen davor, dass Transaktionen später bzw. abseits der Blockchain rückgängig gemacht werden. Andere Normen erreichen diesen Schutzzweck besser, s. nur §§ 27 ff. IO, AnfO.

genügt Programmcode. Auch Übereilungsschutz kann er grundsätzlich sicherstellen. Denn die qualifizierte Signatur eines Programmcodes wird nicht voreiliger erfolgen als jene eines gewöhnlichen Textdokuments. Dient das Schriftformgebot aber auch der Aufklärung und Information, genügt Programmcode (noch) nicht.[116]

Zu untersuchen ist schließlich noch, ob ein Notariatsakt mit einer Programmiersprache errichtet werden kann. Unerheblich ist dafür, ob sich die Parteien und der Notar physisch treffen oder nicht. Der Notariatsakt kann auch elektronisch unter Nutzung einer elektronischen Kommunikationsmöglichkeit aufgesetzt werden (§ 69b NO).[117] Für die Erstellung eines Notariatsakts muss die Endfassung – hier der Text in Programmcode – verständlich sein, in dieser Fassung verlesen und beurkundet werden. Denn der Notar ist unter anderem verpflichtet, die Parteien über den Sinn und die Folgen des Geschäfts zu belehren, sich von ihrem ernstlichen und wahren Willen zu überzeugen und ihre Erklärung mit voller Klarheit und Bestimmtheit schriftlich aufzunehmen.[118] Nach der Verlesung muss er sich durch persönliches Befragen der Parteien vergewissern, dass der Akt ihrem Willen entspricht. Diese Voraussetzungen könnten erfüllt sein, wenn die Parteien und der Notar die gewählte Programmiersprache beherrschen. De lege lata scheitert die Errichtung eines Notariatsakts in Programmcode aber an §§ 12, 56 ff., 90 NO:[119] Ein Notariatsakt darf in einer anderen als der deutschen Sprache nur dann verfasst werden, wenn die Sprache im Sprengel des Notars üblich ist und das zuständige OLG die Befugnis zur Aufnahme in dieser Sprache erteilt, weil der Notar seine Kenntnis dieser Sprache ausweist.[120] Ansonsten darf ein Notariatsakt oder eine notarielle Beurkun-

116 Vgl. für Smart Contracts allgemein Schwimann/Kodek/Riedler ABGB § 883 Rn. 4; Pittl/Gottardis immolex 2019, 194 (196).

117 Siehe ENG und NEIV. Für einige wenige Rechtshandlungen und -geschäfte ist der elektronische Notariatsakt nicht möglich. Dazu gehören der Erbvertrag, letztwillige Anordnungen (§§ 67, 70 ff. NO), der Wechselprotest (§ 89 NO) und die Beurkundung über die Bekanntmachung von Erklärungen sowie über die Zustellung von Urkunden (§ 83 NO).

118 Es ist nicht zwingend, dass der Notar die Erklärungen verfasst. Für die Solennisierung einer Privaturkunde bestimmt § 54 NO, dass die Privaturkunde nach den Vorschriften des § 52 NO zu prüfen ist.

119 Jeder Notar muss die deutsche Sprache als Staats- und grundsätzlich Urkundensprache beherrschen (§ 12 NO iVm Art. 8 B-VG), s. Wagner/Knechtel NO § 12 Rn. 1, § 62 Rn. 1 (Stand 1.1.2007).

120 Daher ist es in den Gerichtsbezirken Eisenkappel, Bleiburg und Ferlach für Notare möglich, Notariatsakte und Beurkundungen in Kroatisch oder Slowenisch vorzu-

dung[121] in einer fremden Sprache nur dann erfolgen, wenn die Parteien es ausdrücklich verlangen und der Notar oder der den Akt aufnehmende Substitut seine Sprachbefähigung nach § 62 Abs. 1 NO nachweist.[122] Diese Voraussetzungen können für eine Programmiersprache derzeit nicht erfüllt werden: Sie ist weder üblich iSd § 12 NO noch können die Sprachnachweise des § 62 NO erbracht werden. Hätte ein Notar ein Studium abgeschlossen, das ihn für Programmiersprachen ähnlich befähigt wie das Studium der Translationswissenschaften für die studierte Fremdsprache, wäre die analoge Anwendung der Normen zu prüfen. Beide Normen sind aber – wohl bewusst – eng formuliert. Denn der Gesetzgeber hat an Kommunikationsmethoden, die andere als traditionelle Zeichen[123] (also Codes) verwenden, und damit an ähnliche Fälle wie Programmcodes gedacht. So genügt etwa Blindenschrift[124] für den Notariatsakt nicht. De lege lata ist die Errichtung eines Notariatsakts oder einer notariellen Beurkundung in Programmcode daher nicht möglich. Rechtsgeschäfte, die der Notariatsaktsform oder notariellen Beurkundung bedürfen, können daher nicht mit Smart Contracts in Programmcode erfolgen.[125] Das gilt etwa für die Übertragung von GmbH-Geschäftsanteilen (§ 76 Abs. 2 GmbHG) oder die notarielle Beurkundung beim Erwerb einer Liegenschaft mit Privaturkunden (§ 31 GBG).

Im Ergebnis hängt die Möglichkeit gesetzliche oder vertragliche Formpflichten einzuhalten, davon ab, ob der Programmcode (i) die objektiven Merkmale der Form aufweist und (ii) dem Zweck der Formpflicht nach-

---

nehmen, ohne Dolmetscher oder Übersetzer für Kroatisch oder Slowenisch sein zu müssen. Siehe dazu Wagner/Knechtel NO § 12 Rn. 1.

121 § 90 NO.

122 Der Notar oder Substitut muss danach als allgemein beeideter und gerichtlich zertifizierter Dolmetscher in der betreffenden Sprache bestellt sein oder an einer Universität ein ausreichendes Studium der Translationswissenschaft in der betreffenden Sprache abgeschlossen oder die Fachprüfung für Übersetzer bestanden haben.

123 Traditionelle Zeichen sind für die deutsche Sprache jene der lateinischen Schrift. Erfüllt der Notar oder sein Substitut die Voraussetzungen des § 62 NO für die Aufnahme des Notariatsakts in einer fremden Sprache, kann die Urkunde in fremder Schrift, errichtet werden, wenn die fremde Sprache andere (zB arabische, chinesische, cyrillische, hebräische) Schriftzeichen verwendet. Vgl. zur fremden Schrift Wagner/Knechtel NO § 62 Rn. 3 (Stand 1.1.2007).

124 Zu denken wäre etwa an die Brailleschrift oder das Moonalphabet. In diesem Rahmen kann nicht näher untersucht werden, ob § 59 iVm § 62 NO verfassungskonform anders interpretiert werden können oder die Bestimmungen gleichheitswidrig iSd Art. 7 Abs. 1 Satz 3 und 4 B-VG sind. Für die Zulässigkeit von Programmcodes könnte daraus nichts gewonnen werden.

125 Gegen die Möglichkeit, mit einem Smart Contract die Notariatsaktsform wahren zu können, auch Schwimann/Kodek/Riedler ABGB § 883 Rn. 4.

kommen kann. Das kann de lege lata bei Textform und qualifizierter elektronischer Signatur zu bejahen sein, bei herkömmlicher Schriftlichkeit und Notariatsaktsform demgegenüber nicht.

2. Maschinencode

Maschinencode besteht aus einer Aneinanderreihung von Nullen und Einsen. Soll der Vertrag nach dem Parteiwillen nur aus Maschinencode bestehen, sind die Fassungen vor der Übersetzung in und nach der Rückübersetzung von Maschinencode[126] nicht maßgeblich. Wäre diese Vereinbarung zulässig, gilt bei Abweichungen zwischen Programm- und Maschinencode nur der Maschinencode, weil nur er als Vertragsgrundlage gewählt wurde.

Aus Formgesichtspunkten ist anders als beim Programmcode bereits fraglich, ob der Maschinencode die Schwelle der Textform erreicht. Das BGB, das anders als das ABGB[127] eine Legaldefinition der Textform enthält, beschreibt diese in § 126b BGB als „eine *lesbare* Erklärung, in der die Person des Erklärenden genannt ist, auf einem dauerhaften Datenträger". Der Maschinencode kann von Menschen nicht gelesen – im Sinne von nachvollzogen – werden. Eine Bezugnahme auf die Textform findet sich auch im österreichischen Gesellschaftsrecht: Schreibt das AktG diese Form vor, muss „die Erklärung" auf eine „zur dauerhaften Wiedergabe in Schriftzeichen geeignete Weise abgegeben" werden (§ 13 Abs. 2 AktG).[128] Lesbarkeit verlangt diese Norm nicht.[129] Die Erklärung muss aber dauerhaft wiedergegeben werden können.[130] War etwas – wie Maschinencode – für Menschen bereits ursprünglich unlesbar, darf auch seine Wiedergabe unlesbar sein. Ein solches Verständnis greift aber nach dem Sinn und Zweck des

126 Zu diesem Prozess s. § 2 C.

127 Nach den Materialien soll der Anwendungsbereich des § 13 Abs. 2 AktG auf das AktG beschränkt bleiben. Die Definition ist damit zumindest nicht im Analogieweg verallgemeinerbar. Siehe ErläutRV 208 BlgNR 24. GP 9.

128 Schriftzeichen sind nicht nur Buchstaben, sondern auch „/&<" und Zahlen. Ansonsten wäre die Textform fast nie erfüllt, weil Dokumente regelmäßig Sonderzeichen und Zahlen beinhalten.

129 Siehe aber ErläutRV 208 BlgNR 24. GP 9: „Die Regelung entspricht fast wortgleich dem § 126b dBGB".

130 Dabei handelt es sich um ein allgemeines Merkmal, wie die Betrachtung anderer Normen, die die Textform verlangen, zeigt. Siehe etwa §§ 40, 47, 49 ZaDiG, §§ 6, 9, 11, 14, 19, 21 f., 24 VKrG, §§ 5 f., 15 TNG. Zu Art. 19 Abs. 5 MAR s. Gruber/F. Hartlieb BörseG 2018 Art. 19 MAR Rn. 119 ff. (Stand 1.7.2020).

„dauerhaft wiedergeben" zu kurz. Nach dem Sinn und Zweck ist zumindest ähnliches wie Lesbarkeit gemeint; es geht – allgemeiner formuliert – um die dauerhafte Aufbewahrung von Informationen, die für den Menschen grundsätzlich nachvollziehbar sind. Das ist bei Maschinencode nicht möglich: Übermittelt jemand nur Maschinencode, können Menschen daraus keinen Inhalt entnehmen. Die Rückübersetzung in lesbaren Programmcode mit einem Decompiler entspricht nicht vollständig dem, was im Maschinencode erklärt war.[131] Maschinencode erfüllt die objektiven Anforderungen an die Textform daher nicht.

Aus ähnlichen Gründen kann der Maschinencode die Schriftlichkeit nicht erfüllen; und zwar selbst dann nicht, wenn der Maschinencode die qualifizierte elektronische Signatur in Nullen und Einsen darstellt. Denn signiert wäre dann allenfalls der Text der Vorstufe, also etwa die Ausführungen in Programmcode. Schriftlichkeit verlangt aber die Unterschrift unter dem finalen Text.[132] Weil der Compiler den Text nachträglich verändert, ist dieser Output nicht von der Unterschrift erfasst.[133]

Schließlich scheitert auch die Einhaltung der Notariatsaktsform. Da der Maschinencode für Menschen nicht verständlich ist, kann der Notar seiner Pflicht, den Text des Notariatsakts in der Endfassung zu verlesen, nicht nachkommen. Es ist ihm auch nicht möglich zu prüfen, ob die Parteien die Endfassung verstehen (§ 52 NO). Im Übrigen kann auf oben verwiesen werden: Selbst wenn die technische Identität der Übersetzung gewährleistet wäre, stehen die §§ 12, 56 ff., 90 NO der Abfassung eines Notariatsakts oder eine notariellen Beurkundung in Maschinencode entgegen.

IV. Zwischenergebnis

Der Grundsatz der Formfreiheit stellt es den Parteien frei, Verträge unmittelbar in Programm- oder Maschinencode festzuhalten. Ob der Programm- oder Maschinencode gesetzliche oder vertragliche Formvorgaben erfüllt, hängt davon ab, ob er die objektiven Merkmale der Form aufweist (i) und

131 Zum Problem der Rückübersetzbarkeit § 2 C. am Ende.

132 Das kann mE sogar daraus abgeleitet werden, dass die Unterschrift am Textende erfolgen muss. Siehe dazu OGH 2 Ob 538/78, SZ 51/85. Nachträgliche Zusätze oder handschriftliche Ergänzungen des elektronischen Haupttextes müssen separat mit Unterschrift zum Inhalt der Urkunde gemacht werden, s. Rummel/Lukas/Dullinger ABGB § 886 Rn. 8 (Stand 1.11.2014).

133 Würde erst der Output signiert, wäre eine Verarbeitung nicht möglich, weil der Code nicht mehr nur aus Nullen und Einsen besteht.

ob er dem Zweck der Formpflicht gerecht wird (ii). Für Programmcode ist das bei der Textform und qualifizierten elektronischen Signatur, nicht hingegen bei herkömmlicher Schriftlichkeit und Notariatsaktsform möglich. Maschinencode erfüllt bereits die objektiven Merkmale dieser Formen nicht.

De lege ferenda sollte der österreichische Gesetzgeber – dem Beispiel der §§ 126 ff. BGB folgend – an allgemeiner Stelle einheitlich zusammenfassen, welche Voraussetzungen er an die jeweilige Formpflicht knüpft. Die Zersplitterung und Begriffsvielfalt[134] schafft unnötige Rechtsunsicherheit. Bei dieser Gelegenheit böte es sich überdies an, den zu eng geratenen Wortlaut des § 883 ABGB zu öffnen. Ließe der Gesetzgeber Satz 1 des § 883 ABGB ersatzlos entfallen und ersetzte er in Satz 2 das Wort „Diese" mit „Die", wären sowohl derzeit bestehende als auch künftige Formen vom Wortlaut erfasst.[135]

§ 4 Vertragsabschluss

Die folgenden Kapitel überprüfen, ob es abschlusswilligen, geschäftsfähigen Parteien möglich ist, Verträge unmittelbar in Programm- oder Maschinencode zu verfassen. Dazu gehören auch Fälle, in denen Schriftstücke oder Absprachen in herkömmlicher Sprache bestehen, aber erst in Maschinen- oder Programmcode bindend werden sollen (§ 884 ABGB).[136] Erfasst sind überdies „zweisprachige" Verträge, bei denen neben dem Vertrag in traditioneller Sprache auch ein identer Smart Contract bestehen soll.[137] Für

134 Genannt seien nur die „Mitteilung auf Papier oder anderem dauerhaften Datenträger" (zB ZaDiG, VKrG u TNG), die „Textform" (§ 13 Abs. 2 AktG) oder die „geschriebene Form" (§ 1b VersVG).

135 „Die Verschiedenheit der Form macht, außer den im Gesetze bestimmten Fällen, in Ansehung der Verbindlichkeit keinen Unterschied." In den Materialien könnte festgehalten werden, dass das Wort „Form" im weitesten Sinne zu verstehen ist. Alle Formen von der Konkludenz, über Zeichen, Mündlichkeit bis hin zur Notariatsaktsform und künftig erst hervortretende Formen sollen privatautonom zur Wahl stehen.

136 Solche Vorabsprachen sind keine eigenständigen Verträge. Umgekehrt sind bloße Übersetzungen eines bereits abgeschlossenen traditionellen Vertrags oder bestimmter Klauseln eines solchen Vertrags in Code nicht die Vertragsgrundlage. Sie dienen meist nur dem Zweck, eine (teilweise) automatische Durchführung einer traditionellen Vertragsbeziehung zu erreichen.

137 Den zusätzlichen Problemen solcher zweisprachigen Verträge kann aus praktischer Sicht begegnet werden, wenn die Parteien sich auf eine Version als für die Ausle-

Smart Contracts gilt es daher zu klären, ob Codes den Anforderungen an Angebot und Annahme gerecht werden (Abschnitt A.). Zu prüfen ist überdies, ob bei Zugang, Bindung und Fristenberechnung Besonderheiten bestehen (Abschnitt B.). Sonderproblemen für Smart Contracts on-chain widmet sich Abschnitt C.

A. Angebot und Annahme

Nach §§ 861, 863, 870 ff. ABGB kommt ein Vertrag zustande, wenn mindestens zwei Parteien durch fristgerechten Austausch übereinstimmender Willenserklärungen einen Konsens herbeiführen.[138] Jede Willenserklärung muss gemäß § 869 ABGB[139] frei, ernstlich, bestimmt und verständlich abgegeben werden. Soll eine Willenserklärung in Programm- oder Maschinencode abgegeben werden, sind die Erfordernisse der Bestimmtheit (Abschnitt I.) und Verständlichkeit (Abschnitt II.) genauer zu beleuchten. Darüber hinaus ist zu untersuchen, ob solche Willenserklärungen einen endgültigen Bindungswillen erkennen lassen (Abschnitt III.).

I. Bestimmtheit und essentialia negotii

Damit ein Angebot hinreichend bestimmt ist, muss es zumindest die essentialia negotii und die wesentlichen Rechtsfolgen des Geschäfts bestimmen. Das erfordert keine Ausdrücklichkeit, eindeutige Bestimmbarkeit durch Auslegung der Erklärung und das dispositive Recht genügt.[140] Die (ergänzende) Auslegung und dispositives Recht, mit seinem Anspruch praktikable und gerechte Lösungen abzubilden,[141] können im Regelfall die Unvollständigkeit von Verträgen abfangen. Die Vertragsparteien müssen also nicht sämtliche möglichen Vertragspunkte regeln, wenn sie mit den Lösungen des dispositiven Rechts zufrieden sind.

---

gungsfragen maßgebliche einigen können. Vgl. allgemein Kunkel Vertragsgestaltung S. 108; Hahnkamper VIAC Art. 26 Rn. 17 f. (Stand 1.2.2019).

138 Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 861 Rn. 1 (Stand 2.1.2022); Fenyves/Kerschner/Vonkilch/Schickmair ABGB § 861 Rn. 33.

139 Zum weiten Anwendungsbereich dieser Norm s. Fenyves/Kerschner/Vonkilch/Vonkilch/Walch ABGB § 869 Rn. 14 mwN.

140 Siehe nur OGH 7 Ob 14/11a, Zak 2012/102, 53; Kletečka/Schauer/Pletzer ABGB-ON[1.03] § 869 Rn. 17 ff. mwN (Stand 1.8.2019); Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 861 Rn. 17. (Stand 2.1.2022).

141 Wiebe Elektronische Willenserklärung S. 46 ff., 50.

Das gilt für Smart Contracts zumindest dann nicht gleichermaßen, wenn die Parteien nicht auf analoge Rechtswege und/oder Informationsschnittstellen angewiesen sein wollen: Denn Programm- und Maschinencodes können essentialia negotii und andere komplexe Erklärungsinhalte und Rechtsfolgen zwar durchaus hinreichend bestimmt abbilden. Sie führen aber nur das aus, was im Code abgebildet wurde. Ein Rückgriff auf das außerhalb des Codes liegende dispositive Recht ist (derzeit)[142] nicht möglich. Grenzen setzt auch die gewollte und erlaubte Unbestimmtheit der Sprache:[143] Der Code kann unbestimmte Begriffe derzeit nicht selbstständig auslegen und verarbeiten. Er folgt vielmehr einer Wenn-Dann-Funktion.[144] *Wenn* Bieter-n am Tag X Höchstbieter ist, *dann* versende die Zahlungsaufforderung an ihn und speichere seine Signatur für die Entsperrung des Downloads. *Wenn* 2 ETH bis 31.12.22 an den Smart Contract geleistet werden, *dann* ist Zugriff auf das NFT „MCI Fortbildung rocks" zu gewähren. Ob eine Leistung wegen „geänderter Umstände" nicht erfolgen soll oder die gelieferte Sache „mangelfrei" ist, kann der Code aber (noch) nicht automatisch und digital prüfen. Die Angleichung maschinenlesbarer Sprachen an die menschliche Sprache ist technisch noch nicht vollbracht[145] bzw. Neuland.[146]

Die gewünschte Unbestimmtheit lässt sich am Beispiel des Vorvertrags verdeutlichen. Der Vorvertrag ist ein Vertrag, dessen Hauptpflicht der künftige Abschluss eines Hauptvertrags ist.[147] Der Vorvertrag ist also schlank

142 Es ist nicht ausgeschlossen, dass die Verbindung von Smart Contracts und KI diesbezüglich Änderungen bringen kann.

143 Verträge können über die sprachliche Ausgestaltung viel an Flexibilität gewinnen. Dazu, dass die Vagheit auch Wachsamkeit mit sich bringt, s. Kuntz AcP 220 (2020), 51 (75 f., 79).

144 Siehe § 2 C. C. Paulus/Matzke CR 2017, 769 (771); Linardatos Autonome Aktanten S. 38 f.; Diedrich Ethereum S. 167, 188; Spindler ZGR 2018, 17 (48).

145 Möslein ZHR 183 (2019), 254 (269).

146 XHTML ist ein Format für Dokumente, die Menschen lesen können. In ein solches XHTML-Dokument können mit iXBRL, maschinenlesbare XBRL-Tags, eingebettet werden. Das Ergebnis ist ein Dokument, das für Menschen und Maschinen lesbar ist. Vgl. dazu etwa DelVO (EU) 2018/815 Erwägungsgründe 2–6. Fortschritte für eine maschinenlesbare Sprache, die auch jeder Mensch versteht, verspricht aktuell etwa Diedrich Lexon passim. Auch unter dem Schlagwort „Ricardian Contract" wird diskutiert, den Code rechtsähnlicher zu erstellen, Mandal Ricardian Contract passim.

147 KBB/P. Bydlinski § 936 Rn. 1.

und könnte, wenn keine Formpflicht des Hauptvertrags dagegen spricht,[148] leicht als Smart Contract verfasst werden. Mit Eintritt des Abschlusszeitpunkts[149] oder der Bedingung[150] könnte der Smart Contract den bereits formulierten[151] Hauptvertrag automatisch freigeben. Wollte eine Partei in der Zwischenzeit vertragsbrüchig den Abschluss des Hauptvertrags verweigern, bleibt der anderen Partei die Klage auf Abschluss des Hauptvertrags erspart.[152] Die schwächere Bindung des Vorvertrags ist im Smart Contract demgegenüber schwierig abzubilden:[153] Meint eine Vertragspartei, dass sich die Umstände geändert haben, kann sie ihre Unterschrift im „herkömmlichen" Vertrag unter Berufung auf die Umstandsklausel des § 936 ABGB schlicht unterlassen. Für den Smart Contract ist die Feststellung geänderter Umstände demgegenüber schwieriger.

Ein Hauptzweck des Einsatzes von Smart Contracts – vollautomatisierter Vertragsabschluss und/oder Leistungsaustausch – kann daher noch nicht erreicht werden, wenn die Parteien ihr Rechtsverhältnis von unbestimmten Rechtsbegriffen oder Ereignissen außerhalb des Codes abhängig machen. Das bedeutet aber nicht, dass der Einsatz von Smart Contracts[154] deswegen an sich ausscheidet.[155] Die Implementierung von Informationsschnittstellen (Oracles, Witnesses) ermöglicht die Anknüpfung an analoge und externe Ereignisse.[156] Die Durchführung des Codes kann so etwa an Wetterdaten, Flugverspätungen, Umsatzzahlen, Börsenkurse, Geldeingang auf einem Girokonto oder andere Informationen aus Sensoren von IoT-Geräten geknüpft werden.[157] Mit solchen Informationsschnittstellen erhöht sich zwar das Risiko der Manipulation des Smart Contracts.[158] Vertrauen die Parteien

148 Damit die Formpflicht des Hauptvertrags gewahrt bleibt, muss die Form schon mit dem Vorvertrag gewahrt werden, Kletečka/Schauer/Gruber ABGB-ON[1.06] § 936 Rn. 9 (Stand 1.8.2019).

149 Dieser muss innerhalb einer Einjahresfrist liegen, KBB/P. Bydlinski § 936 Rn. 3, 5.

150 Zur Zulässigkeit OGH 4 Ob 20/03z, immolex 2004, 27 (Pfiel).

151 Der Vorvertrag erlangt nur Verbindlichkeit, wenn der Hauptvertrag (weitgehend) konkretisiert ist, s. KBB/P. Bydlinski § 936 Rn. 2.

152 Zu dieser Klage vgl. etwa OGH 2.9.1993, 6 Ob 570/93; KBB/P. Bydlinski § 936 Rn. 1.

153 Zur Umstandsklausel KBB/P. Bydlinski § 936 Rn. 4; Rummel/Lukas/Reischauer ABGB § 936 Rn. 33 ff. (Stand 1.5.2018).

154 Für Smart Contracts, die mit externen Daten bespeist werden können, findet sich mancherorts der Begriff „Hybrid Smart Contract", s. Chainlink, https://chain.link/.

155 Heckelmann NJW 2018, 504 (505).

156 Linardatos Autonome Aktanten S. 38; Hanzl HdB Blockchain S. 14.

157 Diedrich Ethereum S. 187.

158 Thießen ZfgK 2018, 606 (607). Die Fortentwicklung dieser Schnittstellen muss IT-Sicherheit entsprechend berücksichtigen.

einer einzelnen Quelle nicht, können sie aber mehrere kombinieren.[159] Der Code kann zum Beispiel festlegen, dass vier von sechs Oracles/Witnesses das (Nicht-)Vorliegen des externen Ereignisses bestätigen müssen, um dessen (Nicht-)Vorliegen für die weitere Vertragsabwicklung als wahr anzunehmen. Ergebnisse der Informationsschnittstellen müssen, um vom Smart Contract verarbeitet werden zu können, auf Ja/Nein lauten.[160]

Zusammenfassend können Codes rechtlich relevante Inhalte wie Ware (NFT) und Preis (2 ETH, Höchstbieter) sowie die Bedingungen, unter denen sie auszutauschen sind, bestimmt beschreiben.[161]

II. Verständlichkeit

1. Programmcode

Eine Erklärung ist verständlich, wenn ihr – allenfalls nach Auslegung gemäß §§ 914 f. ABGB – objektiv ein eindeutiger Sinn zugeschrieben werden kann.[162] In Programmiersprache verfasste Erklärungen sind objektiv verständlich: Jeder, der die Programmiersprache erlernt hat, kann dem codierten Text einen eindeutigen Sinn zuschreiben. Programmiersprachen sind aber eigene Fachsprachen. Nur weil jemand Englisch versteht, beherrscht er nicht zugleich Programmiersprachen, die auf englischer Sprache basieren. Sie sind unabhängig von der Fremdsprache, auf der sie basieren, zu erlernen.

Das Kapitel zur Formfreiheit enthält mit dem Notariatsakt ein Beispiel, für den die Parteien diese Fachsprache nicht wählen können. Ein weiteres Beispiel, bei dem der Gesetzgeber den Parteien ausnahmsweise nicht die freie Wahl der Vertragssprache überlässt, ist der Abschluss eines Timesharing-Vertrags. § 7 Abs. 1 TNG lässt nach Wahl des Verbrauchers nur Sprachen jener EU-Mitgliedstaaten zu, in denen der Verbraucher seinen Wohnsitz hat oder denen er angehört. Das wirft die Frage auf, ob etwa

159 Auf die Entwicklung von Technologien, für eine höhere Sicherheit bei der Verwendung von Oracles haben sich bereits Unternehmen spezialisiert (s nur https://provable.xyz/). Mit dezentralen Lösungen s. auch das Oracle-Netzwerk Chainlink, https://chain.link/. Informationsschnittstellen müssen also nicht zwingend zentral sein. So aber Kuntz AcP 220 (2020), 51 (78).

160 Diedrich Ethereum S. 188 f.; Hanzl HdB Blockchain S. 14.

161 Möslein ZHR 183 (2019), 254 (264, 270 ff.); Hanzl/Rubey Zak 2018, 127 (128). AA Djazayeri jurisPR-BKR 12/2016 Anm. 1 bei Fn. 21.

162 Kletečka/Schauer/Pletzer ABGB-ON[1.03] § 869 Rn. 24 f. (Stand 1.8.2019).

ein Verbraucher mit österreichischem Wohnsitz eine Programmiersprache wählen kann, die auf deutscher Sprache basiert.[163] Das ist mit Blick auf den Zweck der Bestimmung zu verneinen. Die Vorgabe der Sprache will (auch) sicherstellen, dass der Vertragstext für den Verbraucher leicht verständlich ist. Die Wahl einer Programmiersprache scheidet daher jedenfalls aus, wenn der Verbraucher sie nicht gleich gut beherrscht wie die Sprache jenes Mitgliedsstaats, in dem er wohnt. Kann er eine Programmiersprache gleich gut, könnte zwar der Zweck der Norm gewahrt werden. Allerdings erlaubt ihr Wortlaut nur die Wahl der Amtssprachen im Mitgliedsstaat des Wohnsitzes oder der Staatsbürgerschaft des Verbrauchers. Die Wahl einer anderen Fremd- oder Fachsprache ist unabhängig davon nicht vorgesehen, ob sie ein Verbraucher gleich gut kann. Wählt der Unternehmer für einen Timesharing-Vertrag daher einen Programm- oder Maschinencode als Vertragsgrundlage, begeht er eine Verwaltungsübertretung (§ 18 Abs. 1 Nr. 4 TNG).

Sprachvorgaben bestehen überdies dort, wo das Gesetz die Nachvollziehbarkeit durch Dritte gewährleisten will.[164] So sind etwa die Bücher und sonst erforderlichen Aufzeichnungen des Unternehmers in einer lebenden Sprache zu führen (§ 190 Abs. 2 UGB).[165] Werden Abkürzungen, Zahlen, Buchstaben oder Symbole verwendet, muss im Einzelfall deren Bedeutung eindeutig feststehen. Zwar wäre die Wahl einer lebenden Fremdsprache möglich. Das kommt praktisch aber kaum vor, weil der Jahresabschluss in deutscher Sprache aufzustellen ist (§ 193 Abs. 4 UGB) und steuerrechtliche Normen sonst die Übersetzung verlangen (§ 131 Abs. 1 Nr. 1 BAO). Die Wahl einer toten Sprache (zB Latein) oder einer Plansprache (zB Esperanto)[166] ist ebenso unzulässig wie die Wahl einer Programmiersprache. Anderes gilt, wenn spezielle Normen Fachsprachen oder -formate vorschreiben. So sind Jahresfinanzberichte kapitalmarktorientierter Unternehmen im XHTML-Format zu erstellen.[167]

163 Selbst die deutschen Programmiersprachen, die es gegeben hat, verwenden englische Schlüsselwörter.

164 Zu diesem Zweck s. Straube/Ratka/Rauter/Gelter UGB § 190 Rn. 22, 24 (Stand 1.12.2022).

165 U. Torggler/Hilber UGB § 190 Rn. 22 (Stand 1.1.2019).

166 Straube/Ratka/Rauter/Gelter UGB § 190 Rn. 24 (Stand 1.6.2017).

167 Siehe Art. 3 DelVO (EU) 2018/815 und Erwägungsgründe 2–6. Zum XHTML-Format s. auch Fn. 146.

Im Regelfall gibt der Gesetzgeber aber keine Sprache vor. Parteien können ihre Vertragssprache dann frei vereinbaren.[168] Sie können sogar eine Fremdsprache wählen, die sie nicht verstehen,[169] eine Geheimsprache, die nur sie verstehen,[170] sonstige Zeichen(folgen)[171] oder eine Programmiersprache. Einbußen der Verständlichkeit gehen bei zweiseitig verbindlichen Verträgen nach § 915 ABGB zum Nachteil desjenigen, der sich der Programmiersprache bedient hat. Individuelle Verständnisschwierigkeiten gehen demgegenüber zu Lasten des Erklärungsempfängers:[172] Er weiß von seinen Verständnisschwierigkeiten und hat auch die Möglichkeit, diesen abzuhelfen und die Erklärung übersetzen zu lassen. Wer einen Vertrag in einer fremden (Programmier-)Sprache abschließt, ohne entweder der (Programmier-)Sprache mächtig zu sein oder dessen Inhalt sonst zu kennen, ist nicht schutzwürdiger als der, der einen Vertrag ungelesen unterzeichnet oder intellektuell nicht verstanden hat.[173] Die Zuordnung des Risikos zur Partei mit den Verständnisschwierigkeiten überzeugt auch rechtsökonomisch, weil sie es leichter als die andere Partei beherrschen kann und damit cheapest cost avoider[174] ist.

Der im Angebot enthaltene Vertragstext wird daher zum Inhalt einer entsprechenden Annahmeerklärung.[175] Der Empfänger der Annahmeerklärung darf darauf vertrauen, dass sein Gegenüber an die Erklärung, die äußerlich eine Willenserklärung ist, gebunden sein will.[176] Der Verkehrs- und Vertrauensschutz rechtfertigen die Bindung. Auch eine Anfechtung kommt aufgrund der bewussten Inkaufnahme des fremdbestimmten Inhalts grund-

168 Vgl. für das BGB Kaulartz DSRITB 2016, 1023 (1029); allgemein Kunkel Vertragsgestaltung S. 108.

169 Vgl. Wagner/Knechtel NO § 62 Rn. 2, 4 und § 64 Rn. 5 (Stand 1.1.2007).

170 Vgl. Leukauf/Steininger/Tipold StGB § 223 Rn. 9 (Stand 1.10.2016); Höpfel/Ratz/Kienapfel/Schroll WK StGB § 223 Rn. 23 (Stand 1.1.2017).

171 Zu Symbolen wie Emojis s. Bich-Carrière, 32 IJSL 2019, 283 (296 ff., 300 f.). Deren rechtliche Auslegung ist mittlerweile Gegenstand einer Vielzahl von Entscheidungen weltweit. Mit prägnantem Überblick zur internationalen Rechtsprechung Pendl NJW 2022, 1054 (1056).

172 Für lebende Fremdsprachen Temming GPR 2016, 38 (40).

173 OGH 1 Ob 30/04z, ÖBA 2004, 957 (Iro); vgl. auch Kaulartz/Heckmann CR 2016, 618 (621 f.); Heckelmann NJW 2018, 504 (506).

174 Vgl. Vögerl immolex 2008, 235 (236); Schäfer/Ott Ökonomische Analyse S. 490 ff., 517, 521 f.

175 KBB/Bollenberger/P. Bydlinski § 871 Rn. 6; Kletečka/Schauer/Pletzer ABGB-ON[1.03] § 871 Rn. 10 mwN (Stand 1.8.2019).

176 Temming GPR 2016, 38 (40).

sätzlich[177] nicht in Frage. Denn es fehlt an der (Fehl-)Vorstellung vom Inhalt.[178] Fehlende Kenntnisse der Programmiersprache können den Bestand des Vertrags hingegen gefährden, wenn der andere Vertragspartner ernsthaft daran zweifeln muss, dass sein Gegenüber die Erklärungen versteht.[179] Dann kommt der Einsatz eines Programmcodes als Vertragsgrundlage allenfalls mit Übersetzung in Frage.[180]

Auch AGB müssen verständlich sein. Im Verhältnis zwischen Unternehmern können die AGB (zB des Herstellers) trotz Sprachunkenntnis des Erklärungsempfängers (zB des Händlers) wirksam einbezogen werden, wenn in der Verhandlungs- und Vertragssprache auf sie hingewiesen wird, sie einsehbar sind und der Erklärungsempfänger dennoch eine uneingeschränkte Annahmeerklärung abgibt.[181] Für das inhaltliche Verständnis ist entscheidend, ob etwa die Herstellung einer Übersetzung zumutbar ist. Das hängt von der Länge, Intensität und Bedeutung der geschäftlichen Beziehung sowie der Verbreitung der verwendeten Sprache im betreffenden Kulturkreis ab.[182] Im Unternehmer-Verbraucher-Geschäft verstößt die Verwendung von AGB in einer Programmiersprache gegen das Transparenzgebot.[183] Möglich wären aber zweisprachige AGB, wenn bei Auslegungsdifferenzen die lebende Sprache vorgeht.[184]

2. Maschinencode

Maschinencode ist für Menschen nicht verständlich.[185] Kein Mensch kann einer Erklärung in Maschinencode einen objektiven Sinn entnehmen. Da-

177 Ein beachtlicher Irrtum kann etwa vorliegen, wenn der Programmcode etwas anderes festhält, als mündlich besprochen wurde.
178 KBB/Bollenberger/P. Bydlinski § 871 Rn. 6.
179 Zu Fremdsprachen s. OGH 1 Ob 30/04z, ÖBA 2004, 957 (Iro); KBB/Bollenberger/P. Bydlinski § 871 Rn. 6; für Smart Contracts s. Kaulartz/Heckmann CR 2016, 618 (622).
180 Vgl. Kaulartz DSRITB 2016, 1023 (1029); Hanzl/Rubey Zak 2018, 184 (185).
181 OGH 10 Ob 19/21y, VbR 2022/35; KBB/Bollenberger/P. Bydlinski § 864a Rn. 2. Vgl. zur Ablehnung des Einbezugs OGH 7 Ob 275/03x, JBl 2004,449.
182 OGH 10 Ob 19/21y, VbR 2022/35.
183 Strittig ist das Verhältnis von § 6 Abs. 3 KSchG zu §§ 869 letzter Satz, 915 ABGB. Siehe dazu Rummel/Krejci, 3. Aufl., ABGB § 6 KSchG Rn. 202 ff. (Stand 1.1.2002); KBB/Kathrein/Schoditsch § 6 KSchG Rn. 31 f.
184 Vergleiche Fn. 137.
185 Siehe dazu § 2 C.

mit stößt die Vertrauenstheorie (§ 863 iVm §§ 870 ff., 914 ABGB)[186] an ihre Grenzen: Nach ihr kommt es darauf an, wie ein objektiver, redlicher Erklärungsempfänger die Erklärung unter Berücksichtigung aller Umstände verstehen durfte und verstanden hat.[187] Die Erklärung aus Nullen und Einsen kann aber von keiner Partei und damit auch nicht vom objektiven Erklärungsempfänger verstanden werden. Der Empfänger kann der Erklärung daher keinen Inhalt entnehmen, auf den ein objektiver Erklärungsempfänger vertrauen würde und dürfte.

Maschinencode erfüllt das Kriterium der Verständlichkeit (§ 869 ABGB) nicht, weil er für Menschen keinen objektiven Erklärungswert[188] hat.[189]

III. Endgültiger Bindungswille

Ein Angebot liegt nur vor, wenn es einen endgültigen Bindungswillen erkennen lässt. Dieser Wille grenzt es von der bloßen Einladung zu Vertragsverhandlungen oder der unverbindlichen Aufforderung zur Angebotslegung (invitatio ad offerendum) ab.[190] Auch auf einer Blockchain kann die Vertragsanbahnung durch eine unverbindliche invitatio ad offerendum codiert sein.[191] Ob das eine oder andere vorliegt, ist durch Auslegung der Erklärung zu ermitteln.

Diese Frage betrifft nur die Programmsprache, weil Menschen Maschinencode wie gezeigt nicht verstehen. Sie können aus ihm daher grundsätz-

186 Schwimann/Kodek/Riedler ABGB § 863 Rn. 1; Rummel/Lukas/Rummel ABGB § 863 Rn. 1 (Stand 1.11.2014).

187 Schwimann/Kodek/Riedler ABGB § 863 Rn. 2; Fenyves/Kerschner/Vonkilch/Vonkilch ABGB § 914 Rn. 130; Rummel/Lukas/Rummel ABGB § 863 Rn. 1, 14 (Stand 1.11.2014); KBB/Bollenberger/P. Bydlinski § 914 Rn. 1; Kletečka/Schauer/Heiss ABGB-ON[1.02] § 914 Rn. 35.

188 Kletečka/Schauer/Pletzer ABGB-ON[1.03] § 869 Rn. 24 f. (Stand 1.8.2019). Darauf wird bei der Frage des Zugangs der Erklärung zurückzukommen sein (s § 4 B. II.).

189 Zum Sonderfall der gemeinsamen Programmierung s. § 4 B. II. 1. und der Maschinen Kommunikation s. § 5 C. II. und III.

190 Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 861 Rn. 18 (Stand 2.1.2022).

191 So konnten Kunden für die smarte Flugverspätungsversicherung von AXA ein Angebot stellen, indem sie das online zur Verfügung gestellte Formular ausfüllten und übersendeten. Klostermeier, 2018, https://www.cio.de; AXA, 2017, https://www.axa.com. Diese wurde Ende 2019 wieder vom Markt genommen, weil der Markt dafür noch nicht reif gewesen sei, Hill, 2019, https://coinrivet.com. Vgl. Kaulartz/Heckmann CR 2016, 618 (621); Pittl/Gottardis immolex 2019, 194 (195).

lich[192] auch keinen Bindungswillen erkennen. Die Erklärung in Programmsprache kann sowohl als invitatio ad offerendum als auch als Angebot mit endgültigem Bindungswillen abgefasst sein. Die Programmsprache im Beispiel[193] macht klar, dass der Künstler sein NFT nur der Höchstbieterin innerhalb der Frist verbindlich anbietet. Der Künstler könnte die Programmsprache alternativ aber auch als invitatio ad offerendum formulieren.

Regelmäßig ist das bloße Anbieten eines begrenzt vorhandenen Produkts in einem Schaufenster, auf einer Webseite, Plattform oder einer Blockchain eine bloße invitatio ad offerendum. Der Verkäufer will sich die Prüfung des Lagerbestands und gelegentlich der Bonität des Käufers vorbehalten.[194] Anderes gilt, wenn der Verkäufer die Anpreisung der Ware als verbindliches Angebot kennzeichnet; etwa, weil seine Webseite mit dem Lagerbestand vernetzt ist. Die Anpreisung unbegrenzt vorhandener digitaler Waren und Leistungen zum Download wird ebenso häufig als Angebot mit endgültigem Bindungswillen zu verstehen sein.[195]

Für den Bindungswillen muss der Empfänger des Angebots nicht bekannt sein. Die Abschlussfreiheit erlaubt mit dem offertum ad incertas personas auch die Wahl eines gänzlich unbekannten Kontrahenten.[196] Häufig will etwa der Verwender von Automaten, Webseiten, Smart Forms oder Smart Contracts mit jedem kontrahieren, der die Bedingungen (Auswahl eines vorhandenen Produkts und entsprechender Münzeinwurf) erfüllt.[197] Auch die pseudonyme Struktur der Blockchain schafft hier folglich keine Hürden, die der Vertragsschlussmechanismus des ABGB nicht bewältigen könnte.

192 Zu den Ausnahmen der gemeinsamen Programmierung s. § 4 B. II. 1. und der Maschinen-Kommunikation s. § 5 C. II. und III.

193 Siehe dazu ab Seite 11.

194 Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 861 Rn. 18 (Stand 2.1.2022).

195 Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 861 Rn. 19 (Stand 2.1.2022). Das gilt jedenfalls dann, wenn überdies nur Voraus- oder Sofortzahlungsmethoden zur Auswahl stehen.

196 Allgemein Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 861 Rn. 21 (2.1.2022); s. auch Hanzl HdB Blockchain S. 82; Möslein ZHR 183 (2019), 254 (274 f.).

197 Allgemein Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 861 Rn. 21 (Stand 2.1.2022); Möslein ZHR 183 (2019), 254 (274 f.); Hanzl/Rubey Zak 2018, 127 (128).

B. Zugang, Bindung und fristgerechte Annahme

Lassen sich Angebot und Annahme voneinander abgrenzen,[198] leitet das Angebot den Vertragsabschluss ein. Dafür muss es kommuniziert werden; also dem jeweiligen Adressaten zugehen. Ein Angebot ist daher eine zugangsbedürftige Willenserklärung.[199] Zugang erfordert das Einlangen im Machtbereich des Oblaten (Empfangstheorie).[200] Für den Zugang genügt die Möglichkeit der Kenntnisnahme.[201] Ein schützenswertes Vertrauen des Oblaten auf die Bindung des Offerenten entsteht aber erst mit tatsächlicher Kenntnisnahme.[202] Der Offerent kann seine Bindung daher verhindern, wenn er sein Angebot widerruft und dem Oblaten der Widerruf vor dem Angebot selbst zur Kenntnis gelangt.[203]

Die Bindung des Offerenten endet mit dem Ablauf der Annahmefrist.[204] Diese umschreibt jenen Zeitraum, innerhalb dem der Oblat dafür gesorgt haben muss, dass dem Offerenten seine Annahme zugeht.[205] Hat der Offerent keine privatautonome Frist gesetzt, kann das Angebot unter Anwesenden sogleich, unter Abwesenden binnen der Zeit des doppelten Transportwegs samt angemessener Überlegungsfrist angenommen werden (§ 862 Satz 2 ABGB). Das entspricht jenem Zeitraum, innerhalb dem der Offerent eine Rückmeldung erwarten darf. Seine Bindung endet daher grundsätzlich parallel mit der Annahmefrist. Der Vertrag kommt zustande,

198 Das ist nicht immer der Fall, wie die gemeinsame Unterzeichnung einer Vertragsurkunde unter Anwesenden zeigt, s. Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 861 Rn. 1 (Stand 2.1.2022).

199 Vgl. III. TN 78 BlgHH 132 ff., 154; Rummel/Lukas/Rummel ABGB § 862a Rn. 1 (Stand 1.11.2014); Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 862a Rn. 1 (Stand 2.1.2022).

200 KBB/Bollenberger/P. Bydlinski § 862a Rn. 4; Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 862a Rn. 1 f. (Stand 2.1.2022).

201 Temming GPR 2016, 38 (40).

202 KBB/Bollenberger/P. Bydlinski § 862 Rn. 1.

203 KBB/Bollenberger/P. Bydlinski § 862 Rn. 1; Koziol FS Iro, 2013, 81 (87); Schwimann/Kodek/Riedler ABGB § 862 Rn. 4; Rummel/Lukas/Rummel ABGB § 862a Rn. 9 (Stand 1.11.2014).

204 Die zwei Fristen sind zu unterscheiden, weil sich ihr Beginn bei Erklärungen unter Abwesenden unterscheidet. Während die Bindungsfrist erst mit tatsächlicher Kenntnisnahme beginnt, muss die Annahmefrist mit der Absendung beginnen, weil ab diesem Zeitpunkt der zweifache Postweg und die angemessene Überlegungsfrist addiert werden, um den spätesten Zeitpunkt für den Zugang einer rechtzeitigen Annahmeerklärung zu ermitteln.

205 Zur Empfangstheorie s. III. TN 78 BlgHH 132 ff., 154; Klang/Gschnitzer ABGB IV/1[2] § 862a S. 68 f.; Schwimann/Kodek/Riedler ABGB § 862a Rn. 1.

wenn die übereinstimmende Annahme innerhalb der Frist im Machtbereich des Offerenten zugeht (§ 862a Satz 1 ABGB). Dasselbe gilt, wenn der Offerent trotz verspätetem Zugang erkennen musste, dass die Annahmeerklärung rechtzeitig abgesendet wurde, und er seinen Rücktritt nicht unverzüglich anzeigt (§ 862a Satz 2 ABGB). In beiden Fällen bestimmt der Zugang der Annahme den Zeitpunkt des Vertragsabschlusses und des Eintritts der Vertragswirkungen. Wann der Offerent die Annahme zur Kenntnis nimmt, ist irrelevant. Nur vor der Kenntnisnahme wäre aber der Widerruf der Annahme durch den Oblaten rechtzeitig und würde den Vertragsschluss verhindern.[206]

Diese allgemeinen Regeln gelten grundsätzlich unabhängig davon, in welcher Gestalt die Willenserklärungen geäußert werden. Zu untersuchen ist, ob bei der Verwendung eines Programm- bzw. Maschinencodes Besonderheiten bestehen. Das gilt insbesondere mit Blick auf den Zugang der Erklärung sowie der Unterscheidung zwischen einem Angebot unter Anwesenden und unter Abwesenden.

I. Programmcode

Zunächst ist zu klären, ob die Parteien ihren Code gemeinsam unter Anwesenden verfassen. Als Angebot unter Anwesenden versteht das Gesetz in § 862 ABGB die gleichzeitige physische Anwesenheit von Offerent und Oblat. Das Telefonat steht dem gleich. Bereits das Hinterlassen einer Sprachnachricht am Anrufbeantworter ist nicht mehr von Person zu Person gemacht.[207] Für die „Anwesenheit" ist nämlich eine aufrechte, interaktive Verhandlungsmöglichkeit entscheidend.[208] Eine live-Kommunikation etwa in einem Chat ist dem analog gleichzusetzen.[209] Sind die Vertragspartner technikaffin, könnten sie den Code also etwa gemeinsam mit Live-Chat oder auf einer interaktiven Plattform schreiben oder während der Eingaben

206 Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 862a (Stand 2.1.2022) Rn. 13. Bei einem Adressatenkreis ist der Widerruf nur rechtzeitig, wenn er gegenüber jedem Adressaten rechtzeitig ist, s. dazu F. Hartlieb Verbandsvertragsrecht S. 248 ff.

207 Vgl. für den Abbruch der Verbindung Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 862 Rn. 2 (Stand 2.1.2022).

208 Vgl. für § 147 Abs. 1 Satz 2 BGB Möslein ZHR 183 (2019), 254 (275).

209 Vgl. auch dazu, dass die Kommunikation via E-Mail nicht unter Anwesenden erfolgt Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 862 Rn. 2 f. (Stand 2.1.2022). § 147 Abs. 1 Satz 2 BGB nennt neben dem Fernsprecher zusätzlich die „sonstige technische Einrichtung", diese Bestimmung wäre daher bereits ihrem Wortlaut nach in einfacher Auslegung offen für dieses Verständnis.

(etwa telefonisch) verbunden sein und verhandeln. Besteht eine solche gegenseitige Kommunikationsmöglichkeit, ist das Angebot sofort anzunehmen.

Besteht keine live-Kommunikation, erfolgt das Angebot unter Abwesenden. In diesem Fall ist zu prüfen, ob das Angebot in den Machtbereich des Oblaten gelangt. Dieser Machtbereich kann etwa eine App,[210] ein Mail-Postfach oder die Software einer Maschine[211] sein. Gedacht sei auch an Angebote mit unbekanntem Adressatenkreis. So ist ein Angebot auf Webseiten oder in Automaten mit deren Freischaltung abgegeben.[212] Es geht jedem zu, der die Möglichkeit der Kenntnisnahme hat.

Auch die Annahme ist grundsätzlich empfangsbedürftig. Insoweit greift das zum Machtbereich des Oblaten Gesagte entsprechend für jenen des Offerenten. Anderes gilt, wenn auf den Zugang verzichtet wird oder wenn nach den Umständen nicht mit dem Zugang einer Annahme zu rechnen ist.[213] Der Zugang entfällt auch bei der Annahme durch Willensbetätigung;[214] etwa durch Versendung des bestimmten Kryptoassets. Die Willensbetätigung ist nicht empfangsbedürftig in dem Sinn, dass die Annahmehandlung gegenüber dem Offerenten gesetzt werden müsste.[215] Der Vertrag entsteht mit der Herstellung des gewünschten Zustands.[216]

Im Ergebnis ist der Austausch von Angebot und Annahme unmittelbar in Programmcode rechtlich möglich.

210 Bei CryptoWine – einer im Aufbau befindliche Plattform zum Handel und zur Lagerung von Wein – soll in der CryptoWine-App Wein gehandelt werden können.

211 Je nachdem, ob die Maschine automatisch bzw. automatisiert Verträge abschließen darf (s § 5 C. II. und III.) wird sie zusätzlich ein Interface brauchen, über das ihr Nutzer kommunizieren kann.

212 Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 861 Rn. 21, § 862a Rn. 4 ff. (Stand 2.1.2022). Selbst wenn man mit Wiebe eine Speichermöglichkeit allgemein verlangt, gibt es mittlerweile Speicher-Tools für Webseiten. So kann mit dem Chrome „atomshot" ein Screenshot von Internetseiten erstellt werden, die zusätzlich die genaue URL sowie die atomgenaue Uhrzeit im Screenshot darstellen.

213 Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 861 Rn. 16/2 (Stand 2.1.2022); Möslein ZHR 183 (2019), 254 (275).

214 Vgl. zum Warenautomaten KBB/Bollenberger/P. Bydlinski § 861 Rn. 3. Für eine Willenserklärung aber Hanzl HdB Blockchain S. 92 f.

215 KBB/Bollenberger/P. Bydlinski § 859 Rn. 9, § 864 Rn. 1.

216 KBB/Bollenberger/P. Bydlinski § 859 Rn. 9.

II. Maschinencode

1. Unter Anwesenden

Anwesende Parteien können gemeinsam programmieren und vereinbaren, dass sie als Vertrag nur den Maschinencode wollen. Der Umstand, dass der Maschinencode keine authentische, menschenlesbare Fassung hat, an der sich die Auslegung im Streitfall orientieren könnte, ist kein Problem. Denn auch ein mündlich geschlossener Vertrag ist später nur schwer auszulegen, weil die genauen Worte meist unwiederbringlich vergangen sind. Der Maschinencode muss nicht ausgelegt werden, wenn die Parteien festlegen, dass er ihre Vertragsgrundlage ist. Er führt nur das aus, was codiert ist, und das ist vertragskonform.

Dass die Parteien nicht wissen, wie der Compiler ihre Eingaben verändert, steht der Möglichkeit, den Maschinencode zur Vertragsgrundlage zu machen, nicht entgegen. Das zeigt insbesondere auch der Vergleich zur Möglichkeit des „aus des Hand Gebens" der Willenserklärung (Blankettunterschrift,[217] direkte Stellvertretung). Auch derjenige ist gebunden, der einen Vertrag ungelesen unterschreibt. Der Erklärende muss den Inhalt seiner Erklärung nicht kennen.[218] Ist er mit dem Durchgeführten unzufrieden, ist er vertraglich dennoch daran gebunden. Das bedeutet freilich nicht im Sinne der „Code-is-Law"-Behauptung,[219] dass die vertragliche Bindung endgültig und unveränderlich ist. Der Vertrag in Maschinencode unterliegt wie jeder andere Vertrag den Korrekturmechanismen des ABGB.[220]

Für diesen – wohl rein theoretischen – Fall sind die obigen Ausführungen zur Verständlichkeit und zum Bindungswillen zu ergänzen: Wollen die Parteien ihre Erklärungen nicht verstehen, aber daran gebunden sein und bedienen sie sich eines Computers oder dergleichen, für den die Erklärungen verständlich sind, genügt auch das.

---

217 Allgemein dazu OGH 1 Ob 43/15b, EvBl 2016/25 (Brenn); Kletečka/Schauer/Pletzer ABGB-ON[1.03] § 871 Rn. 11 f. (Stand 1.8.2019).

218 AA Smets/Kapeller ÖJZ 2018, 293 (294), allerdings nicht zum Maschinencode, sondern zur Abfassung in Programmiersprachen.

219 Siehe Fn. 335.

220 Ist der Vertrag ausgeführt und bemerkt eine Partei, dass sie ihren Willen fehlerhaft gebildet hat, kann sie den Vertrag bei Vorliegen der Voraussetzungen der §§ 870 ff. ABGB anfechten oder anpassen. Ist eine Partei mit dem Empfangenen über die Hälfte verkürzt, kann eine Berufung auf § 934 ABGB erfolgreich sein.

2. Unter Abwesenden

Wird der Maschinencode nicht ausnahmsweise unter Anwesenden zur Vertragsgrundlage gemacht,[221] besteht neben den bereits erwähnten Problemen mit der Vertrauenstheorie[222] und dem Bindungswillen[223] ein weiteres: Ein „Angebot" in Maschinencode kann in menschlicher[224] Kommunikation nicht zugehen. Es fehlt an der Möglichkeit der Kenntnisnahme. Anders als bei Erklärungen in einer fremden Sprache geht es nicht um individuelle Verständnisschwierigkeiten.[225] Niemand kann den Maschinencode lesen. Die Fehlerquelle ist anders als bei der Fremdsprache auch nicht die Übersetzung des Erklärungsempfängers, sondern der Compiler (des Erklärenden): Dieser übersetzt die Eingaben des Erklärenden und streicht Informationen, die der Computer für die Ausführung der Eingaben nicht braucht.[226] Der Grund für die Unmöglichkeit der Kenntnisnahme entsteht folglich bereits beim Erklärenden. Maschinencode kann unter Abwesenden in menschlicher Kommunikation nicht die Vertragsgrundlage bilden.

Daran ändert sich auch nichts, wenn der Erklärungsempfänger das vom Maschinencode bereits Durchgeführte duldet: In der Duldung liegt nämlich keine konkludente Annahme der „Erklärung" in Maschinencode, weil diese wie gezeigt mangels Zugangs kein Angebot iSd ABGB sein kann.[227] Der Maschinencode ist nicht der Vertrag.[228] Erst eine wechselseitige Duldung des jeweils Durchgeführten kann eine (konkludente) vertragliche Grundlage schaffen. So kann beispielsweise die rein in Maschinencode übermittelte Erklärung, am folgenden Tag einen Betrag X zu schenken, nicht zugehen. Sie ist schon deshalb kein Angebot iSd ABGB. Selbst

221 § 4 B.II.1.
222 Siehe dazu § 4 A. II. 2.
223 Siehe dazu § 4 A. III.
224 Zur Maschinen-Kommunikation s. § 5 C. II. und III.
225 Siehe dazu bereits § 4 A. II.
226 Dieser Prozess wird Optimierung genannt.
227 Zur Zugangsbedürftigkeit vgl. III. TN 78 BlgHH 132 ff., 154; Klang/Gschnitzer ABGB IV/1[2] § 862a S. 68 f.
228 Sieht der Maschinencode etwa eine Bedingung über die wechselseitige Akzeptanz aller weiteren Durchführungen vor, kann der Empfänger diese nicht zur Kenntnis nehmen. Sie gilt nicht. Dem Erklärenden bleibt regelmäßig nur die Möglichkeit, den nächsten Durchführungsschritten zu widersprechen und das Vertrauen darauf zu zerstören und/oder zu prüfen, ob das konkludent Geduldete irrtumsrechtlich anfechtbar ist. Dabei ist der Irrtum über die künftige Akzeptanz weiterer Durchführungen grundsätzlich ein unbeachtlicher Irrtum über Zukünftiges.

wenn sie der Empfänger mit einem Decompiler übersetzt und aus der Übersetzung ableitet, dass es sich um eine Schenkung handeln könnte, darf er nicht darauf vertrauen. Er muss nämlich wissen, dass mit Decompilern übersetzte Erklärungen (derzeit) inhaltlich entstellt sein können.[229] Kommt es am folgenden Tag tatsächlich etwa unter dem Verwendungszweck „Schenkung" zum Kontoeingang, kann erst deren Duldung die Vertragsgrundlage für eine wirklich gemachte Schenkung sein.

C. Besonderheiten on-chain

I. Rechtzeitiger Widerruf?

Wird eine Erklärung auf der Blockchain abgegeben, geht sie mit ihrer Aufnahme in einen Block zu. Die Blöcke gehören zum Organisations- und Machtbereich (auch) der adressierten Nutzer, weil sie die Möglichkeit der Kenntnisnahme haben.[230] Erst mit tatsächlicher Kenntnisnahme entsteht allerdings ein geschütztes Vertrauen auf ein verbindliches Angebot bzw. eine Annahme.[231] Der Erklärende kann seine Bindung daher theoretisch verhindern, wenn es ihm gelingt, dem Adressaten(-kreis) seinen Widerruf vor der Erklärung selbst zur Kenntnis zu bringen.

Dafür genügte theoretisch auch die Veröffentlichung des Widerrufs im nächsten Block oder ein Widerruf über andere Medien, den der Adressat(enkreis) vor dem publizierten Block wahrnimmt. Praktisch wird gegenüber einem Adressaten, der die Bindung an die Erklärung will, aber der Nachweis scheitern, dass er den späteren Block oder den sonstigen Widerruf zuerst zur Kenntnis genommen hat.[232] Ist der Vertragspartner bekannt – was insbesondere bei einer privaten Blockchain möglich ist –, könnte

229 Außerdem ist die Schenkung zu diesem Zeitpunkt mangels Übergabe oder Notariatsakt nicht verbindlich.

230 Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 861 Rn. 16/2 (Stand 2.1.2022). Für das BGB vgl. auch Heckelmann NJW 2018, 504 (506). Im Ergebnis gleich, aber mit der Ausführung, dass der dezentrale Charakter einer Blockchain der Denkfigur eines Organisations- und Machtbereichs diametral entgegenstehe, Möslein ZHR 183 (2019), 254 (276). Meines Erachtens machen Nutzer einer Blockchain diese auch zu ihrem Organisationsbereich.

231 KBB/Bollenberger/P. Bydlinski § 862 Rn. 1; Koziol FS Iro, 2013, 81 (87); zur Annahmeerklärung Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 862a Rn. 13 (Stand 2.1.2022).

232 Beweisschwierigkeiten bestehen auch beim traditionellen Widerruf, wenn die erste Erklärung nicht abgefangen werden kann.

immerhin ein rasch nachgeschalteter Telefonanruf oder eine (Chat-)Nachricht mit Lesebestätigung die Kenntnisnahme der auf den Weg gebrachten Erklärung überholen. Wie bei dem Telefonanruf, der den zur Post gebrachten Brief überholt, wird die Erklärung im nächsten Block dennoch zugestellt. Über dessen Timestamp sowie die Einsicht des Erklärenden in die Blockchain ist aber besser nachweisbar, dass die Erklärung zuvor widerrufen wurde. Der Adressat darf nicht auf den Bindungswillen dieser Erklärung vertrauen. Ist auf der Blockchain schon ein Leistungsaustausch in Gang gesetzt, muss der Widerrufende einen Vorbehalt zur Leistung machen, um sich den Rückforderungsanspruch zu sichern.[233] Die Korrektur der Blockchain kann durch einen contrarius actus in späteren Blöcken erfolgen.[234]

Eine Blockchain könnte – um den Widerruf bis zur tatsächlichen Kenntnisnahme zu erleichtern – eine Funktion ergänzen, die es ermöglicht, Erklärungen im Status „ungelesen" mit einem „Widerrufen"-Stempel zu versehen und deren Ausführung damit abzubrechen. Technisch ist das möglich, es führt aber zu Einbußen bei der Fälschungssicherheit.[235] Eine solche Anwendung müsste für die rechtssichere[236] Widerrufsmöglichkeit sicherstellen, dass der „gelesen/ungelesen"-Status für alle Adressaten wahr ist. Die Kenntnisnahme durch andere als die adressierten Netzwerkteilnehmer ist nicht schädlich. Mangels eines darauf gerichteten Willens sind sie nämlich nicht Empfangsboten.

233 Rummel/Rummel, 3. Aufl., ABGB § 1432 Rn. 6 f. (Stand 1.1.2002).

234 Saive DuD 2018, 764 (766). Einigen sich die Parteien nicht auf eine Korrektur, kann das Blockchain-Netzwerk Streitschlichtungsmechanismen vorsehen, Fries/Paal Smart Contracts/Kaulartz S. 73 (75). Freilich steht auch die Wahl staatlicher Einrichtungen offen, die Rückabwicklungs-, Anpassungs-, Anfechtungs- oder Schadenersatzlösungen erzwingbar machen. Der technologieneutrale Geltungsanspruch des Rechts soll allerdings nicht darüber hinwegtäuschen, dass dessen Durchsetzung mit Smart Forms und der Blockchain vor neuen Herausforderungen steht.

235 So könnte eine Hashfunktion (Chameleon-Hash) in den Code der Willenserklärung eingebaut werden. Dieser Chameleon-Hash lässt die Änderungen einer bestehenden Information in einem Block zu, ohne dass deshalb der äußere Hashwert (Header) des Blocks verändert werden müsste und deshalb die Kette der Blockchain invalid werden würde. Siehe dazu Martini/Weinzierl NVwZ 2017, 1251 (1256 f.); Saive DuD 2018, 764 (766).

236 Der Oblat könnte ansonsten etwa mit Screenshot-Tools (Fn. 212) oder unter Berufung auf inhaltliches Wissen zum gemachten Angebot leicht nachweisen, dass dessen Widerruf zu spät und unzulässig war.

II. Annahmefrist

Wird ein Vertrag auf der Blockchain unter Abwesenden geschlossen,[237] und keine Frist gesetzt, beginnt mit Absendung des Angebots die genannte dreiteilige Frist. Ihre Länge ergibt sich aus der üblichen[238] Dauer des Transports des Angebots zum Oblaten, einer angemessenen Überlegungsfrist sowie der üblichen Dauer des Transports der Annahmeerklärung retour zum Offerenten.[239] Die Transportzeit und die Zeit der unverzüglichen Anzeige des verspäteten Zugangs hängen grundsätzlich von dem benutzten Transportmedium sowie der Verkehrsüblichkeit ab.[240] Je nach Blockchain,[241] Aktivität der Miner, Höhe des Block-Rewards und der Transaktionsgebühr kann die Zeit, in der eine Erklärung in einen neuen Block aufgenommen wird, wenige Sekunden bis mehrere Stunden betragen. Für die jeweils benützte Blockchain muss eine Durchschnittsbetrachtung ausschlaggebend sein.[242] Praktisch bedeutend ist die Frage, welche Rolle die Höhe der Transaktionsgebühr bei dieser Durchschnittsbetrachtung einnehmen soll. Derzeit scheint es gerechtfertigt, sie bei der Fristberechnung unberücksichtigt zu lassen. Denn es kann nicht ohne weiteres angenommen werden, dass jemand besondere Transportkosten auf sich nimmt, um seine Erklärung besonders schnell in den Block aufnehmen zu lassen. Die ermittelte Reisezeit entspricht daher dem durchschnittlichen Reiseweg ohne zusätzlichem Kostenaufwand. Entwickeln sich Blockchains hingegen dahin, dass die weit überwiegende Anzahl ihrer Nutzer Transaktionsgebühren ausloben, wird deren durchschnittliche Höhe mit zu berücksichtigen sein.

Das Risiko der (im Verhältnis zur durchschnittlichen Reisedauer) verzögerten Reise der Erklärung trifft nach dem ABGB immer den Erklären-

237 Siehe dazu bereits ab Seite 37 f.

238 Klang/Gschnitzer ABGB IV/1[2] § 862 S. 65.

239 KBB/Bollenberger/P. Bydlinski § 862 Rn. 5; Rummel/Lukas/Rummel ABGB § 862 Rn. 3 (Stand 1.11.2014).

240 Klang/Gschnitzer ABGB IV/1[2] § 862 S. 65; Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 862 Rn. 4 (Stand 2.1.2022).

241 Eine Blockchain kann auch mehrere Layer haben. So gibt es neben dem Bitcoin Mainnet etwa das Bitcoin Lightning Netzwerk, das gerade dazu entwickelt wurde, die Geschwindigkeit und Anzahl der Transaktionen zu erhöhen.

242 Die durchschnittliche Blockzeit im Bitcoin Mainnet beträgt etwa zehn Minuten. Demgegenüber ist der Second-Layer das Bitcoin Lightning Netzwerk deutlich schneller.

den.[243] Hier weist die Blockchain im Vergleich zu herkömmlichen Transportmitteln den Vorteil auf, dass der Offerent den Zeitpunkt, zu dem sein Angebot zugeht, immer genau ermitteln kann. Er sieht nämlich den Timestamp des Blocks, mit dem seine Erklärung an die Blockchain angefügt wird. Er weiß dann, ob bereits die Reise seines Angebots verzögert war. Der Offerent darf nämlich nur unter der Voraussetzung des rechtzeitigen Ankommens seines Angebots mit dem Eintreffen einer Annahme innerhalb des zweifachen Postlaufs samt angemessener Überlegungsfrist rechnen (§ 862 Satz 2 ABGB). Die verzögerte Reise des Angebots verkürzt also nicht die angemessene Überlegungsfrist und durchschnittliche Reisedauer der Erklärung des Oblaten. Die Annahmeerklärung reist demgegenüber auf Gefahr des Oblaten (§ 862a Satz 2 ABGB). Hier ist der Timestamp des Blocks, mit dem seine Erklärung an die Blockchain angefügt wird, noch wichtiger. Denn er legt den Zeitpunkt des Vertragsabschlusses leicht ersichtlich für beide Parteien exakt fest.

III. Technische Störung – Fork

Es kann vorkommen, dass Erklärungen aufgrund technischer Probleme nicht in der Blockchain verbleiben und nicht durchgeführt werden. Das geschieht etwa bei der Gabelung der Blockchain in mehrere Zweige (*Fork*). Solche Gabelungen entstehen (selten aber doch), wenn und weil mehrere Personen (*Miner*) das mathematische Rätsel zur Bildung eines neuen Blocks zeitgleich lösen. Weil Netzwerkteilnehmer nach beiden Blöcken weitere Blöcke anfügen, entstehen zwei unterschiedliche Varianten der Blockchain. Für eine kurze Zeit bestehen zwei Äste mit identischen Blocknummern: Nach Blocknummer 100 folgen also zweimal Blocknummer 101, zweimal Blocknummer 102 usw. In diesem Zeitraum ist völlig offen, welcher Ast weitergeführt werden wird. Da nur einer als „wahr" weiter bestehen soll, wird in der Regel der kürzere, also der langsamer wachsende, Ast (technisch) aufgegeben. Ist eine Erklärung[244] oder der gesamte Vertrag in dem betroffenen Zweig enthalten, fallen sie aus der Blockchain.

243 Vgl. auch KBB/Bollenberger/P. Bydlinski § 862a Rn. 3; Rummel/Rummel, 2. Aufl. 2, ABGB § 862a Rn. 6; aA aber nunmehr Rummel/Lukas/Rummel ABGB § 862a Rn. 8 (Stand 1.11.2014).

244 Angebot und Annahme können in unterschiedlichen Blöcken gespeichert sein, Hanzl HdB Blockchain S. 90; Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 861 Rn. 16/2 (Stand 2.1.2022).

Das ist nicht mit dem rechtzeitigen Widerruf gleichzusetzen. Die Fork ist ein rein technisches Versagen. Ob dieses Versagen rechtliche Konsequenzen hat, ist unklar. Nicht zu folgen ist der Ansicht, dass für die rechtliche Verbindlichkeit von Erklärungen und Verträge auf einer Blockchain generell etwa sechs nachfolgende Blöcke abgewartet werden müsse.[245] Eine solche Wartefrist lässt sich weder aus dem ABGB ableiten noch ist sie ohne besonderen darauf gerichteten Zusatz den Willenserklärungen zu entnehmen. Welche rechtlichen Konsequenzen eine Fork hat, ist daher im Einzelfall zu prüfen. Dabei sind fünf Hauptfälle zu unterscheiden: Das Angebot ist zugegangen und es wurde vor der Fork zur Kenntnis genommen (i) oder es wurde vor der Fork nicht zur Kenntnis genommen (ii). Die Annahme ist zwar zugegangen, durch die Fork aber wieder aus der Blockchain gefallen (iii). Durch die Fork entfällt die fristgerechte Annahme durch Willensbetätigung (iv). Es entfällt jener Block, der beide Willenserklärungen des abgeschlossenen Vertrags enthält (v).

In Fall (i) ist das Angebot zugegangen und zur Kenntnis genommen worden. Es entfällt aber aus der Blockchain, bevor eine Annahme erfolgen konnte. Das führt nicht dazu, dass der Zugang oder die Bindung nachträglich entfallen. Für die rechtliche Verbindlichkeit des Angebots macht es keinen Unterschied, ob die zugegangene und zur Kenntnis genommene digitale Erklärung durch eine Fork vernichtet wird oder eine gelesene analoge Erklärung mit Wasser überschüttet und dadurch unleserlich wird. Sofern für die Annahme der Fortbestand des Angebots in der Blockchain nicht erforderlich ist, kommt mit Zugang der fristgerechten Annahme der Vertrag zustande. Bedarf es nur für die Vertragsdurchführung auch des Angebots in der Blockchain, besteht aus dem geschlossenen Vertrag ein (aus dem Erfüllungsanspruch abgeleiteter) Anspruch des Oblaten auf erneute Ablage des Angebots in der Blockchain. Anderes gilt, wenn das Angebot nur angenommen werden kann, wenn es selbst noch in der Blockchain ist, etwa weil es zugleich die Wallet[246] generiert, an welche zur Annahme Assets gesendet werden sollen. Die Bindungsfrist an dieses Angebot läuft ungenützt aus, weil der Oblat keine Annahme durch Willensbetätigung auf den Weg bringen kann. Es kommt kein Vertrag zustande. Kann der Oblat dem Offerenten innerhalb der Bindungsfrist mitteilen, den Vertrag zu wollen, aber wegen der Fork nicht formgerecht annehmen zu können, ist für den jeweiligen Einzelfall zu prüfen, ob ein Vertrag zustande kommt oder ein

245 So aber Bertram MDR 2018, 1416 (1419).
246 Siehe Fn. 14.

Anspruch auf Wiederholung eines derart entfallenen Angebots besteht: Es käme mit dieser Mitteilung zu einem Vertragsabschluss, wenn das Angebot keine besonderen (Form-)Vorgaben für seine Annahme macht. Ansonsten kann sich die Pflicht zur Wiederholung des Angebots auf der Blockchain aus vorvertraglichen Schutz- und Sorgfaltspflichten des Offerenten ableiten lassen.

In Fall (ii) entfällt der Block, bevor der Adressat das Angebot zur Kenntnis nimmt.[247] Das Angebot ist unabhängig von der Kenntnisnahme mit der Aufnahme in die Blockchain zugegangen.[248] Die Fork führt auch nicht dazu, dass der Zugang entfällt. Da die Erklärung zumindest vorübergehend in einem Block aufgenommen war, bestand die Möglichkeit der Kenntnisnahme unter normalen Umständen.[249] Der besondere Umstand des Risikos einer Fork ist – wie die Zuordnung einer E-Mail zum Spamordner –[250] dem Oblaten zuzuordnen; es verhindert oder vernichtet nicht den Zugang.[251] Im Hinblick auf die Rechtsfolgen ist zu differenzieren: Dem Offerenten steht es frei, das Angebot unter Hinweis auf die Fork zu wiederholen. Denn sieht der Oblat die Erklärung nicht zufällig auf einer Orphan-Blocks-Liste,[252] wird das Angebot sonst in der Regel ungenützt auslaufen. Will der Offerent demgegenüber nicht mehr gebunden sein, kann er hoffen, dass die Bindung an sein Angebot ungenützt ausläuft. Er könnte sein Angebot aber theoretisch auch widerrufen, weil erst mit tatsächlicher Kenntnisnahme ein geschütztes Vertrauen des Oblaten auf das Angebot entsteht.[253]

247 Beweisprobleme ließen sich insbesondere in privaten Blockchains über den oben erläuterten gelesen/ungelesen-Status vermindern. Siehe dazu § 4 C. I. am Ende.

248 Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 861 Rn. 16/2 (Stand 2.1.2022). Für das BGB vgl. auch Heckelmann NJW 2018, 504 (506). Bei Aufnahme in der Nacht oder am Wochenende gilt als Zugangstag der nächste Werktag. Denn hier müssen ähnliche Regeln gelten wie für den Zugang von Fax oder E-Mail. Siehe dazu Wilhelm ecolex 1990, 208 (209); Zankl ecolex 2001, 344.

249 OGH 18.4.1989, 5 Ob 559/88; OGH 8 ObA 254/94, ÖJZ 1995/43.

250 OGH 3 Ob 224/18i, ecolex 2019/285 (Schoditsch).

251 Die Annahme, dass Erklärungen und Transaktionen in beiden Ketten erst zugehen, wenn der Fortbestand ihrer Kette gesichert ist, könnte das System zum Zusammenbruch bringen: Überlegte Nutzer würden keine Transaktionen mehr ablegen wollen, bis geklärt ist, welche Kette fortgeführt wird. Im Extremfall führte das zum Stillstand beider Stränge.

252 Diese Listen führen Transaktion an, die wegen einer Fork aus der Blockchain gefallen sind.

253 Vgl. KBB/Bollenberger/P. Bydlinski § 862 Rn. 1; Koziol FS Iro, 2013, 81 (87); zur Annahmeerklärung Kletečka/Schauer/Wiebe ABGB-ON[1.04] § 862a Rn. 13 (Stand 2.1.2022). AA bzw. widersprüchlich Hanzl HdB Blockchain S. 97 f.

Allerdings wird ihm im Streitfall der Nachweis, dass sein Widerruf vor der Kenntnisnahme des Angebots einlangte, ohne den vorgeschlagenen „Widerrufen"-Stempel schwer gelingen.[254] Gelingt der Beweis nicht, gilt das zu Fall (i) gesagte.

In Fall (iii) entfällt der Block, in dem die Annahme enthalten ist. Die Annahme ist mit der Ablage auf der Blockchain zugegangen.[255] Mit diesem Zeitpunkt kommt der Vertrag zustande. Die Kenntnisnahme ist dafür nicht relevant. Die Parteien sind an den Vertrag gebunden. Keine Partei kann die Fork daher zum Anlass nehmen, sich einseitig von dem (mittlerweile nicht mehr gewollten) Vertrag zu lösen. Da die Rechtsfolgen des Vertrags mit der Aufnahme der Annahme in den (nunmehr entfallenen) Block eintreten, trifft die Vertragsparteien die Obliegenheit, regelmäßig die Orphan-Blocks-Liste zu kontrollieren.[256] Sieht der Offerent die Annahme auf der Orphan-Blocks-Liste, kann er die Wiederholung der Erklärungverlangen. Entsprechendes gilt für den Oblaten. Technisch kann es zu diesem Zeitpunkt erforderlich sein, dass nicht nur die Annahme, sondern zuvor auch das Angebot erneut abgeben werden muss.[257]

Für Fall (iv) ist entscheidend, ob mit der Willensbetätigung dem Angebot fristgerecht in nach außen erkennbarer Weise tatsächlich entsprochen wurde.[258] Das ist zu bejahen, wenn und sobald der Block angefügt ist. Sein nachträglicher Wegfall durch eine Fork ändert mE nichts am Vertragsschluss. Wegen des Wegfalls der bereits gesetzten Erfüllungshandlung ist die Verbindlichkeit aus dem Vertrag aber nicht erloschen.[259] Ist die Leistung durch die Fork verzögert, treten daher die Folgen des objektiven Schuldnerverzugs ein: Der Gläubiger könnte grundsätzlich zwischen Erfüllung und Vertragsrücktritt wählen. Mit der Fork tritt nicht zugleich Gläubigerverzug ein. Denn dieser setzt voraus, dass der Schuldner gehörig betreffend Zeit,

254 Siehe dazu bereits § 4 C. I.
255 Es gilt das für Fall (ii) Ausgeführte.
256 Gleiches gilt etwa auch für den Spamordner, s. OGH 3 Ob 224/18i, ecolex 2019/285 (Schoditsch).
257 Siehe dazu Fall (i) und Fall (iv).
258 Siehe KBB/Bollenberger/P. Bydlinski § 864 Rn. 2.
259 Das kann etwa auch daraus abgeleitet werden, dass eine anfechtbare Zahlung nicht als Erfüllung betrachtet wird. Vgl. dazu Kletečka/Schauer/Stabentheiner/Kolbitsch-Franz ABGB-ON[1.05] § 1412 Rn. 7 (Stand 1.1.2023); Rummel/Lukas/Reischauer ABGB § 1412 Rn. 12 f. (Stand 1.10.2020).

Ort und Art endgültig die Leistung erbringt.[260] Die Fork verhindert das gerade.

In Fall (v) entfällt der Block mit beiden Willenserklärungen. Da der Vertrag aber bereits zustande gekommen ist, ist er verbindlich. Das rein technische Problem der Fork ändert daran ebenso wenig wie das zufällige Verbrennen eines Vertrags aus Papier.[261] Anders als bei einem Papiervertrag führt der Entfall des Vertrags on-chain aber nicht zu Beweisthemen.[262] Besonderheiten ergeben sich aber daraus, dass der Vertrag meist gerade auch die Vertragsdurchführung bewirken soll. Er muss daher wieder in die Blockchain gelangen. Sieht der Vertrag für den Fall einer Fork keine (anderen) Folgen vor, folgt ein entsprechender Anspruch auf Wiederablage in der Blockchain aus der ergänzenden Vertragsauslegung. Denn die Parteien wollten ihre Vertragsbeziehung auf einer Blockchain abwickeln und haben auch für die bekannte Möglichkeit einer Fork keine abweichende Regelung vorgesehen. Wollen sie anderes, müssen sie etwa ihren Vertrag aufschiebend mit dem Nichteintritt einer Fork bedingen.[263] Ansonsten haben beide Vertragspartner aus dem Vertrag einen Anspruch auf erneute Ablage und Durchführung der Transaktion.[264] Fallen dabei (erneut) Kosten an, sind diese mangels abweichender vertraglicher Regelung wie zuvor zu tragen.[265]

D. Zwischenergebnis und Anwendungsbeispiel

Die Ergebnisse des Abschnitts lassen sich am Beispiel des Künstlers veranschaulichen.[266] Er gibt in dem Programmcode auf seiner Webseite ein verbindliches Angebot zum Verkauf des jeweils eingestellten NFT ab. Sein Angebot ist frei und ernstlich und es bezeichnet Ware (eingestelltes NFT)

260 Kletečka/Schauer/Stabentheiner/Kolbitsch-Franz ABGB-ON[1.05] § 1419 Rn. 2 (Stand 1.1.2023).

261 Zweifelnd Hanzl HdB Blockchain S. 97 f.; wohl auch Heckelmann NJW 2018, 504 (505 f.).

262 Orphan-Blocks-Liste belegen Verträge, die wegen einer Fork aus der Blockchain gefallen sind.

263 Dieses Regel-Ausnahmeverhältnis enthält auch § 93 Abs. 1 NO: Mangels abweichender Vereinbarung haben die Parteien unter Kostentragung ein Recht auf wiederholte Ausfertigungen, s. Wagner/Knechtel NO § 93 Rn. 1 (Stand 1.1.2007).

264 So auch D. Paulus/Matzke ZfPW 2018, 431 (448).

265 Blockchains können für Orphan-Blocks unterschiedliche Lösungen vorsehen.

266 Siehe dazu § 3 A.

und Preis (Höchstbieter in EUR) bestimmt. Es ist überdies für jeden verständlich, der die verwendete Programmiersprache erlernt hat. Der Künstler gibt sein Angebot auch mit Bindungswillen ab. Sein Angebot geht ab der Publikation des Programmcodes auf der Webseite jedermann zu, der die Möglichkeit der Kenntnisnahme hat. Es erfolgen Erklärungen von Interessenten. Auf Konsens und damit eine Annahmeerklärung trifft das Angebot nur bei der Bieterin mit UID, die bis zum Tag X das höchste Gebot in EUR abgegeben hat. Diese Bieterin und der Künstler schließen einen Kaufvertrag in Programmcode.

Die eingangs gestellte Frage, ob das ABGB den Abschluss des Vertrags in Programmcode ermöglicht, ist also grundsätzlich zu bejahen. Zusätzliche Anordnungen, wie Formpflichten, Sprachvorgaben oder strengere Vorgaben an die Verständlichkeit im Konsumentenschutzrecht, können dem entgegenstehen oder den Vertragsschluss zumindest aufwendiger machen.

§ 5 Wo ist Code die bessere Vertragsgrundlage?

Es wurde gezeigt, dass Code als Vertragsgrundlage vereinbart werden kann. Auf dieser Grundlage setzen sich die folgenden Abschnitte mit jenen Vorteilen auseinander, die die Verwendung von Codes bringen soll: Es wird untersucht, ob sie im Verhältnis zu analogen Verträgen tatsächlich kostengünstiger (Abschnitt A.) und sicherer sind sowie ohne Intermediäre (Abschnitt B.) auskommen. Überdies ist zu prüfen, ob trotz der sprachlichen Barrieren die Vorteile der Automatisierung des Vertragsabschlusses und der Vertragsdurchführung erreicht werden können (Abschnitt C.). Schließlich tastet ein Ausblick das Potential von Smart Contracts und Smart Forms bei der Vertragsdurchführung ab (Abschnitt D.).

A. Kostenfrage

Die Verwendung von on-chain Smart Contracts birgt nach verbreiteter Ansicht enormes Kosteneinsparungspotenzial: Nach Schätzungen des Bankhauses Goldman Sachs könnten jedes Jahr weltweit über sechs Milliarden US-Dollar eingespart werden, wenn die Nachhandelsaktivitäten bei Wertpapieren mit Smart Contracts durchgeführt würden.[267] Ähnliches Potenzial

267 Zitiert nach Waschbusch/Kiszka/Merz ÖBA 2021, 547 (552).

bestehe bei Hypothekarkrediten.[268] Auch bei Micro-Krediten wird hohes Einsparungspotential gesehen.[269] Darüber hinaus wird recht allgemein vorgebracht, dass Smart Contracts mit geringeren Transaktionskosten einhergehen.[270]

Bei der Beurteilung der Vor- und Nachteile der Verwendung von Smart Contracts dürfen aber die damit verbundenen Kosten nicht außer Acht gelassen werden. Bei Smart Contracts on-chain ist etwa an die auf der Blockchain anfallenden Kosten zu denken: Miner müssen unter Einsatz großer Mengen an Rechenleistung und Hardware die Transaktionen bestätigen. Es bedarf also eines Anreizes für Miner, diese Kosten zu tragen und Transaktionen zu bestätigen. Der Anreiz ist eine Art Finderlohn (Block-Reward) für den Miner, der das mathematische Rätsel für die Bestätigung des nächsten Blocks als erster löst. Dieser Block-Reward besteht derzeit häufig aus neu geschaffenen Kryptoeinheiten.[271] Daraus leitet sich auch der Begriff (Gold)Mining – (Gold)Schürfen – ab.[272] Der Miner erwirbt solche Einheiten originär. Da viele Blockchains nur eine begrenzte Anzahl an neu schürfbaren Einheiten ausgeben, wird der Anreiz der Miner laufend geringer.[273] Das potenzielle Gegenargument, die Kryptowährung werde laufend mehr wert, läuft spätestens dann leer, wenn keine neuen Einheiten mehr geschürft werden können.[274] Denn dann kann kein Finderlohn an Miner mehr ausgezahlt werden. Der Anreiz, dennoch weiter Transaktionen zu bestätigen, muss also irgendwann unmittelbar von den Nutzern der Smart Contracts übernommen werden.

Dieser Anreiz kann in der Zahlung einer Transaktionsgebühr liegen. Nutzer versprechen bereits zusätzlich eine Transaktionsgebühr für die

268 Capgemini, 2016, 11, https://www.capgemini.com.

269 Unter der Voraussetzung einer proof-of-stake-Lösung Hoffmann-Riem Digitale Transformation S. 1.

270 Fraunhofer-Institut, Whitepaper, 2018, https://www.iml.fraunhofer.de; Szabo, Public Networks, 1997, https://nakamotoinstitute.org; Fries/Paal Smart Contracts/Finck S. 1 (7); Fries/Paal Smart Contracts/Erbguth S. 25 (25); Fries/Paal Smart Contracts/Matzke S. 99 (107 ff.); Bolesch/Mitschele ZfgK 2016, 1125 (1128); Forgó/Zöchling-Jud 20. ÖJT II/1/Forgó S. 285 (344); Kaulartz/Heckmann BM 2016, 34 (35).

271 Piska/Völkel Blockchain/Völkel Rn. 1.52 ff.: Block-Rewards.

272 Piska/Völkel Blockchain/Völkel Rn. 1.52.

273 So wird die Höhe der Belohnung der Miner für die Bestätigung einer Transaktion mit jedem Bitcoin-Halving halbiert. Das passiert alle 210.000 Blöcke, bis 21 Millionen Bitcoins geschürft wurden.

274 Bei Bitcoin also, sobald 21 Millionen geschürft wurden.

Durchführung von Smart Contracts on-chain.[275] Sie tun das, damit ihr Transaktionswunsch (schneller) in einen Block gespeichert wird. Je höher sie die Auslobung festsetzen, desto schneller wird der Smart Contract von einem Miner in einen Block integriert. Das ist bedeutsam, wenn im nächsten Block nicht genügend Speicherplatz frei ist, um sämtliche ausstehenden Transaktionen abzulegen. Wollen die Parteien den Smart Contract daher schnell schließen, müssen sie bereits eine entsprechend hohe Transaktionsgebühr ausloben. Jener Miner, dem es als erstes gelingt, den Block samt der Transaktion zu bestätigen, erhält diese Auslobungssumme.[276]

Neben diesen unmittelbaren Transaktionskosten sind auch „mittelbare" Kosten zu berücksichtigen. Blockchains mit Konsensmechanismen wie dem gerade geschilderten[277] verbrauchen enorme Energiemengen.[278] Das belastet die Umwelt und äußert sich in regionaler Energieknappheit oder im Steigen des allgemeinen Energiepreises.[279] Rechtsökonomisch könnten solche externen Kosten[280] – im Einklang mit einem Vorstoß der Europäischen Kommission[281] – ein Verbot energieintensiver Konsensmechanismen rechtfertigen. Die hohen Kosten sind überdies ein Hauptgrund, warum

275 Piska/Völkel Blockchain/Völkel Rn. 1.53: Transaction Fees. Auf der Ethereum Blockchain werden die Transaktionsgebühren als „Gas" bezeichnet. Die Zwischenschaltung von Gas erfolgt, weil Ether sehr volatile Kurse hat. Die Kosten der Energie für die Transaktionen schwanken hingegen nicht in gleichem Ausmaß. Um einen stabilen Preis für Transaktionen gewährleisten zu können, wird zunächst festgesetzt, wie viel Gas zu zahlen ist, das dann umgerechnet in Ether zu bezahlen ist, s. Hanzl HdB Blockchain S. 38 f.

276 So auch Völkel ZFR 2021, 532 (538); Piska/Völkel Blockchain/Völkel Rn. 1.57 f. Der Miner nimmt bei der Ablage auf der Blockchain (nur) eine Art Botenstellung ein. Er wird durch das Mining nicht zum Auftragnehmer, weil er keinen rechtsgeschäftlichen Willen bildet und nicht zum Werkhersteller, weil er das Mining auf eigenes Risiko beginnt und keinen Erfolg schuldet.

277 Das ist ein proof-of-work-Konsensmechanismus.

278 Rutz Blockchain S. 59; Hoffmann JSSI 2021, 1 (6 f.); Reder/Eckard Cash S. 108 f. Der Bitcoin Electronic Waste Monitor (s https://digiconomist.net/bitcoin-energy-consumption/) zeigt, dass das Bitcoin-Netzwerk rund 130 Terrawattstunden Energie im Jahr verbrauche, soviel wie Argentinien. Eine Bitcoin-Transaktion benötige rund 1.407 Kilowattstunden. Ein durchschnittlicher US-amerikanischer Haushalt komme damit über 48 Tage aus.

279 Perlaki, 2018, https://brutkasten.com/.

280 Zu den Externalitäten s. etwa Engert in Grundmann/Möslein 153 (176 ff.); Schäfer/Ott Ökonomische Analyse S. 679. Blockchains mit proof-of-work laufen seit 2008 (Satoshi Nakamoto, Bitcoin White-Paper, 2008, https://bitcoin.org/bitcoin.pdf).

281 Im Zuge der Einführung der MiCA-VO (EU) 2023/1114 kam es zu Diskussionen, ob der proof-of-work-Mechanismus auf EU-Ebene zu verbieten sei.

Blockchain-Lösungen nicht so skalierbar sind wie zentrale Systeme.[282] Andere Konsensmechanismen[283] und Technologien[284] versuchen daher die Energiekosten zu senken. Bisher ungelöst ist allerdings die mit geringeren Kosten einhergehende höhere Fälschungsanfälligkeit.[285]

Berücksichtigt man die genannten Kosten, ist die Initialisierung eines Smart Contracts on-chain sehr teuer.[286] Die Belastung bleibt selbst dann hoch, wenn ein bestehender Smart Contract mehrfach verwendet wird. Denn auch dann fallen Kosten für jede Durchführung an. Der Behauptung, dass Smart Contracts on-chain mit geringeren Transaktionskosten auskommen, kann derzeit also nicht in dieser Allgemeinheit zugestimmt werden.

B. Fälschungssicherheits- und Dezentralitätsfrage

Aufgrund der genannten Kosten laufen die meisten Smart Contracts off-chain.[287] Der Code des Smart Contracts ist dann nicht in einem Block der Blockchain abgelegt, sondern allenfalls – aber nicht zwingend – mit dieser Blockchain verlinkt. Dafür wird mit Verweisen auf externe Quellen oder Hashwerten gearbeitet.[288] Dadurch geht aber ein wesentlicher Vorteil verloren: die Dezentralität, und damit zusammenhängend die Fälschungssicherheit.[289]

---

282 Thießen ZfgK 2020, 706 (711); zum Vergleich von Kredit- und Debitkartenlösungen s. Hoffmann JSSI 2021, 1 (5 f.).

283 Mit Grafik Sutherland Joule 2019, 917 (918). Bei proof-of-stake wählt ein Algorithmus Nutzer mit entsprechend großem (Kapital-)Anteil aus, die den Block bestätigen. Das ist weniger energieintensiv, weil nicht alle Miner um die Wette rechnen.

284 Intel will das Energieproblem für Mining von Kryptoassets und NFT-Mint mit einem 1000-fach effizienteren Chip lösen, https://www.intel.com/content/www/us/en/newsroom/opinion/thoughts-blockchain-custom-compute-group.html#gs.p5bb09. Lösungen sucht auch COTI, s. https://coti.io/.

285 Ein gewichtiges Problem der Blockchain ist, dass sie – zumindest bei proof-of-work-Konsensmechanismen – teuer sein muss, um eine hohe Fälschungssicherheit aufrecht zu erhalten. Wäre es nicht unwirtschaftlich, viele Blöcke zu ändern, könnten Hacker vereinfacht gesagt viele Benutzerkonten anlegen, so die Mehrheit im Netz erlangen und die gesamte Blockchain neu minen und schreiben. Siehe dazu bereits § 2 A..

286 Kucsko/Pabst/Tipotsch/Tyrybon ecolex 2021, 495 (498).

287 Diedrich Ethereum S. 30, 37.

288 Diedrich Ethereum S. 30, 37; zum Selbstversuch, Kucsko/Pabst/Tipotsch/Tyrybon ecolex 2021, 495 (498).

289 Zum Zusammenhang s. auch Fries/Paal Smart Contracts/Pesch S. 13 (23).

Smart Contracts auf einer Blockchain sollen die Funktion zentraler Intermediäre (Notar, Gericht, Rechtsanwalt, Bank oder Zahlungsdienstleister) übernehmen können. Statt in eine Person, die speichert, verwaltet, kontrolliert, sperrt und löscht, könne in viele vertraut werden.[290] Wird allerdings nur der Hashwert als Fingerabdruck[291] des Vertragscodes on-chain abgelegt, besteht die Dezentralität gerade nicht. Zwar lässt sich binnen Sekunden beweisen, dass der Code manipuliert ist, wenn sein aktueller Hashwert nicht mit dem abgelegten Hashwert übereinstimmt. Überdies kann der Leistungsaustausch davon abhängig gemacht werden, dass ein Programm vor der Durchführung die Übereinstimmung der Hashwerte bestätigt.[292] Der gerade nicht dezentral gespeicherte Code selbst bleibt aber manipulierbar. Die Grundidee dezentraler Peer-to-Peer-Systeme ist dann nicht umgesetzt.[293]

Dieses ursprüngliche Anliegen der Dezentralität ist aber mittlerweile auch sonst nicht verwirklicht. Der Zugang zu Netzwerken, die Zusammenführung von Käufer und Verkäufer oder auch nur die Passwortverwahrung[294] hat den Jedermann überwältigt. Krypto-Dienstleister,[295] die das erleichtern, sind mittlerweile so (markt-)mächtig, dass sie zu Gatekeepern geworden sind.[296] Hinzu kommt, dass Blockchain-Protokolle regelmäßig mittels hard Fork geändert werden können.[297] Dafür müssen ausrei-

290 Im Detail s. bereits § 2 A.

291 Siehe dazu bereits § 2 A.

292 Diedrich Ethereum S. 30, 37.

293 Siehe dazu § 2 A.

294 In einem echten dezentralen System hat niemand ein Backup von Passwörtern. Verliert jemand den Private Key zu seiner Wallet (Fn. 14), ist der Zugang zu den darin abgelegten Coins unwiederbringlich verloren.

295 Siehe Forgó/Zöchling-Jud 20. ÖJT II/1/Forgó S. 285 (331 Fn. 1043).

296 Das ist gerade in streng regulierten Branchen wie dem Bankensektor gefährlich. Für die Energiewirtschaft krit. Krönke/Tschachler RdU 2021/127, 250.

297 Nach allgemeinen vertragsrechtlichen Regeln ist grundsätzlich (nur) eine einvernehmliche Korrektur der Vertragsgrundlage möglich. Anderes gilt nur dann, wenn die Vertragsgrundlage selbst Mehrheiten für ihre Änderung genügen lässt; s. für die GesbR Kletečka/Schauer/Warto ABGB-ON[1.04] § 1175 Rn. 9 (Stand 15.1.2021). Für die Teilnehmer einer Blockchain lässt sich aber nicht argumentieren, dass sie sich immer zu einer GesbR zusammenschließen. Fassen sie diesen Entschluss doch, was etwa bei DAO möglich ist, sind Vertragsänderungen, die nachträglich negativ in die zentralen Rechte der Mitglieder eingreifen, selbst dann nur mit deren Zustimmung möglich, wenn die Vertragsgrundlage ansonsten Mehrheiten für ihre Änderung genügen lässt. Zu dieser Kernbereichslehre s. etwa U. Torggler/Diregger GmbHG § 50 Rn. 17 (Stand: 1.8.2014); F. Hartlieb Verbandsvertragsrecht S. 480 ff.; U. Torggler/Kraus UGB § 119 Rn. 18 (Stand 1.1.2019).

chend viele Netzwerkteilnehmer oder Netzwerkteilnehmer mit ausreichend Stimmgewicht die Änderung akzeptieren.[298] Das geschah bei dem bekannten DAO-Hack.[299] Die Netzwerkteilnehmer stimmten dafür, den Code umzuprogrammieren und eine Transaktion rückgängig zu machen.[300] Die Möglichkeit einer Hard Fork untergräbt damit das Versprechen, ein „neutraler" Code erfülle „unveränderlich" den Vertrag. Denn die Mehrheit oder besonders mächtige Gatekeeper können – unter Verfolgung von Eigeninteressen – einen Vertrag rückgängig machen und sich damit über den neutralen Code hinwegsetzen. Vom Versprechen, nicht auf einen Intermediär angewiesen zu sein, ist damit wenig übrig.

C. Einsatz im Massengeschäft und Lösung der Sprachbarriere

Ein weiterer Vorteil von Smart Contracts liege darin, mit Codes den Vertragsabschluss und (jedenfalls zwischen leistungswilligen Parteien)[301] die Vertragsdurchführung zu automatisieren. Im Massengeschäft bringt das Erleichterungen. Damit dieses Potenzial realisiert werden kann, muss die Kommunikation in Code, die für viele Menschen eine Barriere ist, aber vereinfacht werden. Welche Auswirkungen das auf die Vertragsgrundlage hat, ist zu zeigen (Abschnitt I.). Zu diskutieren ist überdies, wie und ob Menschen die Hürden der Kommunikation in Code durch den Einsatz von Maschinen (Abschnitt II.) und autonomen Softwareagenten (Abschnitt III.) bewältigen können.

298 Piska/Völkel Blockchain/Brameshuber Rn. 14.1.

299 Die 2016-DAO war ein komplexer Code auf der Ethereum Blockchain, der Crowdfunding-Lösungen umsetzte. Innerhalb weniger Monate vereinnahmte die 2016-DAO Ether im Gegenwert von ungefähr 150 Millionen USD. Eine Split-Funktion ermöglichte es Anlegern, auszuscheiden und ihr Kapital in eine Tochtergesellschaft abzuziehen. Ein Fehler dieser Funktion ermöglichte es einem Hacker, rund 3,6 Millionen Ether (damals ungefähr 50 Millionen USD) abzuziehen. Siehe dazu Rodrigues ILR 104 (2019) 679, 681, 704; Bergmann, 2016, https://bitcoinblog.de; Hoppen, 2016, http://www.cr-online.de.

300 Rodrigues ILR 104 (2019) 679, 706: über 85 %.

301 Zum Besitzschutz s. § 5 D. I.

I. Code im Hintergrund versus äußeres Erscheinungsbild

Gedanklicher Ausgangspunkt der folgenden Ausführungen ist der klassische Warenautomat: Dieser kann interne mechanische und technische Abläufe aufweisen, die der Käufer der Ware nicht versteht. Das ist für den Abschluss des Kaufvertrags aber irrelevant. Es reicht zu wissen, dass er – solange der Vorrat reicht – durch Münzeinwurf im angegebenen Ausmaß eine der ausgestellten Waren erwerben kann. Laut Anzeige bekommt er etwa für zwei Euro einen Schokoriegel. Der Vertragsschluss funktioniert insofern automatisiert, als der Aufsteller durch die Inbetriebnahme des Automaten an einen unbestimmten Personenkreis anbietet und jedermann durch Willensbetätigung, nämlich Münzeinwurf, annehmen kann.[302] Ist der Automat intern so eingestellt, dass er den Schokoriegel erst ab dem Einwurf der zweiten 2-Euro-Münze ausgibt, ist auszulegen, was Vertragsgrundlage geworden ist. Der objektive, redliche Erklärungsempfänger darf unter Berücksichtigung aller Umstände das Angebot so verstehen, der Anzeige am Automaten entsprechend die Ware um zwei Euro zu erwerben. Die interne Einstellung ist weder Inhalt des Angebots noch des Vertrags geworden. Leistet der Automat entgegen seinem äußeren Erscheinungsbild nach dem Einwurf der ersten 2-Euro-Münze nicht, liegt darin ein Vertragsbruch.

Ganz ähnlich, aber digital lässt sich off- und on-chain der Vertragsabschluss und dessen Durchführung automatisieren. Die Tools dafür werden häufig als Smart Contract bezeichnet. Das ist aber zu pauschal, es ist vielmehr rechtlich zu differenzieren:[303]

Bietet das Tool etwa on-chain oder auf einer Webseite in herkömmlicher Sprache eine Software zum Download an und tritt der Code dabei für die Nutzer des Tools nicht in Erscheinung, wird der Programm- oder Maschinencode nicht zur Vertragsgrundlage. Der Code dient dann als bloße Smart Form im Hintergrund der Ausführung eines in herkömmlicher Sprache geschlossenen Vertrags. Weicht die Smart Form von dem ab, was nach dem äußeren Erscheinungsbild Vertragsgegenstand wurde, leistet sie vertragswidrig.[304] So kann etwa ein Vermieter auf einer Webseite den Abschluss eines Mietvertrags der Wohnung Ia in herkömmlicher Sprache anbieten. Der Mieter kann durch Überweisung des Betrags X an die angegebene Adresse der Smart Form annehmen. Die Smart Form überweist sodann

302 KBB/Bollenberger/P. Bydlinski § 861 Rn. 3.
303 Zur Unterscheidung von Smart Contracts und Smart Forms s. § 3 B.
304 Vgl. Buchleitner/Th. Rabl ecolex 2017, 4 (9).

den Betrag X an den Vermieter und entriegelt das Mietobjekt für den Mieter.[305] Entriegelt die Smart Form statt Wohnung Ia die Wohnung IIa, ist zu ermitteln, was Vertragsgrundlage geworden ist: das äußere Erscheinungsbild oder der im Hintergrund laufenden Code. Der Mieter sieht den Code nicht, sondern nur das äußere Erscheinungsbild in herkömmlicher Sprache. Nimmt er das Angebot an, kommt der Vertrag so zustande, wie sich das äußere Erscheinungsbild des Angebots für den objektiven Erklärungsempfänger darstellt. Die Vertragsgrundlage ist also die Darstellung auf der Webseite.[306] Daran ändert auch nichts, dass die Kommunikation zwischen Smart Form, Webseite, Wohnung und gegebenenfalls Blockchain in Programm- oder Maschinencode läuft. Geschuldet ist die Entriegelung von Wohnung Ia. Weicht der Code von dem äußeren Erscheinungsbild ab, führt er den Vertrag nicht richtig durch. Die Smart Form ist fehlerhaft und der Vermieter in Verzug.

Formulieren die Parteien ihren Vertrag gemeinsam mit Hilfe eines Baukastens,[307] wird mangels abweichender Vereinbarung nur das äußere Erscheinungsbild des Baukastens Träger der Willenserklärungen und nicht der vom Baukasten im Hintergrund produzierte Programmcode.[308] Das äußere Erscheinungsbild des Baukastens kann aber dann irrelevant sein, wenn (nur) eine Partei den Programmcode mit einem Baukasten generiert und diese Partei in der Folge nur den Programmcode an den präsumtiven Vertragspartner oder an die Blockchain übermittelt. Der Oblat darf die Erklärung so verstehen, wie sie ihm zugeht, also in Programmcode. Nimmt er das Angebot zum Vertragsschluss an, entsteht der Vertrag auf der Grundlage des Programmcodes. Es liegt dann nicht bloß eine Smart Form, sondern ein Smart Contract vor.

Für die Erwerber eines NFT des Künstlers[309] über die Plattform mag die Verkaufsmitteilung, die Abbildung und danach die Freischaltung des Downloads im Hintergrund über Smart Forms gesteuert sein. Die Vertragsgrundlage besteht aber nur so, wie der objektive Erklärungsempfänger das

305 Vgl. dazu auch aber unter der Bezeichnung Smart Contract Wilkens/Falk Smart Contracts S. 30 ff. und die Abbildung auf Seite 32.

306 Vgl. für das BGB Wilkens/Falk Smart Contracts S. 31.

307 Siehe zum hier verwendeten EtherScripter § 2 C.

308 Ist der Baukasten fehlerhaft und entsteht aufgrund der fehlerhaften Vertragsdurchführung ein Schaden, kann das in Abhängigkeit vom Auftreten des Baukasten-Anbieters Schadenersatzfolgen für ihn haben. Vertragliche Schadenersatzansprüche hätten etwa Parteien, die beim Anbieter des Baukastens ein entgeltliches Abonnement zur Herstellung von Smart Contracts beziehen.

309 Siehe dazu § 3 A.

Angebot „Heute für [NFT-Abbildung] *hier* mitbieten" verstehen durfte, also in deutscher Sprache.

Es ist zu erwarten, dass sich in der breiten Masse nur Anwendungen durchsetzen, deren äußere Erscheinungsbilder verständlicher sind als Programm- oder Maschinencode oder die ohne unmittelbare menschliche Interaktion auskommen.[310] Die nach außen nicht erkennbaren Programm- und Maschinencodes sind dann nicht die vertragliche Grundlage. Sie dienen als Smart Forms auf verschiedensten Wegen der Automatisierung des Vertragsabschlusses und der Vertragsdurchführung. Der Inhalt der Erklärungen und des Vertrags ist nach dem äußeren Erscheinungsbild und dem Input der Nutzer zu ermitteln. Weicht die Smart Form von dem ab, was Inhalt der Erklärungen oder des Vertrags war, ist sie erklärungs- und/oder vertragswidrig.

II. M2M-Erklärungen

Menschen können sich bei der Erzeugung und Übermittlung ihrer Willenserklärungen technischer Hilfsmittel bedienen.[311] Im Internet of Things (IoT) können Maschinen ihre Ersatzteile nachbestellen, Reparaturaufträge vergeben, sich automatisch auffüllen oder für bestimmte Sachen bieten (zB Drucker, Kühlschränke, Bietagenten).[312] Diese M2M[313]-Kommunikation lässt sich im Standardfall mit bereits erarbeiteten Grundsätzen lösen: Es ist nicht notwendig, dass Menschen die Erklärung formulieren, verstehen und abschicken.[314] Es genügt, dass sie die mit vordefinierten Vertragsschlussoptionen arbeitende Maschine willentlich einsetzen.[315]

Kommunizieren die Maschinen in Programm- oder Maschinencode, ist zu ermitteln, ob Smart Contracts entstehen. Das ist nicht der Fall, wenn die Erklärungen beim Empfänger durch einen Prozess, der noch dem Erklärenden zuzurechnen ist, ein äußeres Erscheinungsbild in herkömmlicher

310 Zu Letzterem siehe sogleich Abschnitt § 5 C. II.

311 D. Paulus JuS 2019, 960 (961 f.). Die Zurechnung von automatisierten Vorgängen als Willenserklärungen beschäftigt die Rechtswissenschaften seit Jahrzehnten, s. Köhler AcP 182 (1982), 126.

312 Grünwald/Nüßing MMR 2015, 378; Wulf/Burgenmeister CR 2015, 404 (406 f.); Möslein ZHR 183 (2019), 254 (262); Mandl immolex 2019, 200; D. Paulus/Matzke ZfPW 2018, 431 (440); Simmchen MMR 2017, 162 (164); Heckelmann NJW 2018, 504 (504).

313 Machine To Machine.

314 Möslein ZHR 183 (2019), 254 (270); aA Smets/Kapeller ÖJZ 2018, 293 (294).

315 D. Paulus JuS 2019, 960 (962).

Sprache bekämen. Das ist überdies nicht der Fall, wenn die Vorgaben der Maschine so eng sind, dass nahezu alles vorab definiert ist, inklusive aller Erklärungsempfänger. Das kann bei IoT-Geräten der Fall sein, wenn etwa der Drucker nur bei seinem Hersteller neue Patronen kaufen darf. Dann setzen die Maschinen bloß die Bedingung für einen vorab in herkömmlicher Sprache verfassten, aufschiebend bedingten Vertrag um. Smart Contracts entstehen aber etwa, wenn die Maschine aus den invitationes ad offerendum vieler anderer Maschinen der günstigsten ein Angebot macht:

Mit dem willentlichen Einsetzen der Maschinen besteht eine ausreichende Rückbindung an den Willen einer natürlichen Person. Die automatisierten Willenserklärungen sind Willenserklärungen des Nutzers. Er setzt die Maschine bzw. die Software quasi als verlängerten Arm ein. Weil er so seinen Aktionsradius erweitert, kommen ihm die Vorteile zugute. Gleichzeitig bestimmt die Rechtsordnung, dass er auch allfällige Nachteile zu tragen hat („Guter Tropfen – Böser Tropfen").[316] Das gilt auch dann, wenn die Maschine fehlerhaft arbeitet. Er kann sich gegenüber dem dritten[317] Erklärungsempfänger nicht darauf berufen, nicht gebunden zu sein, weil die Maschine Fehler gemacht hat.[318] Der Erklärungsempfänger darf die Erklärung so verstehen bzw. durch seine Maschine verarbeiten lassen, wie sie nach dem übermittelten Code objektiv verstanden und verarbeitet werden darf.

Auch eine Berufung auf eine fehlende Bindung analog § 1019 ABGB mit der Folge, dass dem Erklärungsempfänger die Maschine als falsus procurator hafte, kommt nicht in Frage. Eine Analogie scheitert an der fehlenden Ähnlichkeit des zu regelnden Sachverhalts: Es handelt für den Nutzer nämlich kein Rechtssubjekt, das selbst für seine Fehler verantwortlich werden kann. Daher führen auch die Rechtsfolgen des § 1019 ABGB – eine planwidrige Unvollständigkeit des positiven Rechts hypothetischerweise vorausgesetzt – nicht zu einer Lösung: Für den Dritten ist die Maschine weder Haftungssubjekt noch hat sie eine eigene Haftungsmasse. Überdies transportieren diese Maschinen lediglich die Willenserklärungen ihrer Nutzer; eigene Willenserklärungen geben sie nicht ab.

316 Vgl. auch Koziol FS Rey, 2003, 427 (431); D. Paulus/Matzke ZfPW 2018, 431 (445).
317 Anderes kann für den Hersteller der Maschine gelten.
318 Ihm können neben den Instrumenten des Irrtumsrechts allenfalls auch Gewährleistungs- oder Schadenersatzansprüche gegen den Hersteller/Verkäufer der Maschine zustehen.

III. Einsatz autonomer Softwareagenten

Die meisten derzeit für M2M-Erklärungen diskutierten Beispiele operieren auf der Grundlage von durch Menschen vordefinierten Regeln. Als solche „willigen" Instrumente sind sie ihren menschlichen Nutzern im Vertragsrecht wie im Haftungsrecht zurechenbar. Nun rütteln aber autonome Softwareagenten[319] am Bild des willigen Instruments. Denn autonome Softwareagenten sind mit kognitiven Merkmalen – wie der Fähigkeit, aus Erfahrungen zu lernen und unabhängige Entscheidungen zu treffen – ausgestattet.[320]

Über die rechtliche Möglichkeit autonomer Softwareagenten, eigene Willenserklärungen abzugeben, sagt das aber noch nichts. Vielmehr knüpft das ABGB das eigene rechtsgeschäftliche Handeln an bestimmte Fähigkeiten, die es nur Menschen zuschreibt: § 865 ABGB zeigt, dass das Gesetz für die Geschäftsfähigkeit ausschließlich natürliche Personen vor Augen hat, wenn und weil es die Vermutung aufstellt, dass volljährige Personen voll geschäftsfähig sind. Zwar sind auch juristische Personen und andere rechtsfähige Gebilde rechtsfähig. Sie können diese Rechte und Pflichten aber nicht durch eigenes Handeln begründen. Sie sind nicht selbst handlungsfähig, sondern brauchen (menschliche) Vertreter, die für sie handeln.[321] Das österreichische Recht geht also davon aus, dass der rechtsgeschäftliche Wille von Menschen gebildet wird.[322] De lege lata kann daher keine eigene Willenserklärung des autonomen Softwareagenten angenommen werden.

Aber auch eine Willenserklärung des Nutzers liegt beim Vertragsabschluss durch autonome Softwareagenten nicht ohne weiteres vor: Auf-

319 Der Begriff Roboter ist zu eng, da er meist eine verkörperte Software bedeutet. Näher zur Terminologie Teubner AcP 218 (2018), 155 (156).

320 Entschließung des Europäischen Parlaments vom 16. Februar 2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL)), 4; Kirn/Müller-Hengstenberg MMR 2014, 225 (229); Müller-Hengstenberg/Kirn MMR 2014, 307; Borges NJW 2018, 977; Specht/Herold MMR 2018, 40 (41); D. Paulus JuS 2019, 960 (965).

321 Diese Vertreter dürfen wiederum nur voll handlungsfähige physische – also natürliche – Personen sein (s nur § 15 GmbHG). Auch die GmbH & Co KG, deren einziger vertretungsbefugter Gesellschafter eine GmbH (also eine juristische Person) ist, stellt nur scheinbar eine Ausnahme dar. Denn die Willensbildung dieser GmbH erfolgt wiederum durch deren Geschäftsführer, also eine natürliche Person.

322 F. Bydlinski Privatautonomie S. 127.

grund von Machine Learning und Deep Learning[323] ist es möglich, dass weder der Programmierer noch der Nutzer im Einzelnen determinieren oder prognostizieren kann, wie der Algorithmus handeln wird.[324] Je autonomer die Entscheidungsfindung, desto heikler wird die Rückbindung an einen Rechtsfolgewillen und damit eine Willenserklärung des menschlichen Nutzers.[325] Der Abschluss von Verträgen durch autonome Softwareagenten, die nicht bloß automatisiert, sondern autonom über den Inhalt, Abschluss und Rücktritt von Verträgen sowie über Sanktionen im Fall des Vertragsbruchs entscheiden, berührt daher dogmatische Grundfesten der Vertragslehre. Mit der zunehmenden Autonomie der Softwareagenten drängt sich die Frage auf, welche Rolle der menschliche Wille für die vertragliche Bindung hat.

Dabei ist zu berücksichtigen, dass das Willenselement der Willenserklärung in einem beweglichen System eingebettet ist.[326] Das ABGB anerkennt zum Teil das Zustandekommen von Verträgen, obwohl eine Partei keinen oder nur einen fehlerhaften Willen gebildet hat. Das ergibt sich daraus, dass die Privatautonomie mit anderen Prinzipien wie dem Vertrauensschutz abgewogen werden muss. Beispiele sind die Möglichkeit der Annahme des bloß zum Vorteil gemachten Versprechens durch Geschäftsunfähige,[327]

323 Das sind spezielle Methoden der Informationsverarbeitung; Kirn/Müller-Hengstenberg MMR 2014, 225 (229); Specht/Herold MMR 2018, 40 (41); D. Paulus JuS 2019, 960 (965); Borges NJW 2018, 977.

324 Entschließung des Europäischen Parlaments vom 16. Februar 2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL)), 8. Teubner AcP 218 (2018), 155 (176 f.); Borges NJW 2018, 977 (978 f.); Specht/Herold MMR 2018, 40 (43).

325 Allgemein zum Bewusstsein, Rechtsfolgen auszulösen, P. Bydlinski AT Rn. 4/4. Vgl. auch Teubner AcP 218 (2018), 155 (175); Borges NJW 2018, 977 (979); Specht/Herold MMR 2018, 40; Heckelmann NJW 2018, 504 (506). Siehe auch vbw-Studie, 2017, 26, https://www.vbw-bayern.de.

326 So schon F. Bydlinski Privatautonomie S. 123 f.

327 So konnte nach der Rechtslage bis zum 2. Erwachsenenschutz-Gesetz ein unter 7-Jähriger oder ein Volljähriger, der geschäftsunfähig ist, ein bloß zu seinem Vorteil gemachtes Versprechen nicht annehmen. Das ABGB unterstellte, dass er keinen rechtsgeschäftlichen Willen bilden kann. Er konnte also auch eine nur vorteilhafte Schenkung als zweiseitiges, einseitig verpflichtendes Rechtsgeschäft nicht annehmen. Nunmehr bestimmt § 865 Abs. 2 ABGB, dass jede Person ein bloß zum Vorteil gemachtes Versprechen annehmen kann.

das AGB-[328] und Irrtumsrecht[329] sowie die Rechtswirkungen der Blankettunterschrift.[330] Damit können Probleme, die aus der Verwendung von autonomen Softwareagenten entstehen, mit den Regelungen des ABGB grundsätzlich gelöst werden: Es genügt, dass der Nutzer willentlich ein System einsetzt, von dem er weiß oder wissen muss, dass es auch Entscheidungen treffen wird, die er nicht vorhersehen kann und die er nicht will. Von dem System geschlossene Rechtsgeschäfte kommen zustande und sind dem Nutzer grundsätzlich[331] zuzurechnen.[332] Der Nutzer kann sich nicht darauf

328 Im AGB-Recht verdünnt der Verwender die Willensfreiheit seines Vertragspartners, weil er den Vertrag nur unter Einbezug seiner AGB schließen wird, weiterführend Bollenberger ÖBA 2016, 26. Die AGB-Kontrolle will diese verdünnte Willensfreiheit ausgleichen, wenn sie – vereinfacht gesagt – bedenkliche Klauseln nicht gelten lässt. Die verdünnte oder sogar fehlende Willensfreiheit setzt sich damit aber auf Seiten des Verwenders fort. Er ist an den Restvertrag gebunden auch, wenn er den Vertrag ohne die Klausel (so) nicht geschlossen hätte.

329 Ein fehlerhaft gebildeter Wille führt nicht dazu, dass überhaupt kein Vertrag zustande kommt. Der Vertrag kommt vielmehr mit dem nicht gewollten Inhalt zustande und ist nur unter den Voraussetzungen der §§ 871 ff. ABGB anfecht- oder anpassbar. Die Zurechnung trotz mangelhafter Willensbildung setzt das Irrtumsrecht damit voraus. Ob der Vertrag wegen des Willensmangels angefochten oder angepasst werden kann, hängt wiederum von einer Interessenabwägung ab. § 871 Abs. 1 Fall 1–3 ABGB wägen die Willensfreiheit und Selbstbestimmung der irrenden Partei gegen den Verkehrs- und Vertrauensschutz der anderen Partei ab. Siehe F. Bydlinski FS Stoll, 2001, 113 (120); Schauer in Fischer-Czermak/Hopf/Kathrein/Schauer, ABGB 51 (60); Köhler AcP 182 (1982), 126.

330 Sie belegen die Möglichkeit und Erlaubtheit des „aus der Hand Gebens" der Willensbildung eindrücklich. So bereits Köhler AcP 182 (1982), 126 (134 f.); Möslein ZHR 183 (2019), 254 (273 f.); vgl. auch D. Paulus/Matzke ZfPW 2018, 431 (444); D. Paulus JuS 2019, 960 (965). Die Erklärung ist dem Aussteller bei verdeckter Ausfüllung zuzurechnen und er kann diese allenfalls irrtumsrechtlich anfechten. Allgemein dazu OGH 1 Ob 43/15b, EvBl 2016/25 (Brenn); Kletečka/Schauer/Pletzer ABGB-ON[1.03] § 871 Rn. 11 f. (Stand 1.8.2019).

331 Eine Grenze der Bindung selbst an ausdrückliche Erklärungen muss dort erreicht sein, wo der Handlungsbereich des Softwareagenten dem Dritten genau bekannt ist. Das wäre etwa der Fall, wenn der Nutzer nach außen unübersehbar einen Handlungsrahmen festsetzt oder sonst unübersehbar erkennbar macht, dass er bestimmte Rechtsgeschäfte nicht will. Der Dritte darf in diesem Bereich kein Vertrauen auf gültige Rechtshandlungen bilden. Vgl. F. Bydlinski Privatautonomie S. 123 f., 166. Ist nicht sichergestellt, dass der Agent gesteckte Grenzen nicht überschreitet oder Hinweise darauf entfernt, darf der Nutzer den autonomen Softwareagenten nicht für sich einsetzen. Durch diesen Nichteinsatz hat er die Möglichkeit, unerwünschten Rechtsfolgen entgegenzuwirken. Diese Möglichkeit verhindert, dass die Untergrenze der Selbstbestimmung unterschritten wird (dazu F. Bydlinski Privatautonomie S. 126 f., 155).

berufen, dass ihm der Bindungs- und Rechtsfolgewille fehlte. Für solcherart erzeugte Erklärungen und Verträge gelten die allgemeinen Regeln.[333]

All das zeigt, dass autonome Softwareagenten künftig ein Anwendungsfeld für Smart Contracts und Smart Forms bilden können.[334] Mit ihrem Einsatz ist zu erwarten, dass fließend zwischen herkömmlicher Sprache und Code hin und her übersetzt werden wird, sodass Menschen mit dem Code gar nicht unmittelbar konfrontiert sind.

D. Ausblick auf die Vertragsdurchführung

Smart Contracts dürfen als Verträge übergeordnetem zwingendem Recht nicht widersprechen.[335] Das gilt sowohl für den Vertragsschluss und hier insbesondere für den Inhalt, den die Vertragsparteien vereinbaren. Das gilt aber auch für die Vertragsdurchführung: Hier könnte insbesondere ein Konflikt mit dem Besitzschutz entstehen. Diese Fragen sind für die Unterbrechung des Bezugs im Dauerschuldverhältnis (Abschnitt I.) und für die Verschaffung dinglicher Rechte zu stellen (Abschnitt II.).

---

332 AA und für eine Zurechnung gegenüber dem Programmierer Heckelmann NJW 2018, 504 (506).

333 So können sie etwa nichtig sein, wenn sie gegen zwingendes Recht und/oder die guten Sitten verstoßen. Liegen die Voraussetzungen der §§ 871 ff. ABGB vor, können sie irrtumsrechtlich angefochten oder angepasst werden.

334 Selbstlernende Algorithmen können Smart Contracts initiieren und dabei nur in Maschinencode kommunizieren, vgl. Borges NJW 2018, 977 (978 f.); Möslein ZHR 183 (2019), 254 (273); Specht/Herold MMR 2018, 40 (41). Smart Contracts selbst können auch mit anderen Smart Contracts kommunizieren oder neue Smart Contracts unmittelbar in Maschinencode erzeugen, vgl. Hupel c't 2021, 150 (151).

335 Recht erhebt einen technologieneutralen Geltungsanspruch, s. Ehrke-Rabel/Eisenberger/Hödl/Pachinger/Schneider jusIT 2017, 87 (90); Möslein ZHR 183 (2019), 254 (266, 270); Wilhelm WM 2020, 1807 (1810); Möslein ZBB 2018, 208 (217 f.); Fries/Paal Smart Contracts/Riehm S. 85 (87); Fries/Paal Smart Contracts/Kaulartz S. 73 (73 f.); Kaulartz/Heckmann CR 2016, 618 (623). Die überkommene Code-is-Law-These geht auf eine (überinterpretierte) Aussage von Lessig (Code is Law, Harvard Magazine, 2000, https://www.harvardmagazine.com) zurück. Aktuell für diese Position etwa https://aragon.org/; ähnlich Blue Frontier Campaign, https://blue-frontiers.com/de; s. auch Fairfield W&L-LawRev 71 (2014), 35 (39); s. auch Savelyev ICTL 26 (2017), 116 (130 ff.).

I. Automatische Unterbrechung des Bezugs im Dauerschuldverhältnis

Smart Forms können nicht nur den Leistungsaustausch automatisieren, sie könnten insbesondere bei Dauerschuldverhältnissen auch den vertragswidrigen Leistungsbezug technisch verhindern: Für den qualifiziert säumigen Strombezieher fließt der Strom nicht, für den qualifiziert säumigen Kreditnehmer startet das Leasingfahrzeug nicht oder lässt sich nicht wiederaufladen und Smart Locks versperren die finanzierte Wohnung.[336] Ob Smart Forms das dürfen und damit legitim einen Trend der teilweisen Privatisierung der Rechtsdurchsetzung fortsetzen,[337] ist fraglich. Denn im Grundsatz gilt, dass der Vertragspartner einer nicht mehr leistungswilligen Partei staatliche Gerichte zur Durchsetzung seines vertraglichen Anspruchs anrufen muss.[338] Smart Forms stehen folglich im Spannungsverhältnis zwischen erlaubter und verbotener Selbsthilfe und dem Besitzschutz.[339]

Innerhalb gewisser Grenzen gibt es erlaubte Selbsthilfe (zB §§ 19, 344, 471, 970c, 1101, 1321 ABGB).[340] Keine verbotene Eigenmacht und damit keine (unerlaubte) Selbsthilfe läge vor, wenn die Zustimmung zum Eingriff in den Besitz der vertragsbrüchigen Partei bereits im Voraus verbindlich gegeben werden könnte. Diese Voraus-Einwilligung ist nach manchen nicht zulässig,[341] nach anderen frei widerruflich.[342] Eigenmacht liegt nach beiden

336 Vgl. zu solchen Beispielen Fn. 389.

337 Diesen Trend sieht man etwa in privater Schiedsgerichtsbarkeit, Schiedsgutachtenverfahren, Schlichtungs- und Mediationsverfahren. Vgl. auch Wagner AcP 222 (2022), 56 (61 f.).

338 Wagner AcP 222 (2022), 56 (64).

339 Für Deutschland Fries/Paal Smart Contracts/Riehm S. 85 (89 ff.); C. Paulus/Matzke CR 2017, 769 (772 f.); Möslein ZBB 2018, 208 (219 f.); Wagner AcP 222 (2022), 56 (69); vgl. auch Frankenreiter JITE 2019, 149. Sach- und Rechtsbesitzer genießen auch Besitzschutz, wenn sie in Verzug sind, Schwimann/Kodek/Anzenberger ABGB § 311 Rn. 7.

340 Allgemein zu den Voraussetzungen der Selbsthilfe s. Schwimann/Kodek/Posch ABGB § 19 Rn. 5 ff.; Kletečka/Schauer/Kodek ABGB-ON[1.03] § 344 Rn. 1 ff. (Stand 1.1.2018); Koziol Haftpflichtrecht I C/1/113 ff. Vgl. auch §§ 227 ff. BGB, §§ 539 Abs. 2, 997 BGB (Wegnahmerechte), § 562b BGB (Selbsthilferecht des Vermieters) oder §§ 273, 320 BGB (Zurückbehaltungsrechte); dazu Wilhelm WM 2020, 1807 (1811) mwN.

341 Klang/F. Bydlinski ABGB IV/2[2] § 1063 S. 554: Regeln zum Besitz sind zwingendes Recht.

342 Kletečka/Schauer/Kodek ABGB-ON[1.03] § 339 Rn. 18 (Stand 1.1.2018); Fenyves/Kerschner/Vonkilch/Kodek ABGB § 339 Rn. 205; Iro/Riss SR Rn. 2/62; zum BGB s. Fries/Paal Smart Contracts/Riehm S. 85 (90 ff.); dazu, dass Reue nach dem Zugriff nichts ändert s. Möslein ZBB 2018, 208 (220).

Ansichten[343] sohin vor, wenn der Besitzer spätestens im Zeitpunkt des Eingriffs zu erkennen gibt, dass er damit nicht einverstanden ist. Selbst eine ursprünglich rechtmäßige Selbsthilfe würde rechtswidrig werden, wenn die Maßnahme fortgesetzt wird, ohne mögliche gerichtliche Schritte einzuleiten.[344] Wird der geschaffene Zustand aufrecht erhalten, ohne unverzüglich eine einstweilige Verfügung zu beantragen, wird die Selbsthilfe nachträglich rechtswidrig und zur Besitzstörung. Smart Forms leisten daher unerlaubte Selbsthilfe, wenn sie Zugänge zu Wohnungen wegen ausbleibender Zahlungen versperren und versperrt lassen.[345] Gerichtliche Hilfe käme nämlich nicht zu spät. Für automatisiert ausgelöste Wegfahrsperren gilt gleiches.[346] Es genügt, dass sie die (Haupt-)Nutzung der Sache entziehen, weil das ABGB nach hA[347] den bestimmungsgemäßen Gebrauch schützt. Bereits die Beeinträchtigung desselben ist daher eine Besitzstörung.[348]

Inwiefern Smart Forms vor dem Hintergrund dieser besitzrechtlichen Restriktionen den vertragswidrigen Leistungsbezug, etwa im Mietverhältnis, verhindern dürfen, ist strittig. Ein Ansatzpunkt könnte darin liegen, zwischen Vermieter und Mieter Mitbesitz anzunehmen, wenn sie eine wirksame Sperrmöglichkeit vereinbaren.[349] Solange der Vermieter mit der Sperre nur seinen Mitbesitz ausübt und dem Mieter den Besitz nicht gänzlich entzieht, läge darin keine Besitzstörung.[350] Das Problem wird damit –

343 Eine dritte Ansicht unterscheidet danach, ob der Eingriff von innen kommt. Der Besitzschutz erfasse nur Beeinträchtigungen, die von außen kommen. Eine Beeinträchtigung von innen führe nicht zu verbotener Eigenmacht. Die Sachherrschaft sei von Beginn an mit einer eventuellen späteren Selbstsperrung der Sache behaftet. Siehe zu diesem Argument außerhalb von AGB, Fries NJW 2019, 901 (902, 905).

344 Fenyves/Kerschner/Vonkilch/Meissel ABGB § 19 Rn. 20, 34; Fenyves/Kerschner/Vonkilch/Kodek § 344 Rn. 39 f.

345 Mandl immolex 2019, 200 (202); C. Paulus/Matzke CR 2017, 769 (773 ff.); vgl. auch Wagner AcP 222 (2022), 56 (84); Lindner NZM 2021, 665 (668).

346 In Deutschland str.: Unerlaubte Selbsthilfemaßnahme vertreten BGH NJW 2022, 3575 Rn. 18a): Fernzugriff auf vermietete Autobatterie; Möslein ZBB 2018, 208 (220); Fries/Paal Smart Contracts/Riehm S. 85 (95 f.); für Erlaubtheit demgegenüber Fries NJW 2019, 901 (902, 905); andere differenzieren nach einem persönlichkeitsschutzbezogenen Ansatz, s. Wilhelm WM 2020, 1807 (1812).

347 Vgl. nur Kletečka/Schauer/Kodek ABGB-ON[1.03] § 339 Rn. 5 (Stand 1.1.2018); Mandl immolex 2019, 200 (203); Rummel/Lukas/Holzner ABGB § 339 Rn. 12 (Stand 1.7.2016); BGH NJW 2022, 3575.

348 Mandl immolex 2019, 200 (203).

349 Strobel NJW 2022, 2361 (2362 f.); krit. BGH NJW 2022, 3575 Rn. 23b).

350 Vgl. § 866 BGB; in Österreich muss gleiches aus der Vertragsauslegung der Mitbesitzer folgen. Daher wird Mitbesitz nur durch Besitzentziehung oder Störung der bestehenden Gebrauchsordnung gestört, s. Iro/Riss SR Rn. 2/14 f. 2/59; Rum-

ähnlich wie bei der Voraus-Einwilligung – auf die Frage der Wirksamkeit der Vereinbarung von Mitbesitz durch Sperrmöglichkeiten verlagert. Im Verbrauchergeschäft müsste die Klausel jedenfalls auch festlegen, dass die Sperre automatisch wieder entfällt, sobald überfällige Zahlungen einlangen.[351]

Jedenfalls begründet der Besitzschutz nur Abwehrrechte, nicht aber neue – unentgeltliche – Leistungsansprüche.[352] Ausgehend davon ist der Einsatz von Smart Forms für die Abstellung wiederkehrender Versorgungsleistungen (Strom, Software etc)[353] bei qualifiziertem Verzug zulässig: Für erst künftig zu beziehende Leistungen kann gegenüber dem Lieferanten kein Besitzschutz bestehen. In den Besitz unkörperlicher Sachen oder Rechte kommt der Bezieher nämlich erst durch deren Gebrauch im eigenen Namen (§ 312 ABGB). Der – wenn auch regelmäßige – Bezieher von Strom, Software udgl erweitert daher (erst) mit jedem Leistungsbezug seinen Rechtskreis. Es greift allein das Vertragsrecht, das bei qualifizierter Nichtzahlung die Abschaltung der Versorgungsleistung kennt.[354] Diese Wertung muss für andere wiederkehrende Versorgungsleistungen analog gelten: Der eine Vertragspartner soll nicht weiter neue Leistungen schulden und seinen Schaden sowie das Insolvenzrisiko weiter erhöhen müssen, obwohl der andere qualifiziert säumig ist.[355] Überdies greift das Leistungsverweigerungs-

---

mel/Lukas/Holzner ABGB § 339 Rn. 9 a) (Stand 1.7.2016); Kletečka/Schauer/Kodek ABGB-ON[1.03] § 339 Rn. 12 (Stand 1.1.2018).

351 Unberücksichtigt bliebe, ob etwa eine Mietzinsminderung rechtmäßig war. Die Klagslast würde auf den Mieter verschoben. Der BGH hält dem ganz grundsätzlich entgegen, dass Risiken wie die (Ab-)Nutzung nach Vertragsbeendigung oder die Mietzinsminderung dem Vermieter zuzuschreiben sind. Er habe dagegen ausreichende Schutzmechanismen wie die Kaution oder die Nutzungsentschädigung (BGH NJW 2022, 3575 Rn. 28). Problemmieter sind hingegen oft jene, deren Kaution nicht ausreicht und die auch sonst keine Mittel für eine Nutzungsentschädigung haben.

352 Zum BGB Fries/Paal Smart Contracts/Riehm S. 85 (94 f.); ähnlich Kuschel AcP 220 (2020), 98 (122 ff.). Zur korrekturbedürftigen Ansicht in Österreich s. Fn. 355.

353 Zum Besitz an Rechten Fenyves/Kerschner/Vonkilch/Kodek ABGB § 311 Rn. 22 ff.; aA Iro/Riss SR Rn. 2/7 f.

354 Neben den allgemeinen §§ 918 ff. ABGB für den Teilverzug ergibt sich diese Rechtsfolge teilweise explizit aus Spezialgesetzen, s. nur § 82 Abs. 3 ElWOG 2010; § 127 Abs. 3 GWG; §§ 2, 7 Gasnetzdienstleistungsqualitäts-VO, BGBl. 2012 II 172. Kritisch zum Mahnverfahren Th. Rabl, ecolex 2012, 772.

355 Vgl. BGH NJW 2009, 1947 wonach die Einstellung von Versorgungsleistungen der gemieteten Geschäftsräumlichkeit keine Besitzstörung war. Dem Vermieter drohe ein weiterer Schaden, wenn er zusätzlich weiter die aus dem Mietvertrag geschuldeten Warmwasser- und Heizleistungen erbringen müsse. In Österreich wird diese

recht (§ 1052 ABGB; § 369 UGB).[356] Die Einstellung oder Unterbrechung der Versorgung mit Strom erfolgt gegenüber dem qualifiziert säumigen Bezieher daher zurecht.

Während die Betretung des Bezugsobjekts zur Unterbrechung der Energieversorgung im Streitfall mit gerichtlicher Hilfe durchgesetzt werden müsste, schaffen Smart Meter, Smart Forms und Smart Contracts dafür eine Lösung, weil sie die Abschaltung ohne Zutritt zum Bezugsobjekt bewerkstelligen.[357] Gleiches gilt für den Bezug von Daten, Software oder Updates für die Geräte in einem Smart Home. Eine entsprechend codierte Smart Form dürfte hier mE eingesetzt werden und nach der Wirkungslosigkeit von Mahnungen sowie einer Androhung der Abschaltung die Sperre automatisch aktivieren.[358]

II. Verschaffung dinglicher Rechte

Soll mit der Smart Form ein dingliches Recht verschafft werden, erfordert das nach der Lehre von titulus et modus adquirendi neben einem Verpflichtungsgeschäft ein aus Übergabe und Übernahme bestehendes Verfügungsgeschäft (§ 425 ABGB). Die Vertragsparteien müssen das Verfügungsgeschäft nicht persönlich durchführen, wie etwa das Beispiel eines Boten oder Bevollmächtigen zeigt. Die Privatautonomie gewährt die Freiheit, das Verfügungsgeschäft über Codes auszulösen und automatisiert durchzuführen.[359] Sie müssen es aber selbst wollen.[360] Der Einsatz einer Smart Form,

---

Lösung über die „Vertragskoppelung" verhindert. Danach sei zu differenzieren, ob der Mieter den Stromvertrag selbst oder über seinen Vermieter abgeschlossen hat. Im letzteren Fall sei auch der Strombezugsvertrag vom Besitzschutz erfasst. Siehe etwa LGZ Wien 41 R 601/82 MietSlg 34.025; Fenyves/Kerschner/Vonkilch/Kodek ABGB § 311 Rn. 32; Mandl immolex 2019, 200 (203) mwN; Kodek wobl 2009/122.

356 Kletečka/Schauer/Kodek ABGB-ON[1.03] § 339 Rn. 19 (Stand 1.1.2018); Hoyer wbl 1997, 147 (151).

357 Fries/Paal Smart Contracts/Riehm S. 85 (95); Wagner AcP 222 (2022), 56 (89).

358 Vgl. Fries/Paal Smart Contracts/Matzke S. 99 (108). Wo die letzte Mahnung mit eingeschriebenem Brief zu erfolgen hat (vgl. § 82 Abs. 3 ElWOG 2010), ist derzeit eine Mitwirkung physischer Personen noch erforderlich.

359 Siehe Möslein ZHR 183 (2019), 254 (267 f.); Wilhelm WM 2020, 1807 (1810). Codes erhalten dafür vereinfacht gesagt Zugriff auf Sachen iSd § 285 ABGB.

360 Übergabe und Übernahme sind keine bloßen Realakte, sondern müssen von einem rechtsgeschäftlichen Übergabe- bzw. Übernahmewillen getragen, Fritzer Form der Schenkung S. 73 Fn. 575, 85 Fn. 651 mwN zum Theoriestreit seit Spielbüchler JBl 1971, 589; aktuell aA Kletečka/Schauer/Mader ABGB-ON[1.03] § 425 Rn. 2 mwN (Stand 1.3.2019). Für das BGB für Realakte Heckelmann NJW 2018, 504 (508).

die auf die automatisierte Durchführung des Vertrags ausgerichtet ist, setzt also voraus, dass der Wille zur Durchführung (= Verfügungsgeschäft) gefasst wurde.

Unerheblich ist, dass die Smart Form den dazugehörigen Akt erst später bewirkt. Zwar könnte der Verkäufer seinen sachenrechtlichen Übergabewillen vor der Durchführung – obligationswidrig – zurücknehmen und damit den Eigentumsübergang zunächst verhindern. Da die Smart Form die Übergabe aber trotzdem durchführt, müsste der Veräußerer den Erwerber auf Herausgabe klagen. Er wird dabei unterliegen, weil ihm der Erwerber den schuldrechtlichen Titel entgegenhalten kann. Das zeigt zum einen, dass der Streit um die dingliche Einigung auch beim Einsatz von Smart Forms rein theoretisch ist.[361] Zum anderen zeigt es, dass Smart Forms auf wirksame Weise Rechtsstreitigkeiten verhindern, wo obligationswidrig nicht übergeben werden würde. Die Smart Form führt die Leistungen durch, auch wenn eine Partei nicht mehr will. Sie weist damit jenem die Klagslast zu, der behauptet, aus dem (dennoch so) geschlossenen Vertrag bzw. der vorab (dennoch so) bestimmten Durchführung nicht gebunden zu sein. Gerichte werden also nicht ausgehebelt, das staatliche Gewaltmonopol ist nicht „ausgetrocknet".[362]

Widerruft eine Partei ihren Übergabewillen, bevor der Code den Leistungsaustausch vollzieht, kann der Vollzug des Codes besitzentziehend wirken.[363] Das gilt etwa dann, wenn der Code Zugriff auf Vermögenswerte erhält und diese mit Fälligkeit aus dem Besitz der widerrufenden Partei entzieht.[364] Mit der Besitzklage würde der Widerrufende grundsätzlich die Wiederherstellung des letzten ruhigen Besitzstands erlangen können. Dabei sollte berücksichtigt werden, dass die Parteien sich einvernehmlich auf den

361 Umfassend dazu sowie zur (zwar obligationswidrigen), aber sachenrechtlich wirksamen einseitigen Rücknahme des Übergabewillens Riss ÖBA 2010, 215 (221, 225 ff.).

362 Siehe auch Wagner AcP 222 (2022), 56 (62, 89), der treffend darlegt, dass die außergerichtliche Durchsetzung tatsächlich bestehender Ansprüche keine Umgehung des Gerichtssystems ist.

363 Vgl. Iro/Riss SR Rn. 6/40. Anderes gilt etwa für den Fall, dass der Smart Contract bei Widerruf den Austausch beider Leistungen verhindert. Das ist durch das Leistungsverweigerungsrecht gedeckt (§ 1052 ABGB; § 369 UGB). Siehe Kletečka/Schauer/Kodek ABGB-ON[1.03] § 339 Rn. 19 (Stand 1.1.2018); Hoyer wbl 1997, 147 (151).

364 Der Einsatz des Codes wurde von den Parteien bestimmt und geht damit auf eine menschliche Handlung zurück; s. dazu Iro/Riss SR Rn. 2/60.

Einsatz des Codes geeinigt haben.[365] Die Durchführung des Codes geht daher auf beide Parteien – sohin auch die widerrufende Partei – zurück. Beide Parteien wären damit Störer.[366] Beruft sich die widerrufende Partei auf Besitzschutz, verstößt sie mE gegen das Verbot des venire contra factum proprium.[367] Letztlich kann sich die andere Partei – als rechtlicher Besitzer –[368] auch mit der actio publiciana wehren.[369]

Klagte der Widerrufende auf Schadenersatz, wäre ihm der Einwand des rechtmäßigen Alternativverhaltens entgegenzuhalten:[370] Der Schaden wäre selbst dann eingetreten, wenn die andere Partei den Code unterbrochen oder – falls das technisch nicht möglich ist – die Sache umgehend zurückgestellt hätte. Denn dann hätte sie ihren Anspruch unter Berufung auf den Vertrag mit gerichtlicher Hilfe durchgesetzt und wäre so zu stellen gewesen, wie sie stünde, wenn der Code ursprünglich durchgeführt worden wäre. Im Ergebnis wäre somit für den Widerrufenden die gleiche Situation und damit der gleiche „Schaden" eingetreten. Mangels Kausalität der Leistungsdurchführung besteht kein Schadenersatzanspruch.

Die Rechtsordnung kennt aber auch Rechtsgeschäfte, deren Verpflichtungserklärung (sanktionslos) zurückgenommen werden darf, bis der entsprechende Teil des Verfügungsgeschäfts (= die Übergabe) wirklich gemacht ist. So ist die ohne Notariatsakt errichtete Schenkung für den Geschenkgeber erst dann verbindlich, wenn das Geschenk wirklich übergeben und nicht nur versprochen ist.[371] Dafür genügt es, wenn im Code eine Übergabe durch Erklärung codiert ist, diese Erklärung zugeht und

365 Es erscheint daher sachgerechter, hier – analog zur mehrseitigen Treuhand – nur den Widerruf aller Vertragsparteien für relevant zu erklären (vergleiche dazu Rummel/Lukas/Geroldinger/Hartlieb/Zollner ABGB § 1020 Rn. 13 (Stand 1.8.2022)), und dies auch sachenrechtlich auf den Besitzschutz wirken zu lassen. Andeutungsweise könnte GlU 604 in diese Richtung verstanden werden. Das gleiche Problem müsste sich auch bei analogen Treuhandvereinbarungen stellen.

366 Iro/Riss SR Rn. 2/61.

367 Zum Problem der Voraus-Einwilligung und Eigenmacht s. bereits bei Fn. 341 f.

368 Sein Besitz ist echt, weil er sich auf einen tauglichen Rechtsgrund stützen kann. Sein Besitz ist redlich, weil er sich für berichtigt halten darf, die Besitzhandlung auszuüben. Sein Besitz ist überdies echt, weil er keine Absicht fehlerhafter Besitzergreifung hatte. Zum weiteren Begriff der Eigenmacht s. Iro/Riss SR Rn. 2/26.

369 Allgemein zur Klage Iro/Riss SR Rn. 2/68 ff.

370 Allgemein dazu OGH 5 Ob 229/20t, JMG 2021, 65 (Niernberger); Kletečka/Schauer/Kodek ABGB-ON[1.03] § 1295 Rn. 9 ff. (Stand 1.1.2018); Karollus Schutzgesetzverletzung S. 405 ff.; auch der Normzweck spricht mE nicht dagegen; vgl. auch dazu Koziol Haftpflichtrecht I C/10/77 ff.

371 Fritzer Form der Schenkung passim.

zur Kenntnis gelangt, bevor der Geschenkgeber seinen Willen ändert. Programmiert daher die Geschenkgeberin, die ihr NFT noch für die nächste virtuelle Galerieausstellung nutzen möchte, dass sie es mit Besitzkonstitut ihrem Gatten schon heute schenkt (aber erst nach der Ausstellung übersendet), ist sie gebunden, sobald er dies zur Kenntnis genommen hat. Nimmt er an, ist die Schenkung mit Besitzkonstitut verbindlich geworden.[372] Ist im Code hingegen noch keine Übergabe programmiert, liegt bis zur Übergabe eine unverbindliche, formfehlerhafte Schenkung vor. Die Smart Form würde diese aber unabhängig davon durchführen, ob der Geschenkgeber nach Abgabe der Schenkungserklärung, aber vor der automatisierten Übergabe des Geschenks erklärt, seinen Schenkungswillen aufzugeben. In solchen Fällen würde die Smart Form rechtlich nicht haltbare Tatsachen schaffen. Daran ändert sich auch nichts, wenn man den Beginn der Übergabe bereits im Akt der Codierung erblicken wollte, weil die Übergabe bis zur Durchführung des Codes jedenfalls nicht abgeschlossen wäre. Ein Widerruf muss zu jeder Zeit bis zum Abschluss der Übergabehandlung rechtzeitig sein. Das bestätigt der parallel gelagerte Fall der Vollmacht zur Übergabe eines Geschenks: Auch die Vollmacht kann bis zur Vollendung der Übergabe jederzeit widerrufen werden.[373] Es macht aber keinen Unterschied, ob sich der Geschenkgeber für die Übergabe einen Menschen oder einen Code zur Hilfe nimmt. Auch eine Heilung des Formmangels kommt nicht in Frage, weil der automatische Vollzug ohne entsprechendem Erfüllungswillen nicht als heilende wirkliche Übergabe qualifiziert werden kann.[374]

Zu einem anderen Ergebnis führt der Einsatz einer Smart Form demgegenüber bei der Abwicklung eines erlaubten Glücksvertrags. Dieser wäre aufgrund der Anordnung des § 1271 ABGB grundsätzlich nicht verbindlich, solange der bedungene Wetteinsatz nicht wirklich entrichtet oder hinterlegt worden ist. Der Gesetzgeber versagt der Durchsetzung solcher Verträge gerichtliche Hilfe (§ 1271 Satz 2 ABGB), weil Glücksverträge keinen volkswirtschaftlichen Nutzen haben.[375] Der Zweck der Form liegt also nicht wie bei der Schenkung darin, einen Freigiebigen vor Übereilung zu schützen.[376]

372 Entgegen der hA s. Fritzer Form der Schenkung S. 174 ff auch mit Nachweisen zur umfangreichen gegenteiligen Rsp etwa in Fn. 1318.

373 Fritzer Form der Schenkung S. 276 ff.

374 Für die Möglichkeit der Heilung des Formmangels ist kein Rückgriff auf § 1432 ABGB nötig, sie ist aus § 1 Abs. 1 lit. d NotAktsG abzuleiten, s. Fritzer Form der Schenkung S. 96 ff.

375 Siehe v. Zeiller Commentar III/2 § 1271 Anm. 7 f.

376 Fritzer Form der Schenkung S. 65 ff.

Der Einsatz der Smart Form kann also so erfolgen, dass der Wetteinsatz bis zum Feststehen des Wettergebnisses nicht ausgezahlt, danach aber automatisiert an den Wettsieger übermittelt wird. Ein Rückforderungsbegehren des Wettverlierers scheitert dann an § 1432 ABGB, weil Zahlungen, deren Eintreibung das Gesetz bloß die Klagbarkeit versagt, nicht zurückgefordert werden können.[377] Dem steht weder der Formzweck entgegen noch ist der Rückforderungsausschluss[378] auf willentliche Erfüllungshandlungen beschränkt. Es genügt eine Zahlung, die vom Wettgewinner weder erzwungen noch listig herbeigeführt wurde.[379] Diese Erfordernisse sind bei einer automatischen Zahlung durch die Smart Form – die ja einvernehmlich vereinbart wurde – erfüllt.

§ 6 Zusammenfassende Betrachtung

A. Vertragsbegriff

Technisch sind Smart Contracts computergestützte Protokolle, die klare Wenn-Dann-Bedingungen festhalten und gegebenenfalls ausführen. Ein Computer kann diese Protokolle nur verarbeiten, wenn sie in Maschinencode – eine Aneinanderreihung von Nullen und Einsen – übersetzt sind. Da Menschen Maschinencode nicht formulieren können, verfassen sie ihre Eingaben mit Programmiersprachen. Der Computer kann diese mit einem Compiler in Maschinencode übersetzen. Maschinencode kann aber nur eingeschränkt in ein menschenlesbares Format zurück übersetzt werden.

Die Technik sollte sich des Begriffs „Vertrag" nur dann bedienen, wenn von einem Vertrag im Rechtssinne gesprochen wird. Rechtlich liegt ein Smart Contract daher nur vor, wenn ein Vertrag in Programm- oder Maschinencode verfasst ist. Demgegenüber liegt eine Smart Form bereits dann vor, wenn Programm- oder Maschinencodes irgendwie beim Abschluss oder der Durchführung eines Vertrags (ungeachtet dessen traditioneller oder codebasierter Form) unterstützen sollen. Die Codes können in beiden Fällen die codierten Vorgaben kontrollieren und durchführen, sie können da wie dort mit einer Blockchain verbunden sein oder nicht.

377 Schwimann/Kodek/Mader, 4. Aufl., ABGB § 1432 Rn. 2; anderes gilt bei verbotenen Glücksspielen s OGH 1 Ob 182/22d, Zak 2022,354.

378 Strittig ist, ob die Zahlung (immer) eine echte Heilung oder bloß einen Rückforderungsausschluss bewirkt. Siehe Dehn Formnichtige Rechtsgeschäfte S. 257 ff. mwN; Pisko JBl 1934, 511 (516).

379 Schwimann/Kodek/Mader ABGB § 1432 Rn. 1.

B. Formfreiheit

Das geltende Vertragsrecht ist grundsätzlich flexibel genug, um den Abschluss eines Smart Contracts zu ermöglichen: Der Grundsatz der Formfreiheit stellt es den Parteien frei, Verträge unmittelbar in Programm- oder Maschinencode festzuhalten. Bestehen hingegen gesetzliche Formvorgaben, ist für Programm- oder Maschinencode zu prüfen, ob sie die objektiven Merkmale der Form aufweisen (i) und ob sie dem Zweck der Formpflicht gerecht werden (ii).

Maschinencode kann bereits die objektiven Merkmale der Textform, Schriftlichkeit, notariellen Beurkundung oder des Notariatsakts nicht erreichen. Auch Programmcode kann die objektiven Merkmale der Notariatsaktsform und der notariellen Beurkundung nicht abbilden. Programmcode eignet sich aber objektiv für Willenserklärungen und Verträge in Textform. Er kann über die Einbindung einer qualifizierten elektronischen Signatur überdies die objektiven Merkmale der Schriftlichkeit erreichen. Dient die Textform oder die Schriftlichkeit bloß dem Beweis-, Übereilungs- oder Gläubigerschutz, steht dem Einsatz von Programmcodes nichts entgegen. Hat die Formvorgabe hingegen auch eine Informations- oder Aufklärungsfunktion, scheidet der Einsatz von Programmcodes aus, weil ihnen Informationen nur mit Sonderwissen entnehmbar sind.

De lege ferenda sollte der Gesetzgeber an allgemeiner Stelle einheitlich zusammenfassen, welche Voraussetzungen er an die jeweilige Formpflicht knüpft. Für den zu eng geratenen Wortlaut des § 883 ABGB sollte Satz 1 des § 883 ABGB ersatzlos entfallen und in Satz 2 das Wort „Diese“ mit „Die“ ersetzt werden.

C. Vertragsabschluss

Programmcode kann rechtlich relevante Inhalte wie Ware und Preis sowie die Bedingungen, unter denen sie auszutauschen sind, bestimmt beschreiben. Er ist auch objektiv verständlich: Jeder, der die Programmiersprache erlernt hat, kann dem codierten Text einen eindeutigen Sinn zuschreiben. Der Programmcode kann sowohl als invitatio ad offerendum als auch als Angebot mit endgültigem Bindungswillen verfasst sein. Der Austausch von Angebot und Annahme unmittelbar in Programmcode ist rechtlich sowohl unter Anwesenden als auch unter Abwesenden möglich.

Maschinencode ist menschlich nicht formulier- oder lesbar. Menschen können aus ihm daher auch keinen Bindungswillen erkennen. Neben

einem theoretischen Restanwendungsbereich bei der gemeinsamen Programmierung kann Maschinencode daher nur bei M2M-Erklärungen oder beim Einsatz autonomer Softwareagenten zur Vertragsgrundlage werden.

On-chain bestehen einige rechtliche Besonderheiten. Erstens geht eine Erklärung auf der Blockchain schon mit ihrer Aufnahme in einen Block zu. Zweitens können Timestamps Beweisschwierigkeiten beim Widerruf eines Angebots oder einer Annahme abmildern. Gelingt vor der Kenntnisnahme ausnahmsweise ein rechtzeitiger Widerruf, ist der Widerrufende auf eine Korrektur der Blockchain, etwa durch einen contrarius actus in späteren Blöcken, angewiesen. Drittens weist die Blockchain hinsichtlich des Risikos der (im Verhältnis zur durchschnittlichen Reisedauer) verzögerten Reise der Erklärung im Vergleich zu herkömmlichen Transportmitteln den Vorteil auf, dass der Erklärende den Zeitpunkt, zu dem seine Erklärung zugeht, immer genau ermitteln kann: Er sieht den Timestamp des Blocks, mit dem seine Erklärung an die Blockchain angefügt wird. Viertens kann eine Fork zum Entfall von Blöcken führen, die Willenserklärungen enthalten. Die Fork vernichtet rechtlich weder den Zugang der Erklärung(en) noch ist sie für eine Partei als Widerruf ihrer Erklärung zu verstehen. Die Parteien trifft daher die Obliegenheit zu ermitteln, welche Rechtsfolgen (zB erneute Ablage der Erklärungen) sie im Einzelfall treffen.

D. Wo ist Code die bessere Vertragsgrundlage?

Smart Contracts können die Auswahl des Vertragspartners und die Durchführung des Vertrags automatisieren. Bei letztgenanntem Aspekt ist der Einsatz von Smart Contracts und Smart Forms aber durch die zwingenden Grenzen des Besitzschutzes stark eingeschränkt.

Die Behauptung, dass Smart Contracts on-chain dabei mit geringeren Transaktionskosten auskommen, lässt sich derzeit in dieser Allgemeinheit nicht belegen. Block-Rewards, Transaktionsgebühren und Kosten für Hardware und Energie machen den Vertragsabschluss und die Vertragsdurchführung auf Blockchains teuer. Die meisten Smart Contracts liegen daher off-chain. Dadurch gehen die versprochenen Vorteile der Dezentralität und Fälschungssicherheit verloren. Auf diese Art können Smart Contracts die Funktion zentraler Intermediäre folglich nicht übernehmen. Auch on-chain schwindet das Versprechen der Dezentralität, weil sich Intermediäre mit viel Marktmacht als Gatekeeper herausbilden.

Für Smart Contracts off-chain fallen zwar diese Kosten nicht an. Jede technisch entsprechend versierte Person mit Zugriff auf den Code kann diesen aber manipulieren. Als Mittelweg kann der Hashwert des ursprünglichen Vertrags on-chain gespeichert werden. Das kostet weniger, weil weniger Speicherplatz erforderlich ist und hat den Vorteil, dass die Manipulation des Codes zwar nicht ausgeschlossen, aber leichter nachzuweisen ist. Überdies kann der Leistungsaustausch davon abhängig gemacht werden, dass der aktuelle und damals abgelegte Hashwert des Vertrags übereinstimmen.

Es ist zu erwarten, dass sich in der breiten Masse nur Anwendungen durchsetzen, deren äußeres Erscheinungsbild verständlicher ist als Programm- oder Maschinencode. Bloß intern gebliebene Programm- und Maschinencodes bilden dann nicht die vertragliche Grundlage. Sie dienen als Smart Form auf verschiedensten Wegen automatischen Vertragsabschlüssen und -durchführungen. Anderes kann gelten, wenn keine menschliche Interaktion erforderlich ist. In der M2M-Kommunikation sowie beim Einsatz von autonomen Softwareagenten können Smart Contracts abgeschlossen werden, obwohl der Nutzer die Codes nicht zu Gesicht bekommt.

Literaturverzeichnis

Achenbach Dirk/Baumgart Ingmar/Rill Jochen, Die Blockchain im Rampenlicht – Technologie von der Stange - oder besser nach Maß? DuD 2017, 673

Anderl Axel/Aigner Markus/Schelling Dominik, Smart Contracts, in Anderl (Hrsg), Blockchain in der Rechtspraxis (2020) 78

Antonopoulos Andreas, Bitcoin & Blockchain – Grundlagen und Programmierung: Die Blockchain verstehen, Anwendungen entwickeln (2018)

Anzinger Heribert, Smart Contracts in der Sharing Economy, in Fries Martin/Paal Boris P. (Hrsg), Smart Contracts (2019) 33

AXA, AXA goes blockchain with fizzy, vom 13.9.2017 https://www.axa.com/en/magazine/axa-goes-blockchain-with-fizzy

BaFin, Geiling Luisa, Distributed Ledger: Die Technologie hinter den virtuellen Währungen am Beispiel der Blockchain, 15.2.2016, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2016/fa_bj_1602_blockchain.html

Baier Anton/Bredow Jens/Busse Daniel ua, Schieds- und Mediationsordnung: VIAC, Handbuch Wiener Regeln und Handbuch Schieds- und Mediationsordnung[2] (Stand: 1.2.2019)

Bergmann Christoph, Die Abwicklung der DAO, bitcoinblog, 30.6.2016, https://bitcoinblog.de/2016/06/30/die-abwicklung-der-dao/

Bertram Ute, Smart Contracts, MDR 2018, 1416

Bich-Carrière Laurence, Say it with [A Smiling Face with Smiling Eyes]: Judicial Use and Legal Challenges with Emoji Interpretation in Canada, 32 International Journal for the Semiotics of Law 2019, 283

Bolesch Lara/Mitschele Andreas, Revolution oder Evolution? Funktionsweise, Herausforderungen und Potenziale der Blockchain-Technologie, ZfgK 2016, 1125

Bollenberger Raimund, Vertragsabschluss unter beiderseitig verdünnter Willensfreiheit, ÖBA 2016, 26

Borges Georg, Rechtliche Rahmenbedingungen für autonome Systeme, NJW 2018, 977

Braegelmann Tom/Kaulartz Markus, Einleitung, in Braegelmann Tom/Kaulartz Markus (Hrsg), Rechtshandbuch Smart Contracts (2019) 4

Brameshuber Georg, Spaltungen einer Blockchain im Steuerrecht, in Piska Christian/Völkel Oliver (Hrsg), Blockchain rules (2019) 303

Brownworth Anders, Blockchain Demo, https://andersbrownworth.com/blockchain/hash

Buchleitner Christina/Rabl Thomas, Blockchain und Smart Contracts: Revolution oder alter Wein im digitalen Schlauch? ecolex 2017, 4

Buterin Vitalik, Ethereum White Paper, 2014, http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Buterin Vitalik, Ethereum: A next generation cryptocurrency and decentralized application platform, bitcoinmagazine, 2014, https://bitcoinmagazine.com/business/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211

Bydlinski Franz, Das österreichische Irrtumsrecht als Ergebnis und Gegenstand beweglichen Systemdenkens, in FS Stoll (2001) 113

Bydlinski Franz, Privatautonomie und objektive Grundlagen des verpflichtenden Rechtsgeschäftes (1967)

Bydlinski Franz, System und Prinzipien des Privatrechts (1996)

Bydlinski Peter, Bürgerliches Recht I: Allgemeiner Teil, 9. Aufl., (2021)

Bydlinski Peter/Perner Stefan/Spitzer Martin (Hrsg), KBB – Kurzkommentar zum ABGB, 7. Aufl., (2023)

Capgemini Consulting, Smart Contracts in Financial Services: Getting from Hype to Reality, 2016, 11, https://www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/08/smart_contracts_paper_long_0.pdf

Corkery Michael/Silver-Greenberg Jessica, Miss a Payment? Good Luck Moving that Car, New York Times vom 24.9.2014, https://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/

Dehn Wilma, Formnichtige Rechtsgeschäfte und ihre Erfüllung: Rückforderungsausschluss und Heilung nach § 1432 ABGB (1998)

Diedrich Henning, Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations (2016)

Diedrich Henning, Lexon: Digital Contracts (2020)

Diermann Ralph, Wie Blockchain-Technik das Energiesystem revolutionieren kann, Süddeutsche Zeitung vom 14.8.2016, https://www.sueddeutsche.de/wissen/energie-wie-blockchain-technik-das-energiesystem-revolutionieren-kann-1.3117309

Djazayeri Alexander, Rechtliche Herausforderungen durch Smart Contracts, jurisPR-BKR 12/2016 Anm. 1 bei Fn. 21

Ehrke-Rabel Tina/Eisenberger Iris/Hödl Elisabeth/Pachinger Stephan/Schneider Eva, Kryptowährungen, Blockchain und Smart Contracts: Risiken und Chancen für den Staat (Teil I), jusIT 2017, 87.

Engert Andreas, In dubio pro libertate – zum Optionswert rechtlicher Experimente, in Grundmann Stefan/Möslein Florian (Hrsg), Innovation und Vertragsrecht 153

Erbguth Jörn, Transparenz von Smart Contracts, in Fries Martin/Paal Boris (Hrsg), Smart Contracts (2019) 25

Eschenbruch Klaus/Gerstberger Robert, Smart Contracts: Planungs-, Bau- und Immobilienverträge als Programm? NZBau 2018, 3

Fairfield Joshua, Smart Contracts, Bitcoin Bots, and Consumer Protection, W&L-LawRev 71 (2014) 35

Fasching Markus/Bernsteiner Lisa, Das ABGB in der digitalen Welt: Überlegungen zur rechtlichen Einordnung von NFT, RdW 2022, 234

Fenyves Attila/Kerschner Ferdinand/Vonkilch Andreas (Hrsg), Klang, 3. Aufl., (2014) §§ 1 – 43

Fenyves Attila/Kerschner Ferdinand/Vonkilch Andreas (Hrsg), Klang, 3. Aufl., (2017) §§ 285 – 352

Fenyves Attila/Kerschner Ferdinand/Vonkilch Andreas (Hrsg), Klang, 3. Aufl., (2017) §§ 552 – 646

Fenyves Attila/Kerschner Ferdinand/Vonkilch Andreas (Hrsg), Klang, 3. Aufl., (2022) §§ 859 – 887

Fenyves Attila/Kerschner Ferdinand/Vonkilch Andreas (Hrsg), Klang, 3. Aufl., (2011) §§ 897 – 916

Fenyves Attila/Kerschner Ferdinand/Vonkilch Andreas (Hrsg), Klang, 3. Aufl., (2019) §§ 1002 – 1044

Fenyves Attila/Kerschner Ferdinand/Vonkilch Andreas (Hrsg), Klang, 3. Aufl., (2019) §§ 1045 – 1089

Finck Michèle, Blockchain Regulation and Governance in Europe (2018)

Finck Michèle, Grundlagen und Technologie von Smart Contracts, in Fries Martin/Paal Boris (Hrsg), Smart Contracts (2019) 1

Forgó Nikolaus in Forgó Nikolaus/Zöchling-Jud Brigitta, Das Vertragsrecht des ABGB auf dem Prüfstand: Überlegungen im digitalen Zeitalter, 20. ÖJT Band II/1, 285

Frankenreiter Jens, The Limits of Smart Contracts, JITE 2019, 149

Fraunhofer-Institut, Blockchain und Smart Contracts: Effiziente und sichere Wertschöpfungsnetzwerke, Whitepaper, Juli 2018, https://www.iml.fraunhofer.de/content/dam/iml/de/documents/OE260/10_Whitepaper_BlockchainSmart-Contracts_Ausgabe_10_WEB.pdf

Fries Martin, Schadensersatz ex machina, NJW 2019, 901

Fritzer Marie-Therese, Die Form der Schenkung unter Lebenden (2018)

Gorzala Jeannette, Connected Cars: Smarte Fahrzeuge als potenzielle Vertragspartner? RdW 2019/60

Griller Stefan, Drittwirkung und Fiskalgeltung von Grundrechten, ZfV 1983, 109

Gruber Michael (Hrsg), Börsegesetz/Marktmissbrauchsverordnung: BörseG 2018/MAR (Stand 1.7.2020, rdb.at)

Grünwald Andreas/Nüßing Christoph, Machine To Machine (M2M)-Kommunikation – Regulatorische Fragen bei der Kommunikation im Internet der Dinge, MMR 2015, 378

Gupta Manav, Blockchain, IBM Limited Edition (2017)

Hahn Christopher/Wilkens Robert, ICO vs. IPO – Prospektrechtliche Anforderungen bei Equity Token Offerings, ZBB 2019, 10

Hancock Matthew/Vaizey Ed, Distributed Ledger Technology: beyond block chain – A report by the UK Government Chief Scientific Adviser, 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Hanzl Martin, Handbuch Blockchain und Smart Contracts (2020)

Hanzl Martin, Smart Contracts – eine zivilrechtliche Betrachtung, in Hanzl Martin/Pelzmann Helen/Schragl Markus (Hrsg), Handbuch Digitalisierung (2021) 263

Hanzl Martin/Rubey Tamara, Blockchain – frischer Wind im Gesellschaftsrecht? GesRZ 2018, 102

Hanzl Martin/Rubey Tamara, Smart Contracts – die intelligente Art Verträge zu schließen? Zak 2018, 127

Hanzl Martin/Rubey Tamara, The smartest contract? Zak 2018, 184

Hartlieb Franz, Verbandsvertragsrecht (2023)

Heckelmann Martin, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504

Heinze Christian, Kann die Blockchain das klassische Grundbuch ablösen? Handelsblatt vom 10.7.2019, https://www.handelsblatt.com/finanzen/steuern-recht/recht/gastkommentar-kann-die-blockchain-das-klassische-grundbuch-abloesen/24575822.html?ticket=ST-1l748280-31Lw5C3wLTciTO1U9Gbn-ap1

Hill Elliot, AXA drops Ethereum-based flight insurance platform, vom 10.11.2019, https://coinrivet.com/de/axa-drops-ethereum-based-flight-insurance-platform/

Hoffmann Christian, Blockchain Use Cases Revisited: Micro-Lending Solutions for Retail Banking and Financial Inclusion, JSSI 2021, 1

Hoffmann-Riem Wolfgang, Recht im Sog der digitalen Transformation (2022)

Hohn-Hein Nicolas/Barth Günter, Immaterialgüterrechte in der Welt von Blockchain und Smart Contract, GRUR 2018, 1089

Höpfel Frank/Ratz Eckart (Hrsg), Wiener Kommentar zum Strafgesetzbuch (Stand 15.8.2023, rdb.at)

Hoppen Peter, „The DAO-Hack" und der letzte Flug Otto Lilienthals, CRonline, vom 9.8.2016, http://www.cr-online.de/blog/2016/06/21/thedao-hack-und-der-letzte-flug-otto-lilienthals-am-09-08-1896/

Hoyer Hans, Zum possessorischen Schutz des Rechtsbesitzes, wbl 1999, 341

Hupel Lars, Benutzerfreundlicher Äther: Smart Contracts in dezentrale Applikationen einbetten, c't 2021, 136

Hupel Lars, Den Äther programmieren: Smart Contracts für die Ethereum-Blockchain schreiben, c't 2021, 150

Iro Gert/Riss Olaf, Bürgerliches Recht IV: Sachenrecht, 8. Aufl., (2023)

Jänich Volker/Schrader Paul/Reck Vivian, Rechtsprobleme des autonomen Fahrens, NZV 2015, 313

Karollus Martin, Funktion und Dogmatik der Haftung aus Schutzgesetzverletzung: Zugleich ein Beitrag zum Deliktssystem des ABGB und zur Haftung für casus mixtus (1992)

Kaulartz Markus, Die Blockchain-Technologie: Hintergründe zur Distributed Ledger Technology und zu Blockchains, CR 2016, 474

Kaulartz Markus, Herausforderungen bei der Gestaltung von Smart Contracts, InTer 2016, 201

Kaulartz Markus, Rechtliche Grenzen bei der Gestaltung von Smart Contracts, DS-RITB 2016, 1023

Kaulartz Markus, Smart Contract Dispute Resolution, in Fries Martin/Paal Boris (Hrsg), Smart Contracts (2019) 73

Kaulartz Markus/Heckmann Jörn, Blockchain: Rechtliche Hürden für „Smart Contracts", BM 2016, 34

Kaulartz Markus/Heckmann Jörn, Smart Contracts – Anwendungen der Blockchain-Technologie, CR 2016, 618

Kiffer Lucianna/Levin Dave/Mislove Alan, Analyzing Ethereum's Contract Topology, IMC 2018, 494

Kirn Stefan/Müller-Hengstenberg Claus, Intelligente (Software-)Agenten: Von der Automatisierung zur Autonomie? Verselbstständigung technischer Systeme, MMR 2014, 225

Klang Heinrich/Gschnitzer Franz (Hrsg), Kommentar zum allgemeinen bürgerlichen Gesetzbuch IV/1, 2. Aufl., (1968)

Klang Heinrich/Gschnitzer Franz (Hrsg), Kommentar zum allgemeinen bürgerlichen Gesetzbuch IV/2, 2. Aufl., (1978)

Kletečka Andreas/Schauer Martin (Hrsg), Online-Kommentar zum ABGB – ABGB-ON^{Version} (Stand 15.9.2023, rdb.at)

Klostermeier Johannes, Axa startet erste Blockchain-Versicherung, vom 18.1.2018, https://www.cio.de/a/axa-startet-erste-blockchain-versicherung,3563749

Knoll Martin, Blockchain und Smart Contracts - ein kurzer Abriss, ZIIR 2016, 406

Koch Bernhard, Wie relevant ist Dziubak in Österreich? VbR 2020/27

Kodek Georg (Hrsg), Kommentar zum Grundbuchsrecht, 2. Aufl., (Stand: 1.9.2016, rdb.at)

Kodek Georg, NFTs und das ABGB - Schnittstellenfragen zwischen Netz und realer Welt, Zak 2022, 24

Kogler Gabriel, Non Fungible Tokens und Sachenrecht, JBl 2021, 685

Köhler Helmut, Die Problematik automatisierter Rechtsvorgänge, insbesondere von Willenserklärungen, AcP 182 (1982) 126

Kotrba David, Wien Energie führt ersten Gashandel mit Blockchain durch, 4.11.2017, https://futurezone.at/b2b/wien-energie-fuehrt-ersten-gashandel-mit-blockchain-durch/292.835.890

Koziol Helmut, Haftpflichtrecht I, 4. Aufl., (Stand 1.4.2020, rdb.at)

Koziol Helmut, Risikoverteilung bei auftragswidrigem Handeln des Bevollmächtigten, in FS Rey (2003) 427

Koziol Helmut, Sache, Eigentum und persönliche Sachenrechte: vernachlässigte dogmatische Schätze des österreichischen ABGB? Überlegenswerte Anregungen für künftige Kodifikationen, in FS Canaris zum 80. Geburtstag (2017) 1087

Koziol Helmut, Von der rechtgeschäftlichen Bindung zur Vertrauenshaftung, in FS Iro (2013) 81

Kramer Ernst, Juristische Methodenlehre, 5. Aufl., (2016)

Kratzenstein Patrick in Adensamer Nikolaus/Mitterecker Johannes (Hrsg), Gesellschafterstreit (2021) Kapitel 5: Zur Wurzel allen Übels: Vorbeugung von Gesellschafterstreitigkeiten durch Smart Contracts

Krönke Christoph/Tschachler Elissa, Decentralized Energy, RdU 2021/127

Kucsko Guido/Pabst Alexander/Tipotsch Katharina Anna/Tyrybon Dominik, NFT – Ein Selbstversuch, ecolex 2021, 495

Kunkel Carsten, Vertragsgestaltung: Eine methodisch-didaktische Einführung (2015)

Kuntz Thilo, Konsens statt Recht? Überlegungen zu Chancen und Herausforderungen der Blockchain-Technologie aus juristischer Sicht, AcP 220 (2020) 51

Kuschel Linda, Digitale Eigenmacht: Digitale Eingriffe in vernetzte Sachen als Herausforderung für den possessorischen Besitzschutz, AcP 220 (2020) 98

Lessig Lawrence, Code is Law: On Liberty in Cyberspace, Harvard Magazine, vom 1.1.2000, https://www.harvardmagazine.com/2000/01/code-is-law-html

Leukauf Otto/Steininger Herbert (Hrsg), StGB Update 2020 Strafgesetzbuch Kommentar[4] (Stand 1.2.2020, rdb.at)

Levy Karen, Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law, ESTS 2017, 1, https://estsjournal.org/index.php/ests/article/view/107/61

Leyens Patrick /Heiss Stefan/Soritz Lukas, Smart Contracts im unternehmerischen Rechtsverkehr (B2B): Grundsatzfragen, Vertragsgestaltung und AGB-Kontrolle, JBl 2022, 137

Linardatos Dimitrios, Autonome und vernetzte Aktanten im Zivilrecht (2021)

Lindner Eric, Der programmierte Mietvertrag, NZM 2021, 665

Mandal Lopamudra, Ricardian Contract (2019)

Mandl Oliver, Das Smart Home als Instrument der digitalen Rechtsdurchsetzung? immolex 2019, 200

Mann Maximilian, Die Decentralized Autonomous Organization – ein neuer Gesellschaftstyp? Gesellschaftsrechtliche und kollisionsrechtliche Implikationen, NZG 2017, 1015

Martini Mario/Weinzierl Quirin, Die Blockchain-Technologie und das Recht auf Vergessenwerden: zum Dilemma zwischen Nicht-Vergessen-Können und Vergessen-Müssen, NVwZ 2017, 1251

Matzke Robin, Smart Contracts statt Zwangsvollstreckung? in Fries Martin/Paal Boris (Hrsg), Smart Contracts (2019) 99

Möslein Florian, Dispositives Recht: Zwecke, Strukturen und Methoden (2011)

Möslein Florian, Rechtliche Grenzen innovativer Finanztechnologien (FinTech): Smart Contracts als Selbsthilfe? ZBB 2018, 208

Möslein Florian, Rechtsgeschäftslehre und Smart Contracts, in Braegelmann Tom/Kaulartz Markus (Hrsg), Rechtshandbuch Smart Contracts (2019) 81

Möslein Florian, Smart Contracts im Zivil- und Handelsrecht, ZHR 183 (2019) 254

Müller Lukas/Seiler Reto, Smart Contracts aus Sicht des Vertragsrechts: Funktionsweise, Anwendungsfälle und Leistungsstörungen, AJP/PJA 2017, 317

Müller-Hengstenberg Claus/Kirn Stefan, Intelligente (Software-)Agenten: Eine neue Herausforderung unseres Rechtssystems: Rechtliche Konsequenzen der „Verselbstständigung" technischer Systeme, MMR 2014, 307

Nakamoto Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, White-Paper, 2008, https://bitcoin.org/bitcoin.pdf

Ofner Julius, Der Ur-Entwurf und die Beratungs-Protokolle des österreichischen allgemeinen bürgerlichen Gesetzbuches I (1889) zitiert als Ofner, Ur-Entwurf I Seite §

Ofner Julius, Der Ur-Entwurf und die Beratungs-Protokolle des österreichischen allgemeinen bürgerlichen Gesetzbuches II (1889) zitiert als Ofner, Ur-Entwurf II Seite §

Paulus Christoph/Matzke Robin, Digitalisierung und private Rechtsdurchsetzung, CR 2017, 769

Paulus Christoph/Matzke Robin, Smart Contracts und Smart Meter – Versorgungssperre per Fernzugriff, NJW 2018, 1905

Paulus David, Die automatisierte Willenserklärung, JuS 2019, 960

Paulus David/Matzke Robin, Smart Contracts und das BGB – Viel Lärm um nichts? ZfPW 2018, 431

Pendl Matthias, Emojis auf dem Weg ins (Privat-)Recht – ein Schlaglicht, NJW 2022, 1054

Perlaki Dominik, Island: „Nicht genug Energie“ für Krypto-Mining, 14.2.2018, https://brutkasten.com/island-nicht-genug-energie-fuer-krypto-mining/

Pesch Jo Paulina, Blockchain, Smart Contracts und Datenschutz, in Fries Martin/Paal Boris (Hrsg), Smart Contracts (2019) 13

Pfeffer Alexandra/Rauter Alexander Roman (Hrsg), Handbuch Kunstrecht, 2. Aufl. (Stand 15.1.2020, rdb.at).

Pisko Oskar, Erfüllung und Heilung formungültiger Geschäfte, JBl 1934, 511

Pittl Raimund/Gottardis Lukas, Smart Contracts - ein Fall für das Wohn- und Immobilienrecht? immolex 2019, 194

pwc, Blockchain – Change für Energieverbraucher? Kurzstudie (2016) https://www.pwc.de/de/energiewirtschaft/blockchain-chance-fuer-energieverbraucher.pdf

Rabl Thomas, ElWOG 2010 und GWG 2011: Mahnen ohne oder doch mit Methode? ecolex 2012, 772

Rabl Thomas, Recht smart 1.03: Blockchains - Ketten, die Ketten sprengen (sollen)! ecolex 2019, 214

Raskin Max, The law and legality of smart contracts, GEO. L. TECH. REV. 2017, 305, https://georgetownlawtechreview.org/wp-content/uploads/2017/05/Raskin-1-GEO.-L.-TECH.-REV.-305-.pdf

Reder Matthias/Eckard Katja, Cash aus coins: Das Krypto 1x1 (2022)

Reusch Philipp, Future Law, 2. Aufl., (Stand 1.7.2022, rdb.at)

Riehm Thomas, Smart Contracts und AGB-Recht, in Braegelmann Tom/Kaulartz Markus (Hrsg), Rechtshandbuch Smart Contracts (2019) 99

Riehm Thomas, Smart Contracts und verbotene Eigenmacht, in Fries Martin/Paal Boris (Hrsg), Smart Contracts (2019) 85

Riss Olaf, Die sachenrechtliche Wirksamkeit des einseitig erklärten Eigentumsvorbehaltes – neue Gedanken zu einer alten Streitfrage, ÖBA 2010, 215

Rodrigues Usha, Law and the Blockchain, ILR 104 (2019) 679

Rühl Giesela, Smart Contracts und anwendbares Recht, in Braegelmann Tom/Kaulartz Markus (Hrsg), Rechtshandbuch Smart Contracts (2019) 147

Rummel Peter/Lukas Meinhard/Geroldinger Andreas (Hrsg), Kommentar zum Allgemeinen Bürgerlichen Gesetzbuch, 4. Aufl. (1.3.2023, rdb.at)

Rutz Victor, Blockchain quo vadis: Eine Stärken-Schwächen-Analyse des Private- und des Public-Blockchain-Ansatzes (2020)

Saive David, Rückabwicklung von Blockchain-Transaktionen, DuD 2018, 764

Savelyev Alexander, Contract law 2.0: ‘Smart’ contracts as the beginning of the end of classic contract law, ICTL 26 (2017) 116

Schäfer Hans-Bernd/Ott Claus, Lehrbuch der ökonomischen Analyse des Zivilrechts, 6. Aufl., (2021)

Schauer Martin, Reformbedarf im Allgemeinen Teil und im Schuldrecht Allgemeiner Teil, in Fischer-Czermak/Hopf/Kathrein/Schauer (Hrsg), ABGB 2011 – Chancen und Möglichkeiten einer Zivilrechtsreform (2008) 51

Schopper Alexander/Raschner Patrick, Privat- und aufsichtsrechtliche Rahmenbedingungen für Krypto-Banking, ÖBA 2022, 262

Schrey Joachim/Thalhofer Thomas, Rechtliche Aspekte der Blockchain, NJW 2017, 1431

Schulz Hajo, Das macht Blockchain: Die Technik hinter Bitcoin & Co, c't 23/2017, 103

Schulz Hajo, Vertrag denkt mit: Smart Contracts in der Ethereum-Blockchain, c't 23/2017, 108

Schwimann Michael/Kodek Georg (Hrsg), Praxiskommentar zum Allgemeinen Bürgerlichen Gesetzbuch V[5] (2021)

Schwimann Michael/Kodek Georg (Hrsg), Praxiskommentar zum Allgemeinen Bürgerlichen Gesetzbuch IV[5] (2018)

Schwimann Michael/Neumayr Matthias (Hrsg), ABGB Taschenkommentar, 5. Aufl., (2020)

Seeber Thomas/Schweiger Manuel/Schachner Martin, Immobilientransaktionen über die Blockchain, immolex 2018, 38

Simmchen Christoph, Blockchain (R)Evolution, MMR 2017, 162

Smets Sascha/Kapeller Siegfried, Smart Contracts: Vertragsabschluss und Haftung, ÖJZ 2018, 293

Specht Louisa/Herold Sophie, Roboter als Vertragspartner? Gedanken zu Vertragsabschlüssen unter Einbeziehung automatisiert und autonom agierender Systeme, MMR 2018, 40

Spielbüchler Karl, Übereignung durch mittelbare Leistung, JBl 1971, 589

Spindler Gerald, Gesellschaftsrecht und Digitalisierung, ZGR 2018, 17

Stadler Arthur/Bichler Jacqueline, Was man von Klimts digitalem „Kuss" tatsächlich kauft, Der Standard, vom 14.2.2022, https://www.derstandard.at/story/2000133332083/was-man-von-klimts-digitalem-kuss-tatsaechlich-kauft?ref=article

Straube Manfred/Ratka Thomas/Rauter Alexander Roman (Hrsg), Wiener Kommentar zum Unternehmensgesetzbuch[3] (Stand 1.11.2023, rdb.at)

Strobel Benedikt, Digitaler Fernzugriff und verbotene Eigenmacht, NJW 2022, 2361

Sun Enchang/Meng Kang/Yang Ruizhe/Zhang Yanhua/Li Meng, Research on Distributed Data Sharing System based on Internet of Things and Blockchain, JSSI 2021, 239

Sutherland Brandon, Blockchain´s first consensus implementation is unsustainable, Joule 2019, 917

Szabo Nick, Formalizing and Securing Relationships on Public Networks, 1997, https://nakamotoinstitute.org/formalizing-securing-relationships/

Szabo Nick, on Blockchains and Smart Contracts, at Lykke, abrufbar als Video https://www.youtube.com/watch?v=tWuN2R2DC6c

Szabo Nick, Smart Contracts, 1994, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

Szabo Nick, Smart Contracts: Building Blocks for Digital Markets, 1996, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Tapscott Don/Tapscott Alex, Die Blockchain-Revolution: Wie die Technologie hinter Bitcoin nicht nur das Finanzsystem, sondern die ganze Welt verändert (2016)

Temming Felipe, Verstehen Sie Deutsch? Sprachenunkenntnis beim Vertragsschluss und bei der AGB-Kontrolle, GPR 2016, 38

Teubner Gunther, Digitale Rechtssubjekte? Zum privatrechtlichen Status autonomer Softwareagenten, AcP 218 (2018) 155

Teubner Gunther, Elektronische Agenten und große Menschenaffen: Zur Ausweitung des Akteurstatus in Recht und Politik, ZfRsoz 27 (2006) 5

Thiele Clemens, Smart Contracts – Revolution der Rechtsdurchsetzung? 20. ÖJT 2018 II/2 201

Thießen Friedrich, Das Ende der Blockchain? ZfgK, 2018, 606

Thießen Friedrich, Öffentliche und private Blockchains in der Finanzwirtschaft – eine Stärken-Schwächen Analyse, ZfgK 2020, 706

Torcasso David, Das Traditionshaus Gübelin setzt auf Blockchain: Bei Edelsteinen lässt sich so die gesamte Lieferkette nachvollziehen, Handelszeitung vom 10.1.2018, https://www.handelszeitung.ch/unternehmen/gubelin-prasentiert-erste-blockchain-fur-farbedelsteine

Torggler Ulrich (Hrsg), Gesetz über Gesellschaften mit beschränkter Haftung (Stand: 1.8.2014, rdb.at)

Torggler Ulrich (Hrsg), UGB Unternehmensgesetzbuch Kommentar, 3. Aufl., (Stand: 1.1.2019, rdb.at)

vbw-Studie, Blockchain und Smart Contracts: Recht und Technik im Überblick, erstellt vom Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht, Universität Passau, Oktober 2017, https://www.vbw-bayern.de/Redaktion/Frei-zugaengliche-Medien/Abteilungen-GS/Wirtschaftspolitik/2019/Downloads/190509-Blockchain-und-Smart-Contracts_neu.pdf

Veronesi Tullia/Pugl Marie-Luise, Immobilien-Investitionen über die Blockchain, ImmoZak 2021/44

Vögerl Christina, Das neue Bauträgervertragsrecht aus rechtsökonomischer Sicht, immolex 2008, 235

Völkel Oliver, Die Blockchain: Von Fehlern und Irrtümern, ZFR 2021, 532

Völkel Oliver, Grundlagen der Blockchain-Technologie und virtueller Währungen in Piska Christian/Völkel Oliver (Hrsg), Blockchain rules (2019) 1

Völkel Oliver, Privatrechtliche Einordnung virtueller Währungen, ÖBA 2017, 385

Vonkilch Andreas/Knoll Matthias, Bitcoins und das Sachenrecht des ABGB, JBl 2019, 139

Wagner Gerhard, Algorithmische Rechtsdurchsetzung, AcP 222 (2022) 56

Wagner Gerhard, Prozessverträge: Privatautonomie im Verfahrensrecht (1998)

Wagner Kurt/Knechtel Gerhard (Hrsg), Notariatsordnung und alle einschlägigen Rechtsvorschriften (Stand 1.1.2014, rdb.at)

Waschbusch Gerd/Kiszka Sabrina/Merz Jan, Einsatz von Smart Contracts in der Finanzbranche, ÖBA 2021, 547

Wiebe Andreas, Die elektronische Willenserklärung: Kommunikationstheoretische und rechtsdogmatische Grundlagen des elektronischen Geschäftsverkehrs (2002)

Wilburg Walter, Entwicklung eines beweglichen Systems im bürgerlichen Recht (1950)

Wilhelm Alexander, Smart Contracts im Zivilrecht (Teil I), WM 2020, 1807

Wilhelm Alexander, Smart Contracts im Zivilrecht (Teil II), WM 2020, 1849

Wilhelm Georg, Telefax: Zugang, Übermittlungsfehler und Formfragen, ecolex 1990, 208

Wilkens Robert/Falk Richard, Smart Contracts: Grundlagen, Anwendungsfelder und rechtliche Aspekte (2019)

Wright Aaron/De Filippi Primavera, Decentralized Blockchain Technology and The Rise of Lex Cryptographia, SSRN 2015, 1, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664

Wulf Hans/Burgenmeister Clemens, Industrie 4.0 in der Logistik – Rechtliche Hürden beim Einsatz neuer Vernetzungs-Technologien: Anwendungsbeispiele und Lösungswege zu sechs zentralen Bereichen der Logistik, CR 2015, 404

Zankl Wolfgang, Rechtsqualität und Zugang von Erklärungen im Internet, ecolex 2001, 344

Zeiller Franz von, Commentar über das allgemeine bürgerliche Gesetzbuch für die gesammten deutschen Erbländer der oesterreichischen Monarchie I (1811) zitiert als von Zeiller, Commentar I § Anm

Zeiller Franz von, Commentar über das allgemeine bürgerliche Gesetzbuch für die gesammten deutschen Erbländer der oesterreichischen Monarchie III/1 (1812) zitiert als von Zeiller, Commentar III/1 § Anm

Zeiller Franz von, Commentar über das allgemeine bürgerliche Gesetzbuch für die gesammten deutschen Erbländer der oesterreichischen Monarchie III/2 (1813) zitiert als von Zeiller, Commentar III/2 § Anm

Zöchling-Jud Brigitta, Internet der Dinge, 20. ÖJT 2018 II/1 273

Anhang

LLL Ansicht der Abbildung eines Vertrags im EtherScripter

```
(seq

;; Ein Vertrag zum Erwerb des NFT "MCI Fortbildung rocks" um "2 ether im Dezember 2022"
;; Ethereum Adresse des Veräußerers:
(sstore "VERÄUßERER" 0x6af26739b9ffef8aa2985252e5357fde)
;; Ethereum Adresse des Erwerbers:
(sstore "ERWERBER" 0xfeab802c014588f08bfee2741086c375)
(return 0 (lll (seq;; START BODY
```

```
;; Wenn 2 ether bis 24:00 Uhr des 31.12.22 auf der Adresse des Vertrags eingegangen sind,
(when (and (>= (balance) 2ether) (<= (timestamp) (sload "31.12.22")))
(seq
;; dann versende das NFT "MCI Fortbildung rocks" an den ERWERBER und 2 ether an den VERÄUßERER.
(sstore "NFT_MCI Fortbildung rocks" (sload "ERWERBER"))
(call (- (gas) 100) (sload "VERÄUßERER") (balance) 0 0 0 0)
)
)

) 0));; END BODY
```

)

XML Ansicht der Abbildung eines Vertrags im EtherScripter

```
<xml xmlns="http://www.w3.org/1999/xhtml">
<block type="INIT" id="47" x="52" y="55">
<statement name="INIT">
<block type="COMMENT" id="48">
<field name="NOTE"> Ein Vertrag zum Erwerb des NFT "MCI Fortbildung rocks" um "2 ether im Dezember 2022"</field>
<next>
<block type="COMMENT" id="49">
<field name="NOTE">Ethereum Adresse des Veräußerers:</field>
<next>
<block type="STORE" id="50" inline="true">
<field name="POOL">sstore</field>
<value name="SPOT">
<block type="VAL" id="51">
<field name="VAL">VERÄUßERER</field>
</block>
</value>
<value name="VAL">
<block type="VAL" id="52">
<field name="VAL">0x6af26739b9ffef8aa2985252e5357fde</field>
</block>
```

```
</value>
<next>
<block type="COMMENT" id="53">
<field name="NOTE">Ethereum Adresse des Erwerbers:</field>
<next>
<block type="STORE" id="54" inline="true">
<field name="POOL">sstore</field>
<value name="SPOT">
<block type="VAL" id="55">
<field name="VAL">ERWERBER</field>
</block>
</value>
<value name="VAL">
<block type="VAL" id="56">
<field name="VAL">0xfeab802c014588f08bfee2741086c375</field>
</block>
</value>
</block>
</next>
</block>
</next>
</block>
</next>
</block>
</next>
</block>
</statement>
<statement name="BODY">
<block type="COMMENT" id="57">
<field name="NOTE">Wenn 2 ether bis 24:00 Uhr des 31.12.22 auf der Adresse des Vertrags
eingegangen sind, </field>
<next>
<block type="WHEN" id="58" inline="false">
<field name="WORD">when</field>
<value name="COND">
<block type="LOGIC" id="59" inline="false">
<field name="OP">and</field>
```

<value name="A">
<block type="COMPARE" id="60" inline="true">
<field name="OP">>=</field>
<value name="A">
<block type="CONTRACT" id="61">
<field name="PROP">balance</field>
</block>
</value>
<value name="B">
<block type="CURRENCY" id="62" inline="true">
<field name="DENOM">ether</field>
<value name="AMT">
<block type="VAL" id="63">
<field name="VAL">2</field>
</block>
</value>
</block>
</value>
</block>
</value>
<value name="B">
<block type="COMPARE" id="64" inline="true">
<field name="OP"><=</field>
<value name="A">
<block type="BLOCKINFO" id="65">
<field name="PROP">timestamp</field>
</block>
</value>
<value name="B">
<block type="LOAD" id="66" inline="true">
<field name="POOL">sload</field>
<value name="SPOT">
<block type="VAL" id="67">
<field name="VAL">31.12.22</field>
</block>
</value>
</block>

```
</value>
</block>
</value>
</block>
</value>
<statement name="THEN">
<block type="COMMENT" id="68">
<field name="NOTE">dann versende das NFT "MCI Fortbildung rocks" an den ERWERBER
und 2 ether an den VERÄUßERER.</field>
<next>
<block type="STORE" id="69" inline="true">
<field name="POOL">sstore</field>
<value name="SPOT">
<block type="VAL" id="70">
<field name="VAL">NFT_MCI Fortbildung rocks</field>
</block>
</value>
<value name="VAL">
<block type="LOAD" id="71" inline="true">
<field name="POOL">sload</field>
<value name="SPOT">
<block type="VAL" id="72">
<field name="VAL">ERWERBER</field>
</block>
</value>
</block>
</value>
<next>
<block type="SPEND" id="73" inline="true">
<value name="AMOUNT">
<block type="CONTRACT" id="74">
<field name="PROP">balance</field>
</block>
</value>
<value name="TO">
<block type="LOAD" id="75" inline="true">
<field name="POOL">sload</field>
```

<value name="SPOT">
<block type="VAL" id="76">
<field name="VAL">VERÄUßERER</field>
</block>
</value>
</block>
</value>
</block>
</next>
</block>
</next>
</block>
</statement>
</block>
</next>
</block>
</statement>
</block>
</xml>

Diskutierte Anwendungsgebiete

Unter dem Begriff Smart Contracts werden diverse, teilweise de lege lata wohl nicht realisierbare, Einsatzbereiche diskutiert. Im Folgenden sind einige aufgezählt:

Vorbeuge gegen Gesellschafterstreitigkeiten[380]
Handel mit Kryptoassets[381]
Durchführung von Initial Coin Offerings (ICOs)[382]
Anlageberatung (Robo-Advisor)[383]

380 Kratzenstein in Adensamer/Mitterecker, Gesellschafterstreit Rn. 5/1.
381 Schopper/Raschner, ÖBA 2022, 262.
382 Hahn/Wilkens ZBB 2019, 10.
383 https://roboadvisors.com/; https://at.scalable.capital/.

Abwicklung von Geschäftsmodellen der Sharing Economy[384] etwa „pay as you drive"-Tarife[385] und Bezahlsysteme an Ladestationen für Elektroautos[386]
Erwerbsgeschäfte,[387] Werklohnzahlungen,[388] Vermietung, Leasing, Kreditfinanzierung („Interrupt Devices" und „Smart Locks")[389]
Erwerbsgeschäfte für Diamanten und Kunstgegenstände[390]
Neue Treuhandkonstellationen[391]
Grundbuchsrechtliche Lösungen[392]
Handel mit Energie (Enerchain)[393]
Ökonomisierung der Logistik[394]

384 Wilhelm WM 2020, 1807 (1809); Sun/Meng/Yang/Zhang/Li, JSSI 2021, 239; D. Paulus/Matzke ZfPW 2018, 431 (435); Fries/Paal Smart Contracts/Anzinger S. 33 (43).

385 vbw-Studie, 2017, 38 f., https://www.vbw-bayern.de.

386 Gorzala, RdW 2019/60; Kaulartz/Heckmann CR 2016, 618 (618); Jänich/Schrader/Reck, NZV 2015, 313; pwc, 2016, 13, https://www.pwc.de.

387 Zum Kauf eines e-Books s. Hanzl/Rubey Zak 2018, 127 (128); zur Übertragung oder Lizensierung von Immaterialgüterrechten s. Hohn-Hein/Barth, GRUR 2018, 1089 (1093); für Immobilientransaktionen vgl. Seeber/Schweiger/Schachner, immolex 2018, 38.

388 Eschenbruch/Gerstberger, NZBau 2018, 3 (3).

389 „Starter interrupt devices" sind in den USA bereits im Einsatz, s. Corkery/Silver-Greenberg, 2014, https://dealbook.nytimes.com; Kaulartz/Heckmann CR 2016, 618 (618); Veronesi/Pugl, ImmoZak 2021/44; Heckelmann NJW 2018, 504 (505); D. Paulus/Matzke ZfPW 2018, 431 (434); C. Paulus/Matzke NJW 2018, 1905; Knoll ZIIR 2016, 406 (409); Hoffmann-Riem Digitale Transformation S. 267; Fries/Paal Smart Contracts/Riehm S. 85 (86, 93 f.); Simmchen MMR 2017, 162 (164); Mandl immolex 2019, 200 (201); Leyens/Heiss/Soritz, JBl 2022, 137 (138).

390 Provenienz und jede Änderung der Eigentumsverhältnisse sollen festgehalten werden. Der derivative Erwerb soll mit Smart Contracts erfolgen. Vergleiche Torcasso, 2018, https://www.handelszeitung.ch/.

391 Szabo, Smart Contracts, 1994, http://www.fon.hum.uva.nl; Heckelmann NJW 2018, 504 (504).

392 Heinze, 2019, https://www.handelsblatt.com; Pittl/Gottardis immolex 2019, 194 (196); Veronesi/Pugl, ImmoZak 2021/44 (79); Hoffmann-Riem Digitale Transformation S. 46.

393 Die Smart Contracts auf dieser Plattform sollen kostengünstigeren und unbürokratischeren Handel selbst kleiner Energiemengen erlauben. Wien Energie hat über diese Plattform 2017 den ersten realen Gas-Einkauf bei einem dänischen Lieferanten getätigt. Das Gas wurde einen Tag später geliefert. Siehe Kotrba, 2017, https://futurezone.at. Vergleiche auch http://brooklynmicrogrid.com/ sowie Diermann, 2016, http://www.sueddeutsche.de; Krönke/Tschachler RdU 2021/127.

394 Möslein ZHR 183 (2019), 254 (262); Wulf/Burgenmeister CR 2015, 404; Eschenbruch/Gerstberger, NZBau 2018, 3 (6).

Abwicklung von Versicherungsleistungen[395]

395 Siehe nur das deutsche Start-up Etherisc https://fdd.etherisc.com. Die Versicherungsgesellschaft AXA hat mit „Fizzy" die erste voll automatisierte Versicherung auf Blockchain-Basis für Flugverspätungen auf den Markt gebracht, Klostermeier, 2018, https://www.cio.de; AXA, 2017, https://www.axa.com. Diese wurde Ende 2019 wieder vom Markt genommen, weil der Markt dafür noch nicht reif gewesen sei, Hill, 2019, https://coinrivet.com.

Die einseitige Änderungsbefugnis des Unternehmers bei Bereitstellung digitaler Inhalte

Robert Eitel

§ 1 Einleitung[1]

A. Einführung in die Rechtsgrundlage

Die EU hat die Richtlinie für Digitale Inhalte[2] (im Folgenden DID-RL) und die Warenkaufrichtlinie[3] (im Folgenden WK-RL) eingeführt, um den digitalen Binnenmarkt für Europa zu regulieren und zu vereinheitlichen.[4] Die DID-RL ist zum 20.05.2019 in Kraft getreten, war bis zum 1.7.2021 ins nationale Recht der Mitgliedstaaten umzusetzen und diese umgesetzten Bestimmungen sind auf Verträge, die ab 1.1.2022 geschlossen werden, anzuwenden.[5] Durch die in Art. 4 DID-RL und WK-RL festgelegte Vollharmonisierung soll ein „modernes Vertragsrecht für Europa" in einem digitalen Binnenmarkt[6] geschaffen werden[7], wobei sich die Regelungsinhalte der Richtlinien ergänzen.[8] Die einseitige Änderungsbefugnis des Unternehmers bei digitalen Inhalten ist Teil des durch die DID-RL eingeführten Regelungskomplexes (Art. 19 DID-RL) und wurde zum 1.1.2022 in der Bundesrepublik Deutschland (BRD) und der Republik Österreich (RÖ) eingeführt.

1 Soweit und sofern in dieser Arbeit geschlechtsspezifische Terminologie verwendet wird, sind immer auch alle anderen Geschlechter gemeint.

2 RL (EU) 2019/770 des EP und des Rates vom 20. 5. 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, ABl L 2019/136, 1.

3 RL (EU) 2019/771 des Europäischen Parlaments (EP) und des Rates vom 20. 5. 2019 über bestimmte vertragsrechtliche Aspekte des Warenkaufs, zur Änderung der VO (EU) 2017/2394 und der RL 2009/22/EG sowie zur Aufhebung der RL 1999/44/EG.

4 Schmidt-Kessel/Erler/Grimm/Kramme, GPR 2016, 2, 2; Lunk/Meurer, BB 2022, 387, 387.

5 Kühner/Piltz, CR 2021, 1, 2 Rn. 7.

6 Maute/Mackenrodt Recht als Infrastruktur für Innovation/Datta 155, 158.

7 Mitteilung der Kommission an das Europäische Parlament, den Rat und den Europäischen Wirtschafts- und Sozialausschuss: Ein modernes Vertragsrecht für Europa – Das Potenzial des elektronischen Handels freisetzen vom 9.12.2015, KOM (2015) 633.

8 Lunk/Meurer, BB 2022, 387, 388.

In BRD mit Neufassung der §§ 327 ff. BGB (Änderungsbefugnis des Unternehmers in § 327r BGB), in RÖ mit dem Verbrauchergewährleistungsgesetz (VGG) (Änderungsbefugnis in § 27 VGG).

Die Änderungsbefugnis des Unternehmers ermöglicht diesem, im Rahmen eines laufenden Vertrags Anpassungen am Vertragsgegenstand vorzunehmen, die nicht zur Erhaltung der Vertragsmäßigkeit notwendig wären. Die Einführung dieser Regelung ist bedeutsam, da Verträge mit digitalen Elementen häufig über längere Zeit laufen und sich während dieser Vertragslaufzeit aufgrund wirtschaftlicher oder technischer Entwicklungen gewichtige Anpassungsbedarfe ergeben. Im Kontrast dazu steht der althergebrachte „pacta sunt servanda" -Grundsatz, nach dem Verträge so zu erfüllen sind, wie sie geschlossen wurden.[9] Bei digitalen Inhalten können bspw. Sicherheitsaktualisierungen notwendig werden, weil in der ursprünglichen Version einer Software eine bei Auslieferung nicht erkennbare Sicherheitslücke entdeckt wurde; oder die Software einer Heizungsanlagensteuerung verwendet eine mittlerweile nicht mehr unterstützte Programmiersprache. Steigende Nutzerzahlen können zu einer nicht mehr ausreichend performanten Software führen oder es können sich Anforderungen an den Datenschutz geändert haben[10]; möglich sind auch Änderungen von optischen Elementen aufgrund der stetigen technischen Weiterentwicklung, von technischen Grundlagen einer Software oder zur Sicherstellung der Wirtschaftlichkeit der Bereitstellung, indem nur die aktuelle Variante des Produkts gepflegt werden muss, um die Software weiterhin einer Vielzahl von Kunden anbieten zu können.[11] Solche Änderungen können sowohl im als auch gegenläufig zum Interesse des Nutzers sein.[12] Bei Dauerschuldverhältnissen ist eine solche Änderung aber nicht vorgesehen, denn bei diesen wird die Leistung zwischen den Parteien bei Vertragsschluss definiert und danach nicht mehr geändert.[13] Der Unternehmer kann aus o.g. Gründen zur Veränderung gezwungen sein, während der Nutzer entweder die digitale Leistung weiterhin wie gewohnt nutzen können und entsprechende Funktionalitäten vorfinden möchte oder aber ebenfalls eine Änderung wünscht, um die Interoperabilität mit anderen Komponenten weiterhin sicher zu stellen; es

9 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 1.
10 Möllnitz, MMR 2021, 116; Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 1.
11 Hunzinger, CR 2022, 349, Rn. 1; Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 1.
12 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 1.
13 Möllnitz, MMR 2021, 116, 116.

resultiert daher ein „Spannungsverhältnis zwischen Vertragsbindung und -Kontinuität sowie Flexibilitätserfordernissen".[14] Eine solche Änderung der digitalen Inhalte oder digitalen Dienstleistungen, die über den Vertragsmäßigkeitserhalt hinausgeht, sieht Art. 19 DID-RL vor, wobei ein Ausgleich zwischen den unternehmerischen Interessen und denen des Verbrauchers erfolgen soll.[15]

Dazu bedarf es erstens der Gestattung einer solchen Änderung bereits im zugrunde liegenden Vertrag, der triftige Gründe nennen muss, dem Verbraucher dürfen zweitens keine zusätzlichen Kosten entstehen und drittens muss der Unternehmer den Verbraucher durch eine klare und verständliche Mitteilung über die Änderung informieren.[16] In Art. 19 Abs. 1 lit. d) DID-RL ist noch eine kumulative vierte Bedingung enthalten, sofern der Verbraucher durch die Änderung bei Zugang oder Nutzung der digitalen Inhalte oder Dienstleistungen nicht nur geringfügig beeinträchtigt wird, wobei dann eine Unterrichtung über Merkmale und Zeitpunkt der Änderung im Vorfeld auf einem dauerhaften Datenträger erfolgen muss. Aus der Mitteilung muss sich auch ergeben, dass der Verbraucher innerhalb von 30 Tagen zur Beendigung des Vertrags berechtigt ist.[17] Bei der Umsetzung der Digitalisierung in Vertragsrecht ist der Gesetzgeber trotz der Tendenz zur Vernetzung der Technik am Leitbild der bilateralen Konnexität verhaftet geblieben. Dem Verbraucher wird nur ein Ansprechpartner, der Unternehmer, gegenüber gestellt,[18] um so eine einfachere Rechtsdurchsetzung zu ermöglichen.

B. Forschungsfrage und Relevanz

Der Änderungsmaßstab tritt in der gesetzlichen Umsetzung und der DID-RL nicht hinreichend klar zu Tage. So ist es für Unternehmer und Verbraucher schwer ersichtlich, welche Veränderungen der Vertragsleistung die im Gesetz vorgesehenen Grenzen des triftigen Grundes und der geringfügigen Änderung überschreiten. Daher liegt dieser Arbeit die Forschungsfrage zugrunde, anhand welcher Unterscheidungskriterien bestimmt werden kann, was ein triftiger Grund und eine nicht nur geringfügige Änderung ist.

14 Möllnitz, MMR 2021, 116, 116; Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 2.
15 Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 2.
16 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 2.
17 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 3.
18 Legner, NJOZ 2022, 353, 357.

Dadurch soll Unternehmern und Verbrauchern ein Leitfaden an die Hand gegeben werden, zur Einschätzung, was eine entsprechende Änderung ist und der nachträglichen gerichtlichen Kontrolle ein Kontrollmaßstab an die Hand gegeben werden.

C. Aufbau der Arbeit und Methodik

Mit der vorliegenden Arbeit wird nach einer Abgrenzung von DID-RL und WK-RL ein Überblick über die rechtlichen Rahmenbedingungen auf europäischer Ebene und die konkreten Umsetzungen in der BRD und der RÖ gegeben. Zunächst werden die unterschiedlichen Anforderungen und Regelungen beleuchtet, wobei rechtsvergleichend auf die Gemeinsamkeiten und Unterschiede zwischen EU- und den beiden nationalen Gesetzeswerken eingegangen wird. In einem nächsten Abschnitt wird die Änderungsbefugnis von der Änderungspflicht abgegrenzt. Anschließend wird der dieser Arbeit zugrunde liegenden Forschungsfrage des Maßstabs der Änderung nachgegangen. Diese Fragestellung wird im nächsten Kapitel mittels Transfers ähnlicher gesetzlicher Regelungen gelöst, anhand derer durch allgemein bekannte Methodiken der Gesetzesauslegung eine entsprechende Anwendung auf IT-Verträge vorgenommen wird. Ansatz der Arbeit ist, die Rechtsfigur der Gestaltungsrechte und der für diese vorhandenen Bewertungskriterien auf die Änderungsbefugnis des Unternehmers zu übertragen. Abschließend wird die Problematik in den Gesamtzusammenhang eingeordnet und ein Ausblick gegeben, was zukünftige Umsetzungen bringen könnten und sollten, um Unternehmern und Verbrauchern klare Regelungen an die Hand zu geben.

§ 2 Abgrenzung WK-RL und DID-RL

WK-RL und DID-RL sind zusammen in Kraft getreten und haben ähnliche Regelungsinhalte, die sich im Detail jedoch unterscheiden. Im Folgenden wird daher eine Abgrenzung vorgenommen.

A. DID-RL

Die *DID-RL* dient als vollharmonisierte eigenständige Auffangregelung von Gewährleistungsrechten für alle Vertriebsformen digitaler Leistungen, die nicht Bestandteil des Kaufvertrags sind.[19] Sie gilt auch in Fällen, wenn die gekaufte Sache ihre Funktionen auch ohne das digitale Produkt erfüllen kann oder wenn der Vertrag über die Bereitstellung digitaler Produkte nicht Bestandteil des Vertrags über den Kauf der Sache ist.[20]

B. WK-RL

In den Anwendungsbereich der *WK-RL* fallen dagegen all jene digitalen Inhalte und Dienstleistungen, die in eine Ware integriert oder mit ihr verbunden sind und laut dem geschlossenen Kaufvertrag mit ihr bereitgestellt werden.[21] Bei Sachen mit digitalen Elementen ist zu beachten, dass diese von der Warenkaufrichtlinie betroffen sind, sofern sie ein funktionales (die gekaufte Sache kann bei Fehlen der digitalen Produkte ihre Funktion nicht erfüllen) und ein vertragliches Element (die Bereitstellung der digitalen Produkte wird gem. dem Kaufvertrag über die Sache geschuldet) beinhalten.[22]

Jene digitalen Inhalte, deren Bereitstellung sich nicht aus dem Kaufvertrag explizit ergibt, fallen unter die DID-RL, also fällt bspw. bei einem Smartphone das Betriebssystem unter die WK-RL, während die aus dem App-Store herunterladbaren Programme unter die DID-RL fallen; anderes gilt, sofern der Verkäufer explizit nur die Hardware verkauft.[23] Sofern Zweifel bestehen, gelten digitaler Inhalt / digitale Dienstleistung als mitverkauft, wobei die Beschaffenheit der Ware, objektiver Empfängerhorizont und öffentliche Erklärungen von Verkäufer und Hersteller zu berücksichtigen sind.[24] Eine Fitness-Uhr, bei der es zur Auswertung der von dieser aufgezeichneten Daten noch eine App auf dem Smartphone braucht, unterfällt samt ihrem Betriebssystem als auch die herstellereigene, zusätzlich

19 *J.* Flume, ÖJZ 2022, 137, 138; Fida, Updates, Patches & Co. Zivilrechtliche Fragen zur Softwareaktualisierung, 39.
20 Fida, Updates, 40.
21 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kern 33, 46.
22 Kühner/Piltz, CR 2021, 1 Rn. 16.
23 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kern 33, 48.
24 Heckmann/Paschke juris-PK Internetrecht/Paschke Rn. 584, 585.

aus dem Smartphone-App-Store herunterzuladende, Auswertungs-App der WK-RL[25]; während ein zusätzlicher Vertrag, der in der Werbung als solcher auch klar offeriert werden muss, über die Auswertung dieser Daten und Erstellung personalisierter Trainingspläne hingegen unter die DID-RL fällt.[26] Ziel der WK-RL ist weitgehend eine Anpassung der Regelungen der Verbrauchsgüterkaufrichtlinie über Waren.[27]

C. Unterschiede – Einheit

Möglichkeiten digitale Leistungen bereitzustellen, gibt es unzählige, ähnlich hoch kann die Varianz der entsprechenden Vertragstypen sein, die sich vom bisherigen „Paradigma des Güteraustauschs" entfernen, trotz allem beschränkt durch Titel und Modus des ABGB bzw. der entsprechenden Regelungen des BGB.[28] Die große Besonderheit der digitalen Welt stellt die nicht mehr dauerhafte Zuweisung von Rechten, sondern der bloße Zugang zu Dienstleistungen dar; wobei das kurzzeitige Nutzungsrecht an einer Dienstleistung, wie einem Computerprogramm, Rechenkapazität oder Cloud-Speicherplatz Eigentum und Besitz ablöst.[29] Damit hängen komplexe Fragen der Mehrpersonenverhältnisse zusammen, so wenn bspw. der Dienstleister des Herstellers das Produkt des Herstellers dem Verbraucher zur Verfügung stellt, solche des Urheberrechts, ob also Anbieter und Verbraucher überhaupt die Berechtigung des Herstellers haben, dessen Produkt zu nutzen und möglicher sachenrechtlicher Regelungen. Idealerweise sind die beiden Richtlinien nicht jeweils als eigenständige Einzelne zu betrachten, sondern als eine Einheit, die nach dem Willen des Gesetzgebers für die Schaffung eines digitalen Binnenmarkts[30] naht- und lückenlos zusammenpassen und für digitale Gegenstände möglichst entsprechende Regelungen treffen, obwohl die Terminologie manchmal divergiert, bspw. „digitales Produkt" und „Ware mit digitalen Elementen", die den gleichen Gegenstand meinen.[31]

25 Jaensch, jM 2022, 96, 97.
26 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kern 33, 49.
27 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kern 33, 34.
28 *J.* Flume, ÖJZ 2022, 137, 138.
29 *J.* Flume, ÖJZ 2022, 137, 139.
30 Artz/Gsell Verbrauchervertragsrecht/Lehmann 19, 22.
31 Schneider/Streitz, CR 2022, 141; Maute/Mackenrodt Recht als Infrastruktur für Innovation/Datta 155, 159.

§ 3 Ziel der DID-RL

Ziel der DID-RL ist die Harmonisierung des digitalen Binnenmarkts. In diesem Kapitel werden das Ziel im engeren Sinn, die Regelungsinhalte, Ausschlüsse sowie mögliche Schwachstellen angesprochen.

A. Ziel im engeren Sinn

Die DID-RL stellt eine „bereichsspezifische Ergänzung der Verbraucherrechterichtlinie für den digitalen Bereich dar".[32] Ziel ist es, vorherige Regelungslücken im EU-Verbraucherrecht bzgl. bestimmter vertragsrechtlicher Aspekte der Bereitstellung digitaler Produkte zu schließen, da es zuvor keine harmonisierten Vorschriften zum Schutz der Verbraucher gab[33], wobei die Richtlinie technologieneutrale und zukunftssichere Regelungen aufstellen soll.[34] Die nicht harmonisierten Regelungen führten bisher zu erhöhten Transaktionskosten für Unternehmen sowie Rechtsunsicherheiten bei den Verbrauchern im grenzüberschreitenden Handel mit digitalen Produkten.[35] Somit ist die RL Ausdruck des EU-Binnenmarktes, indem grenzüberschreitender Handel, insbesondere von kleinen und mittleren Unternehmen (KMU)[36], und Vertrauen der Verbraucher beim Erwerb digitaler Produkte durch vollharmonisierte Regelungen gestärkt werden sollen.[37]

B. Regelungsinhalte

Umfasst sind nach Art. 3 DID-RL Verträge zwischen Unternehmern (natürliche oder juristische Personen) und Verbrauchern über dauerhafte entgeltliche Bereitstellung digitaler Inhalte und Dienstleistungen.[38] Welcher Vertragsart diese Verträge zu unterstellen sind, lässt die Richtlinie offen[39],

32 Kühner/Piltz, CR 2021, 1, Rn. 4.
33 Kühner/Piltz, CR 2021, 1, Rn. 5.
34 Schneider, CR 2022, 1-9, 5.
35 Heckmann/Paschke juris-PK Internetrecht/Paschke Rn. 566.
36 Artz/Gsell Verbrauchervertragsrecht/Lehmann 19, 22.
37 Kühner/Piltz, CR 2021, 1, 2 Rn. 5.
38 juris-PK/Kaesling § 327r Rn. 1; Kühner/Piltz, CR 2021, 1, 2 Rn. 6; Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kern 33, 38.
39 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kern 33, 39.

eine Unterscheidung anhand unterschiedlicher Vertragstypen erfolgt nicht mehr, vielmehr werden Vertragspflichten (insbesondere der Leistungsgegenstand[40]) und Gewährleistungsrechte abstrakt aufgestellt.[41] Im Geltungsbereich der DID-RL werden Regelungen zur genaueren Spezifikation der Leistungspflicht des Unternehmers sowie zu den Rechtsbehelfen des Verbrauchers aufgestellt.[42] Die Vertragsmäßigkeit wird anhand kumulativ zu erfüllender[43] subjektiver und objektiver Anforderungen an das digitale Produkt sowie dessen sachgemäße Integration beschrieben, wodurch der Verbraucher bei Mangelleistung im Gewährleistungsrecht Hilfsmittel an die Hand bekommt.[44] Neben einer Gegenleistung in Geld kann mittels elektronischer Wertgutscheine oder virtueller Währung („digitale Darstellung eines Wertes") bezahlt werden; sogar die Bereitstellung personenbezogener Daten des Verbrauchers oder das Versprechen dies zu tun, was bisher als unentgeltliche Leistung angesehen wurde, unterfällt nach der DID-RL dem umfassten Regelungsinhalt, womit auch sich über die Nutzerdatennutzung finanzierende soziale Netzwerke wie Facebook umfasst sind[45].[46]

C. Ausschlüsse

Der DID-RL unterfallen nicht herkömmliche Dienstleistungen ohne digitale Inhalte, selbst wenn der Unternehmer zur Erstellung oder Überbringung des Ergebnisses der Dienstleistungserbringung digitale Formen oder Mittel einsetzt.[47] Nicht umfasst sind ferner Software unter einer freien und quelloffenen Lizenz, Gesundheits-, Glücksspiel- und Finanzdienstleistungen sowie elektronische Kommunikationsdienste[48] (wobei nummernunabhängige interpersonelle Dienste wie Skype oder WhatsApp doch unter die DID-RL fallen).[49]

40 Artz/Gsell Verbrauchervertragsrecht/Lehmann 19, 21.
41 Heckmann/Paschke juris-PK Internetrecht/Paschke Rn. 565.
42 Kühner/Piltz, CR 2021, 1, 2 Rn. 6.
43 Schneider, CR 2022, 1-9, 5.
44 Kühner/Piltz, CR 2021, 1, 2 Rn. 6.
45 Artz/Gsell Verbrauchervertragsrecht/Lehmann 19, 22.
46 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kern 33, 39; Heckmann/Paschke juris-PK Internetrecht/Paschke Rn. 565.
47 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kern 33, 41.
48 juris-PK/Kaesling § 327r Rn. 14; Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 11.
49 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kern 33, 41.

D. Mögliche Schwachstellen

Problematisch erscheint, dass die DID-RL weiterhin von einem Zwei-Personen-Vertragsverhältnis ausgeht. Dieses ist in der digitalen Welt zwar noch üblich, es weist aber Schwächen auf, sobald ein Dritter als (Zwischen-) Verkäufer ins Spiel kommt, etwa bei den beiden großen Smartphone-Betriebssystem-Anbietern Google (Android) und Apple (iOS), die mit dem auf ihren Geräten bereitgestellten App-Store dem Kunden Apps von Dritten (App-Anbieter /-Entwickler) vermitteln.[50] So kommt es auf der einen Seite vor, dass der Verkäufer selbst die Bereitstellung der digitalen Inhalte schuldet und soweit er diese Vertragsinhalte nicht selbst leisten kann, sich deren Herstellers bedient (bspw. der Rechenzentrums-Betreiber, der für den Nutzer eine Office-Installation von Microsoft anbietet oder die gerade genannten App-Store Betreiber als bloße technische Plattform[51]); sollten diese Inhalte dann nicht vertragsgemäß sein, haftet der Verkäufer unmittelbar aus dem Vertrag.[52] Im Gegenfall ist der Verkäufer lediglich Vermittler zwischen Verbraucher und dem die digitalen Elemente bereitstellenden Hersteller, ohne eigene vertragliche Verpflichtungen. Bei einem zwischen diesen Fällen beheimateten Geschäftsmodell übernimmt der Verkäufer die Garantie zur Bereitstellung der digitalen Elemente durch den Hersteller und das haftungsmäßige Einstehen für Versäumnisse des Erbringers.[53] Die DID-RL sieht nicht vor, dass der Verkäufer die digitalen Elemente selbst bereitstellen müsste, als unmittelbarer Vertragspartner hat er nur Sorge dafür zu tragen, dass der Verbraucher Aktualisierungen erhält und über diese informiert wird.[54] Wie er dies aber ohne Einwirkungsmöglichkeit sicher stellen soll, regelt die DID-RL nicht. Ebenfalls unglücklich scheint die Regelung, dass der Kunde seine Daten aktiv als Gegenleistung zur Verfügung stellen muss, damit die DID-RL eingreift, da gerade die passive Datenerhebung im Hintergrund mittels Cookies und sonstiger Tracking-Elemente für viele Anbieter die weitüberwiegende Datenerhebungsmethode darstellt.[55] Die DID-RL umfasst auch Folgen der Rückabwicklung und das Recht auf

50 Maute/Mackenrodt Recht als Infrastruktur für Innovation/Datta 155, 156.
51 Maute/Mackenrodt Recht als Infrastruktur für Innovation/Datta 155, 156.
52 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Wendehorst 111, 118.
53 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Wendehorst 111, 119.
54 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Wendehorst 111, 120.
55 Maute/Mackenrodt Recht als Infrastruktur für Innovation/Datta 155, 163.

Schadensersatz, was eine zusätzliche Komplexität in Bezug auf das nationale Recht aufbaut.[56]

§ 4 Nationale Umsetzungen in Republik Österreich und Bundesrepublik Deutschland

Rechtsvergleichend wird in Kapitel 4 die nationale Umsetzung der DID-RL in der Republik Österreich (RÖ) und der Bundesrepublik Deutschland (BRD) näher beleuchtet, bevor anschließend auf Gemeinsamkeiten und Unterschiede bei der Umsetzung eingegangen wird.

A. Umsetzung in der Republik Österreich

Die Regelungen der DID-RL sind in RÖ hauptsächlich im VGG umgesetzt worden, das sich auf Verbraucherverträge über den Kauf von Waren mit digitalen Elementen bezieht, wobei eine Haupt- oder Nebenfunktion ohne die digitale Leistung nicht erfüllt werden kann, sowie auf die Bereitstellung selbstständiger digitaler Leistungen in Abschnitt 3.[57] Des Weiteren findet das VGG auch auf den Kauf von Waren Anwendung.[58] Die Aufnahme der Regelungen in das ABGB wurde aufgrund der umfangreichen, Technik lastigen, sehr Verbraucher freundlichen und komplexen Vorschriften kritisch gesehen; aufgrund des Umfangs wurden die neuen Regelungen auch nicht in das Konsumentenschutzgesetz (KSchG) aufgenommen.[59] Mittels des Gewährleistungsrichtlinien-Umsetzungsgesetz (GRUG) wurde das VGG eingeführt und zusätzliche Anpassungen im ABGB und KSchG vorgenommen.[60] Die in Erwägungsgrund (Erwgr.) 13 DID-RL enthaltene Möglichkeit, die neuen Regelungen auch auf B2B-Geschäfte zu übertragen, wurde nicht ausgeschöpft.[61] Es wird kein neuer Vertragstypus eingeführt, sondern für digitale Leistungen gegen Zahlungen sowie datenfinanzierte Geschäftsmodelle ein allgemeines Verbrauchergewährleistungsrecht einge-

56 Artz/Gsell Verbrauchervertragsrecht/Lehmann 19, 33.
57 Bischinger/Weber-Woisetschläger, JAP 2021/2022, 104.
58 Stabentheiner, ÖJZ 2021, 965, 968.
59 Flume/Kronthaler/Laimer VGG/Schwartze Rn. 2.
60 Stabentheiner, ÖJZ 2021, 965, 966.
61 Flume/Kronthaler/Laimer VGG/Schwartze Rn. 2.

führt.[62] Bei verbundenen digitalen Leistungen hat der Verkäufer der Ware für Gewährleistungspflichten einzustehen, bei unverbundenen der Bereitsteller der digitalen Leistung.[63] Digitale Inhalte sind dabei Daten, die in digitaler Form erzeugt bzw. zur Verfügung gestellt werden (Fotos, E-Books, Musik, Videos), ebenso ist auch die Bereitstellung digitaler Dienstleistungen umfasst, wobei durch diese dem Verbraucher die Erstellung, Verarbeitung und Speicherung von Daten oder Zugang zu solchen offeriert wird; umfasst sind auch Interaktionsplattformen mit digital hochgeladenen Daten bspw. in sozialen Netzwerken, Smartphone-Anwendungen, Computerprogramme, Cloudspeicher-Servicedienste, Streamingdienste.[64] Digitale Inhalte und Dienstleistungen werden zur „digitalen Leistung" zusammen gefasst, die gegen Zahlung eines (sehr weit zu verstehenden) Entgelts oder Hingabe personenbezogener Daten iSd DS-GVO erbracht werden.[65] Das VGG gilt für die Bereitstellung digitaler Leistungen ab 1.1.2002, ist daher auch für vor dem 1.1.2022 abgeschlossene Verträge anwendbar, solange die Leistung über diesen Stichtag hinaus angeboten wird. Das hier thematisierte Recht des Unternehmers auf Änderung der digitalen Leistung gilt allerdings nur, wenn auch der Vertrag ab dem 1.1.2022 geschlossen wurde, § 29 Abs. 3 S. 2 VGG. Bei fortlaufender Bereitstellung einer digitalen Leistung sieht § 27 VGG ein Leistungsänderungsrecht des erbringenden Unternehmers vor, das dieser einseitig ausschöpfen kann.[66] Es gibt Parallelen zum Gewährleistungsrecht beim Warenkauf mit Weiterentwicklungen und Ausdifferenzierungen, jedoch sind dem bisher recht einheitlichen Gewährleistungsrecht des ABGB (§§ 922 ff ABGB) nunmehr komplexe und technikbezogene Vorschriften des VGG zur Seite gestellt worden, was künftig zu zwei unterschiedlichen Gewährleistungskomplexen führen wird.[67] Insbesondere ist in § 27 Abs. 2 S. 1 VGG ein Sonderkündigungsrecht für digitale Inhalte bei wesentlichen Änderungen vorgesehen, was sich nach der Ausgestaltung als Dauerschuldverhältnis darstellt und für solche eigentlich im ABGB

62 Flume/Kronthaler/Laimer VGG/Kronthaler/J.W. Flume/Ziegler Rn. 23; *J.* Flume, ÖJZ 2022, 137, 140.

63 Bischinger/Weber-Woisetschläger, JAP 2021/2022, 104, 105.

64 Bischinger/Weber-Woisetschläger, JAP 2021/2022, 104, 105.

65 Bischinger/Weber-Woisetschläger, JAP 2021/2022, 104, 105.

66 Bischinger/Weber-Woisetschläger, JAP 2021/2022, 181, 185; Siehe zu den Richtlinienvorgaben Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141; zu § 27 VGG: Stabentheiner, ÖJZ 2021, 965, 975; Stabentheiner, VbR 2022 2021, 188, 193.

67 *J.* Flume, ÖJZ 2022, 137, 140; Stabentheiner, ÖJZ 2021, 965, 967.

kein Sonderkündigungsrecht vorgesehen ist.[68] Im Zusammenspiel mit den übrigen Regelungen des VGG wird deutlich, dass die in § 27 VGG geregelte Änderungsbefugnis ausschließlich Änderungen umfassen kann, die nicht bereits in § 7 VGG genannt sind, also solche, die zur Aufrechterhaltung der Vertragsmäßigkeit der vertraglichen Leistung dienen.[69] In Bezug auf § 6 Abs. 2 Z. 3 KSchG, der besagt, dass nur dann eine einseitige Änderung durch den Unternehmer erfolgen kann, wenn sie geringfügig und sachlich gerechtfertigt ist, verdrängt § 27 VGG diese Regelung als lex specialis, so dass hier § 6 Abs. 2 Z. 3 KSchG keine Anwendung findet, obwohl § 27 VGG zusätzliche Voraussetzungen nennt.[70]

B. Umsetzung in der Bundesrepublik Deutschland

Der deutsche Gesetzgeber hat sich zu einer Einbettung der Regelungen der DID-RL in das BGB entschieden, in der Tradition der bisher ebenfalls genutzten Vorgehensweise anhand eines systematischen Konzepts[71]. Hier wurde in das allgemeine Schuldrecht ein neuer Titel 2a eingefügt, der in §§ 327 – 327u BGB Verträge zwischen einem Unternehmer (§ 14 Abs. 1 BGB) und einem Verbraucher (§ 13 BGB) über digitale Produkte unabhängig davon regelt, ob ein Kauf-, Miet- (der neue § 548a BGB regelt die analoge Anwendung des Sachmietrechts auf Mietverträge über digitale Produkte[72]) oder Dienstvertrag über ein digitales Produkt vorliegt.[73] Dieser Regelungskomplex trat zum 1.1.2022 in Kraft. B2B- und C2C-Verträge haben keine Regelung erfahren.[74] Keine Anwendung finden die Regelungen auf diverse Dienstleistungsverträge nach Maßgabe des § 327 Abs. 6 BGB.[75] Der Terminus „digitales Produkt" umfasst sowohl digitale Inhalte als auch digitale Dienstleistungen; Begriffe, welche, um Entwicklungsoffenheit sicherzustellen, weit zu verstehen sind.[76] Dabei sind digitale Inhalte Daten, die in

68 *J.* Flume, ÖJZ 2022, 137, 142.
69 Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 32.
70 Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 33.
71 Müller-Graff, GPR 2009, 106, 119.
72 Redecker, ITRB 2022, 187.
73 Kühner/Piltz, CR 2021, 1, 2.
74 Flume/Kronthaler/Laimer VGG/Schwartze Rn. 3.
75 *A.* Staudinger/Artz, Neues Kaufrecht und Verträge über digitale Produkte. Einführung in das neue Recht1 (2022) 134.
76 Heckmann/Paschke juris-PK Internetrecht/Paschke Rn. 571, 574.

digitaler Form er- und bereitgestellt werden, § 327 Abs. 2 S. 1 BGB, und digitale Dienstleistungen sind solche, die entweder die Erstellung, Verarbeitung oder Speicherung von Daten in digitaler Form oder den Zugang zu solchen Daten ermöglichen bzw. die gemeinsame Nutzung der […] hochgeladenen oder erstellten Daten oder sonstige Interaktion mit diesen Daten ermöglichen, § 327 Abs. 2 S. 2 BGB.[77] Besondere Relevanz erhalten diese Vorschriften, da sie grds. einen zwingenden Charakter aufweisen, § 327s Abs. 1, 2 BGB.[78] Die Bereitstellung der vertraglichen Leistung unterscheidet zwischen einmaliger, § 327b Abs. 3 BGB, mehrfacher, § 327b Abs. 5 BGB sowie fortlaufender über einen Zeitraum hinweg, § 327b Abs. 4 BGB.[79] Die Änderungsbefugnis des Unternehmers ist in der Bundesrepublik Deutschland in § 327r BGB umgesetzt worden, in dem Voraussetzungen und Rechtsfolgen geregelt sind.[80] In Abs. 1 sind die für nachteilige und positive Änderungen erforderlichen Voraussetzungen geregelt, in Abs. 2 zusätzliche bei nachteiligen Abweichungen, in Abs. 3 ist das Kündigungsrecht des Verbrauchers bei nachteiligen Änderungen geregelt bzw. in Abs. 4 dessen Ausschluss, sofern der Verbraucher zwischen neuer und alter Produktversion wählen kann.[81] Dabei wird nicht selbst ein Änderungsrecht vorgesehen, sondern stattdessen die vertragliche Begründung und Ausgestaltung von solchen eingehegt.[82] Es sind ausschließlich Änderungen durch den Unternehmer umfasst, auch solche von Dritten wie dem Hersteller, die er sich über § 278 BGB zurechnen lassen muss.[83] Die Regelung, die dem Unternehmer über den zum Erhalt der Vertragsmäßigkeit hinausgehende Produktänderungen während der dauerhaften Bereitstellung digitaler Produkte ermöglicht,[84]

77 Schneider, CR 2022, 1-9, 4; Heckmann/Paschke juris-PK Internetrecht/Paschke Rn. 580, 581.

78 Lunk/Meurer, BB 2022, 387, 392; Heydn, CR 2021, 709, 714 Rn. 35.

79 Schneider, CR 2022, 1-9, 4.

80 MüKo-BGB/Metzger § 327r Rn. 1. Vgl. als Beispiel https://policies.google.com/terms?hl=en („develop, improve, and update Google services"): Anpassungen an neue Technologien, an sich ändernde Nutzerzahlen, um Änderungen in den Lizenzierungsmodellen ggü. Dritten zu implementieren, um Missbrauch oder Beschädigungen abzuwenden und schließlich um gesetzliche, regulatorische, sicherheitsrelevante etc. Änderungen vorzunehmen. Vgl. zur Praxis gängiger Cloud-Anbieter, ihre Nutzungsbedingungen zu ändern, European Commission, Comparative Study on cloud computing contracts: Final Report (2015), 54 f., https://op.europa.eu/s/o6bI. (jeweils zuletzt abgerufen am 13.12.2023).

81 MüKo-BGB/Metzger § 327r Rn. 1.

82 juris-PK/Kaesling § 327r Rn. 1.

83 MüKo-BGB/Metzger § 327r Rn. 4.

84 MüKo-BGB/Metzger § 327r Rn. 1.

ist im triadischen Zusammenspiel mit § 327f BGB, der Änderungen bei Erfüllung der Aktualisierungspflicht regelt, sowie mit § 327h BGB, der Abweichungen zur Absenkung der Anforderungen bei Vertragsschluss ermöglicht, zu sehen.[85] Zur Anwendung gelangt man, sofern es sich um einen Verbrauchervertrag (Vertrag zwischen Unternehmer, § 14 BGB, und Verbraucher, § 13 BGB) handelt, der Verbraucher einen Preis oder Daten als Gegenleistung zu erbringen hat und es sich bei der Leistung des Unternehmers um ein digitales Produkt handelt.[86] Bisher waren solche Änderungsbefugnisse oftmals Teil von Vereinbarungen in AGB und nur unter bestimmten Voraussetzungen möglich, § 308 Nr. 4 BGB.[87] Die Regelungen des Titels 2a sollen nicht bei fehlender vertraglicher Grundlage, sofern der Verbraucher im Gegenzug Werbung eingeblendet erhält, anzuwenden sein.[88] Bei der Umsetzung der DID-RL fällt auf, dass in dieser Software nur einer von unterschiedlichen weiteren Gegenständen ist, in der deutschen Umsetzung jedoch wird nur Software genannt.[89] Durch die neue Rechtsfigur für die Leistung des Unternehmers, die Bereitstellung von Daten, wird dafür ein neuer Vertragstyp in den §§ 327 ff. BGB geschaffen, wobei die Vertragsgegenstände digitale Inhalte und digitale Dienstleistungen über die Art ihrer Leistung bzgl. Daten eingruppiert werden.[90]

In § 327a Abs. 3 S. 2 BGB gibt es eine „Im-Zweifel-Regelung", nach der §§ 327 ff BGB nicht auf Kaufverträge über Waren mit digitalen Elementen anzuwenden sind, weil nach § 475b Abs. 1 S. 2 BGB „im Zweifel anzunehmen ist, dass die Verpflichtung des Verkäufers die Bereitstellung der digitalen Inhalte oder digitalen Dienstleistungen umfasst."[91] Sofern der Verbraucher einen Preis für das digitale Produkt zu zahlen hat, so finden die Vorschriften der §§ 327 ff. BGB als auch diejenigen der §§ 474 ff. BGB Anwendung; während bei einer Gegenleistung in Form von Daten nach § 327 Abs. 3 BGB die §§ 327 ff. BGB Anwendung finden, aber die Regelungen im besonderen Schuldrecht nach § 433 Abs. 2 BGB die Leistung eines vereinbarten Kaufpreises erfordert, Daten hier also explizit ausgeschlossen sind.[92] Allerdings sind die Vorschriften der §§ 327 ff. BGB nicht anzuwenden, wenn

85 Schneider, CR 2022, 1-9, 8 Rn. 54.
86 Buchmann/Panfili, KuR 2022, 73, 74.
87 Lunk/Meurer, BB 2022, 387, 394.
88 Heckmann/Paschke juris-PK Internetrecht/Paschke Rn. 572.
89 Schneider, CR 2022, 1-9, 3.
90 Schneider, CR 2022, 1-9, 4.
91 Schneider/Streitz, CR 2022, 141, 142.
92 Buchmann/Panfili, KuR 2022, 73, 74.

die vom Verbraucher bereitgestellten Daten dem Unternehmer lediglich dazu dienen, überhaupt seine Leistungspflicht erfüllen zu können, bspw. Adressdaten zur Abwicklung einer Bestellung.[93]

C. Gemeinsamkeiten

I. Keine Ausdehnung

Von der in Erwgr. 16 DID-RL enthaltenen Möglichkeit, den Schutz auch auf NGO's, KMU oder neu gegründete Unternehmen auszuweiten, wurde kein Gebrauch gemacht.[94] Umfasst sind in beiden Ländern lediglich Verträge zwischen Unternehmer und Verbraucher. Damit wurde der Regelungsinhalt auf die kleinstmögliche Gruppe beschränkt und andere dem Verbraucher ähnlich schutzwürdige Gruppen nicht eingeschlossen.

II. Vertragsschluss

An den grundlegenden Erfordernissen des Vertragsschlusses ändert sich in beiden Umsetzungen nichts, so bedarf es sowohl im Internet als auch in der analogen Welt übereinstimmender Willenserklärungen der Parteien, die seit der ricardo.de-Entscheidung des BGH[95] auch elektronisch übermittelt werden können, sofern im Verbrauchergeschäft der Bestellbutton mit „zahlungspflichtig bestellen" beschriftet ist[96].[97] Ob und wann ein Vertrag zu Stande kommt, bestimmt sich nach den §§ 145 ff. BGB, §§ 861, 862, 864, 869 ABGB insbesondere nach dem objektiven Empfängerhorizont §§ 133, 157 BGB, §§ 863, 914 ff ABGB, es muss ein Rechtsbindungswille vorliegen und die Gesamtumstände hinzugezogen werden[98]. Praxisnah ist davon auszugehen, dass der Unternehmer seine Leistung mit Einnahmeerzielungsabsicht

93 Buchmann/Panfili, KuR 2022, 73, 75.
94 Heckmann/Paschke juris-PK Internetrecht/Paschke Rn. 577.
95 BGH VIII ZR 13/01, ricardo.de: Zustandekommen von Verträgen im Internet https://openjur.de/u/62092.html.
96 Heckmann/Paschke juris-PK Internetrecht/Paschke Rn. 4.
97 Härting Internetrecht/Härting Rn. 635; ABGB-ON/Wiebe § 861 Rn. 17, 18, 20.
98 Buchmann/Panfili, KuR 2022, 73, 74; Härting, Härting-Vertragsrecht, Härting Rn. 689; Heckmann/Paschke juris-PK Internetrecht/Paschke Rn. 10; ABGB-ON/Wiebe § 861 Rn. 18.

erbringt, bspw. indem mittels Tracking-Verfahren personalisierte Werbung gezielt geschaltet werden kann.[99]

III. Daten als alleinige Gegenleistung

In beiden Ländern sind auch Verträge umfasst, die keine klassische Geldzahlung als Gegenleistung beinhalten, sondern wo der Verbraucher den Unternehmer mit Bereitstellung von Daten bezahlt.[100] Eine analoge Anwendung ist bei ähnlichen Gegenleistungen möglich, bspw. Rechenkapazität oder Speicherplatz. Bereits eine Einwilligung zur Verpflichtung, personenbezogene Daten bereitzustellen, eröffnet den Anwendungsbereich der Regelung[101], sofern jedoch der Unternehmer die durch den Nutzer zur Verfügung gestellten Daten nur zur Erfüllung seiner Leistungspflicht oder rechtlicher Anforderungen verarbeitet, ist der Anwendungsbereich der §§ 327 ff BGB, des VGG nicht eröffnet, §§ 327 Abs. 3, 312 Abs 1a S. 2 BGB, § 1 Abs. 1 Nr. 2 lit b) VGG.[102] Die bloße Bereitstellung anderer, nicht-personenbezogener Daten ist von der Regelung nicht umfasst. „Bereitstellung" umfasst sämtliche Verarbeitungen personenbezogener Daten durch den Anbieter in Verbindung mit dem Vertragsgegenstand oder auch zu weitergehenden Zwecken (wie Werbung)[103], wobei die in der DS-GVO niedergelegten Rechte Anwendung finden.[104] Eine aktive Übermittlung der Daten durch den Verbraucher ist nicht notwendig.

D. Unterschiede

I. Unterschiedliche Vorgehensweisen bei der Neuregelung

In der BRD wurden die Änderungen in das bestehende BGB eingefügt, wobei entweder nur §§ 327 ff oder aber zusätzlich auch §§ 474 ff BGB Anwendung finden; in RÖ wurde das neue VGG geschaffen, das auch für Warenkäufe und Werkverträge gilt, mit Anpassungen im KSchG und ABGB.

99 Kühner/Piltz, CR 2021, 1, 2 Rn. 11.
100 Jaensch, jM 2022, 96, 97; Kühner/Piltz, CR 2021, 1, 3 Rn. 11.
101 Kühner/Piltz, CR 2021, 1, 3 Rn. 11.
102 Lunk/Meurer, BB 2022, 387, 392.
103 Lunk/Meurer, BB 2022, 387, 392.
104 Heckmann/Paschke juris-PK Internetrecht/Paschke Rn. 593.

II. Unterschiedliche Begrifflichkeiten

Im VGG findet der einschlägige 3. Abschnitt auf „digitale Leistungen" Anwendung, die in § 2 Z. 1 VGG als „digitale Inhalte" oder „digitale Dienstleistungen" aufgetrennt werden. In den Regelungen der §§ 327 BGB findet sich „digitale Leistung" als Begriff nicht, dort wird als Oberbegriff „digitales Produkt" verwendet, das in „digitaler Inhalt" und „digitale Dienstleistung" unterschieden wird. Während in § 327e BGB der Produktmangel sowohl subjektiv wie objektiv thematisiert wird, sind in § 5 VGG die vertraglich vereinbarten Eigenschaften (subjektiv) und in § 6 VGG die objektiv erforderlichen Eigenschaften genannt.

III. Aufbau

Der Aufbau von § 327r BGB und § 27 VGG unterscheiden sich. So ist die Regelung bzgl. der den Verbraucher benachteiligenden Änderung in § 27 als Abs. 1 Ziff. 4 gefasst, während im § 327r diese Regelung in Abs. 2 zu finden ist.

Die Regelung der weiteren Zugriffsmöglichkeit auf das unveränderte digitale Produkt ist in § 327r Abs. 4 BGB, § 27 Abs. 4 VGG geregelt, hat aber einen leicht abweichenden Inhalt, indem das Produkt nicht „unverändert" sein muss, sondern „weiterhin dem Vertrag entspricht".

§ 5 Änderungsbefugnis in Abgrenzung zur Änderungspflicht

Im neuen Regelungspaket ist die Unterscheidung zwischen Änderungspflicht und Änderungsbefugnis entscheidend. Der Unternehmer muss einerseits Änderungen zur Erhaltung der Mangelfreiheit des Produkts durchführen (Änderungspflicht), kann andererseits aber auch Anpassungen am Produkt vornehmen, um andere Zwecke zu erreichen (Änderungsbefugnis).[105]

A. Grundsätzliche Annahmen für beide Änderungsarten

Änderungsbefugnis und Änderungspflicht verbinden verschiedene Kennzeichen. So werden sie vom Unternehmer durchgeführt und sie müssen,

105 Möllnitz, MMR 2021, 116, 116.

um wirksam zu werden, auf das Gerät des Nutzers gelangen. Dabei unterfällt der Verbraucher keinem Zwang zur Installation, der Unternehmer hat keine Befugnis zum Zugriff auf das Gerät des Verbrauchers, während jeweils das unternehmerische Interesse Berücksichtigung findet.

I. Kein Installationszwang

Der Verbraucher ist nicht verpflichtet, eine Änderung zu installieren, der Unternehmer muss den Verbraucher nur über das Vorliegen einer Änderung informieren. Es besteht für den Unternehmer keine Verpflichtung, Sicherheitsaktualisierungen zwangsweise am Verbraucher vorbei zu installieren, wobei er dann auch nicht (mehr) für Produktmängel aufgrund des Fehlens der Aktualisierung haftet[106], vielmehr soll der Verbraucher selbst entscheiden, ob und wann er eine Aktualisierung installiert.[107] Hier treffen zwei Interessensphären aufeinander: Der Verbraucher kann durchaus berechtigte Gründe haben, auf eine Aktualisierung zu verzichten, weil er bspw. Auswirkungen auf seine Infrastruktur fürchtet oder bekannt ist, dass das Update einen Fehler auf dem spezifischen Gerät des Verbrauchers verursacht, was zum Totalschaden führt; während der Unternehmer hingegen allgemein bekannte Sicherheitslücken schließen oder zukünftige technische Entwicklungen vornehmen möchte, bspw. indem die Hausautomation mit einem neuen Protokoll kommuniziert oder eine neue Skriptsprache, die weniger Kapazität braucht, eingeführt werden soll.[108] Bei Sicherheitsaktualisierungen erscheint es plausibel, im Rahmen der vertraglichen Schutzpflichten gem. § 242 BGB eine entsprechende Vornahmepflicht des Unternehmers anzunehmen, um den Verbraucher bei der Installation zu unterstützen und illegale Aktivitäten wie Bot-Netze zu vermeiden, da hier eine Pflicht zum Selbstschutz besteht (bspw. die Verwendung von Anti-Viren-Software), die auch in Bezug auf Drittnutzer, welche durch den fehlenden

106 Lunk/Meurer, BB 2022, 387, 394.

107 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Wendehorst 111, 124; zur Zulässigkeit von Zwangsupdates hat das LG Frankfurt entschieden, dass die pauschale Einwilligung in die Installation sämtlicher Updates einen Verstoß gegen das Klausel-Verbot des § 308 Nr. 4 BGB darstellt, wenn der Änderungsvorbehalt unabhängig davon vereinbart wurde, ob er für den Verbraucher zumutbar ist, LG Frankfurt 2–24 O 246/12 CR 2013, 744 Rn 59.

108 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Wendehorst 111, 125.

Schutz gefährdet sind, gelten kann.[109] In einem solchen Fall greifen die Verkehrssicherungspflichten, die es dem Gefahrquellenverursacher auferlegen, den Schadenseintritt bei einem Dritten zu verhindern, aufgrund einer vom Nutzer geschaffenen und nicht beherrschten Gefahrenquelle.[110] Hier erscheint es interessengerecht, die in § 327f Abs. 2 Nr. 2 BGB, § 7 Abs. 3 VGG getroffene Regelung entsprechend anzuwenden, nach der der Unternehmer nicht für einen Produktmangel haftet, der allein auf das Fehlen einer Aktualisierung zurückzuführen ist; sofern der Unternehmer über die Verfügbarkeit der Aktualisierung, die Folgen einer Nichtinstallation informiert und die Tatsache, dass der Verbraucher die Aktualisierung nicht installiert hat, nicht auf eine dem Verbraucher bereitgestellte, mangelhafte Installationsanleitung zurückzuführen ist.

II. Berücksichtigung des Unternehmerischen Interesses

Durch die Änderungsbefugnis des Unternehmers bei der dauerhaften Bereitstellung digitaler Produkte werden Veränderungen ermöglicht, die über das zur Aufrechterhaltung der Vertragsmäßigkeit erforderliche Maß hinausgehen und notwendig sind, um Produkt und Dienstleistung auf dem Stand der Technik zu halten, was auch die Schnelllebigkeit digitaler Produkte und damit das unternehmerische Interesse berücksichtigt, nicht mehrere unterschiedliche Versionen pflegen zu müssen, ohne jedoch verpflichtende Änderungen zu sein.[111]

B. Zeitraum und Nutzungsdauer

Änderungspflicht und Änderungsbefugnis haben je nach Nutzungs-Dauer und Nutzungs-Zeitraum unterschiedliche Anforderungen zu erfüllen.

109 Fida, Updates, 168; Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Wendehorst 111, 126.
110 Fida, Updates, 171.
111 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 142, 143, 145.

III. Aktualisierungspflicht für einen gewissen Zeitraum

Für Waren mit digitalen Elementen und digitale Leistungen muss der Unternehmer eine Aktualisierungspflicht über einen gewissen Zeitraum einhalten (bspw. Sicherheitsupdates), um so die Ware / digitale Leistung weiterhin sicher und im vertragsgemäßen Zustand zu halten.[112] Die ausgelieferte Version muss der zum Zeitpunkt des Vertragsabschlusses aktuellen Version entsprechen, allerdings sind nachträglich auch Änderungen zur Erhaltung der Vertragskonformität durch zu führen.[113] Im Übrigen kann sich der Unternehmer auch vertraglich zur Bereitstellung von Aktualisierungen verpflichten[114], insbesondere auch solchen Aktualisierungen zur Beibehaltung der IT-Sicherheit, die aber über die Verjährungsfrist für Mängel hinausgehen können.[115]

IV. Unterschiede je nach Nutzungsdauer

Bei Einmalleistungen hat der Unternehmer für eine unter Berücksichtigung der Umstände und Art des Vertrags vernünftigerweise zu erwartende Zeitdauer im Rahmen seiner Organisationspflicht[116] Aktualisierungen bereitzustellen.[117] Bei fortlaufender Leistung über einen befristeten oder unbefristeten Zeitraum ist für den gesamten Bereitstellungszeitraum, § 327f Abs. 1 S. 3 Nr. 1 BGB, § 7 Abs. 2 Nr. 2 VGG (übliche Nutzungsdauer) eine Aktualisierung geboten, mindestens jedoch zwei Jahre nach Übergabe[118], da der Unternehmer über diesen Zeitraum auch die Mangelfreiheit bzw. die Mangelbeseitigung verspricht.[119] Ebenso ist auch bei einem einmaligen Leistungsaustausch eine dauerhafte Verpflichtung zum Erhalt der Mangelfreiheit der Leistung gegeben[120], wobei hierbei Art und Zweck des digitalen Produkts sowie Umstände und Art des Vertrags maßgeblich sind, § 327f

112 Möllnitz, MMR 2021, 116, 116; Stabentheiner, ÖJZ 2022, 99, 102; Lunk/Meurer, BB 2022, 387, 393.
113 Stabentheiner, ÖJZ 2022, 99, 102.
114 Lunk/Meurer, BB 2022, 387, 393.
115 Schneider, CR 2022, 1-9, 3.
116 Rieländer, GPR 2021, 257, 267.
117 Jaensch, jM 2022, 96, 98; Stabentheiner, ÖJZ 2022, 99, 102.
118 Stabentheiner, ÖJZ 2022, 99, 102; Jaensch, jM 2022, 96, 98; Lunk/Meurer, BB 2022, 387, 394.
119 *J.* Flume, ÖJZ 2022, 137, 141.
120 Buchmann/Panfili, KuR 2022, 159, 161.

Abs. 1 S. 3 Nr. 2 BGB, § 7 Abs 2 Nr. 1 VGG.[121] Bei Sicherheitsaktualisierungen hat der Verbraucher oftmals eine gesteigerte Erwartung, was die in der DID-RL genannte „vernünftige Verbrauchererwartung" noch umfasst.[122] Sofern der Verbraucher besonders davon in Kenntnis gesetzt wird, sowie ausdrücklich und gesondert zustimmt, können Verbraucher und Unternehmer durch Abweichungsvereinbarung von dieser Änderungspflicht abweichen (In § 1 Abs. 3 VGG ist eine solche Vereinbarung auch zwischen Unternehmern möglich, dann jedoch auch konkludent oder mittels AGB).[123] Eine Abbedingung ist nur im besonderen Falle möglich, § 327h BGB, § 6 Abs. 1 S. 2 VGG.[124]

C. Mangelbehebung

Die Behebung des Mangels obliegt dem Unternehmer, dieser hat bei der Wahl des Mittels der Nacherfüllung die Freiheit, ob er eine Aktualisierung anbietet, oder dem Verbraucher ein neues digitales Produkt bereitstellt.[125] Sofern es sich beim Unternehmer nicht um den Hersteller handelt, muss dieser mit seinem Lieferanten entsprechende Verträge abschließen, um die Aktualisierungspflicht überhaupt erfüllen zu können.[126] Die Aktualisierungspflicht lässt sich daher auch als Teil des Mangelbegriffs bzw. der Gewährleistung auffassen, nicht als eigenständige Verpflichtung[127], da sie die allgemeine Gewährleistung nach § 18 VGG, § 327e BGB ergänzt, um einen aufgrund eines fehlerhaften oder unterlassenen Updates auftretenden Mangel zu beheben, wodurch die Gewährleistung nicht mehr statisch im Zeitpunkt der Bereitstellung zu betrachten ist, sondern als ein „fortlaufender dynamischer Prozess".[128] Neben die Aktualisierungspflicht tritt die Informationspflicht über die Aktualisierung sowie über die Folgen bei Nichtinstallation, § 327f Abs. 1 S. 1 BGB, § 7 Abs. 3 Nr. 1 VGG.[129] Der Verbraucher hat die Wahl, die Aktualisierungen zu installieren; sollte er es

121 Lunk/Meurer, BB 2022, 387, 394.
122 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Maier 51, 58.
123 Stabentheiner, ÖJZ 2022, 99, 102.
124 Lunk/Meurer, BB 2022, 387, 393.
125 Buchmann/Panfili, KuR 2022, 159, 161.
126 Lunk/Meurer, BB 2022, 387, 393.
127 Buchmann/Panfili, KuR 2022, 159, 161.
128 *J.* Flume, ÖJZ 2022, 137, 141.
129 Lunk/Meurer, BB 2022, 387, 393.

jedoch unterlassen, führt dies zum Totalverlust seiner Mängelrechte bzw. zur Kürzung etwaiger Ersatzansprüche wegen Mitverschuldens, § 254 BGB, § 1304 ABGB.[130] Sofern der Unternehmer die Bereitstellung oder Information einer Aktualisierung unterlässt, besteht ein Produktmangel, wobei dem Verbraucher die Gewährleistungsrechte des § 327i BGB, § 20 VGG zustehen.[131]

D. Mögliche Folgeprobleme

Durch die Änderungspflicht auch lange nach Bereitstellung des Produkts können sich für den Unternehmer u.U. problematische Situationen ergeben, wenn die Aktualisierung wiederum einen Fehler enthält. Nach dem Telos der Regelung müsste die fehlerhafte Aktualisierung als Lieferung einer mangelhaften Sache aufzufassen sein, mit der wiederum das allgemeine Mängelfolgeschema eingreifen würde.

Schließlich lassen sich aus der Änderungsbefugnis und der Änderungspflicht auch Folgekonstellationen denken: So aktualisiert der Unternehmer unter den unten genannten Gesichtspunkten im Rahmen seiner Änderungsbefugnis das Produkt, baut darin einen Fehler ein und muss dann im Rahmen der Aktualisierungspflicht diesen Fehler wieder korrigieren. So kann die rechtlich eigentlich dem Unternehmer entgegenkommende Möglichkeit, sein Produkt auf neue technische Änderungen anzupassen, negative Folgen zeitigen.

§ 6 Voraussetzungen der Änderungsbefugnis

Im Folgenden wird auf das Kernthema dieser Arbeit rekurriert, die Änderungsbefugnis des Unternehmers. Zunächst werden in diesem Kapitel die allgemeinen Voraussetzungen der vertraglich gestatteten Änderung aus triftigem Grund dargestellt, bevor dann im nächsten Kapitel auf die Kernproblematik vorgestoßen wird, ab wann ein triftiger Grund vorliegt bzw. welcher Maßstab für die Veränderung angewandt wird.

130 Rieländer, GPR 2021, 257, 267.
131 Lunk/Meurer, BB 2022, 387, 394.

A. Begriff der Änderung

Die einseitige Änderung muss im Vertrag bereits vorgesehen und vereinbart sein, wie dies bereits bisher häufig in AGB der Anbieter der Fall ist[132], und kann nicht nachträglich vereinbart werden.[133] Eine Definition für „Änderung" bleiben § 327r BGB, § 27 VGG als auch Art. 19 DID-RL schuldig. In Erwgr. 74 zur DID-RL werden Aktualisierungen und Verbesserungen genannt, wobei Verbesserungen mit Upgrades gleichgesetzt werden und Aktualisierungen als Updates bezeichnet werden. Die Unterscheidung zwischen Update und Upgrade macht der RL-Geber jedoch nicht deutlich.[134] Änderungen und Aktualisierungen sind voneinander abzugrenzen. Letztere erhalten die Vertragsmäßigkeit, indem die Funktionalität, Kompatibilität und Interoperabilität des digitalen Produkts sichergestellt werden.[135] Änderungen sind weniger klar und jenseits der festgelegten Anforderungen an die Vertragsmäßigkeit über alle Produktteile zu sehen.[136] Eine Änderung meint dabei sowohl Aktualisierungen, Verbesserungen als auch Verschlechterungen, also jegliche Abweichung vom bisherigen Leistungsgegenstand, soweit nicht § 327e BGB, §§ 5, 6 VGG umfasst sind.[137] Entscheidend ist, ob die Änderung über das erforderliche Maß hinausgeht, ob also das geänderte digitale Produkt ein Aliud zum ursprünglich bereitgestellten Produkt darstellt, was anhand der Verkehrsanschauung beurteilt wird, bspw. ob es durch die Änderungen qualitativ oder quantitativ erhebliche zusätzliche Funktionen aufweist, während untergeordnete neue Funktionen für die Wertung als ein neues digitales Produkt nicht ausreichen.[138]

B. Hauptvoraussetzungen

Damit der Unternehmer die ihm aus dem Vertragsverhältnis begründete Änderungsbefugnis ausüben kann, muss er mehrere Hauptvoraussetzungen erfüllen. Es muss ein triftiger Grund für die Vornahme der Änderung vorliegen, sodann muss das zu ändernde Produkt dauerhaft bereitgestellt

132 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 145.
133 MüKo-BGB/Metzger § 327r Rn. 6.
134 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 6.
135 juris-PK/Kaesling § 327r Rn. 4.
136 juris-PK/Kaesling § 327r Rn. 4.
137 Möllnitz, MMR 2021, 116, 116.
138 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 6.

werden, schließlich dürfen dem Kunden daraus keine Kosten entstehen und er nur geringfügig beeinträchtigt werden.

I. Triftiger Grund

Eine Änderung muss vertraglich aufgrund eines triftigen Grundes vorgesehen sein, der hinreichend konkret spezifiziert sein und dann auch tatsächlich vorliegen muss, ein bloß abstraktes Verweisen auf dessen Notwendigkeit ist nicht ausreichend[139]; die Notwendigkeit für den triftigen Grund ist schon in der Klausel-RL enthalten gewesen, die AGB-Klauseln für ungültig erklärt hat, nach denen der Unternehmer ohne triftigen Grund Änderungen vornehmen kann.[140] Da ein solcher Grund in der Vertragsurkunde „enthalten" sein soll (nicht bloß vorgesehen oder erforderlich), muss er konkret benannt sein und dem Verbraucher dadurch die Chance gegeben werden, das Ob des Eintretens und den Umfang der Änderung bereits bei Vertragsschluss einzuschätzen, um so seine Kaufentscheidung bewusst treffen zu können.[141] Durch Abwägung des Unternehmerinteresses an der Änderung mit dem Verbraucherinteresse an deren Unterbleiben ist zu bestimmen, was ein triftiger Grund ist.[142] Unvorhersehbare Änderungen sind schwierig zu erfassen.[143] Änderung soll dasjenige sein, was über den bloßen Erhalt der Vertragsmäßigkeit hinausgeht.[144] Eine Modifikation des Leistungsumfangs ist genauso umfasst, wie bspw. die Anpassung an neue technische Gegebenheiten, Nutzerzahlen, wegen Änderungen der Technik des Betriebs oder solchen in der Sphäre des Unternehmers[145]. Der Umfang der zukünftigen Änderung ist hingegen noch nicht im Vertrag zu konkretisieren, was gerade aufgrund der schnellen Entwicklungen im digitalen Bereich wohl auch schwerlich erfüllbar wäre; zumal der Verbraucher aufgrund der Informationspflicht über den konkreten Umfang Kenntnis

139 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 15; Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 11.
140 juris-PK/Kaesling § 327r Rn. 5; MüKo-BGB/Metzger § 327r Rn. 7.
141 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 15; Müller-Graff, GPR 2009, 106 Rn. 15; Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 11; juris-PK/Kaesling § 327r Rn. 5.
142 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 15.
143 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 147.
144 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 9.
145 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 146.

erlangt und auch dann noch eine Zeitspanne zur Reaktion erhält.[146] Es ist unerheblich, ob die Änderung obligatorisch oder fakultativ ausgestaltet ist.[147] Der triftige Grund muss bei Änderungsvornahme bestehen und die Änderung darauf zielen, genau diesen triftigen Grund zu beheben.[148] Es erscheint naheliegend, dass bei nur begünstigenden Änderungen die Schwelle für den „triftigen Grund" herabzusetzen wäre; insbesondere da der Unternehmer bereits bei Vertragsschluss zukünftige Entwicklungen vorhersehen und mögliche Änderungsbedarfe einschätzen können muss, was selbst bei sorgfältigem Vorgehen im Bereich der IT mit großen Unsicherheiten behaftet ist.[149] Dem Verbraucher soll die Änderung keine zusätzlichen Kosten verursachen, wobei auch Zahlungen mit personenbezogenen Daten hierunter zu fassen sind[150], also bspw. eine Ausweitung der Datenübermittlung nicht umfasst ist.

II. Dauerhafte Bereitstellung

Der Unternehmer muss verpflichtet sein, ein digitales Produkt dauerhaft bereit zu stellen (§ 327e Abs. 1 S. 3 BGB; § 27 Abs. 1 VGG), auf einmalige Bereitstellung findet die Vorschrift keine Anwendung, ebenso wenig, sofern der Unternehmer die Leistung wiederholt bereitstellen muss; eine analoge Anwendung der Regelungen ist aufgrund fehlender Planwidrigkeit der Regelungslücke als auch Vollharmonisierung der Richtlinie nicht denkbar.[151]

Bei fortlaufender Bereitstellung (über befristeten oder unbefristeten Zeitraum) kann der Unternehmer die digitale Leistung ändern, wenn dies im Vertrag inkl. eines triftigen Grundes vereinbart ist, dem Verbraucher keine Kosten entstehen und der Verbraucher klar über die Veränderung informiert und nur geringfügig beeinträchtigt wird.[152] Ist die Beeinträchtigung des Verbrauchers nicht bloß geringfügig, muss er im Vorhinein mittels eines dauerhaften Datenträgers (auch E-Mail) über die Merkmale und den

146 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 15.
147 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 7; aA: Schöttle, MMR 2021, 683, 688, auch MüKo-BGB/Metzger § 327r Rn. 4.
148 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 145; Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 15; Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 11.
149 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 145; Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 11.
150 juris-PK/Kaesling § 327r Rn. 5.
151 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 5.
152 Möllnitz, MMR 2021, 116, 116.

Zeitpunkt der Änderung sowie über sein Recht auf Vertragsauflösung sowie über die Möglichkeit der unveränderten Beibehaltung informiert werden. In einem solchen Fall einer nicht bloß geringfügigen Beeinträchtigung hat der Verbraucher das Recht zu einer kostenfreien Vertragsauflösung binnen 30 Tagen ab Änderung bzw. ab Zugang der Information, je nachdem, was später erfolgt.

III. Kostenneutralität

Zusätzliche Kosten dürfen für den Verbraucher durch eine Änderung nicht entstehen.[153] Davon umfasst sind sowohl die Erhebung einer Gebühr für die Änderung als auch die Anhebung des Produktpreises aus Anlass der Änderung.[154] Gerade durch Änderungen, die indirekte Kosten nach sich ziehen, indem die Interoperabilität der weiteren Verbrauchergeräte eingeschränkt wird, könnten sich erhebliche Belastungen ergeben, die der Verbraucher überhaupt nicht beeinflussen kann, auch diese sind ausgeschlossen.[155] Dabei wäre bei einem Aufwendungsersatzanspruch des Verbrauchers gegen den Unternehmer der Verbraucher erheblich schlechter gestellt, da er das Insolvenzrisiko sowie eine mögliche Last aus dem Prozess zu tragen hätte. Es sind auch Verträge umfasst, bei denen der Verbraucher nicht zur Zahlung eines Preises verpflichtet ist, der Verbraucher also auch nicht weitere persönliche Daten zur Verfügung stellen muss.[156]

IV. Einseitigkeit

Nicht im expliziten Wortlaut genannt, ist der Regelungsumfang aber nur auf einseitige Änderungen des Unternehmers ausgedehnt.[157] Einvernehmliche Absprachen zwischen Unternehmer und Verbraucher zur Vertragsände-

153 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 16; Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 14.
154 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 17.
155 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 17; Möllnitz, MMR 2021, 116, 116, 119; Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 14; zurückhaltender aber MüKo-BGB/Metzger § 327r Rn. 8.
156 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 16; Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 147.
157 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 10.

rung sind nicht umfasst, ebenso wenig wie neue Verträge über die durch die Änderung betroffenen Produkte.[158]

C. Maß der zugelassenen Änderungen

Es können sowohl positive als auch nachteilige Änderungen vorkommen.[159] In diesem Fall greifen § 327r Abs. 2 BGB, § 27 Abs. 2 VGG, Art. 19 Abs. 2 DID-RL, die bei nicht nur unerheblicher bzw. geringfügiger Beeinträchtigung (Zugriffsmöglichkeit / Zugänglichkeit oder Nutzbarkeit werden eingeschränkt) weitere Anforderungen vorsehen.[160] Nutzbarkeit meint die Tauglichkeit des digitalen Produkts zur vertraglich geschuldeten Verwendung, wobei diese nicht nur bei der Betroffenheit der Nutzung selbst, sondern auch eine Veränderung der digitalen Umgebung des Verbrauchers und damit seiner Nutzungsmöglichkeit umfassen kann, so bspw. wenn die Software plötzlich erheblich größere Hardware-Anforderungen hat.[161] Die Beurteilung erfolgt anhand eines objektiven Kriterienkatalogs, der Art und Zweck des digitalen Produkts, Qualität, Funktionalität, Kompatibilität und andere übliche wesentliche Merkmale berücksichtigt.[162]

D. Kontrollmechanismen

Um die Änderungsbefugnis nicht uferlos werden zu lassen, hat der Gesetzgeber zwei Kontrollmechanismen eingeführt: es muss eine vertragliche Vereinbarung getroffen sein, die einer Transparenzkontrolle sowie dem AGB-Recht standhält.

158 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 10.
159 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 8.
160 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 14, 21.
161 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 21; Ehle/Kreß, CR 2019, 723, 729 f.
162 juris-PK/Kaesling § 327r Rn. 7; Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 21.

I. Vertragliche Vereinbarung und Transparenzkontrolle

Die Befugnis, eine Änderung durchzuführen, muss im Vertrag zwischen den Parteien vereinbart worden sein.[163] Es handelt sich also nicht um ein gesetzliches Änderungsrecht, sondern um eines, das in die Vertragsfreiheit der Parteien gestellt und besonderen Bestimmungen unterworfen ist.[164] Das Änderungsrecht des Art. 19 Abs. 1 lit. a DID-RL muss dabei nicht in einer bestimmten Form geregelt sein und wird daher häufig in besonderen, deutlich strengeren Rechtsvorschriften unterfallenden,[165] AGB geregelt werden.[166] Im Verbraucherfall sind individuelle Beschaffenheitsvereinbarungen selten und eine von objektiven Anforderungen abweichende Regelung kann nur geschlossen werden, wenn der Unternehmer den Verbraucher explizit über diese Abweichung informiert und der Vertrag genau diese Abweichung aufgreift.[167]

II. Anwendbarkeit des AGB-Rechts

Eine Klausel ist jedoch missbräuchlich, sofern darin „der Gewerbetreibende die Merkmale des zu liefernden Erzeugnisses oder der zu erbringenden Dienstleistung einseitig ohne triftigen Grund ändern kann" (Anhang Abs. 1 lit. k Klausel-RL).[168] Eine einseitige Änderungsbefugnis für den Unternehmer, die nicht einzeln ausgehandelt wurde, ist nach § 6 Abs. 2 Z 3 KSchG, § 308 Nr. 4 BGB nichtig, außer die Änderung bzw. Abweichung ist aufgrund Geringfügigkeit oder sachlicher Rechtfertigung für den Verbraucher zumutbar.[169] Dies hat der EuGH noch dahingehend präzisiert, dass „Anlass und Modus der Änderung" in der vertraglichen Regelung offensichtlich erläutert wird, der Verbraucher die Möglichkeit der Vertragskündigung eingeräumt bekommt, er davon auch tatsächlich Gebrauch machen kann, und er darüber auch informiert worden ist.[170] Die in Art. 19 Abs. 1 lit. a DID-

163 Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 10.
164 Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 10.
165 Hunzinger, CR 2022, 349, 353, Rn. 28.
166 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 146; Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 10.
167 Redecker, ITRB 2022, 68, 70.
168 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 146; Hunzinger, CR 2022, 349, 353, Rn. 30.
169 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 146.
170 MüKo-BGB/Metzger § 327r Rn. 3.

RL vorgesehene Änderungsbefugnis würde daher leerlaufen, da sie dann nicht vereinbart werden könnte. Insofern ist auf das im Vertrag vorgesehene Änderungsrecht und das zusätzliche Erfordernis des triftigen Grundes Wert zu legen, zumal nach Abs. 2 der Verbraucher ein Beendigungsrecht eingeräumt bekommt.[171] Daraus lässt sich schließen, dass Art. 19 DID-RL als lex specialis nach dem Grundsatz „lex specialis derogat legi generali" der Regelung in der Klausel-RL vorgeht. Die Regelungen sind ansonsten parallel zu berücksichtigen und das AGB-Recht wird nicht durch §§ 327r BGB, 27 VGG verdrängt, da ersteres die Änderungsklauseln auf ihre Wirksamkeit prüft, während in §§ 327r BGB, 27 VGG die tatsächliche Änderung rechtlich geprüft wird.[172] Auch der EuGH hat in der Entscheidung RWE Vertrieb ./. Verbraucherzentrale ein einseitiges Änderungsrecht des Unternehmers mit anschließender Beendigungsbefugnis für den entsprechend informierten Verbraucher als unbedenklich angesehen.[173]

E. Absolute Grenze der Änderung

Ein Zustimmungserfordernis des Verbrauchers zur Änderung besteht nicht, daher besteht eine absolute Grenze der Änderung, die erreicht ist, wenn durch Modifikationen ein gänzlich anderes digitales Produkt entsteht. Problematisch scheint, ob eine Änderung einen tatsächlichen Eingriff in das Produkt erfordert oder auch bloße Umgebungsveränderungen bereits eine Änderung darstellen können und ob bei einer oder mehreren Änderungen, die ein gänzlich neues Produkt nach sich ziehen, überhaupt die Regelung der §§ 327r BGB, 27 VGG, Art. 19 DID-RL Anwendung findet. Hier ist nach den Erwägungsgründen und der Gesetzesbegründung davon auszugehen, dass in solchen Fällen auch ein neuer Produktvertrag zu Stande kommen darf, wobei dann Telos-gerecht bei Entstehung eines gänzlich neuen Produkts von einer Ersetzung gesprochen wird und die Änderungsbefugnis als Interessenausgleich der Parteien nur bei einem im Kern nicht veränderten Produkt erhalten bleibt und daher bei einer gänzlichen Änderung nicht eingreift.[174]

171 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 146.
172 MüKo-BGB/Metzger § 327r Rn. 3.
173 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 147.
174 Möllnitz, MMR 2021, 116, 118.

§ 7 Maßstab zur Beurteilung des Ausmaßes der Änderung

Um das Ausmaß der Änderung zu beurteilen, braucht es einen Maßstab. Eine Referenzgruppe wird durch die DID-RL nicht vorgegeben, damit ist die Vorgehensweise für eine objektive Bestimmung offen; möglich scheint eine Beurteilung der Üblichkeit, die aber angesichts der rasanten technischen Entwicklung schwer zu ermitteln ist.[175]

A. Wertende Betrachtung

Anhand einer wertenden Betrachtung ist dasjenige Maß für die Beeinträchtigung[176] der Änderung auf die Nutzung des digitalen Produkts zu bestimmen, das neben Art und Zweck der digitalen Produkte, Qualität, Funktionalität, Kompatibilität und andere wesentliche Merkmale berücksichtigt, welche vergleichbare digitale Produkte dieser Art aufweisen, dem Vertragszweck entspricht und unter der Schwelle der „Wesentlichkeit" im österreichischen Recht liegt.[177] So sollte zunächst untersucht werden, wie sich die Veränderung auf die betroffenen Produkteigenschaften sowie wie stark diese sich auf das gesamte Produkt auswirkt, und ob der Kern des Produkts verändert wird[178].[179] Diese Anforderungen sind unterschiedlich zu gewichten, beinhalten aber teilweise Überschneidungen, wie die Qualität, die auch Kompatibilität, Sicherheit und Interoperabilität beinhaltet.[180] Subjektive und objektive Anforderungen stellen nur scheinbar klar voneinander zu scheidende Kriterien dar, die Maßstäbe müssen einerseits rechtssicher ermittelt werden aber auch lebensnah ausgelegt werden[181], wobei besonders auf die Interoperabilitäts- und Kompatibilitätsanforderungen zu achten ist, da nach Erwgr. 50 DID-RL mittels offener Dateiformate auch nicht personenbezogene Daten exportiert und importiert werden können sollen.[182]

175 Stiemerling, ITRB 2022, 64-67, 65.
176 Möllnitz, MMR 2021, 116, 121.
177 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 148; MüKo-BGB/Metzger § 327r Rn. 15.
178 Möllnitz, MMR 2021, 116, 118.
179 MüKo-BGB/Metzger § 327r Rn. 15.
180 Schneider, CR 2022, 1-9, 7.
181 Schneider, CR 2022, 1-9, 7.
182 Schneider, CR 2022, 1-9, 7.

B. Übliche Beschaffenheit

Die übliche Beschaffenheit bemisst sich danach, was auf dem Markt für den Produkttyp üblich ist und was der durchschnittliche[183] Verbraucher dabei erwarten kann,[184] § 327e Abs. 3 S. 1 Nr. 2 BGB, § 6 Abs. 2 Nr. 5 VGG, wodurch das subjektive Kriterium eine Objektivierung erfahren muss.[185] Dies lässt sich auch durch die Mangelregelung in § 327e BGB, § 6 VGG negativ abgrenzen, die die bisherigen Mangelbegriffe auf digitale Produkte konkretisieren und dabei in die gleichberechtigt geltenden subjektiven, objektiven und Integrations-Anforderungen untergliedern.[186] So unterfallen den subjektiven Anforderungen Menge, Funktionalität, Kompatibilität und Interoperabilität, sowie eventuelle zusätzliche Leistungen wie Zubehör, Anleitungen, Kundendienst und Aktualisierungen.[187] Der bunte Strauß der Anforderungen kann nicht in allen Belangen gleichermaßen erreicht werden, schon gar nicht in der höchsten Ausprägung.[188] Die subjektiven Erwartungen des einzelnen Verbrauchers sind nicht ausschlaggebend, da diese von den zu unterschiedlichen Fähigkeiten der Verbraucher abhingen.[189] Bei den objektiven Anforderungen an Zugänglichkeit, Kontinuität und Sicherheit[190] sind gem. Art. 8 Abs. 1 lit. a) DID-RL besonders technische Normen zu berücksichtigen.[191] Berücksichtigung finden sollte auch die jeweilige Machbarkeit bzw. Maßstäbe wie Angemessenheit oder Zumutbarkeit der Kosten.[192]

C. Stärke der Beeinträchtigung

Die Stärke der Beeinträchtigung hängt von Art und Zweck der digitalen Leistung und der Qualität, der Funktionalität, der Kompatibilität und anderer wesentlicher Merkmale, wie sie bei digitalen Leistungen gleicher

183 Möllnitz, MMR 2021, 116, 121.
184 Schneider, CR 2022, 1-9, 8.
185 Schneider, CR 2022, 1-9, 5.
186 Stiemerling, ITRB 2022, 64-67, 65; Redecker, ITRB 2022, 68, 68.
187 Stiemerling, ITRB 2022, 64-67, 65.
188 Schneider, CR 2022, 1-9, 7.
189 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 148.
190 Stiemerling, ITRB 2022, 64-67, 65.
191 Schneider, CR 2022, 1-9, 7.
192 Schneider, CR 2022, 1-9, 7, 8.

Art üblich sind, ab. Durch die Änderung sind die Anforderungen in ihrer Gesamtheit einer Dynamik unterworfen, wodurch Flexibilität nötig wird.[193] Es soll berücksichtigt werden, dass der Verbraucher zwar einer Änderungsmöglichkeit zugestimmt hat, deren Tragweite er zum Zustimmungszeitpunkt jedoch nicht abschätzen konnte.[194] Eine objektive Mess- und Fassbarkeit der Beeinträchtigung ist daher erforderlich; eine bloß subjektiv empfundene ist für einen Auflösungsanspruch nicht ausreichend.[195] Nach § 327r Abs. 2 S. 1 BGB, § 27 Abs. 2 S. 1 VGG, Art. 19 Abs. 2 DID-RL steht dem Verbraucher dann ein Auflösungsrecht zu, sofern eine substantiell nachteilige Änderung vorliegt, indem der Zugang zu Inhalten oder deren Nutzung beeinträchtigt wird.[196] Damit wird von der in Erwgr. 49 der DID-RL angeregten „ausreichenden Flexibilität" Gebrauch gemacht, mittels derer die objektiven Anforderungen nicht unverrückbar sind, sondern von denen abgewichen werden kann.[197] Die einzelnen Parameter können je nach digitalem Produkt funktional und leistungsmäßig bis zu einem je nach Produkt unterschiedlichen Minimum angepasst werden.[198]

D. Hierarchisierung

Sofern zwischen den Anforderungen Wirkmechanismen gelten, wie bspw. technisch, preislich oder organisatorisch, muss eigentlich eine Gewichtung und Hierarchisierung vorgenommen werden, was angesichts der im Gesetz angelegten Gleichrangigkeit problematisch scheint, aber für die praktische Anwendung notwendig ist.[199] So könnten sich Anforderungen gegenseitig verstärken, während andere sich antagonistisch zueinander verhalten und so konkurrieren.[200] Eine Rolle spielt auch die Positionierung des Produkts durch den Hersteller. Assistenzsysteme sind bspw. manchmal unterstützend und manchmal paternalistisch ausgelegt oder es wird stärker oder schwä-

193 Schneider, CR 2022, 1-9, 7.
194 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 148.
195 juris-PK/Kaesling § 327r Rn. 10.
196 juris-PK/Kaesling § 327r Rn. 9; Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 28; Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 148.
197 Schneider, CR 2022, 1-9, 7.
198 Schneider, CR 2022, 1-9, 7.
199 Schneider, CR 2022, 1-9, 7.
200 Schneider, CR 2022, 1-9, 8.

cher auf das Nutzerverhalten reagiert, wodurch das Nutzerverhalten gesteuert werden kann.[201] So kann der Nutzer von Sicherheit, Usability und Kompatibilität einerseits profitieren, für den Hersteller ergeben sich daraus aber große Anforderungen an sein Produkt.[202] Gesetzlich nicht ausdifferenziert ist, was bei negativen Wechselwirkungen zwischen Anforderungen gilt, was für den Verbraucher noch tolerabel ist und ab wann er ein Kündigungsrecht besitzt.[203] Eine weitere Problemzone könnte sich beim Thema Sicherheit des Produkts eröffnen, da bei diesem Bereich Nutzerfreundlichkeit und Funktionsumfang des Produkts in Konflikt geraten können, bspw. bei den Grundsätzen / Sicherheit der Verarbeitung personenbezogener Daten nach der DS-GVO, bei denen Risiko-Potential und Sicherheitsbedarf in Relation zueinander zu setzen sind, wobei bei den im Rahmen der Änderungsbefugnis betroffenen Verbrauchern insbesondere die Ausspähung zu Werbezwecken einen hohen Schutzbedarf vermuten lässt.[204] Bei Änderungen der Zugriffsmöglichkeit und Nutzbarkeit treffen den Unternehmer besondere Informationspflichten nach § 327r Abs. 2 BGB, § 27 Abs. 2 VGG, wobei bei deren Erfüllung dann die entsprechenden Änderungen erlaubt sind.[205]

In der gesetzlichen Regelung finden sich keine eineindeutigen Kriterien, anhand derer man einen Maßstab für die Beurteilung der Änderung aufbauen könnte. Im weiteren Verlauf der Arbeit wird daher durch Anwendung der Regelungsinhalte anderer Gestaltungsrechte ein Kriterienkatalog erarbeitet. Um die Bedeutung zu unterstreichen, werden im folgenden Kapitel zunächst die Rechtsfolgen einer Änderung aufgezeigt.

§ 8 Einfluss des Änderungsmaßes auf die Rechtsstellung des Verbrauchers

Sofern eine ausreichende Information des Verbrauchers erfolgt, gibt es zwei Möglichkeiten: Die tatsächliche Änderungsdurchführung ohne Verbraucherrechte oder bei einer erheblichen Änderung ein Recht zur Vertragsbeendigung.

201 Schneider, CR 2022, 1-9, 8.
202 Schneider, CR 2022, 1-9, 8.
203 Schneider, CR 2022, 1-9, 9.
204 Schneider, CR 2022, 1-9, 7.
205 Schneider, CR 2022, 1-9, 9.

A. Anforderungen an die Information

Die Anforderungen unterscheiden sich danach, ob eine nur geringfügige oder eine den Verbraucher nicht nur unerheblich beeinträchtigende Änderung vorgenommen werden soll.

I. Information bei unerheblich beeinträchtigender Änderung

Der Unternehmer muss dem Verbraucher eine klare und verständliche Information über die Änderung zukommen lassen.[206] Umfasst sind dabei neben der Information über Vornahme und Merkmale der Änderung auch der voraussichtliche Änderungszeitpunkt; dies gilt auch, wenn diese den Verbraucher nur geringfügig oder gar nicht beeinträchtigt.[207] Die bloße Möglichkeit der Änderung durch Niederlegung in der Vertragsurkunde ist nicht ausreichend, der Verbraucher muss über jede einzelne Anpassung vom Unternehmer informiert werden, spätestens zeitgleich bei einer verbraucherfreundlichen Änderung.[208] Diese Information soll es dem Verbraucher ermöglichen, eventuelle Änderungen in seiner digitalen Umgebung vor Änderungseintritt durchzuführen, was bei einer nachträglichen Information nicht gewährleistet wäre.[209] Die Information muss zwei Aspekte enthalten: Zunächst muss die Änderung des digitalen Produkts mitgeteilt werden, sodann der Umfang der Änderung, wobei diese nicht die Anforderungen des § 327r Abs. 2 S. 2 Nr. 1 BGB, § 27 Abs. 1 Nr. 4 VGG erfüllen muss, jedoch dem Verbraucher ausreichend verdeutlichen, wie das digitale Produkt in Zukunft ausgestaltet sein wird.[210] Durch den Änderungsvorbehalt im ursprünglichen Vertrag erlangt der Verbraucher diese Information nicht, weil zwar der Grund genannt, aber nicht der Umfang der zukünftigen Änderungen deutlich wird.[211] Eine reine Nachricht, es erfolge ein Update auf eine höhere Version, reicht nicht aus, da so nicht klar wird, was der

206 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 18; MüKo-BGB/Metzger § 327r Rn. 9.
207 Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 16; MüKo-BGB/Metzger § 327r Rn. 13.
208 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 18; MüKo-BGB/Metzger § 327r Rn. 9.
209 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 18.
210 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 19; Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 147.
211 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 19.

Unternehmer zukünftig schuldet.[212] Um zu vermeiden, dass die Informationspflicht leer läuft, muss die durchgeführte Änderung nach Art und Umfang der Angekündigten entsprechen, sollte sie darüber hinausgehen, wäre sie mangels Information insgesamt unzulässig; tatsächliche Änderung und Information sind daher kongruent zu gestalten.[213]

II. Information bei nicht nur geringfügiger Beeinträchtigung

Bei mehr als geringfügiger Beeinträchtigung muss die Information im Vorhinein „mit angemessener Frist"[214] (je nach Einzelfall, bspw. auch technisch notwendiger Kurzfristigkeit[215], jedoch so, dass eine gewisse Vorbereitung auf die Änderung möglich ist, unabhängig von der 30-tägigen Frist des § 327r Abs. 3 BGB[216], § 27 Abs. 2 VGG, Art. 19 Abs. 2 DID-RL) klar und verständlich[217] mittels dauerhaftem Datenträger (Art. 2 Nr. 13 DID-RL) und aktiv erfolgen (der Verbraucher muss die Möglichkeit haben, die Erklärung so aufzubewahren oder zu speichern, dass sie während eines für ihren Zweck angemessenen Zeitraums zugänglich ist, und er die Erklärung unverändert wiedergeben kann, bspw. mittels Papier, DVD, USB-Stick; eine Anzeige in einem Online-System wie Homepage oder Social-Media-Kanal des Unternehmers oder Pop-Up-Benachrichtigungen reicht dafür nicht, da keine dauerhafte Abspeicherung möglich ist, eine Benachrichtigung per E-Mail hingegen durchaus[218]) und die Merkmale enthalten, also besonders Umfang und Auswirkungen der Änderung auf Zugriffsmöglichkeit und Nutzbarkeit des digitalen Produkts, Zeitpunkt der Änderung sowie Rechte des Verbrauchers nach § 327r Abs. 3, 4 BGB, § 27 VGG Abs. 2, Art. 19 Abs. 2 DID-RL, also zur kostenlosen Vertragsauflösung binnen einer Frist von 30 Tagen ab Änderung / verspäteter Information bzw. den Ausschluss dieses

212 Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 18.
213 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 19.
214 Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 19, 21.
215 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 147; MüKo-BGB/Metzger § 327r Rn. 11; Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 21; juris-PK/Kaesling § 327r Rn. 8.
216 MüKo-BGB/Metzger § 327r Rn. 11.
217 Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 16, 18.
218 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 25; Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 147; MüKo-BGB/Metzger § 327r Rn. 12; Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 16, der aber eine Anzeige in einem „Online-System", unter das er die Homepage des Anbieters nicht fasst, als ausreichend ansieht.

Rechts unter bestimmten Bedingungen, sowie die Modalitäten der Rechtsausübung.[219] Auch Rechtsfolgen der Vertragsbeendigung, die Erstattung der bereits geleisteten Zahlungen sowie Rechte und Pflichten des Verbrauchers nach §§ 327o, 327p BGB, §§ 24, 25 VGG, Artt. 16, 17 DID-RL sind mitzuteilen.[220] Dem Verbraucher muss es möglich sein, eine technische und rechtliche Prüfung der Veränderung und besonders auch eine Datensicherung durchzuführen, auch wenn der Verbraucher sich gegen die Änderung nicht wehren, sondern nur den Vertrag nach der weiteren 30-tägigen Frist des Abs. 3 (BGB) bzw. Abs. 2 (VGG) beenden kann.[221] Sofern keine Benutzerschnittstelle zwischen „smarter Sache" und Verbraucher existiert (bspw. bei Geräten ohne Display wie internetfähigen Haushaltsgeräten), muss der Unternehmer einen Informationskanal für den Verbraucher eröffnen, bspw. ein Nutzerkonto oder einen sonstigen Kommunikationskanal.[222]

B. Rechtsfolgen einer zulässigen Änderung

Sofern eine zulässige Änderung durchgeführt wird, hat der Verbraucher eine Duldungspflicht, der Unternehmer aber keine Eingriffsmöglichkeit in die Geräte des Nutzers. Sofern der Unternehmer die Verbraucherinformation regelkonform vorgenommen hat, darf er die Änderung durchführen.

I. Duldungspflicht

Der Verbraucher hat bei Vorliegen der Voraussetzungen des § 327r Abs. 1 BGB, § 27 Abs. 1 VGG sowie ggfs zusätzlich § 327r Abs. 2 BGB, § 27 Abs. 1 Nr. 4 VGG eine Duldungspflicht für die Änderung des digitalen Produkts, woraus sich eine Änderung des Vertragsinhalts ergibt.[223] Es besteht kein Recht für den Verbraucher, weiterhin die unveränderte Version des digitalen Produkts bereit gestellt zu erhalten. Das geänderte Produkt wird dann

219 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 147; Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 15, 20; MüKo-BGB/Metzger § 327r Rn. 14.

220 MüKo-BGB/Metzger § 327r Rn. 14.

221 MüKo-BGB/Metzger § 327r Rn. 11.

222 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 20; Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 16.

223 MüKo-BGB/Metzger § 327r Rn. 11; Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 23.

auch nicht vertragswidrig. In § 327r BGB, § 27 VGG sind Voraussetzungen und Rechtsfolgen von Änderungen abschließend geregelt, insbesondere ist der Interessenausgleich abschließend.[224] Das geänderte Produkt muss die Qualitätsstandards der übrigen Regelungen des VGG (insb. § 7 VGG) bzw. BGB erfüllen.[225]

II. Eingriffsrecht des Unternehmers bzw. Anspruch auf Durchführung der Änderung

Problematisch für den Unternehmer wird es, wenn das digitale Produkt seiner Kontrolle entzogen ist, weil es bspw. auf den Geräten der Verbraucher läuft und nicht auf den Servern des Unternehmers, denn dieser hat aus § 327r BGB, § 27 VGG keine Eingriffsbefugnis in die technische und digitale Umgebung des Verbrauchers, da das Eigentum, die Achtung des Privatlebens, insbesondere der Kommunikation (Art. 7 GRCh), sowie der Schutz der persönlichen Daten (Art. 8 GRCh) besonderen Schutz genießen.[226] Aus der Systematik der Vorschrift sollte eigentlich eine Durchsetzungsmöglichkeit für den Unternehmer vorhanden sein. Dies ist jedoch nicht der Fall, daher kann keine Selbstvornahme durch den Unternehmer erfolgen, wenn die zu ändernden Daten gar nicht in seiner Zugriffssphäre sind. So wird der Integritätsschutz für die Systeme gewährleistet und die Beeinträchtigung der Sphäre des Verbrauchers so gering wie möglich gehalten. Durch eine Änderung können sich Probleme mit Kompatibilität und Interoperabilität der digitalen Geräte des Verbrauchers ergeben, wodurch sich u.U. starke Beeinträchtigungen ergeben könnten. Digitale Inhalte und Dienstleistungen ermöglichen einen ferngesteuerten Zugriff und auch eine Deaktivierung,[227] die den Nutzer allerdings unzulässig in seinen Rechten beeinträchtigen würden und die daher nicht eingesetzt werden können, um Änderungen durchzuführen.

224 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 26.
225 Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 24.
226 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 27; Fida, Updates, 166; juris-PK/Kaesling § 327r Rn. 12 (der es als zu klären ansieht, ob der Verbraucher in gewissen Grenzen zur Mitwirkung bei Implementierung der Änderungen verpflichtet ist); Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 23.
227 Fida, Updates, 167.

C. Rechtsfolgen einer nicht nur geringfügigen Änderung

Bei einer nicht nur geringfügigen Änderung hat der Verbraucher mehrere Möglichkeiten. Er kann entweder die Änderung akzeptieren und das Produkt in der geänderten Form weiternutzen (oder dies für 30 Tage versuchen). Sodann kann er sofort oder innerhalb dieser 30 Tage Frist das Produkt kündigen. In diesem Fall ergeben sich Rechtsfolgen in Bezug auf die Nutzerdaten.

I. Auflösungsrecht bei nicht nur geringfügiger Beeinträchtigung

Bei nur geringfügiger Beeinträchtigung des Zugangs zum digitalen Produkt oder dessen Nutzung durch die Änderung ist der Verbraucher nicht zur Beendigung des Vertrags berechtigt, vielmehr muss er diese hinnehmen[228], sofern jedoch eine stärkere Beeinträchtigung vorliegt, hat der Verbraucher das Recht, den Vertrag aufzulösen.[229]

II. Auflösungsfrist

Das Auflösungsrecht muss innerhalb von 30 Tagen nach dem Zeitpunkt der Änderungsmitteilung (positive Kenntnis des Verbrauchers erforderlich) bzw. nach Eintritt der Änderung (je nachdem, was später eintritt) ausgeübt werden, wobei so die Möglichkeit gegeben ist, die Änderung zunächst auszuprobieren; zur Fristberechnung kann auf die üblichen Vorschriften der §§ 187, 188, 193 BGB; § 902 ABGB abgestellt werden.[230] Ein Recht auf Beendigung besteht auch bei unterlassener Information durch den Unternehmer, die Informationspflicht ist nur Voraussetzung für die nachteilige Änderung des Produkts.[231] Die Auflösungserklärung ist dabei nicht formgebunden (also genügt einfache Textform) und wirkt auf den Zeitpunkt der Änderungsvornahme zurück.[232] Sofern eine Vertragsauflösung erklärt

228 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 29; Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 148.
229 Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 24.
230 juris-PK/Kaesling § 327r Rn. 9; Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 30; Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 149; MüKo-BGB/Metzger § 327r Rn. 19.
231 MüKo-BGB/Metzger § 327r Rn. 17.
232 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 149.

wird, gelten die Regelungen zur Vertragsauflösung, es entsteht ein Rückabwicklungsverhältnis, wobei der Verbraucher seine Zahlung anteilig ab Änderungseintritt zurückerstattet erhält[233] und die Beendigung ihm keine Kosten verursachen darf, § 327r Abs. 3 S. 1 BGB, § 27 Abs. 2 VGG[234]. Der Verbraucher kann die Änderung nicht verhindern, sondern nur den Vertrag beenden.[235] Sofern der Unternehmer dem Verbraucher die unveränderte Beibehaltung der digitalen Leistung ohne zusätzliche Kosten ermöglicht und die digitale Leistung weiterhin dem Vertrag entspricht, besteht kein Auflösungsrecht, § 327r Abs. 4 Nr. 2 BGB, § 27 Abs. 4 VGG, vielmehr hat der Verbraucher die Wahl zwischen der bisherigen unveränderten unter den bisherigen Konditionen und der neuen geänderten Variante.[236] Die Vertragsbeendigung muss der Verbraucher gegenüber dem Unternehmer ausüben, §§ 327r Abs. 5 BGB iVm § 327o Abs. 1 BGB, §§ 24 – 26 VGG.[237]

III. Auswirkungen einer Kündigung

Der Unternehmer kann eine Änderung vornehmen, ohne dass das digitale Produkt dadurch vertragswidrig wird, sofern die Vereinbarung den Anforderungen der §§ 327r Abs. 1, 2 BGB, § 27 Abs. 1, 2 VGG entspricht; wobei der Verbraucher diese zu dulden hat (s. o.).[238] Die Rechtsfolgen bei einer Vertragsbeendigung bemessen sich nach §§ 327o II – V und 327p BGB, §§ 24 – 26 VGG.[239] Nach der Vertragsbeendigungserklärung durch den Verbraucher gegenüber dem Unternehmer entsteht ein Rückgewährschuldverhältnis, § 327o Abs. 2 BGB, § 24 Abs. 2 VGG. Der Unternehmer darf personenbezogene Inhalte, die bei der Nutzung des vom Unternehmer bereitgestellten Produkts angefallen sind, nicht mehr weiter nutzen, muss sie dem Verbraucher jedoch auf dessen Verlangen zur Verfügung stellen [es kann hier nicht auf die Frage eingegangen werden, ob der Nutzer ein

233 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 32.
234 Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 33.
235 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 149.
236 juris-PK/Kaesling § 327r Rn. 10; Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 29; MüKo-BGB/Metzger § 327r Rn. 20.
237 juris-PK/Kaesling § 327r Rn. 11; Erman-BGB/Bernzen/Specht-Riemenschneider § 327r Rn. 31.
238 juris-PK/Kaesling § 327r Rn. 12.
239 juris-PK/Kaesling § 327r Rn. 13; Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 29.

Dateneigentum[240] hat].[241] Der Verbraucher darf das digitale Produkt nach der Beendigung des Vertrags nicht mehr nutzen, § 327p Abs. 1 S. 1 BGB, § 24 Abs. 3 VGG, der Unternehmer darf aufgrund der Kontrollschwierigkeiten gem. S. 2 / Hs. 2 eine aktive Unterbindung der Nutzung vornehmen, bspw. durch Lizenz- oder Kontensperrung.[242]

D. Ausnahme: Weiternutzung des bisherigen Produkts

Nach Art. 19 Abs. 4 DID-RL, § 327r Abs. 4 Nr. 2 BGB, § 27 Abs. 4 VGG kann der Unternehmer dem Verbraucher die unveränderte Weiternutzung des im Funktionsumfang der Vertragsgemäßheit entsprechenden Dienstes anbieten, wobei dann die Abs. 2 und 3 nicht angewendet werden.[243] Art. 19 Abs. 1 DID-RL, § 327r Abs. 1 BGB, § 27 Abs. 1 VGG gelten jedoch auch in dieser Konstellation, der Unternehmer darf also auch bei einer vorgesehenen Weiternutzungsmöglichkeit nur dann eine einseitige Änderung des Vertragsgegenstands vornehmen, wenn der Verbraucher einer einseitigen Veränderung im Vertrag bereits zugestimmt hatte und ein triftiger Grund vorliegt.[244] Der Verbraucher erhält in dieser Konstellation ein Wahlrecht, die zuletzt von ihm benutzte Version (ein Zurückspringen auf ältere Versionen wird nicht ermöglicht) weiter zu nutzen, wobei der Unternehmer weiterhin eine einschränkungsfreie Vertragsgemäßheit zu leisten hat, oder aber die neue Veränderte.[245] Auch die Nutzung des unveränderten Produkts darf keine weiteren Kosten nach sich ziehen, sollte das anders sein, greift wiederum das Beendigungsrecht nach Abs. 3.[246]

§ 9 Transfer bereits existierender Maßstäbe auf die Änderungsbefugnis

Dem Leser der Richtlinien-Regelungen und deren gesetzlicher Umsetzungen fällt auf, dass es für den Unternehmer zwar scheinbar klare Regelun-

240 Maute/Mackenrodt Recht als Infrastruktur für Innovation/Schmidt 265, 265.
241 Heckmann/Paschke juris-PK Internetrecht/Paschke Rn. 642, 643.
242 Jaensch, jM 2022, 96, 102; Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 29.
243 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 150; MüKo-BGB/Metzger § 327r Rn. 21; Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 30.
244 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Kodek 141, 150.
245 MüKo-BGB/Metzger § 327r Rn. 21; Flume/Kronthaler/Laimer VGG/Parzmayr Rn. 30.
246 MüKo-BGB/Metzger § 327r Rn. 23.

gen gibt, wie er bei Änderungen vorzugehen hat. Auch ist begrüßenswert, dass der (Europäische) Gesetzgeber die Relevanz der nachträglichen vertraglichen Anpassbarkeit bei Dauerschuldverhältnissen in der langfristigen Bereitstellung digitaler Inhalte und Dienstleistungen erkannt hat. Jedoch ist es allein auf Grundlage der Richtlinie und der sie umsetzenden Gesetze nicht möglich, zu bestimmen, welche Auswirkungen eine Änderung hat. Zwar wird durch die Beurteilung anhand bestimmter generalisierender und objektiver Maßstäbe der Blickwinkel weg vom Einzelnutzer mit einer speziellen digitalen Umgebung hin zu einer Vielzahl an Nutzern gelenkt.

Durch die Änderung können sich auch erst nachträglich nach Ablauf der 30-tägigen Kündigungsfrist nachteilige Auswirkungen für den Verbraucher zeigen. Der Verbraucher ist dann darauf angewiesen, das Produkt weiter zu nutzen, sofern er den Vertrag nicht ordentlich kündigen möchte. Eine weitere Nutzung des bisherigen Produkts scheint zwar technisch grundsätzlich möglich, dies wäre aber der bloßen Zuvorkommenheit des Unternehmers geschuldet, nicht weil er gesetzlich dazu verpflichtet wäre.

Die Bereitstellung von Software über die Cloud stellt nur einen kleinen Bruchteil der gesetzlichen Fälle dar. Ausschlaggebender werden eher Anwendungsszenarien sein, die auf den ersten Blick gar nichts oder nur wenig mit digitalen Inhalten zu tun haben. So ist bei modernen Autos oft auch ein Entertainment- und Steuerungs-System verbaut, das digitale Dienste beinhaltet, so bspw. die Funktionalität der Navigation, damit wird das Fahrzeug komplex, da es neben der reinen Stoffansammlung auch noch Software, Lizenzen und digitale Dienste umfasst.[247] Diese werden – sofern in der Grundausstattung des Wagens mitgeliefert – der WK-RL unterfallen. Werden jedoch zusätzliche abopflichtige Dienstleistungen angeboten, wie bspw. eine aktive Stauumfahrung, die Freischaltung bestimmter Extras oder die Bereitstellung neuen angepassten Kartenmaterials über einen bestimmten Zeitraum, werden diese Dienste der DID-RL unterfallen. Die Nutzungsdauer eines Fahrzeugs ist zumeist über mehrere Jahrzehnte. Wenn nun in dieser langen Zeit der Unternehmer die Software zur Bereitstellung dieser Dienste auf einen neuen Stand bringen möchte, was bspw. auch mit einer neuen Nutzerführung verbunden ist, wäre wohl eine Änderung im Sinne der hier thematisierten Vorschriften gegeben. Diese Änderung müsste dann bereits in den Vertragsbedingungen zu den Abodiensten angelegt werden und der konkrete Umstand als triftiger Grund genannt sein. Sofern

247 Wendehorst, NJW 2016, 2609, 2609.

der Nutzer sich weigert, die Änderung durchzuführen und die Bedienungsstruktur dann beim alten System bleibt, könnte bspw. ein Unfall entstehen, weil dieses stark Untermenü-lastig aufgebaut ist und dadurch der Fahrer beim Einstellen stärker abgelenkt wird als bei der neuen Oberfläche. Sofern das Gericht zum Schluss kommt, dass die Software ursächlich für den Fehler des Nutzers ist, so könnte dieser sich wohl gegen den Unternehmer wenden. Hier gäbe es im bisherigen Recht zahlreiche Möglichkeiten des Regresses / Schadensersatzes. Durch die Änderung der Funktionalität hat der Unternehmer aber gerade die Software verkehrssicher gestaltet, nur der Verwender hat die Änderung nicht implementiert. Somit kann sich der Unternehmer enthaften,[248] da die Nichtdurchführung der Aktualisierung in der Sphäre des Verbrauchers liegt, Art. 8 Abs. 3 DID-RL bzw. Art. 7 Abs. 4 WK-RL, § 327f Abs. 2 BGB, § 7 Abs. 3 VGG.[249] Dem Verbraucher bliebe dann ein großes Haftungsrisiko, das er bei Nutzung der Software und dem Ablehnen des Updates sehr wahrscheinlich gar nicht abschätzen können wird.

Wenn hinter dem Unternehmer als Vertragspartner des Verbrauchers noch ein untätiger Hersteller steht, der die erforderliche Aktualisierung nicht bereitgestellt hat, haftet der Unternehmer dem Verbraucher trotzdem.[250]

Bei den eingangs dieser Arbeit erwähnten Beispielen ist die DID-RL ein großer Schritt zur kontrollierten Regelung einer bisher weitgehend ungeregelten Rechtsmaterie. Der Heizungsbauer bspw. kann dadurch seine Steuerungssoftware verändern. Er müsste in dem Vertrag über die Bereitstellung der Software mit dem Verbraucher einen triftigen Grund ausreichend spezifisch geregelt haben. Hier wäre in Anbetracht der Umstellung auf eine neue Programmiersprache eine Formulierung „der Unternehmer behält sich die Änderung der Software vor, sofern Umstände eintreten, die die Unterstützung der der Software zugrundeliegenden Programmiersprache nicht mehr gewährleisten“ denkbar. Die Umstellung auf eine neue Programmiersprache stellt eine gravierende Änderung im Programmcode dar. Dem Verbraucher entstehen durch die Änderung jedoch keine Kosten, da er auch bisher mit der Software nur insofern zu tun hatte, als er die Steuerung der Heizung mit ihr vorgenommen hat. Der Unternehmer hat den

248 Wendehorst, NJW 2016, 2609, 2610.

249 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Wendehorst 111, 126; Heckmann/Paschke juris-PK Internetrecht/Paschke Rn. 630.

250 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Wendehorst 111, 126.

Verbraucher über die anstehende Änderung zu informieren. Dies wird er durch Brief oder E-Mail tun, da der Standort der Heizung im Haushalt des Verbrauchers bekannt ist und darin beschreiben, was das Problem mit der Software ist, wie die Änderung durchgeführt wird und inwiefern die anschließende Nutzung davon betroffen ist (bspw. ist die Steuerung für das warme Wasser jetzt in einem anderen Unterpunkt zu finden). Auch unter Beachtung technischer Regelungen handelt es sich bei der Umstellung der Programmiersprache einer Software um eine größere Änderung. Jedoch ist die Software nach der Umstellung als Steuerung für das Gerät des Verbrauchers weiterhin nutzbar und dieses daher einsatzfähig. Es stellt sich allerdings die Frage, wie der Unternehmer die Änderung durchführen kann, wenn der Verbraucher ihn nicht in den Keller, in dem die Heizung steht, lässt. Dann wird der Unternehmer keine Möglichkeit zur Änderung haben, gleichzeitig aber auch nicht aus dem Vertrag aussteigen können. Der Verbraucher wird in diesem Fall trotz einer gravierenden Änderung kein Interesse daran haben, aus dem Vertrag auszusteigen, da er dann das Gerät nicht mehr nutzen könnte. Dadurch wird der Unternehmer zukünftig seine vertraglich geschuldete Leistung nicht mehr erbringen können. Hier zeigt sich, dass der Verbraucher durch die Entscheidung für ein bestimmtes Gerät mit einer herstellereigenen Software-Lösung auch leicht in eine Abhängigkeit geraten kann und der Unternehmer andererseits keine Durchgriffsmöglichkeit hat, die Änderung in der Sphäre des Verbrauchers durchzuführen.

Sofern eine Software aufgrund steigender Nutzerzahlen angepasst werden muss, ist der bisherige Nutzer vermutlich weniger stark betroffen. Er profitiert möglicherweise sogar davon, dass zukünftig neue Nutzer zum Produkt greifen, weil er so leichter Kollaborationsfunktionen nutzen können wird.

Am markanten Beispiel der Microsoft Office Bedienoberfläche lässt sich Wohl und Wehe der Regelung der DID-RL demonstrieren. Microsoft hatte mit Einführung der Office Suite 2007 beschlossen, die Nutzerführung / Menüstruktur auf eine „Ribbon" Oberfläche umzustellen.[251] Sofern es damals diese Regelung der DID-RL bereits gegeben hätte und Office so wie heute als Software-Dienst im Abo-Modell angeboten worden wäre, so wäre dies eine Änderung gewesen, die den jeweiligen Nutzer stark betroffen hätte. Es gingen unzählige Nutzerbeschwerden ein, die teilweise auch stark for-

251 https://techterms.com/definition/ribbon, zuletzt abgerufen am 05.09.2022.

derten, die Nutzeroberfläche wieder umzustellen, es gab sogar Programme, die die Nutzeroberfläche wieder auf die frühere Variante umstellten.[252] Die Änderung der Nutzerführung war eine gravierende Änderung, die nach einem objektiven Maßstab eine Vielzahl von Nutzern betroffen hätte. All diese Nutzer hätten dann ein Vertragsbeendigungsrecht gehabt. Dem Unternehmer entsteht bei der Einführung einer Änderung ein wirtschaftliches Risiko. Er muss darauf achten, die Änderung im Rahmen des eingangs erwähnten Flexibilitätserfordernisses vorzunehmen und gleichzeitig die Kunden nicht so stark zu beeinträchtigen, dass diese in großer Zahl von ihren Kündigungsrechten Gebrauch machen. Bei einer großen Änderung sind in der modernen Welt auch viele Nutzer tatsächlich oder vermeintlich betroffen, da diese Nutzungseinschränkungen feststellen. Ein objektiver Maßstab lässt sich aufstellen, aber die konkrete Einschränkung kaum ermessen. Zur Behebung der aufgezeigten Unschärfen wird die Übertragung bereits im Gesetz verankerter, von der Rechtsprechung aufgestellter und anerkannter Regelungsinhalte sowie die Auslegung der Regelungen nach deren Telos helfen.

A. Verfassung als Ausgangspunkt der Innovation

Im abgestuften Bau der Rechtsordnung liegt jeglicher staatlicher Regelung die Verfassung zugrunde, die die gesetzgebende Gewalt bindet.[253] Da die Verfassung Geltungsvorrang vor dem einfachen Gesetz hat,[254] muss eine Innovation bereits in dieser angelegt sein. Stärker als die Verfassung, die einerseits Stabilität für die langfristige Dauer ihrer Existenz verkörpern muss, sich andererseits aber auch der Dynamik des Fortschritts nicht verschließen darf, unterfallen einfache Gesetze kontrafaktischen Besonderheiten[255], wodurch sie leichter auf Innovationen reagieren können. Durch stetige Veränderungen im schnelllebigen technischen Bereich sind Innovationen nur eine logische Folge,[256] an die bestehende Produkte angepasst werden müssen, um Markt-Chancen haben zu können. Neuerungen als Beschreibung von Innovationen müssen eine gewisse Signifikanz, Qualität,

252 https://www.addintools.com/german/default.htm, zuletzt abgerufen am 05.09.2022.
253 Isensee/Kirchhof HdB StR/Badura 591, 592.
254 Isensee/Kirchhof HdB StR/Badura 591, 594.
255 Hornung, Grundrechtsinnovationen (2015), 76, 77.
256 Hornung, Grundrechtsinnovationen, 139, 140.

Merklichkeit oder Bedeutung aufweisen.[257] Gerade bei Innovationen ist die „Störung von Erfahrung und Routine"[258] immanent, was bei völlig Neuem (Basisinnovation) der Fall ist, aber auch bereits bei bloßer Umbildung, -Gestaltung oder Kombination wird das Bisherige signifikant neu gestaltet und weiter entwickelt (inkrementelle Innovation), um so eine Diffusion (gelungene Verbreitung) am Markt zu erreichen.[259] Im Gesetz muss daher das Interesse des Unternehmers ermöglicht werden, sein Produkt möglichst lange am Markt zu halten, indem am steten Strom der Innovationen partizipiert wird, diese in das Produkt einfließen, um so aufgrund eines attraktiven Angebots Kunden anzusprechen.[260] Das Gesetz kann jedoch niemals alle Möglichkeiten abdecken, daher muss es allgemein formuliert sein, um auch zukünftige Entwicklungen abbilden zu können, ohne dabei jedoch spezifische Vorgaben außer Acht zu lassen. Im Folgenden werden Anpassungsbedarfe und anschließend verschiedene gesetzliche Regelungen aufgezeigt, die bereits bisher einseitige Gestaltungsrechte beinhalten, um deren Aussagegehalt auf die neue Regelung zu übertragen.

B. Innovationsgetriebene Änderungsbefugnis als Ausfluss des einseitigen Gestaltungsrechts

Wie im Fall der DID-RL mit der Änderungsbefugnis für den Unternehmer können verallgemeinernd mit dem privaten Gestaltungsrecht konkret bestehende Rechtsbeziehungen durch einseitiges (subjektives) Rechtsgeschäft ausgestaltet[261] oder verändert werden.[262] Dabei werden durch Gestaltungsrecht Verträge (Schuldverhältnisse) überhaupt begründet, und deren Inhalt kann ebenso im Rahmen der Gestaltung geändert werden.[263] Wahlrechte bestehen dann, wenn bestimmte Interessen einer Partei als schutzwürdig angesehen werden. Bei auf Einigung der Parteien basierenden Gestaltungs-

257 Hornung, Grundrechtsinnovationen, 143.
258 Luhmann, Organisation und Entscheidung2 (2006), 162, zit. n. Hornung, Grundrechtsinnovationen, 144.
259 Hornung, Grundrechtsinnovationen, 144, 152.
260 Hornung, Grundrechtsinnovationen, 154, 156.
261 MüKo-BGB/Emmerich § 311 Rn. 22.
262 Seckel nach Adomeit, Gestaltungsrechte, Rechtsgeschäfte, Ansprüche. Zur Stellung der Privatautonomie im Rechtssystem (1969), 10. Scholz, Gestaltungsrechte im Leistungsstörungsrecht (2010), 43. ABGB-ON/Wiebe § 859 Rn. 11.
263 Adomeit, Gestaltungsrechte, 14; Scholz, Gestaltungsrechte, 54.

rechten begibt sich der spätere Gegner bewusst der Rechtsgestaltung und ermächtigt den Inhaber zur einseitigen Veränderung, auf deren Eintritt er keinen Einfluss mehr hat.[264] Durch die einseitige rechtsgeschäftliche Erklärung ist die Rechtslage veränderbar, ohne dass der andere Teil mitwirken müsste, was die Schutzbedürftigkeit des anderen Teils nach sich zieht, soweit die Rechtsgestaltung nicht dem vorausgegangenen Konsens entspricht und daher einen Eingriff darstellt.[265] Zur Regelung vertraglicher Gestaltungsrechte sind als essentialia negotii neben Berechtigtem, Gegner, das betroffene Rechtsverhältnis sowie die herbeizuführende Rechtsfolge zu nennen.[266] Der Schutz des Gegners ist in formaler Hinsicht auf Sicherheit und Klarheit des Rechts sowie in inhaltlicher Sicht auf die Einhegung der Gestaltungsrechtsfolgen gerichtet, wie bspw. mithilfe der Billigkeitskontrolle des § 315 Abs. 3 BGB, was je nach Gestaltungsrecht und individueller Vereinbarung unterschiedlich ausgestaltet ist.[267] Gerade dem formalen Schutz des Gestaltungsgegners vor dem ungewissen Eintritt des Ob und Wann der Ausübung[268] dient die Regelung des Art. 19 DID-RL.

C. Anpassungsbedarfe

Anpassungsbedarfe können in den unterschiedlichsten Bereichen auftreten und sich aus verschiedensten Gründen ergeben, wie Gesetzes- und Rechtsprechungsänderungen, Evolutionen der gesellschaftlichen und wirtschaftlichen Verhältnisse, die Auswirkungen auf Haftungs-, Anzeige- und Hinweispflichten haben können.[269] In einzelnen Bereichen war auch bisher schon eine einseitige Vertragsanpassung vom Gesetzgeber ermöglicht, insbesondere in Massenvertragsverhältnissen (was auch teilweise für die der vorliegenden Arbeit zugrunde liegenden digitalen Inhalte zutrifft) bspw. im Versicherungsrecht (§§ 164, 176, 203 Abs. 4 VVG), Energieversorgung (§ 5 Abs. 2 StromGVV bzw GasGVV), Bausparkassen (§ 9 Abs. 1 BausparkG) und bei Investment-Verträgen (§ 43 Abs. 2 und 5 InvG), obwohl dies eine große Missbrauchsgefahr und Benachteiligungsfolgen für den zumeist un-

264 Scholz, Gestaltungsrechte, 57; Adomeit, Gestaltungsrechte, 36; Schellhase, Gesetzliche Rechte zur einseitigen Vertragsgestaltung (2013), 50.
265 MüKo-BGB/Emmerich § 311 Rn. 23; Schellhase, Vertragsgestaltung, 47, 50.
266 Schellhase, Vertragsgestaltung, 52.
267 Schellhase, Vertragsgestaltung, 57.
268 Schellhase, Vertragsgestaltung, 62.
269 Schellhase, Vertragsgestaltung, 24.

terlegenen Vertragspartner nach sich ziehen kann, da insoweit ein „Einbruch in die Privatautonomie" erfolgt.[270] Solch einseitige Vertragsgestaltungen sind auch Regelungen, die einen ausbleibenden Widerspruch binnen einer vorgegebenen Frist als Zustimmung fingieren, wie sie bspw. in § 675g Abs. 2 BGB Eingang gefunden hat.[271] Der BGH hat 1999 in einer Entscheidung über vertragliche Bedingungsanpassungen zur Interessenlage festgestellt, dass bei Berücksichtigung beiderseitiger Interessen eine Vertragsanpassung nur rechtfertigbar ist, wenn unvorhersehbare Veränderungen vorhandene Äquivalenzanforderungen nicht nur unbedeutend gestört haben; das Gesetz bezwecke lediglich, Benachteiligungen gegen Treu und Glauben für den Vertragspartner zu verhindern.[272] Ähnlich zur Regelung in der DID-RL treffen auch Unternehmen in verschiedenen anderen Bereichen die Pflicht zur Unterhaltung des Kommunikationskanals (bspw.: § 36 Abs. 1 EnWG, § 14 WpÜG, § 21 GasNZV).[273] Im Versicherungsrecht ist auch die Einschaltung eines Treuhänders möglich, der die Leistung näher bestimmt (wie in § 317 Abs. 1 BGB vorgesehen) und die Angemessenheit der Vertragsänderung bestätigt.[274] Im gerichtlichen Verfahren wird die Einhaltung der allgemeinen Grenzen der §§ 134, 138 BGB sowie des AGB-Rechts geprüft (zumeist anhand § 308 Nr. 4 BGB), sodann auf die ergänzende Vertragsgestaltung abgestellt, wobei ein vertragsspezifischer Regelungsgehalt in Anbetracht der objektiven Parteiinteressen zur Verfügung steht, und schließlich der Maßstab des billigen Ermessens des § 315 Abs. 1 BGB herangezogen.[275]

D. Einseitige Änderungsbefugnisse in anderen Regelungen

Nach der Herleitung der Anpassungsbedarfe aufgrund der innovativen wirtschaftlichen und technischen Gesellschaft wird im Folgenden das Herausarbeiten eines Erheblichkeitsmaßstabs für die Änderung angestrebt, wozu verschiedene Regelungen vorgestellt werden, die ebenfalls einseitige Änderungsbefugnisse einräumen. Hierbei werden allgemein bekannte sowie spezielle Regelungen im BGB thematisiert, bevor solche des ABGB angesprochen werden.

270 Schellhase, Vertragsgestaltung, 25.
271 Schellhase, Vertragsgestaltung, 26.
272 BGH IV ZR 218–97 (Düsseldorf), Unwirksame Bedingungsanpassungsklausel in der Rechtsschutzversicherung, NJW 1999, 1865.
273 Schellhase, Vertragsgestaltung, 168.
274 Schellhase, Vertragsgestaltung, 126, 127
275 Schellhase, Vertragsgestaltung, 130, 131.

I. Anpassung der essentialia negotii als Änderung

Die einseitige Änderungsbefugnis von wesentlichen Vertragselementen (essentialia negotii) gibt es nur selten. Eine Vertragsänderung über eine Zustimmungsfiktions-Klausel, die keine Beschränkung zum Schutz des Verbrauchers vor unangemessenen Nachteilen enthält, verstößt gegen das Transparenzgebot in § 6 Abs. 3 KSchG, besonders wenn die Vertragspflichten zu Gunsten des Verwenders in jede Richtung und in unbeschränktem Umfang geändert werden können. Der Verbraucher muss daher bereits zu Anfang über die Gründe und maßgeblichen Gesichtspunkte der Änderung informiert werden, da sonst Unklarheiten über die Auswirkungen der Klausel bleiben.[276]

II. Störung der Geschäftsgrundlage: § 313 BGB

1. Gesetzlicher Regelungsinhalt

§ 313 BGB schafft die Möglichkeit, eine Vertragsanpassung durchzuführen, wenn die Vertragsparteien unter Berücksichtigung der neuen Gegebenheiten in den Vertrag andere Bedingungen hineingeschrieben hätten. In § 313 Abs. 3 S. 1 BGB ist als Gradmesser für eine Anpassung oder Aufhebung des Vertrags die Zumutbarkeit heranzuziehen, um eine möglichst interessengerechte Verteilung des verwirklichten Risikos bei möglichst geringem Eingriff in die ursprüngliche Regelung zu gewährleisten.[277] Dabei ist besonders das Parteiinteresse nach § 157 BGB zu beurteilen, um einen Ausgleich für das adäquate Maß übersteigender Einschränkung zu erzielen.[278]

2. Transfer

Auf die Änderungsbefugnis des Unternehmers angewendet, ergibt sich für das Maß der Änderung vor allen Dingen der Ansatz, das nach § 157 BGB zu beurteilende Parteiinteresse zu berücksichtigen. Indem der Verbraucher sich zu Beginn der Vertragsbeziehung über die von ihm gewünschte Leistung klar wurde, hat er den Unternehmer als seinen Vertragspartner ausge-

276 OGH 5 Ob 103/21 i, Energieversorger: Preisanpassungsklauseln VbR 2022/26 K2 Teil 1, Rn. 9.
277 MüKo-BGB/Finkenauer § 313 Rn. 88.
278 MüKo-BGB/Finkenauer § 313 Rn. 89.

wählt. Hier wäre jedoch problematisch, dass zu sehr auf den einzelnen Verbraucher abgestellt werden könnte, statt auf den Grad der Beeinträchtigung des Durchschnittsnutzers.

III. Leistungsbestimmung durch eine Partei: § 315 BGB

1. Gesetzlicher Regelungsinhalt

In § 315 I BGB ist der Fall geregelt, dass die Vertragsleistung durch eine Partei nach billigem Ermessen bestimmt werden soll, wobei im Konfliktfall eine Leistungsbestimmungskontrolle und eine Ersatzvornahme durch Gerichtsentscheidung vorgesehen ist.[279] Dabei liefert der Vertrag als Grundgeschäft den Leistungsanspruch, wobei in der Übereinkunft das Leistungsbestimmungsrecht als Gestaltungsrecht zu Umfang, Grenzen und Entscheidungsrichtlinien ausgeformt und eine wirksame Leistungsbestimmung vereinbart ist.[280] Bei der Grundversorgung dienenden Energielieferverträgen steht die Versorgungssicherheit für die Zukunft im Fokus, aufgrund der langfristigen Vertragslaufzeit ist es wirtschaftlich notwendig, Anpassungsmöglichkeiten in den Vertrag aufzunehmen[281], ebenso ist es auch bei den in ihrer Bedeutung stetig gewachsenen Internet und IT-basierten Dienstleistungen / Inhalten[282], die höchstrichterlich inzwischen als Teil der Grundversorgung anerkannt sind[283]. Diese Anpassungsklauseln müssen besonderen Anforderungen genügen, zumal es sich in den allermeisten Fällen um AGB handelt, wohingegen Individualvereinbarungen unüblich sind.[284] Es greifen die Vorschriften der AGB-Kontrolle ein, die Transparenz und inhaltliche Angemessenheit erfordern. Im Kern soll bei Ausgleich von Missverhältnissen trotzdem die vertragsrechtliche Eigenverantwortung erhalten bleiben.[285] Ähnlich zu den hier thematisierten Software-Anbietern ist der Kunde eines Versorgers diesem teilweise ausgeliefert, trotzdem soll dieser erst später nach Vertragsschluss die Bestimmung eines Vertragsbestandteils

279 Schellhase, Vertragsgestaltung, 27.
280 Staudinger BGB/Rieble § 315 Rn. 276.
281 Ehricke, JZ 2005, 599, 599.
282 https://ourworldindata.org/grapher/supercomputer-power-flops, letzter Zugriff am 03.09.2022; Hilbert/López, Science (New York, N.Y.) 2011, 60, 64.
283 BGH III ZR 98/12, BGH erkennt Schadensersatz für den Ausfall eines Internetanschlusses zu - juris = NJW 2013, 1072-1074 Rn. 17
284 Büdenbender, NJW 2013, 3601, 3601.
285 Ehricke, JZ 2005, 599, 599.

vornehmen können, um eine eventuelle Lücke zu schließen.[286] Die Regelung des § 315 Abs. 3 S. 2 BGB greift mit einer Billigkeitskontrolle der einseitigen Leistungsbestimmung gegenüber dem sozial Schwächeren ein, woraus sich Schranken gegen den Missbrauch wirtschaftlicher Ungleichgewichtslagen herausgebildet haben, die aber nur greifen, wenn der Kunde einem Kontrahierungszwang ausgesetzt ist.[287] Eine entsprechende Anwendung der Rechtsgedanken des § 315 BGB erscheint naheliegend. Nach § 315 Abs. 3 S. 2 BGB ist die Leistungsbestimmung danach zu messen, ob der Berechtigte seinen unternehmerischen Gestaltungsspielraum ausgenutzt hat, wobei sich dies an den vergleichbaren Konkurrenzprodukten bemisst, bzw. wenn solche nicht am Markt vorhanden sind, anhand der Interna des Festsetzenden, die auf Plausibilität geprüft werden.[288]

2. Transfer

Auf IT-Verträge gewendet, ist eine Anpassung an geänderte Nutzungsszenarien ohne Probleme möglich, wohingegen eine plötzliche Steigerung der Hardware-Anforderungen ohne erkennbare Notwendigkeit, da Konkurrenzprodukte auf dem bisherigen Stand verharren, nicht möglich ist. Auch eine Änderung der Programmiersprache, weil die bisherige nicht mehr genug Programmierern bekannt ist oder nicht mehr schließbare Sicherheitslücken aufweist und damit erhebliche Kostensteigerungen nach sich zieht, ist vom unternehmerischen Gestaltungsspielraum gedeckt.

IV. Einseitige Vertragsanpassung durch den Arbeitgeber

1. Grund der Auswahl

Das Arbeitsrecht ist Paradebeispiel für ein Über-/Unterordnungs- und Abhängigkeitsverhältnis, ähnlich wie es auch zwischen einem Verbraucher und einem Unternehmer besteht.

286 Ehricke, JZ 2005, 599, 600.
287 Ehricke, JZ 2005, 599, 600.
288 Ehricke, JZ 2005, 599, 603, 604.

2. Gesetzlicher Regelungsinhalt

Im Arbeitsverhältnis herrscht ein besonderes Abhängigkeitsverhältnis und damit ein Interessenungleichgewicht vor, da der Arbeitgeber ein Direktionsrecht bezogen auf Arbeitsausführung und sonstiges Verhalten hat.[289] Dieses Direktionsrecht leitet sich aus der im Arbeitsvertrag niedergelegten Berechtigung ab, wobei der Arbeitgeber nach billigem Ermessen Inhalt, Ort und Zeit der Arbeitsleistung bestimmen kann.[290] Die Erfordernisse des billigen Ermessens sind erfüllt, wenn die wesentlichen Einzelfallumstände und die „widerstreitenden Interessen angemessen berücksichtigt" worden sind.[291] So muss sich der Arbeitgeber bereits vertraglich oder nach den Umständen einen Wechsel der Beschäftigungsart eingeräumt haben, auch ein Wechsel des Beschäftigungsorts muss mit der Leistungspflicht des Arbeitnehmers korrelieren.[292] Schließlich sind bei Regelungen zum Verhalten sowie geregelten Arbeitsablauf und Zusammenwirken dem Betriebsrat Mitspracherechte eingeräumt.[293]

3. Transfer

Aus all dem wird deutlich, dass der Arbeitgeber nur im Rahmen bereits vorab geregelter Direktionsrechte bestimmen darf und bei besonderen Situationen auch der auf Seiten der Arbeitnehmer deren gemeinsame Interessen wahrnehmende Betriebsrat einzubeziehen ist. Übertragen auf die Änderungsbefugnis der §§ 327r BGB, 27 VGG lässt sich daraus ableiten, dass eine dritte Instanz zur Bewertung die Sicherstellung der Interessenwahrung mehrerer gewährleisten kann und bei großen Interessenungleichgewichten dadurch auch eine Befriedungsfunktion übernehmen kann.

289 Kiel Münchener Handbuch Arbeitsrecht/Fischinger Rn. 4.
290 Kiel Münchener Handbuch Arbeitsrecht/Fischinger Rn. 5.
291 Kiel Münchener Handbuch Arbeitsrecht/Fischinger Rn. 6.
292 Kiel Münchener Handbuch Arbeitsrecht/Fischinger Rn. 8, 9.
293 Kiel Münchener Handbuch Arbeitsrecht/Fischinger Rn. 11.

V. Gebot des fairen Verhandelns im Arbeitsrecht

1. Grund der Auswahl

Wie bereits bei der einseitigen Anpassung durch den Arbeitgeber ist auch beim übrigen Verhandeln im Arbeitsrecht ein Unter-/Überordnungsverhältnis gegeben. Der Schutz des Arbeitnehmers ist dabei für den Gesetzgeber ein vordringliches Ziel.

2. Gesetzlicher Regelungsinhalt

Bei der Anpassung eines arbeitsrechtlichen Vertrags wird auch der Prozess bis zum Vertragsschluss in die Betrachtung einbezogen, wobei sich ein Verbot bspw. aus Missbrauch oder Kreierung einer psychischen Druck- oder Überraschungssituation ergeben kann, soweit nicht ein „Mindestmaß an Fairness" gegeben ist.[294] Nach dem BAG ist das Mindestmaß nicht eingehalten, wenn beim Aufhebungsvertrag die erkennbare Schwäche der Arbeitnehmerseite ausgenutzt worden wäre.[295] Dabei wirken die aus dem zugrunde liegenden Arbeitsvertrag bestehenden Nebenpflichten nach § 241 Abs. 2 BGB auf die Verhandlungen, um so die Rücksichtnahme auf die Rechte, Rechtsgüter und Interessen des anderen sicherzustellen (also deren Berücksichtigung), wobei der Rücksichtnahme-Katalog im Einzelfall zu bestimmen ist.[296]

3. Transfer

Auf die Änderungsbefugnis der §§ 327r BGB, 27 VGG angewendet, muss der Unternehmer fair mit dem Verbraucher umgehen, indem er dessen schwächere Position anerkennt und seine Entscheidungen an dieser ausrichtet, ohne sie aber auszunutzen, indem er bspw. verlangt, ein zusätzliches Produkt aus seinem Portfolio zu erwerben, eine künstliche Abhängigkeit von einem solchen Produkt erzeugt, indem sonst keine Kompatibilität mit anderer Software mehr vorhanden ist.

294 Staudinger BGB/Fischinger/Hengstberger § 134 Rn. 19.
295 BAG 6 AZR 75/18, Aufhebungsvertrag - Widerruf BAGE 165, 315-329 - juris Rn. 9, 34.
296 BAG 6 AZR 75/18, Aufhebungsvertrag - Widerruf BAGE 165, 315-329 - juris Rn. 31, 33.

VI. Abonnement-Veränderungen in Pay-TV-Verträgen

1. Grund der Wahl

Bei Pay-TV-Verträgen hat der Verbraucher ein spezifisches Produkt, bestehend aus verschiedenen Programmkanälen gebucht. Auch hier handelt es sich zumeist um ein standardisiertes Paket, das nicht auf den Verbraucher zugeschnitten ist.

2. Gesetzlicher Regelungsinhalt

Veränderungsrechte für den Anbieter von Pay-TV-Verträgen müssen mit § 308 Nr. 4 BGB konform sein. Sofern in diesen Bestimmungen unklar geregelt ist, ob und in welchem Maß die „Zusammensetzung der vom Kunden gebuchten Programmpakete" abgewandelt werden darf, ist die Kontrolle gescheitert.[297] Der Verbraucher muss entgegen seines eigenen Verständnisses eine andere als die vertraglich geregelte Leistung als vertragsgemäß gelten lassen.[298] Im Rahmen einer Interessenabwägung der Beteiligten dürfen für keine Seite unzumutbare Änderungen vorgenommen werden, dabei muss die Klausel in „ihren Voraussetzungen und Folgen für den anderen Vertragsteil zumindest" eine Gewähr für eine gewisse Kalkulierbarkeit der möglichen Leistungs-Anpassungen zeitigen.[299] Ein grundloses Abänderungsrecht auch bei Erhalt des „Gesamtcharakters" ist nicht gedeckt, wohingegen die Aufnahme konkretisierter und triftiger Umstände in die Bedingungen durchaus möglich ist, aus denen sich für den Kunden die Wahrscheinlichkeit einer Änderung kalkulieren und absehen ließe.[300]

297 Staudinger BGB/Bieder Anh zu §§ 305-310 Rn A 1, A 15.

298 LG München I 12. Zivilkammer 12 O 1982/18, Wirksamkeit eines Änderungsvorbehalts eines Pay-TV-Dienstleisters in Bezug auf das Leistungsangebot CR 2019, 266-269 - juris Rn. 36.

299 LG München I 12. Zivilkammer 12 O 1982/18, Wirksamkeit eines Änderungsvorbehalts eines Pay-TV-Dienstleisters in Bezug auf das Leistungsangebot CR 2019, 266-269 - juris Rn. 37.

300 LG München I 12. Zivilkammer 12 O 1982/18, Wirksamkeit eines Änderungsvorbehalts eines Pay-TV-Dienstleisters in Bezug auf das Leistungsangebot CR 2019, 266-269 - juris Rn. 37.

3. Transfer

Die Anpassungsklausel der Änderungsbefugnis muss eine konkrete Änderung vorsehen. Aus dieser muss sich für den Verbraucher anhand konkretisierender Angaben ergeben, was möglicherweise und warum zukünftig geändert werden kann.

VII. Pauschalreise-Recht: § 651f BGB

1. Grund der Auswahl

Pauschalreisen sind ein standardisiertes Produkt, bei dem der Verbraucher kaum bis keine Änderungsmöglichkeiten hat, damit ist ein Machtgefälle zwischen ihm und dem Anbieter gegeben.

2. Gesetzlicher Regelungsinhalt

§ 651f BGB, der ebenfalls auf der Umsetzung einer EU-Regelung basiert, nämlich auf Artikel 11 der Pauschalreise-Richtlinie der EU, regelt die Änderungsbefugnis des Unternehmers bei solchen Pauschalreise-Verträgen. Dabei ist ebenfalls eine Anpassungsklausel im Vertrag erforderlich, sowie eine nur unerhebliche Beeinträchtigung des Verbrauchers durch die Änderung; die Mitteilung muss auf einem dauerhaften Datenträger erfolgen.[301] Dabei sind unerhebliche Änderungen solche, die bloße Unannehmlichkeiten bereiten.[302] Ob eine erhebliche Änderung vorliegt, ist nach § 651g BGB anhand der wesentlichen Eigenschaften zu bestimmen, über die vorvertraglich informiert werden muss und die aus der Reisebestätigung ersichtlich sein müssen (im Reiserecht ist darunter v.a. der Hotelwechsel zu sehen).[303] Die Sicht des Reisenden ist nach BGH für die Beurteilung entscheidend, so dass bei Wegfall eines für den Reisenden ausschlaggebenden Reiseumstands für die Wahl der Reise der Reisende diesen Wegfall nicht hinzunehmen braucht.[304] Im Reiserecht ist überdies § 308 Nr. 4 BGB ausgeschlossen,

301 MüKo-BGB/Tonner § 651f Rn. 9, 20.
302 MüKo-BGB/Tonner § 651f Rn.21.
303 MüKo-BGB/Tonner § 651g Rn. 11, 12.
304 MüKo-BGB/Tonner § 651g Rn. 13.

so dass die Zumutbarkeit nicht ausschlaggebend ist, sondern vielmehr auf weitgehend objektive Kriterien abzustellen ist.[305]

3. Transfer

Auf die Änderungsbefugnis entsprechend angewandt folgt aus der Regelung, dass eine gravierende Anpassung eines für die Wahl des digitalen Produkts entscheidenden Umstands vom Verbraucher nicht hingenommen werden muss. Ein solch entscheidender Umstand müsste allerdings aus der Bestellbestätigung des digitalen Dienstes hervorgehen. Darunter könnte bspw. fallen, dass das Produkt eine besondere Funktionalität aufweist wie die sichere 2-Faktor-Identifizierung für einen sicherheitssensiblen Dienst, wie eine Online-Banking-Software.

VIII. Vertragsanpassung aufgrund unwesentlichen Irrtums: § 872 ABGB

1. Grund der Auswahl

Eine Vertragsanpassung aufgrund unwesentlichen Irrtums erfolgt aufgrund einer Änderung eines Nebenumstandes, so wie es auch bei der Änderungsbefugnis grundsätzlich bis zur absoluten Grenze möglich ist.

2. Gesetzlicher Regelungsinhalt

Eine Vertragsanpassung kann nach § 872 ABGB erfolgen, wenn der der Änderung zugrunde liegende Irrtum weder die Hauptsache noch eine wesentliche Beschaffenheit derselben, sondern einen Nebenumstand betrifft.[306] Die Fehlvorstellung bemisst sich nach dem Parteiwillen im Abschlusszeitpunkt, danach ist ein Irrtum „unwesentlich", wenn ein anderer Vertragsinhalt gewählt, der Vertrag jedoch trotzdem geschlossen worden wäre.[307] Nach § 922 Abs. 2 ABGB ist die Vertragsmäßigkeit einer Sache danach zu beurteilen, was über sie öffentlich in Werbung oder direkt vom Veräußerer geäußert wurde. Abzustellen ist auf den hypothetischen Parteiwillen oder

305 MüKo-BGB/Tonner § 651g Rn. 16.
306 ABGB-ON/Pletzer § 872 ABGB Rn. 4.
307 ABGB-ON/Pletzer § 872 ABGB Rn. 4.

sofern dieser nicht zu erforschen ist, auf die Verkehrsauffassung redlicher Parteien.[308] Es kommt darauf an, ob beide Parteien in Ansehung der wahren Lage die anderen Vertragsbedingungen akzeptieren würden.[309]

3. Transfer

Auf die der Arbeit zugrundeliegende Regelung gewendet, folgt aus dieser Norm, dass eine Anpassung in einem nicht zum Kernbereich der Leistung gehörenden Bereich geringeren Anforderungen unterworfen ist. Sofern die digitale Leistung in einer Nebenleistung verändert wird, ist das tolerabel, sofern der Vertrag ursprünglich mit der neuen Bedingung trotzdem geschlossen worden wäre. Dies wäre bspw. der Fall, wenn nachträglich die Benutzeroberfläche nicht mehr weiß-blau, sondern weiß-schwarz erscheinen würde.

IX. Kostenvoranschlag und Änderung: § 1170a ABGB

Die rechtlichen Rahmenbedingungen sind bei Kostenvoranschlag und Änderung ähnlich, auch ist weniger eine einzelne Änderung als vielmehr die Gesamtschau entscheidend.

1. Gesetzlicher Regelungsinhalt

Bei der Kostenüberschreitung eines unverbindlichen Kostenvoranschlags sind unbeträchtliche und unvermeidbare Steigerungen hinzunehmen; für die Beurteilung wird mit der Kündigung aus wichtigem Grund verglichen, wonach eine beträchtliche Überschreitung anzunehmen ist, sobald die Überschreitung dazu führt, dass es für den Bestellenden nicht zumutbar ist, an die Absprache gebunden zu sein.[310] Für die Beurteilung ist das Gesamtbild entscheidend, auch starke Steigerungen einzelner Posten können insgesamt als unbeträchtlich anzusehen sein.[311] Auch in diesem Fall muss der Unternehmer dem Bestellenden die beträchtliche Überschreitung bei

308 ABGB-ON/Pletzer § 872 ABGB Rn. 5.
309 ABGB-ON/Pletzer § 872 ABGB Rn. 6.
310 ABGB-ON/Kletečka § 1170a Rn. 13.
311 ABGB-ON/Kletečka § 1170a Rn. 14.

Unvermeidlichkeit unverzüglich anzeigen, wodurch er nicht mehr an den Kostenvoranschlag gebunden sein will. Der Bestellende erlangt ein Gestaltungsrecht: entweder Festhalten am Vertrag (mit Verpflichtung zum Tragen der Mehrkosten durch die Vertragsanpassung) oder Rücktritt; alternativ könnte er die Anzeige unterlassen und den bisherigen Kostenvoranschlag gegen sich gelten lassen.[312]

2. Transfer

Nach dem Telos der Regelung kommt es auf die Gesamtschau der Veränderungen an. Zwar ist der Kostenvoranschlag nur unverbindlich, insofern hat ein Verbraucher eines zweiseitig verpflichtenden IT-Vertrags eine höhere Schutzwürdigkeit. Jedoch sind die Interdependenzen groß und es gibt hier wie dort häufige Multikausalitäten, die eine Änderung bedingen. Die Rechtsfolgen sind denen der Änderungsbefugnis ähnlich: Rücktritt, Weiternutzung des Bisherigen oder aber Tragen der Änderung und Nutzung des Neuen.

X. Vertragsanpassung im Massengeschäft mit Verbrauchern

Im Massengeschäft mit Verbrauchern handelt es sich um eine ähnliche Konstellation wie bei IT-Verträgen, auch hier werden standardisierte Produkte an eine Vielzahl von Kunden ausgebracht.

1. Gesetzlicher Regelungsinhalt

In Bankverträgen, einem Massengeschäft in Form von Dauerschuldverhältnissen, sind Klauseln, die eine einseitige Leistungsänderung des Unternehmers ermöglichen, anhand von § 6 Abs. 2 Z. 3, Abs. 3 KSchG zu messen, der Geringfügigkeit und sachliche Rechtfertigung verlangt; durch diese inhaltlichen Schranken ist ein Interessenausgleich gewahrt.[313] Der Gesetzgeber gewährt dem Unternehmer daher die Möglichkeit, veränderte Rahmenbedingungen als Ausgangspunkt für eine Anpassung des Vertrags zu nehmen,

312 ABGB-ON/Kletečka § 1170a Rn. 27.
313 Riss, ÖBA 2014, 419, 420.

was sogar mittels AGB (eingeschränkte Willensfreiheit) und gegenüber Verbrauchern (besondere Schutzwürdigkeit) eingeräumt wird.[314] Der OGH geht bei der Beurteilung solcher Klauseln davon aus, dass diese im Rahmen einer vertraglichen Zustimmungsfiktion weitgehend auf eine „einseitige Änderungsbefugnis des Unternehmers hinausläuft".[315] Dabei geht er davon aus, dass eine Klausel gröblich benachteiligend iSv § 879 ABGB sei, sofern nicht ansatzweise eine Eingrenzung erkennbar sei, die den Verbraucher vor „Eintritt unangemessener Nachteile bei Änderungen des Vertrags" schützen würde, wobei die Klausel zusätzlich anhand der RL 93/13/EWG sowie deren nationaler Umsetzung in § 879 ABGB sowie § 6 Abs. 3 KSchG zu beurteilen sei.[316] Anhand von Art. 3 der Richtlinie sind missbräuchliche Klauseln solche, die entgegen dem Gebot von Treu und Glauben zum Nachteil des Verbrauchers ein erhebliches und ungerechtfertigtes Missverhältnis zu Lasten des Verbrauchers verursachen, wobei das bestehende Kräfteverhältnis zwischen den Parteien zu berücksichtigen ist.[317] Bereits in dieser RL hat die EWG / EU in Beispiel j) und k) des Anhangs Vertragsklauseln als missbräuchlich angesehen, die dem Unternehmer eine einseitige Änderung der Merkmale des zu liefernden Erzeugnisses ohne im Vertrag aufgeführten triftigen Grund ermöglichen.

2. Transfer

Der Verbraucher muss gegen unangemessene Nachteile bei Vertragsänderungen geschützt werden. Dabei ist die Anpassung aufgrund geänderter Rahmenbedingungen möglich. Eine unangemessene Benachteiligung läge vor, wenn ein Quasi-Monopolist plötzlich sämtliche bisher exklusiv vom Programm genutzten Spezial-Dateitypen nicht mehr unterstützt und auch keine Möglichkeit in Aussicht stellt, diese Dateien anderweitig nutzbar zu machen.

314 Riss, ÖBA 2014, 419, 420.
315 OGH 10 Ob 60/17x RIS 3.4.
316 OGH 8 Ob 105/20d, NFC-Klausel ist intransparent RIS Rn. 14, 18.
317 RL 93/13/EWG des Rates vom 5. April 1993 über mißbräuchliche Klauseln in Verbraucherverträgen28, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A31993L0013 (10. 9. 2022) Art. 3.

XI. Anwendung auf §§ 327r BGB, 27 VGG

Auf die Regelung der §§ 327r BGB, 27 VGG angewandt, ergibt sich daraus, dass es darauf ankommt, ob die vorvertraglich bekannten besonderen Eigenschaften des digitalen Produkts / der digitalen Dienstleistung für die Entscheidung des Verbrauchers zum Vertragsschluss wesentlich waren; auf die Zumutbarkeit der Änderung; sofern diese Änderung eher einen Nebenbestandteil der Leistung betrifft; ob der Unternehmer im Rahmen seiner wirtschaftlichen Gestaltungsmacht ohne Ausnutzung seiner Marktstellung gehandelt hat; ob die Parteiinteressen bei Vertragsschluss und wie sehr diese durch die Änderung beeinträchtigt sind; ob dem Nutzer durch die Änderung eine bloße Unannehmlichkeit entsteht. Für die Beurteilung ist nach der DID-RL nicht auf den einzelnen Nutzer abzustellen, sondern auf den durchschnittlichen, sodass es darauf ankommt, ob die Änderung eine hinreichende Vielzahl an Nutzern stören wird. Bei der Vertragsauslegung ist anhand eines objektiv systematischen und teleologischen Ansatzes vorzugehen,[318] der auch die o.g. objektiven Kriterien hinzuzieht.

E. Ein allgemein gültiger Maßstab

Einen allgemein gültigen Maßstab für die Erheblichkeitsschwelle herauszuarbeiten, erscheint angesichts der höchst unterschiedlichen angebotenen Software-Produkte, der jeweiligen Kunden und der Hersteller schwierig. Nichtsdestotrotz können aus Verfassersicht mehrere Punkte als besonders berücksichtigenswert herausgestellt werden: Art und Zweck der digitalen Produkte, Qualität, Funktionalität, Kompatibilität und andere wesentliche Merkmale sind zu berücksichtigen, daneben die übliche Beschaffenheit. Die zugrunde liegenden Verträge werden zwischen zwei Parteien geschlossen, die sowohl wirtschaftlich als auch aus Sicht des Gesetzgebers unterschiedliche Schutzniveaus haben. So ist der Unternehmer dazu gehalten, auf den Verbraucher Rücksicht zu nehmen und dieser hat zusätzlich ihn stärkende Rechte. Angesichts dessen lassen sich aus den obigen Beispielen folgende auf das Über-Unterordnungsverhältnis zwischen Unternehmer und Verbraucher anzuwendende Regelungsmaßstäbe herauskristallisieren. Zuerst ist das jeweilige Interesse des Durchschnittskunden und der Vertragsparteien bei Vertragsschluss heranzuziehen. Je nachdem, ob es sich

318 Schrank, ZAS 2019, 255, 256.

um eine Standard-Lösung oder ein kompliziertes Produkt für eine spezielle Zielgruppe (bspw. eine Software-Lösung für ambitionierte Hobby-Fotografen) handelt, ist auch der Nutzerkreis und seine Erwartung verschieden. Hier würde es genügen, wenn zumindest eine signifikante Zahl an Nutzern betroffen ist. Dies könnte anhand einer Prozentzahl festgemacht werden, bspw. 15–20 %. Interessenwahrend könnte auch eine Verbraucherschutzorganisation oder eine staatliche Behörde heranzuziehen sein, um zu beurteilen, ob die Signifikanz-Schwelle erreicht ist. Sodann ist zu beurteilen, ob der Unternehmer mit der Änderung im Rahmen seines unternehmerischen Gestaltungsspielraums im Hinblick auf das Durchschnitts-Verbraucher-Interesse gehandelt hat. Sofern er sich in diesem Rahmen bewegt, ist eine Änderung wohl rechtmäßig, sofern er seine Marktmacht nicht unbillig ausgenutzt hat (was bei großen IT-Unternehmen leicht der Fall sein kann, die in bestimmten Kategorien quasi Monopolisten sind, wie o.g. Microsoft; Google, oder Apple). Daneben ist auch darauf abzustellen, welchen Charakter der konkrete Einzelfall der Änderung im Gesamtzusammenhang der digitalen Leistung aufweist: Handelt es sich um eine bloß kosmetische Korrektur (bspw. die Änderung des Farbschemas oder wird die Benutzeroberfläche umgestaltet), um eine Veränderung des zugrunde liegenden Programmcodes, die Inkompatibilitäten nach sich ziehen kann oder aber um die Implementierung neuer Funktionalitäten, die der Nutzer zwar nicht begrüßt, aber auch nicht nutzen muss.

F. Handlungsbedarf für die Unternehmer

Anbietende Unternehmen müssen Vertragsdokumente sowie AGB für Kunden an neue gesetzliche Vorgaben anpassen, wobei auch die eigenen Lieferantenbeziehungen betroffen sind.[319] Durch die neuen Regelungen bestehen für die Kunden gesetzliche Kündigungsrechte sowie zu erfüllende Informationspflichten für die Unternehmen, um nicht diverse Rechte und Ansprüche der Kunden auszulösen.[320] Es erscheint sinnvoll, zumindest eine Zeitwahl zur Vornahme der Aktualisierung vorzusehen, damit der Verbraucher Vorkehrungen treffen kann.[321] Die Unternehmen sollten um-

319 Lunk/Meurer, BB 2022, 387, 394.
320 Lunk/Meurer, BB 2022, 387, 394.
321 Stabentheiner/Wendehorst/Zöchling-Jud Gewährleistungsrecht/Wendehorst 111, 125.

schreiben, was eine Aktualisierung zur Gebrauchstauglichkeitserhaltung beinhaltet sowie die Informationswege dokumentieren.[322] Dazu könnte auch anhand von klaren informativen Leistungsspezifikationen im Vorfeld des Vertragsschlusses der Erwartungshorizont des Abnehmers eingeordnet werden; durch Angaben zur Verwendung und Einsatz des Produkts kann die Vertragsmäßigkeit leichter kontrolliert werden.[323] Die Gestaltung der Werbung kann leicht eine Haftung für die Bereitstellung eines digitalen Produkts auslösen.[324] Problematisch scheint auch, nach mehreren Jahren eine Vertragsmäßigkeit der digitalen Inhalte zu beweisen.[325]

§ 10 Schluss

Durch die Änderungsbefugnis erhält der Unternehmer die Möglichkeit, sein digitales Produkt an die sich ständig ändernden Verhältnisse und Marktgegebenheiten anzupassen. Dadurch ist gerade bei langfristigen Verträgen über die Bereitstellung von Medien oder Programmen gewährleistet, dass das Produkt nicht mit der Zeit gegenüber neueren Konkurrenzprodukten immer weiter ins Hintertreffen gerät. Sowohl für den Unternehmer als auch den Verbraucher ergeben sich dadurch Mehrwerte: Der Unternehmer kann sein Produkt anpassen, ohne neue Verträge schließen zu müssen, der Verbraucher erhält nicht nur zum Vertragsbeginn ein aktuelles Produkt, sondern dieses wird auch während der Laufzeit an neue Gegebenheiten angepasst und er selbst bekommt die Änderungen handlich serviert. Andererseits ist er dem Unternehmer auch nicht ausgeliefert, da er bei gravierenden Änderungen ein außerordentliches Kündigungsrecht erhält. Es ist begrüßenswert, dass sich der Europäische Normengeber auf dieses Terrain vorgewagt und versucht hat, die im modernen Technikzeitalter mit seiner Software und Digitalisierungs-Fokussierung drängende Frage der Anpassung anzugehen. Problematisch bleibt, dass die Vielzahl der Anwendungsfälle sich kaum in einer einzelnen gesetzlichen Regelung fassen lassen. Es wird den Gerichten obliegen, die zukünftigen Problemstellungen zu beurteilen. Bereits heute erscheint problematisch, dass mit Referenzgruppen, Software, Hardware einfache Begriffe höchst unterschiedliche Gemengelagen beschreiben; so wird an ein Betriebssystem eine andere Lauf-

322 Schneider/Streitz, CR 2022, 141, 348.
323 Schneider/Streitz, CR 2022, 141, 144, 145.
324 Schöttle, MMR 2021, 683, 684.
325 Artz/Gsell Verbrauchervertragsrecht/Lehmann 19, 27.

zeitprognose gestellt werden, als an eine Steuersoftware für ein bestimmtes Steuerjahr, an einen Film eine andere als an eine App zu einem bestimmten Ereignis wie einer Weltmeisterschaft. Die notwendigen Vergleichsmaßstäbe zu etablieren und anzuwenden, wird ein Prozess sein. Für den Verfasser dieser Arbeit handelt es sich bei der Änderungsbefugnis des Unternehmers um ein Gestaltungsrecht. Es erscheint daher sinnvoll, die zu diesem Regelungskomplex bereits bekannten rechtlichen Aspekte und Wertungen auf das neue Änderungsrecht anzuwenden. Dabei haben sich über die Jahre verschiedene Möglichkeiten einer Kontrolle etabliert. Neben der schon angesprochenen gerichtlichen Kontrolle anhand Billigkeitserwägungen und der objektiven Parteiinteressen ist auch die Einschaltung einer eher neutralen Position wie der eines Treuhänders möglich. Hier gäbe es möglicherweise mit dem Beauftragten der Bundesregierung für Informationstechnik (BRD), der Staatssekretärin im Bundesministerium für Digitalisierung und Wirtschaftsstandort (RÖ) oder dem Sachverständigenrat für Verbraucherfragen Anlaufstellen, die Vorschläge erarbeiten könnten. Ansonsten bliebe auch die Möglichkeit, Schiedsstellen einzurichten (so gibt es bei der Bundesnetzagentur eine solche für Telefondienste). Auch wenn im IT-Bereich neue Geschäftsmodelle um sich greifen, so sind diese doch oft auf bekannte rechtliche Regelungen zurückführbar. Insofern scheint auch die Anwendung entsprechender Auslegungen sinnvoll, um die Einheitlichkeit der Rechtsordnung auch in der digitalen Welt zu gewährleisten.

Literaturverzeichnis

Adomeit, Gestaltungsrechte, Rechtsgeschäfte, Ansprüche. Zur Stellung der Privatautonomie im Rechtssystem (1969).

Badura, § 270 Verfassungsänderung, Verfassungswandel, Verfassungsgewohnheitsrecht, in *Isensee/Kirchhof* (Hrsg), Handbuch des Staatsrechts[3] (20XX-) 591.

Bischinger/Weber-Woisetschläger, Das neue Gewährleistungsrecht (Teil I). Verbrauchergewährleistungsgesetz (VGG): Anwendungsbereich und Gewährleistung beim Warenkauf, JAP 2021/2022, 104.

Bischinger/Weber-Woisetschläger, Das neue Gewährleistungsrecht (Teil II). Verbrauchergewährleistungsgesetz (VGG): Gewährleistung bei Bereitstellung digitaler Leistungen und Verjährung; Änderungen in ABGB und KSchG, JAP 2021/2022, 181.

Buchmann/Panfili, Das neue Schuldrecht 2022 (Teil I). Verbrauchervertrags- und Verbrauchsgüterkaufrecht bei digitalen Produkten – Zwei Regelungsregime im Vergleich, KuR 2022, 73.

Buchmann/Panfili, Das neue Schuldrecht 2022 (Teil II). Aktualisierungen bei digitalen Produkten und Waren mit digitalen Elementen, KuR 2022, 159–167.

Büdenbender, Neugestaltung von Preisanpassungsklauseln in Energielieferungsverträgen über Elektrizität und Gas, NJW 2013, 3601.

Datta, Die Haftung bei Verträgen über digitale Inhalte, in *Maute/Mackenrodt* (Hrsg), Recht als Infrastruktur für Innovation. GRUR Junge Wissenschaft, München 2018[1] (2019) 155–178.

Ehle/Kreß, Neues IT-Vertragsrecht für digitale Inhalte und Dienste gegenüber Verbrauchern. Subjektiv-Objektiver Mangelbegriff, Aktualisierungspflicht und Änderungsbefugnis, CR 2019, 723–731.

Ehricke, Die Kontrolle von einseitigen Preisfestsetzungen in Gaslieferungsverträgen, JZ 2005, 599–606.

EWG des Rates, RL 93/13/EWG des Rates vom 5. April 1993 über mißbräuchliche Klauseln in Verbraucherverträgen[28,] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A31993L0013 (10. 9. 2022).

Fida, Updates, Patches & Co. Zivilrechtliche Fragen zur Softwareaktualisierung.

Fischinger, § 11 Einseitige Leistungsbestimmung durch den Arbeitgeber, in *Kiel* (Hrsg), Münchener Handbuch zum Arbeitsrecht[5] (2021).

J. Flume, Digitale Leistungen, ÖJZ 2022, 137.

Grunewald/Maier-Reimer/Westermann, Bürgerliches Gesetzbuch. Kommentar mit Nebengesetzen (AGG, BVersTG, EGBGB, ErbbauRG, ProdhaftG, VBVG, VersAusglG, WEG – teils in Auszügen) und Internationalem Privatrecht – Erman/BGB[17] (2023).

Härting, Vertragsrecht, in *Härting* (Hrsg), Internetrecht[6] (2021).

Henssler, Münchener Kommentar zum Bürgerlichen Gesetzbuch Bd. 6: Schuldrecht – Besonderer Teil III §§ 631–704[8] (2020).

Herberger/Martinek/Rüßmann/Weth/Würdinger, juris-PK BGB[9] (2022).

Heydn, Schuldrechtsreform 2.0: Das neue Gewährleistungsrecht für digitale Produkte in der Praxis. Neue und altbekannte Rechtsbehelfe für Verbraucher und Unternehmen, CR 2021, 709–716.

Hilbert/López, The world's technological capacity to store, communicate, and compute information, Science (New York, N.Y.) 2011, 60–65.

Hornung, Grundrechtsinnovationen 239 (2015).

Hunzinger, Änderungsbefugnisse des Unternehmers nach § 327r BGB. Auslegung und Vertragsgestaltung im Lichte der AGB-Rechtsprechung (§ 327r BGB), CR 2022, 349–355.

Jaensch, Umsetzung der Richtlinien zu digitalen Inhalten und Diensten sowie zum Warenkauf. Teil 1: Verbraucherverträge über digitale Produkte, jM 2022, 96.

Kern, Anwendungsbereich der Warenkauf- und der Digitale Inhalte-RL, in *Stabentheiner/Wendehorst/Zöchling-Jud* (Hrsg), Das neue europäische Gewährleistungsrecht. Zu den Richtlinien (EU) 2019/771 über den Warenkauf sowie (EU) 2019/770 über digitale Inhalte und digitale Dienstleistungen (2019) 33.

Kletečka/Schauer, ABGB-ON.

Kodek, Änderung digitaler Inhalte und digitaler Dienstleistungen (Art 19 DIRL), in *Stabentheiner/Wendehorst/Zöchling-Jud* (Hrsg), Das neue europäische Gewährleistungsrecht. Zu den Richtlinien (EU) 2019/771 über den Warenkauf sowie (EU) 2019/770 über digitale Inhalte und digitale Dienstleistungen (2019) 141.

Kronthaler/J.W. Flume/Ziegler, § 1, in *Flume/Kronthaler/Laimer* (Hrsg), VGG – Verbrauchergewährleistungsgesetz (2022).

Krüger, Münchener Kommentar zum Bürgerlichen Gesetzbuch Bd. 3: Schuldrecht – Allgemeiner Teil II[9] (2022).

Kühner/Piltz, Die Updatepflicht für Unternehmen in Umsetzung der Digitale Inhalte Richtlinie. Der Regelungsmechanismus im Referentenentwurf des BMJV v. 3.11.2020 zur Umsetzung der Richtlinie 2019/770/EU, CR 2021, 1–7.

Legner, Eckpfeiler der Vertragsordnung im digitalen Wandel – beck-online, NJOZ 2022, 353.

Lehmann, Binnenkohärenz des europäischen Verbrauchervertragsrechts, in *Artz/Gsell* (Hrsg), Verbrauchervertragsrecht und digitaler Binnenmarkt. Die europäischen Richtlinienvorschläge zum Fernabsatz von Waren und zur Bereitstellung digitaler Inhalte (2018) 19.

Löwisch, J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen[2020] (2020).

Luhmann, Organisation und Entscheidung[2] (2006).

Lunk/Meurer, Digital und analog – Dringender Handlungsbedarf für Unternehmen durch neue BGB-Vorschriften, BB 2022, 387–395.

Maier, Die wichtigsten Inhalte im Überblick. Änderungen, Neuerungen, Versäumnisse, in *Stabentheiner/Wendehorst/Zöchling-Jud* (Hrsg), Das neue europäische Gewährleistungsrecht. Zu den Richtlinien (EU) 2019/771 über den Warenkauf sowie (EU) 2019/770 über digitale Inhalte und digitale Dienstleistungen (2019) 51.

Möllnitz, Änderungsbefugnis des Unternehmers bei digitalen Produkten. Auslegung und Folgen des § 327r BGB-RefE, MMR 2021, 116.

Müller-Graff, Kodifikationsgewinn durch Inkorporation des Inhalts von Schuldrechtsrichtlinien der EG in das BGB? GPR 2009, 106–121.

Parzmayr, § 27 VGG, in *Flume/Kronthaler/Laimer* (Hrsg), VGG – Verbrauchergewährleistungsgesetz (2022).

Paschke, Kapitel 4: Digitaler Handel, in *Heckmann/Paschke* (Hrsg), juris PraxisKommentar Internetrecht[7] (2021).

Redecker, § 548a BGB – neue Regelung zur Miete digitaler Produkte. Bedeutung, Geltungsbereich, Anwendungsbeispiele, ITRB 2022, 187–190.

Redecker, Beschaffenheitsvereinbarungen bei digitalen Produkten, insbesondere Software, ITRB 2022, 68–71.

Rieländer, Leistungsstörungen im Digitalvertragsrecht (Teil I). Zur Umsetzung der Digitale-Inhalte-Richtlinie im BGB, GPR 2021, 257.

Riss, Mechanismen der Vertragsanpassung im Massengeschäft mit Verbrauchern. Gedanken zu OGH 11. 4. 2013, 1 Ob 210/12g und OGH 29. 8. 2013, 2 Ob 131/12x, ÖBA 2014, 419.

Schellhase, Gesetzliche Rechte zur einseitigen Vertragsgestaltung 73 (2013).

Schmidt, Datenschutz und Big Data – Ein Spannungsverhältnis, in *Maute/Mackenrodt* (Hrsg), Recht als Infrastruktur für Innovation. GRUR Junge Wissenschaft, München 2018[1] (2019) 265.

Schmidt-Kessel/Erler/Grimm/Kramme, Die Richtlinienvorschläge der Kommission zu Digitalen Inhalten und Online-Handel – Teil 1, GPR 2016, 2.

Schneider, Die komplexe Mechanik der neuen Anforderungen im Mängelregime. Warum die Grenzen der Gleichrangigkeit gesetzlicher Leistungsanforderungen für das geschuldete Leistungsprofil so etwas wie „praktische Konkordanz" fordern, CR 2022, 1–9.

Schneider/Streitz, Umsetzung der neuen Anforderungen bei der Vertragsgestaltung Gestaltungsmöglichkeiten, Leistungsspezifikationen und Abwägungsmodell, CR 2022, 141–149.

Scholz, Gestaltungsrechte im Leistungsstörungsrecht 400 (2010).

Schöttle, Software als digitales Produkt. Was bringen die gesetzlichen Neuregelungen? MMR 2021, 683.

Schrank, Fehlerhafte Dienstverträge. Geltungserhaltende Reduktion oder Gesamt-Nichtigkeit fehler- oder lückenhafter Vertragsklauseln? ZAS 2019, 255.

Schwartze, Rechtsvergleichende Betrachtung, in *Flume/Kronthaler/Laimer* (Hrsg), VGG – Verbrauchergewährleistungsgesetz (2022).

Stabentheiner, Ein Überblick über das Gewährleistungsrichtlinien-Umsetzungsgesetz, VbR 2022 2021, 188.

Stabentheiner, Grundzüge des neuen Verbrauchergewährleistungsrechts, ÖJZ 2022, 99.

Stabentheiner, Was ist neu am neuen Gewährleistungsrecht? ÖJZ 2021, 965.

A. Staudinger/Artz, Neues Kaufrecht und Verträge über digitale Produkte. Einführung in das neue Recht[1] (2022).

Stiemerling, Die technische Perspektive zum neuen Produktmangelbegriff in § 327e BGB für digitale Produkte (§ 327e BGB), ITRB 2022, 64–67.

Wendehorst, Aktualisierungen und andere digitale Dauerleistungen. Das neue Gewährleistungsrecht auf dem Prüfstand, in *Stabentheiner/Wendehorst/Zöchling-Jud* (Hrsg), Das neue europäische Gewährleistungsrecht. Zu den Richtlinien (EU) 2019/771 über den Warenkauf sowie (EU) 2019/770 über digitale Inhalte und digitale Dienstleistungen (2019) 111.

Wendehorst, Die Digitalisierung und das BGB, NJW 2016, 2609.

Corporate Digital Responsibility im Kontext eines entstehenden Datenrechts

Darius Ruff[*]

§ 1 Einleitung[**]

Die fortschreitende Digitalisierung verändert die Gesellschaft und Wirtschaft tiefgreifend. Zentrale Treiber dieses Wandels sind digitale Technologien wie Big Data-Analysen, der Einsatz von künstlicher Intelligenz (KI) und Distributed Ledger-Technologien, die Vernetzung von Objekten (Internet der Dinge) und virtuelle Realitäten, Fortschritte in der Robotik sowie neue digitale Geschäftsmodelle. Im Zentrum stehen dabei das Erzeugen, Sammeln, Verarbeiten, Analysieren und Nutzen von Daten. Diese werden deshalb häufig als „Rohstoff" des 21. Jahrhunderts bezeichnet und sind Ausgangspunkt der digitalen Transformation und Ökonomie. Die Digitalisierung verändert das Zusammenleben und Wirtschaften, indem sich bestehende Geschäftsmodelle wandeln, neue Wertschöpfungsformen entstehen und Art und Weise der gesellschaftlichen und privaten Kommunikation beeinflusst werden. Chancen und Risiken der digitalen Transformation liegen hierbei nah beieinander.

Zentrale Akteure und Treiber dieser digitalen Transformation sind Unternehmen, die digitale Anwendungen einsetzen bzw. deren Entwicklung und Einsatz vorantreiben. Jenseits von rechtlichen Regelungen stellt sich die Frage, ob Unternehmen eine besondere unternehmerische Verantwortung für die Entwicklung und den Einsatz von digitalen Technologien

* Darius Ruff, LL.M.oec. ist wissenschaftlicher Mitarbeiter am Institut für Wirtschaftsrecht des Juristischen Bereichs der Martin-Luther-Universität Halle-Wittenberg. Er promoviert ebenda zur Corporate Digital Responsibility aus juristischer Perspektive. Grundlage dieses Beitrags ist eine wissenschaftliche Studienarbeit, die der Autor im November 2022 verfasste. Für die Betreuung der Arbeit und die Ermöglichung dieser Veröffentlichung dankt der Autor Frau Prof. Dr. Anne-Christin Mittwoch herzlichst. Für diese Veröffentlichung wurde der Text zum Stichtag 1.12.2023 aktualisiert.

** Die in diesem Beitrag verwendeten Personenbezeichnungen beziehen sich, soweit nicht anders kenntlich gemacht, gleichberechtigt auf alle Geschlechter. Der Beitrag bemüht sich um geschlechtsneutrale Formulierungen. Auf eine Doppelnennung wird zugunsten einer besseren Lesbarkeit verzichtet.

zukommt und welchen Inhalt diese Verantwortung hat. Die Rede ist von einer *Corporate Digital Responsibility* (kurz: CDR). Dieser vergleichsweise neue Verantwortungsterminus ist bislang vor allem in der wirtschaftswissenschaftlichen Literatur diskutiert worden, weshalb hier bereits vielfältige Analysen existieren. Juristische Betrachtungen von CDR sind dagegen noch rar, welches wohl auch dem Umstand geschuldet ist, dass es sich um eine grundsätzlich freiwillige Verantwortung von Unternehmen handelt. Diese Arbeit soll den juristischen Debattenbeitrag ausbauen und ins Blickfeld nehmen, in welchem bestehenden und zukünftigen Rechtsrahmen sich eine digitale Unternehmensverantwortung bewegt.

Hierzu soll CDR in einem ersten Schritt inhaltlich und akteursbezogen erörtert werden (§ 2). In einem zweiten Schritt wird digitale Unternehmensverantwortung im Lichte des aktuellen und sich entwickelnden digital- und datenrechtlichen Regulierungsrahmens untersucht (§ 3). Im Anschluss werden die Rolle der Corporate Digital Responsibility im Kontext eines entstehenden Datenrechts beleuchtet und mögliche zukünftige Wege einer rechtlichen Implementierung von CDR aufgezeigt (§ 4).

§ 2 Corporate Digital Responsibility

Der Begriff *Corporate Digital Responsibility* wird erstmals 2015 in einer Veröffentlichung der Unternehmensberatung Accenture[1] verwendet und lässt sich sinngemäß als „digitale Unternehmensverantwortung" oder „unternehmerische Digitalverantwortung"[2] übersetzen. Wichtig ist, dass nicht eine *digital wahrgenommene* Verantwortung eines Unternehmens gemeint ist, sondern seine (umfassende) und freiwillige Verantwortung für die Entwicklung, den Einsatz und die damit verbundenen Auswirkungen von digitalen Technologien und Anwendungen.[3] Im deutschen Raum wurde der CDR-Begriff ab 2018 durch die „CDR-Initiative" des Bundesministeriums für Justiz und Verbraucherschutz[4] geprägt. Die Initiative hat das Ziel,

1 Cooper/Siu/Wei, Corporate Digital Responsibility, 2015, S. 1; zur Genese des Begriffs auch Möslein FS Hopt, 2020, 805 (806).

2 Vgl. dazu https://csr-news.org/2018/06/20/corporate-digital-responsibility/ (Stand 1.12.2023).

3 Zu den Begriffsdefinitionen von Corporate Digital Responsibility → § 2 B.

4 Zur Corporate Digital Responsibility-Initiative, aktuell im Ressortbereich des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV), siehe den Webauftritt https://cdr-initiative.de (Stand 1.12.2023). An der

„digitale Verantwortung" branchenübergreifend in Unternehmen zu implementieren.[5] Die Dichte an wissenschaftlicher Literatur zu CDR nimmt – wohl auch vor diesem Hintergrund – seit 2018 stark zu. Da es sich bei CDR um ein vergleichsweise neues Konzept handelt, werden zunächst die Beweggründe für eine digitale Unternehmensverantwortung erörtert (A.). Nachfolgend werden aktuelle Begriffsdefinitionen vorgestellt (B.) und die CDR in den Kontext verwandter Konzepte eingeordnet, besonders der Corporate Social Responsibility und Digitalethik (C.). Schließlich werden die Handlungsformen, Akteure und die konkreten Inhalte der CDR dargelegt (D.).

A. CDR als freiwillige Unternehmensverantwortung

Eine wichtige Ausgangsfrage für eine freiwillige digitale Unternehmensverantwortung ist, aus welchen Gründen sich einerseits Unternehmen einer über den regulatorischen Rahmen hinausgehenden Verantwortung stellen und andererseits staatliche Initiativen freiwillige Verantwortungskonzepte entwickeln und fördern. Dies soll hier mit Fokus auf CDR-spezifische Beweggründe erfolgen.

Der verantwortungsvolle Umgang mit digitalen Technologien kann für Unternehmen in erster Linie betriebswirtschaftlich motiviert sein. So wird in einer nach außen kommunizierten, digitalen Unternehmensverantwortung regelmäßig ein Wettbewerbsvorteil für Unternehmen gesehen, weil diese eine Distinktion von Wettbewerbern ermögliche und deshalb letztendlich wirtschaftlich vorteilhaft sei.[6] Wettbewerbliche Distinktion ist dabei sowohl im nationalen wie auch im internationalen Zusammenhang denkbar. Im internationalen Rahmen wird in CDR deshalb auch die Chance für einen werteorientierten „europäischen Weg der Digitalisierung" gesehen,

CDR-Initiative nehmen mehrere große Unternehmen teil, ua die Otto Group, Zalando, Telefónica, Deutsche Telekom, ING DiBa und Barmer.

5 Vgl. dazu https://cdr-initiative.de/initiative (Stand 1.12.2023).

6 Diese Motivation wird durch eine Studie des Zentrum Digitalisierung.Bayern aus dem Jahr 2019 belegt, in der teilnehmende Unternehmen angaben, dass sie sich *„durch eine nach außen sichtbare ‚gelebte Verantwortung' eine Verbesserung ihrer Wettbewerbsposition"* erhoffen, vgl. Esselmann/Golle/Thiel/Brink, Corporate Digital Responsibility, 2020, S. 10; ebenfalls Cooper/Siu/Wei, Corporate Digital Responsibility, 2015, S. 4; Mueller Bus Inf Syst Eng 64 (2022), 689 (690); Möslein FS Hopt, 2020, 805 (808).

der sich vom liberalen, technikzentrierten Digitalisierungsverständnis in den USA bzw. dem restriktiven, staatszentrierten in China unterscheidet.[7]

Durch den verantwortungsvollen Umgang mit digitalen Technologien können Unternehmen das Vertrauen von Kunden und anderer Stakeholder (zB Mitarbeitende, Geschäftspartner) in das jeweilige Unternehmen bzw. seine (digitalen) Produkte und Dienstleistungen fördern.[8] Dies wird ua durch eine repräsentative Verbraucherbefragung in Deutschland aus dem Jahr 2021 belegt: In dieser gab nur etwa ein Drittel der Befragten an, dass der Umgang deutscher Unternehmen mit der Digitalisierung aktuell „eher oder sehr verantwortungsvoll" sei.[9] Zugleich gaben 70 % der Befragten an, dass ihnen die Übernahme einer digitalen Verantwortung durch Unternehmen „eher oder sehr wichtig" sei und einer noch größeren Mehrheit (78 %) war die Vertrauenswürdigkeit der Anbieter „eher oder sehr wichtig".[10] Die gelebte digitale Verantwortung eines Unternehmens und ein darauf aufbauendes Kundenvertrauen kann deshalb sowohl Unterscheidungsmerkmal zum Wettbewerb, als auch konstitutiv für den Erfolg eines Produkts oder einer Dienstleistung sein.[11] Wirtschaftliche Beweggründe können jedoch auch (vollständig) im Hintergrund stehen, wenn eine digitale Verantwortung aus ethischen und philanthropischen Überzeugungen der Unternehmensleitung bzw. der Mitarbeitenden wahrgenommen wird.[12]

Für staatliche Institutionen – zB bei der deutschen „CDR-Initiative" das Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) – ist die Förderung einer digitalen Unternehmensverantwortung von Interesse, weil einzelne Staaten nur bedingt in der

7 Esselmann/Golle/Thiel/Brink, Corporate Digital Responsibility, 2020, S. 10; Bertelsmann Stiftung Unternehmensverantwortung/Esselmann/Brink/Golle S. 249 (250); Noack ZHR 183 (2019), 105 (113).

8 Dörr Praxisleitfaden CDR S. 28ff.; Brandenburg/Waurick RDi 2023, 365f.; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13; Möslein FS Hopt, 2020, 805 (808); Bertelsmann Stiftung Unternehmensverantwortung/Kemmer S. 80 (83f.).

9 Kettner/Thorun, Corporate Digital Responsibility-Verbraucherbefragung, 2021, S. 4.

10 Kettner/Thorun, Corporate Digital Responsibility-Verbraucherbefragung, 2021, S. 4, 6; ähnlicher Befund bei einer Befragung im Jahr 2018, vgl. Thorun/Kettner/Merck, Ethik in der Digitalisierung, 2018, S. 2.

11 Esselmann/Golle/Thiel/Brink, Corporate Digital Responsibility, 2020, S. 8, 10; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13; ausführlich: Bertelsmann Stiftung Unternehmensverantwortung/Suchanek S. 17 (18f.); Bertelsmann Stiftung Unternehmensverantwortung/Kemmer S. 80 (83f.).

12 Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (17); Mueller Bus Inf Syst Eng 64 (2022), 689 (692); zurückhaltend Dürr ZGE 2021, 165 (168).

Lage sind, große Digitalunternehmen bzw. digitale Anwendungen effektiv zu regulieren.[13] Hierfür gibt es zwei zentrale Gründe: Digitale Anwendungen zeichnen sich einerseits durch ihre Ubiquität bzw. Non-Territorialität aus, sind also potentiell weltweit zeitlich und örtlich unbegrenzt nutzbar.[14] Andererseits sind diese durch eine hohe Entwicklungs- und Innovationsgeschwindigkeit geprägt.[15] Eine effektive staatliche Regulierung steht damit vor der Herausforderung, dass sich Regulierungssubjekte und -objekte schnell verändern und sich zudem regelmäßig nicht im unmittelbaren staatlichen Zugriffsbereich (sondern „im digitalen Raum") befinden. Insofern ist treffend, dass *„der gesellschaftliche Veränderungsprozess der Digitalisierung rechtliche Lücken [provoziert]"*.[16] In der Konsequenz gewinnen freiwillige Steuerungs- und Selbstregulierungsmechanismen an Bedeutung.[17]

B. Definition von Corporate Digital Responsibility

Bei CDR handelt es sich um ein neueres Konzept unternehmerischer Verantwortung, eine „offizielle" Definition existiert bislang nicht. Deshalb ist für die inhaltliche Bestimmung und Abgrenzung eine Begriffsdefinition essentiell. Daher werden zunächst verschiedene Definitionen von CDR vorgestellt, um daraus wichtige Wesensmerkmale von CDR abzuleiten.

Die „CDR-Initiative" des BMUV versteht unter CDR *„freiwillige unternehmerische Aktivitäten, die [...] über das heute gesetzlich Vorgeschriebene hinausgehen und die digitale Welt aktiv zum Vorteil der Gesellschaft mitgestalten."*[18] CDR könne insofern zu einer nachhaltigen Entwicklung beitragen und sei *„Teil einer umfassenden Unternehmensverantwortung."*[19] Letzteres greift auch die Definition des Nachhaltigkeitsnetzwerks der deutschen

13 Dürr ZGE 2021, 165 (171f.); Esselmann/Golle/Thiel/Brink, Corporate Digital Responsibility, 2020, S. 6; Hoffmann-Riem Recht im Sog der digitalen Transformation S. 79ff., 124; zur Rolle von digitalen Plattformen als private Gesetzgeber: Schweitzer ZEuP 2019, 1 (4ff.).

14 Boehme-Neßler Unscharfes Recht S. 102ff., 112ff.; Dürr ZGE 2021, 165 (171); Esselmann/Golle/Thiel/Brink, Corporate Digital Responsibility, 2020, S. 6.

15 Dörr Praxisleitfaden CDR S. 9f.; Dürr ZGE 2021, 165 (171f.); Lobschat et al. Journal of Business Research 122 (2021), 875 (876).

16 So Dürr ZGE 2021, 165 (171).

17 Dürr ZGE 2021, 165 (171); ausführlich: Hoffmann-Riem Recht im Sog der digitalen Transformation S. 124ff., zu den Handlungsformen im Einzelnen → § 2 D. I.

18 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 2.

19 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 2.

Wirtschaft auf, laut dem CDR *„ein Teil der unternehmerischen Verantwortung [ist], welcher die Auswirkungen der digitalen Transformation auf Umwelt, Gesellschaft und Wirtschaft berücksichtigt."*[20] Diese Betrachtungstrias nennen auch andere, die CDR als *„eine Reihe von Praktiken und Verhaltensweisen, die einem Unternehmen helfen, Daten und digitale Technologien auf eine Weise zu nutzen, die als sozial, wirtschaftlich und ökologisch verantwortungsvoll wahrgenommen wird"*, definieren.[21] In weiteren Definitionen wird eine ethische Dimension eingeführt, wenn CDR als *„eine Erweiterung der Verantwortung eines Unternehmens, die die ethischen Chancen und Herausforderungen der Digitalisierung berücksichtigt"*[22] beschrieben wird. Auch der Bundesverband der Digitalwirtschaft (BVDW) greift dies auf und definiert CDR als *„freiwilligen Beitrag der Wirtschaft zu einer ethischen und nachhaltigen digitalen Entwicklung. [...] Ein wesentlicher Bestandteil der CDR ist die wertebasierte Auseinandersetzung mit positiven und negativen sowie direkten und indirekten Auswirkungen des Einsatzes digitaler Technologien."*[23] Nach dem Rahmenwerk „CDR Building Bloxx" des BVDW befasst sich CDR *„mit der Rolle unternehmerischer Verantwortung in einer zunehmend digitalisierten Welt"* und geht *„dabei oft über bestehende regulatorische Anforderungen hinaus und erforder[t] proaktive Selbstverpflichtungsmaßnahmen."*[24]

Die Definitionen zeigen, dass es sich bei CDR (noch) um einen weiten und pluriformen Begriff handelt, den unterschiedliche Akteure verschiedenartig ausfüllen und „betonen".[25] Dennoch wiederholen sich in den Defi-

20 Econsense, Umsetzung digitaler Verantwortung in Unternehmen, 2020, S. 8.

21 Internationales CDR Manifesto, vgl. dazu https://corporatedigitalresponsibility.net/cdr-definition-german (Stand 1.12.2023).

22 Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (17) [Übersetzung des Verfassers aus dem Englischen].

23 Vgl. dazu https://www.bvdw.org/der-bvdw/gremien/corporate-digital-responsibility/cdr-building-bloxx/ (Stand 15.11.2022).

24 Vgl. dazu https://www.cdr-building-bloxx.com/corporate-digital-responsibility/ (Stand 1.12.2023).

25 Diesen Befund teilen auch Dörr Praxisleitfaden CDR S. 38; Brandenburg/Waurick RDi 2023, 365; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (16f.) mit einer Übersicht über weitere Definitionen; Lobschat et al. Journal of Business Research 122 (2021), 875 (886); Panzer-Heemeier/Nemat CCZ 2022, 223 (227); Mueller Bus Inf Syst Eng 64 (2022), 689 (692); Hamadi/Manzo, Corporate Digital Responsibility, 2021, S. 10ff.; Panzer-Heemeier/Nemat/Meckenstock ESG 2022, 104 (106); laut Möslein FS Hopt, 2020, 805 (812) hat CDR aufgrund seiner Datenbezogenheit bereits eine „Kontur".

nitionen charakteristische Merkmale, die zu einer Begriffstopoi zusammengefasst werden können und aus der sich der Kern der CDR ableiten lässt:

- Es handelt sich um grundsätzlich freiwillige Unternehmensverantwortung.
- Die Verantwortung umfasst die (strikte) Einhaltung der gesetzlichen Vorgaben, geht aber inhaltlich über das gesetzlich vorgeschriebene hinaus.
- Die Verantwortung betrifft Digitalisierungsprozesse, insb. die Entwicklung und den Einsatz von digitalen Technologien in Unternehmen und deren Auswirkungen ggü. Stakeholdern und im gesellschaftlichen Kontext.
- Es werden die wirtschaftlichen, sozialen und ökologischen Auswirkungen von digitalen Technologien in den Blick genommen, weshalb CDR einen engen Bezug zu Nachhaltigkeitszielen hat.
- Im Fokus steht eine ethisch-moralische, wertorientierte Betrachtung des Unternehmenshandelns und dessen (Weiter-)Entwicklung.
- Die Digitalverantwortung ist eingebettet in einen breiteren Zusammenhang gesellschaftlicher Unternehmensverantwortung, namentlich Corporate Responsibility bzw. Corporate Social Responsibility (CSR).

Aus den letzten zwei Merkmalen geht hervor, dass CDR bestehende Konzepte der (Digital-)Ethik und andere Formen der unternehmerischen Verantwortung aufgreift. Daraus folgt die Frage, in welcher Beziehung die CDR zu diesen Konzepten steht.

C. Konzeptuelle Hintergründe

Zu diesem Zweck wird CDR in den Kontext der gesellschaftlichen Unternehmensverantwortung (I.) und der digitalen Ethik (II.) eingeordnet.

I. Corporate Social Responsibility (CSR)

Im Zuge von veränderten Erwartungen der Gesellschaft an Unternehmen entwickelte sich in den letzten Jahrzehnten sukzessive das Konzept der

CSR.[26] Auch wenn bis heute keine einheitliche Definition existiert,[27] handelt es sich laut der Europäischen Kommission bei der CSR um ein *„Konzept, das den Unternehmen als Grundlage dient, auf freiwilliger Basis soziale Belange und Umweltbelange in ihre Unternehmenstätigkeit und in die Wechselbeziehungen mit den Stakeholdern zu integrieren*“,[28] bzw. nach neuerer und erweiterter Definition *„die Verantwortung von Unternehmen für ihre Auswirkungen auf die Gesellschaft*“.[29] Mit dem Begriff eng verbunden ist das Prinzip der Nachhaltigkeit bzw. des nachhaltigen Wirtschaftens.[30]

Als grundsätzlich freiwilliges Verantwortungsformat wurde CSR zunächst durch unverbindliche Instrumentarien eingefasst, denen sich Unternehmen anschließen konnten.[31] Hierzu gehören ua der UN Global Compact,[32] die OECD-Leitsätze für multinationale Unternehmen[33] oder Standards der Internationalen Arbeitsorganisation[34]. Im jüngeren Verlauf wurden Inhalte der CSR in rechtliche Regelungen überführt, so zB 2014 in der EU-Richtlinie über nichtfinanzielle Berichterstattung.[35] In der Folge

26 Zur Genese verschiedener CSR-Konzeptionen ausführlich Spießhofer Unternehmerische Verantwortung S. 54ff.; mit einer rechtlichen Betrachtung Mittwoch Nachhaltigkeit und Unternehmensrecht S. 165ff.

27 Mittwoch Nachhaltigkeit und Unternehmensrecht S. 164 mwN; Spießhofer Unternehmerische Verantwortung S. 27ff. mit diversen CSR-Definitionen.

28 Definition der EU-Kommission von 2001, vgl. Grünbuch Europäische Rahmenbedingungen für die soziale Verantwortung der Unternehmen vom 18.7.2001, KOM(2001) 366 endgültig, 7.

29 Definition der EU-Kommission von 2011, vgl. Eine neue EU-Strategie (2011–14) für die soziale Verantwortung der Unternehmen (CSR) vom 25.10.2011, KOM(2011) 681 endgültig, 7.

30 Mittwoch Nachhaltigkeit und Unternehmensrecht S. 163f.; Teicke CCZ 2018, 274; ebenso die CSR-Initiative des Bundesministeriums für Arbeit und Soziales, vgl. dazu: https://www.csr-in-deutschland.de/DE/CSR-Allgemein/CSR-Grundlagen/csr-grundlagen.html (Stand 1.12.2023).

31 Teicke CCZ 2018, 274; Mittwoch Nachhaltigkeit und Unternehmensrecht S. 167ff.

32 Der UN Global Compact ist eine weltweite Initiative für verantwortungsvolle Unternehmensführung in den Bereichen Menschenrechte, Arbeit, Umwelt und Korruptionsbekämpfung, vgl. dazu https://www.unglobalcompact.org/what-is-gc (Stand 1.12.2023).

33 Die OECD-Leitsätze bieten umfassende Verhaltensregeln zur Förderung von verantwortungsvoller Unternehmensführung, vgl. dazu https://doi.org/10.1787/9789264122352-de (Stand 1.12.2023).

34 So ua die Kernarbeitsnormen der Internationalen Arbeitsorganisation, vgl. dazu https://www.ilo.org/berlin/arbeits-und-standards/kernarbeitsnormen/lang--de/index.htm (Stand 1.12.2023).

35 RL 2014/95/EU; die Richtlinie wurde in Deutschland umgesetzt mit dem Gesetz zur Stärkung der nichtfinanziellen Berichterstattung der Unternehmen in

sind heute bestimmte Unternehmen zu nichtfinanziellen Erklärungen über Umwelt-, Arbeitnehmer- und Sozialbelange sowie zu Menschenrechten und zur Korruptionsbekämpfung verpflichtet, vgl. § 289b und § 289c HGB. Auch mit Blick auf die neue EU-Richtlinie zur Nachhaltigkeitsberichterstattung von Unternehmen aus dem Jahr 2022 ist das CSR-Konzept von einer weiteren Verrechtlichung geprägt.[36]

Gemeinsam ist CDR und CSR die Verantwortung von Unternehmen für gesellschaftlich eingeforderte, gemeinwohlorientierte Belange und die Aufnahme von Verantwortungsdimensionen, die neue gesellschaftliche Problemfelder bzw. Modernisierungsfolgen betreffen (ökologische wie digitale Transformation). Anders als bei CDR handelt es sich bei CSR aber um ein bereits gewachsenes und institutionalisiertes Konzept. Es stellt sich folglich die Frage, welcher Zusammenhang zwischen CDR und CSR besteht und weshalb mit CDR ein eigenes Verantwortungsformat etabliert wird.

Die Notwendigkeit eines neuen, erweiterten Verantwortungsformats als CDR wird insb. mit den besonderen Herausforderungen und Charakteristika der digitalen Transformation und Technologien begründet.[37] Diese soll CDR explizit und fokussiert adressieren und die klassischen drei Perspektiven der CSR (wirtschaftlich, sozial, ökologisch) erweitern.[38] Es besteht dabei weitgehend Konsens, dass CDR strukturell und konzeptionell ähnlich zur CSR ist und Schnittmengen bestehen.[39] Uneinigkeit besteht jedoch darüber, inwieweit CDR als spezieller Bestandteil oder als eigenständiges Konzept neben CSR zu betrachten ist. So wird teilweise argumentiert,

---

ihren Lage- und Konzernlageberichten (CSR-Richtlinie-Umsetzungsgesetz) vom 11.4.2017 (BGBl. I 802); Verweise auf CSR finden sich in Erwägungsgrund Nr. 3 RL 2014/95/EU und BT-Drs. 18/9982, 26; insgesamt dazu Mittwoch Nachhaltigkeit und Unternehmensrecht S. 165f., 180ff.; Spießhofer Unternehmerische Verantwortung S. 277f.; Panzer-Heemeier/Nemat CCZ 2022, 223 (224f.); Spießhofer NZG 2018, 441 (443, 445); Teicke CCZ 2018, 274 (275).

36 RL (EU) 2022/2464; vgl. Mittwoch Nachhaltigkeit und Unternehmensrecht S. 184f.

37 Dürr ZGE 2021, 165 (172f.); Lobschat et al. Journal of Business Research 122 (2021), 875 (876); Mihale-Wilson et al. Bus Inf Syst Eng 64 (2022), 127 (128); eine umfangreiche Quellenübersicht gibt es bei Hamadi/Manzo, Corporate Digital Responsibility, 2021, S. 23ff.

38 Dörr Praxisleitfaden CDR S. 39; Dürr ZGE 2021, 165 (172f.); so auch die CSR-Initiative des Bundesministeriums für Arbeit und Soziales, vgl. dazu https://www.csr-in-deutschland.de/DE/CSR-Allgemein/Corporate-Digital-Responsibility/corporate-digital-responsibility.html (Stand 1.12.2023); zu den Wechselwirkungen von Digitalisierung und Nachhaltigkeit vgl. Mittwoch JZ 2023, 376 (381ff.).

39 Vgl. Lobschat et al. Journal of Business Research 122 (2021), 875 (876); Mihale-Wilson et al. Bus Inf Syst Eng 64 (2022), 127 (129).

dass CDR aufgrund der Besonderheiten der Digitalisierung ausdrücklich getrennt von CSR betrachtet werden müsse.[40] Demgegenüber erweitern andere Autoren CSR um Digitalisierungsthemen (letzteres als „CDR"), zB indem das dreigliedrige CSR-Modell für wirtschaftliche, soziale und ökologische Belange um eine vierte Dimension des „digitalen" ergänzt wird.[41] Vorzugswürdig erscheint jedoch eine integrierte Betrachtung, in der die Verantwortung für wirtschaftliche, soziale und ökologische Belange einerseits auf analoge, andererseits auf digitale Handlungsfelder (CDR) bezogen erfolgt.[42] Diese spiegelt richtigerweise wider, dass die Auswirkungen der Digitalisierung gerade die drei Perspektiven – wirtschaftlich, sozial, ökologisch – betreffen und sich in diese einordnen lassen. Zudem widerspräche die Abtrennung des „Digitalen" der fortschreitenden Integration von analoger und digitaler Welt.[43] Gleichermaßen spricht der CDR-Kodex von CDR als *„Teil einer umfassenden Unternehmensverantwortung."*[44]

Die genaue Abgrenzung muss für die vorliegende Themenfrage nicht entschieden werden und ist aufgrund des geringen Konkretisierungsgrads der CDR aktuell noch schwierig. Dennoch handelt es sich dabei zukünftig nicht nur um eine begriffliche Kontroverse, sondern um eine relevante Frage: Betrachtet man CDR als integriertes bzw. spezielles Konzept der CSR könnten oder müssten CDR-Thematiken (auch) über das „Vehikel" der CSR zur Anwendung gebracht werden. Geht man dagegen von einem eigenständigen Konzept aus, könnten Digitalisierungsthemen unter Umständen aus einer klassischen CSR-Betrachtung herausfallen. Dies kann zB mit Blick auf Pflichten zur nichtfinanziellen Berichterstattung von Unternehmen zukünftig zu einer (rechtlich) relevanten Unterscheidung führen. Zu denken ist an die Berichterstattungspflichten in § 289c HGB oder aus der europäischen Richtlinie zur Unternehmens-Nachhaltigkeitsbericht-

40 Lobschat et al. Journal of Business Research 122 (2021), 875 (876); wohl ebenfalls Mihale-Wilson et al. Bus Inf Syst Eng 64 (2022), 127 (128).

41 Esselmann/Golle/Thiel/Brink, Corporate Digital Responsibility, 2020, S. 5; auch Thorun/Kettner/Merck, Ethik in der Digitalisierung, 2018, S. 2.

42 So auch Dörr Praxisleitfaden CDR S. 39f.; Herden et al. NachhaltigkeitsManagement-Forum 29 (2021), 13 (14); Bertelsmann Stiftung Unternehmensverantwortung/Kemmer S. 80 (81).

43 Dörr hebt hervor, dass sich die „Wirkungen digitalen Handelns" auch in der physischen Welt niederschlagen können und eine Wechselbeziehung zwischen digitaler und analoger Welt besteht, vgl. Dörr Praxisleitfaden CDR S. 39.

44 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 2.

erstattung, die aktuell aber beide keine Unterscheidung zwischen digitalem und physischem Unternehmenshandeln treffen.[45]

Es lässt sich festhalten, dass CDR sowohl inhaltlich als auch konzeptionell deutliche Verbindungen zur CSR aufweist. Durch die Fokussierung auf digitale Technologien und ihre Auswirkungen werden mit CDR themen- und verantwortungsspezifische Problemfelder adressiert und für diese ein eigenständiger unternehmerischer Handlungsrahmen geschaffen. Strategisch gesehen ist eine ganzheitliche Unternehmensverantwortung, die klassische CSR und CDR-Themen verbindet, sicher erstrebenswert. Dies folgt aus praktischen Überlegungen zur Integration in Managementaufgaben und Unternehmensstrukturen, bei denen parallele Verantwortungskonzepte Zielkonflikte verursachen und die Integration erschweren können. Zudem kann die Verteilung von Verantwortung auf mehrere Funktionsstellen zu einer diffusen Verantwortungsfestlegung führen und die internen Transaktionskosten erhöhen. Auf der anderen Seite ist jedoch auch das konkrete Betätigungsfeld des Unternehmens zu betrachten: Für ausgeprägt digital getriebene Unternehmen sollte digitale Verantwortung sowohl zentral-integriert wie auch dezentral-prozessbezogen implementiert werden,[46] wohingegen bei weniger digitalisierten Unternehmen eine zentral-integrierte Verantwortung notwendige Anforderungen erfüllen sollte.

II. Digitale Ethik

Corporate Digital Responsibility hat weiterhin starke konzeptionelle Wurzeln in der digitalen Ethik bzw. Datenethik.[47] Die Daten- bzw. Digitalethik

45 RL (EU) 2022/2464; zu CDR und der nichtfinanziellen Berichterstattung Merbecks BB 2021, 2159 (2161ff.) und Brandenburg/Waurick RDi 2023, 365 (367); auch in der aktuellen Fassung der Empfehlungen der Regierungskommission Deutscher Corporate Governance Kodex (DCGK) vom 28.04.2022, zu denen sich börsennotierte Gesellschaften gemäß § 161 AktG erklären müssen, gibt es keine Bezugnahme auf eine digitale Verantwortung, vgl. dazu https://www.dcgk.de//files/dcgk/usercontent/de/download/kodex/220627_Deutscher_Corporate_Governance_Kodex_2022.pdf (Stand 1.12.2023); dazu Möslein FS Hopt, 2020, 805 (819); zur perspektivischen Aufnahme von CDR in den DCGK Noack ZHR 183 (2019), 105 (113).

46 In diese Richtung auch Pauly/Wichert DB-Beil. Heft 21/2023, 44; Mihale-Wilson et al. Bus Inf Syst Eng 64 (2022), 127 (129) grenzt die Perspektiven von CSR und CDR ua daran ab, ob es um untechnisch-strategische Managemententscheidungen oder konkretere (informations)technische Gestaltungen und Best Practices geht.

47 Vgl. Bahreini/Charton/Lukas RDi 2021, 548 (549); Bertelsmann Stiftung Unternehmensverantwortung/Esselmann/Brink/Golle S. 249 (250); Lobschat et al. Journal of

untersucht und bewertet *„moralische Probleme im Zusammenhang mit Daten [...], Algorithmen [...] und entsprechenden Praktiken (einschließlich verantwortungsvoller Innovation, Programmierung, Hacking und Berufskodizes), um moralisch richtige Lösungen [...] zu formulieren und zu unterstützen.“*[48]

Als zentraler Überschneidungspunkt von digitaler Ethik und CDR ergibt sich folglich der Betrachtungsgegenstand, also Daten, Algorithmen und dazugehörige (Unternehmens-)Praktiken sowie die in Bezug darauf formulierten Sollens-Sätze. Des Weiteren sind ethisch-moralische Überlegungen ein anerkannter Maßstab, um Verhalten und Handlungen zu bewerten. Somit können ethisch-moralische Überlegungen relativ unproblematisch zur Entwicklung, Argumentation und Legitimation von handlungsleitenden Sollens-Sätzen (einer CDR) herangezogen werden, auch in Ermangelung oder jenseits von rechtlichen Sollens- und Müssens-Sätzen.[49] Diese inhärente Verbindung von digitaler Verantwortung und digitaler Ethik spiegelt sich in den og Definitionen von CDR und in der Literatur wider.[50] Der CDR-Kodex ist ebenfalls von einer Wert- und Prinzipienorientierung geprägt, die zielsetzungs- und handlungsleitend sein soll und ua auf eine Menschzentrierung, Autonomie, Fairness und Transparenz aufbaut.[51]

Business Research 122 (2021), 875 (876, 879); Mueller Bus Inf Syst Eng 64 (2022), 689 (690f.); Panzer-Heemeier/Nemat/Meckenstock ESG 2022, 104 (106); Thorun/Kettner/Merck, Ethik in der Digitalisierung, 2018, S. 2f.; ausführlich: Dörr Praxisleitfaden CDR S. 30ff.; zu ethischen Fragen der Digitalisierung und insofern Anwendungsbereichen der digitalen Ethik: Schliesky NJW 2019, 3692 (3695ff.).

48 Floridi/Taddeo Phil. Trans. R. Soc A 374 (2016), 20160360 S. 3 [Übersetzung des Verfassers aus dem Englischen]; die digitale Ethik bzw. Datenethik baut ihrerseits wieder auf der Computer- und Informationsethik auf, vgl. Floridi/Taddeo Phil. Trans. R. Soc A 374 (2016), 20160360 S. 2f.

49 Panzer-Heemeier/Nemat CCZ 2022, 223 (227); für Bahreini/Charton/Lukas RDi 2021, 548 (548f.) geht der Inhalt von digital-ethischen Leitlinien in Unternehmen über rechtliche Inhalte hinaus bzw. können diese rechtliche Lücken füllen; zum Verhältnis von Recht und Ethik siehe Schliesky NJW 2019, 3692 (3694f.).

50 Vgl. Bahreini/Charton/Lukas RDi 2021, 548 (549); Bertelsmann Stiftung Unternehmensverantwortung/Esselmann/Brink/Golle S. 249 (250); Lobschat et al. Journal of Business Research 122 (2021), 875 (876, 879); Mueller Bus Inf Syst Eng 64 (2022), 689 (690f.); Panzer-Heemeier/Nemat/Meckenstock ESG 2022, 104 (106); Thorun/Kettner/Merck, Ethik in der Digitalisierung, 2018, S. 2f.; ausführlich: Dörr Praxisleitfaden CDR S. 30ff.; zu ethischen Fragen der Digitalisierung und insofern Anwendungsbereichen der digitalen Ethik: Schliesky NJW 2019, 3692 (3695ff.).

51 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 3; dazu Möslein FS Hopt, 2020, 805 (809f.).

CDR greift also zu ihrer inhaltlichen Ausrichtung und Gestaltung auf digital- bzw. datenethische Normen und Diskurse zurück. Dies zeigt, dass es sich bei CDR um ein interdisziplinäres Konzept an der Schnittstelle von unternehmerischer Verantwortung und digitaler Ethik handelt. Die Wert- bzw. Prinzipienorientierung ist dabei von großer Wichtigkeit. Zum einen gibt diese einer digitalen Unternehmensverantwortung einen normativen und legitimierenden Unterbau und zum anderen erleichtert dieser Rahmen die praktische Formulierung von kohärenten und konkreten Handlungszielen.[52]

D. Handlungsformen, Akteure und Handlungsfelder

Gleichermaßen vielfältig wie die Definitionen von CDR ist die Quellenlandschaft für ihre konkreten Inhalte. Im Folgenden wird daher zunächst beleuchtet, welche Handlungsformen abseits von hoheitlicher Rechtssetzung für CDR zur Verfügung stehen (I.). In einem zweiten Schritt werden konkrete Akteure der CDR und ihre Handlungsformen vorgestellt (II.). Daran anschließend werden die Handlungsfelder der CDR konkretisiert (III.).

I. Handlungsformen nicht-hoheitlicher Normsetzung

Einer freiwilligen Normsetzung iRd Corporate Digital Responsibility liegen inhärent andere Handlungsformen zugrunde als hoheitlicher Normsetzung, die zuvorderst durch Gesetze und Verordnungen bzw. auf EU-Ebene durch Richtlinien und Verordnungen erfolgt → § 3. Davon unterscheiden sich die Erscheinungsformen von privater Regelsetzung.[53]

Im Bereich der Selbstregelung entwickeln die Akteure eigene Verhaltensregeln (etwa Selbstverpflichtungen oder Verhaltenskodizes), die ihre Geltung typischerweise nur im eigenen Wirkungskreis des jeweiligen Akteurs entfalten.[54] Demgegenüber wirkt die (gesellschaftliche) Selbstregulierung über den einzelnen regelsetzenden Akteur hinaus, weil auch andere Perso-

52 Schliesky NJW 2019, 3692 (3697).

53 Dazu Hoffmann-Riem Recht im Sog der digitalen Transformation S. 114ff.; spezifisch für CDR siehe Dürr ZGE 2021, 165 (173ff.).

54 Hoffmann-Riem Recht im Sog der digitalen Transformation S. 114, 116ff.; zur Rolle von digitalen Plattformen als private Gesetzgeber Schweitzer ZEuP 2019, 1 (4ff.).

nen die gesetzten Regeln für sich anerkennen.[55] Hierzu können zB technische Standards oder Verhaltenskodizes von Verbänden gehören, deren Missachtung mit einem Nachteil für den Abweichenden verbunden ist.[56] Schließlich kann eine Koregulierung vorliegen, wenn hoheitliche Stellen an der Gestaltung und Implementierung von selbstregulativ zustande gekommene Regeln mitwirken.[57] Im Folgenden wird sich zeigen, dass CDR in den verschiedenen Spielarten privater Regelsetzung in Erscheinung tritt.

II. Akteure der CDR und ihre Handlungsformen

1. Unternehmen

Als zentrale Akteure von CDR sind in erster Linie (große) Unternehmen zu nennen, sie sind Treiber und Adressaten zugleich. In ihrer Adressatenrolle geht es für Unternehmen zentral um die Frage, *wie* sie digitale Verantwortung übernehmen – welchen Inhalt hat die eigene Verantwortung, wie wird diese im Unternehmen implementiert und mit welchem Verbindlichkeitsgrad? Im Unternehmen lässt sich CDR grob auf drei Ebenen einordnen und realisieren.[58]

Zunächst geht es um die übergeordnete Bestimmung, welche grundsätzlichen Werte, Ziele und Strategien das Unternehmen leiten sollen.[59] Hierzu gehören interne Strategien und Leitlinien, aktuell meist für KI-Anwendungen oder Datenethik.[60] Diese müssen dann in einer zweiten Stufe in kon-

55 Hoffmann-Riem Recht im Sog der digitalen Transformation S. 114, 118f.; teilweise wird in diesem Zusammenhang auch von Soft Law gesprochen, so Dürr ZGE 2021, 165 (176).

56 Hoffmann-Riem Recht im Sog der digitalen Transformation S. 118f.; Dürr ZGE 2021, 165 (176).

57 Hoffmann-Riem Recht im Sog der digitalen Transformation S. 115, 119f., weitere Begriffe sind „hybride Regulierung" oder „regulierte Selbstregulierung"; dazu ebenfalls Dürr ZGE 2021, 165 (174f.).

58 So Lobschat et al. Journal of Business Research 122 (2021), 875 (880ff.); ähnlich Esselmann/Brink Ökologisches Wirtschaften 33, 2 (2020), 11 (12).

59 Lobschat et al. Journal of Business Research 122 (2021), 875 (880).

60 Siehe zB Deutsche Telekom, Leitlinien für Künstliche Intelligenz, 2018, vgl. dazu https://www.telekom.com/resource/blob/544508/ca70d6697d35ba60fbcb29aeef4529e8/dl-181008-digitale-ethik-data.pdf; Telefónica S.A., Principles of Artificial Intelligence, 2018, vgl. dazu https://www.telefonica.com/en/wp-content/uploads/sites/5/2021/08/ia-responsible-governance.pdf; Merck KGaA, Code of Digital Ethics, 2021, zu letzterem ausführlich Bahreini/Charton/Lukas RDi 2021, 548 (549); Bosch, KI-Kodex, 2020, vgl. dazu https://www.bosch.com/de/stories/ethische-leitlinien-fu

krete Normen übersetzt werden, um für den Einzelnen und die Anwendung im Unternehmen handhabbar zu werden.[61] Auf einer dritten Ebene zeigt sich die übernommene Verantwortung anhand konkreter und vielgestaltiger Prozesse, Verhaltensweisen oder Objekte.[62] Dies können zB regelmäßige Pflichtschulungen von Mitarbeitenden, interne Qualitäts- und Controllingschleifen oder Handbücher sein. Die unternehmensspezifische Integration von CDR stellt somit einen Ausgangspunkt dar, um CDR inhaltlich zu gestalten und zu bestimmen.

Die formulierten selbstregelnden Leitlinien und Kodizes reflektieren die Normbildung innerhalb eines Unternehmens und treiben gleichzeitig die Ausformung von CDR voran. Auf die Normbildung wirken gleichzeitig verschiedene unternehmensexterne Akteure ein, sodass es sich um ein Wechselspiel von Unternehmen und weiterer Akteure handelt.[63] Hierzu gehören unternehmensübergreifende Initiativen,[64] in denen sich Unternehmen selbstregulierend zu verantwortlichem Handeln in der digitalen Welt verpflichten, sowohl explizit auf CDR als auch iwS auf die verantwortungsvolle Gestaltung der Digitalisierung bezogen. Im Rahmen der CDR-Initiative des BMUV verpflichten sich deutsche Unternehmen ua dazu, über ihr Engagement im Bereich von CDR zu berichten.[65] Erste Berichte wurden 2022 veröffentlicht[66] und ergänzen gesetzliche Berichtspflichten, in denen sich digitales Verantwortungshandeln bislang nicht ausdrücklich widerspiegelt.[67] Ein weiteres Beispiel ist die „Charta digitale Vernetzung" von 2014, die von mehr als 80 Institutionen unterschrieben wurde und deren Grund-

er-kuenstliche-intelligenz/; SAP, Leitlinien für KI, 2018 und Global AI Ethics Policy, 2022, vgl. dazu https://news.sap.com/germany/2022/03/kuenstliche-intelligenz-ethik/; eine Suchmaschine für KI-ethische Leitlinien bietet das AI Ethics Guidelines Global Inventory von Algorithm Watch vgl. dazu https://inventory.algorithmwatch.org (Stand für alle 1.12.2023).

61 Lobschat et al. Journal of Business Research 122 (2021), 875 (880ff.).

62 Lobschat et al. Journal of Business Research 122 (2021), 875 (882).

63 Ausführlich Lobschat et al. Journal of Business Research 122 (2021), 875 (883ff.); eine Übersicht über Stakeholder gibt Dörr Praxisleitfaden CDR S. 135ff.

64 Übersichten finden sich ua bei Dörr Praxisleitfaden CDR S. 139ff.; Econsense, Umsetzung digitaler Verantwortung in Unternehmen, 2020, S. 17ff.

65 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 9; im Detail vgl. dazu https://cdr-initiative.de/cdr-berichte (Stand 1.12.2023).

66 Die CDR-Berichte können online abgerufen werden, vgl. dazu https://cdr-initiative.de/cdr-berichte (Stand 1.12.2023).

67 Dazu → § 2 C. I.

sätze für eine *„verantwortungsvolle Gestaltung der digitalen Gesellschaft"*[68] teilweise mit Zielen der CDR übereinstimmen.[69] Schließlich wirken Unternehmen über die kommunikativ-strategische Mitarbeit in Verbänden, Foren und Think Tanks an der Ausgestaltung von digitaler Verantwortung mit.[70] Ferner sind Unternehmensberatungen zu nennen, die CDR und ihre unternehmensinterne Realisierung als Betätigungsfeld erkennen und Unternehmen dazu beraten.[71]

2. Politik, öffentliche und private Stakeholder

Wichtige unternehmensexterne Akteure sind öffentliche und private Stakeholder, die sich in Initiativen, Verbänden und Netzwerken zusammengeschlossen haben und – teilweise mit Unternehmen zusammen – digitale Unternehmensverantwortung aus verschiedenen Blickwinkeln untersuchen, ausgestalten und implementieren. Exemplarisch seien hier die CDR-Initiativen des BMUV,[72] des Bundesverbands Digitale Wirtschaft[73]

68 Idee und Entstehung der Charta digitale Vernetzung siehe https://charta-digitale-vernetzung.de/idee-und-entstehung/ (Stand 1.12.2023); dazu Nietsch CSR Compliance/Anzinger § 27 Rn. 18.

69 So zB mit Blick auf die Verantwortung für personenbezogene Daten, die Nutzbarmachung von Daten, Teilhabe und Digitalkompetenz, siehe Charta digitale Vernetzung, abrufbar unter: https://charta-digitale-vernetzung.de/die-charta-im-wortlaut/ (Stand 1.12.2023).

70 Das econsense – Forum Nachhaltige Entwicklung der Deutschen Wirtschaft e.V. hat 49 große Mitgliedsunternehmen und adressiert die CDR, vgl. dazu https://econsense.de/digitale-verantwortung/ (Stand 1.12.2023); der Bundesverband Digitale Wirtschaft hat ein Ressort für Digital Responsibility und die sog. CDR Building Bloxx als besondere CDR-Themenplattform des Verbands, vgl. dazu https://www.bvdw.org/gremien/digital-responsibility/ und https://www.cdr-building-bloxx.com/cdr-building-bloxx-framework/ (Stand 1.12.2023); mit weiteren Beispielen Nietsch CSR Compliance/Anzinger § 27 Rn. 17ff.; Dörr Praxisleitfaden CDR S. 140ff.

71 So zB Deloitte, vgl. dazu https://www2.deloitte.com/de/de/pages/innovation/contents/corporate-digital-responsibility.html; PricewaterhouseCoopers, vgl. dazu https://www.pwc.de/de/digitale-transformation/corporate-digital-responsibility-cdr.html; das ConPolicy-Institut, vgl. dazu https://www.conpolicy.de/themen/digitalisierung/, WiseWay, vgl. dazu https://wiseway.de/angebote/ (Stand 1.12.2023).

72 Vgl. dazu https://cdr-initiative.de/initiative (Stand 1.12.2023).

73 Der Bundesverband Digitale Wirtschaft hat ein Ressort für Digital Responsibility und die sog. CDR Building Bloxx als besondere CDR-Themenplattform des Verbands, vgl. dazu https://www.bvdw.org/gremien/digital-responsibility/ und https://www.cdr-building-bloxx.com/cdr-building-bloxx-framework/ (Stand 1.12.2023).

und des Zentrum Digitalisierung Bayern[74] genannt, das CDR Online-Magazin[75] oder das CDR Manifesto[76]. Diese Akteure wirken an der Gestaltung von CDR durch Kodizes, themenbezogene Veröffentlichungen, Positionspapiere und Rahmenwerke oder auch durch die Verleihung von Preisen mit („CDR Award"[77]). Im weiteren Zusammenhang sind auch Initiativen zu nennen, die sich mit den Herausforderungen der KI, der Digitalethik oder der Digitalisierung im Allgemeinen befassen. Auf Stakeholder-Seite ist dies zB die Bertelsmann Stiftung,[78] die AG Ethik der Initiative D21[79] oder die og „Charta digitale Vernetzung" und auf politischer Ebene die hochrangige Expertengruppe für Künstliche Intelligenz der Europäischen Kommission,[80] die Enquete-Kommission für KI[81] oder die Datenethikkommission der Bundesregierung[82].

Eine Studie im Jahr 2022 hat 91 digital-ethische Leitlinien in Europa zum verantwortungsvollen Umgang mit digitalen Anwendungen untersucht und stellte seit 2016 eine kontinuierliche Zunahme dieser fest.[83] Die Leitlinien werden demnach vor allem durch Non-Profit-Organisationen (42 %) und Unternehmen (33 %) herausgegeben,[84] welches die obige Beobachtung

74 Vgl. dazu https://www.bayern-innovativ.de/de/seite/corporate-digital-responsibility (Stand 1.12.2023).

75 Vgl. dazu https://corporate-digital-responsibility.de (Stand 1.12.2023).

76 Vgl. dazu https://corporatedigitalresponsibility.net/cdr-manifesto (Stand 1.12.2023).

77 Der CDR-Award wird vom Bundesverband Digitale Wirtschaft und der Innovationsplattform Bayern Innovativ ausgerichtet, vgl. dazu https://www.cdr-award.digital/ (Stand 1.12.2023).

78 Die Bertelsmann-Stiftung hat sich in einem Projekt mit der Unternehmensverantwortung im digitalen Zeitalter befasst, abrufbar unter https://www.bertelsmann-stiftung.de/de/unsere-projekte/betriebliche-arbeitswelt-digitalisierung/projektnachrichten/ein-debattenbeitrag-zu-corporate-digital-responsibility (Stand 1.12.2023).

79 Die AG-Ethik der Initiative D21 e.V. als „Netzwerk für die Digitale Gesellschaft" befasst sich mit verschiedenen digital-ethischen Fragestellungen, abrufbar unter: https://initiatived21.de/arbeitsgruppen/ag-ethik/ (Stand 1.12.2023).

80 Diese erarbeitete ua Ethik-Leitlinien für vertrauenswürdige KI (2019), Richtlinien und Investitionsempfehlungen für vertrauenswürdige KI (2019) und eine Bewertungsliste für vertrauenswürdige KI (2020), vgl. dazu https://digital-strategy.ec.europa.eu/de/policies/expert-group-ai (Stand 1.12.2023).

81 Die Kommission stellte ihren Abschlussbericht am 28.10.2020 vor, vgl. dazu https://www.bundestag.de/webarchiv/Ausschuesse/ausschuesse19/weitere_gremien/enquete_ki (Stand 1.12.2023).

82 Die Kommission stellte ihren Abschlussbericht am 23.10.2019 vor, vgl. dazu https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf (Stand 1.12.2023).

83 idigiT, Leitlinien zu digitaler Ethik in Europa, 2022, S. 5, 8.

84 idigiT, Leitlinien zu digitaler Ethik in Europa, 2022, S. 9.

stützt. Die Leitlinien sind mehrheitlich an Unternehmen adressiert (56 %) und betreffen vor allem algorithmische Systeme bzw. Künstliche Intelligenz (66 %) wie auch den Umgang mit Daten (34 %).[85]

3. Wissenschaft

Diese Aktivitäten werden schließlich durch wissenschaftliche Auseinandersetzungen eingefasst, welche das Konzept der CDR interdisziplinär und aus unterschiedlichen Blickwinkeln untersuchen. Hier sind insb. wirtschafts- und sozialwissenschaftliche Fachpublikationen zu nennen, die CDR ua für die Praxis in Unternehmen bzw. die Integration ins unternehmerische Handeln und das Management des Unternehmens aufbereiten.[86]

4. Zwischenfazit

Die zentralen Akteure sind also Unternehmen, staatliche Institutionen, Stakeholder-Gruppen und die Wissenschaft. Die Handlungsformen sind geprägt von Selbstregelung und gesellschaftlicher Selbstregulierung im erläuterten Sinne mit ua Leitlinien und Kodizes. Es zeigt sich, dass die Quellenlandschaft für die Inhalte von CDR vielfältig und bislang wenig konsolidiert ist, wobei es zwischen den Quellen wechselseitige Einflüsse gibt. Letzteres birgt die Chance für einen interdisziplinären und wissenschaftlich-praktischen Austausch über die Herausforderungen der Digitalisierung und eine darauf bezogene Unternehmensverantwortung, aber auch das Risiko, dass sich divergierende Verantwortungskonzepte herausbilden.

III. Handlungsfelder

Auf Grundlage der dargestellten Akteure und ihrer Beiträge werden nun Handlungsfelder von Corporate Digital Responsibility dargestellt.

85 idigiT, Leitlinien zu digitaler Ethik in Europa, 2022, S. 10f.

86 So insb. Dörr Praxisleitfaden CDR S. 21ff.; Lobschat et al. Journal of Business Research 122 (2021), 875ff.; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13ff.; Mueller Bus Inf Syst Eng 64 (2022), 689ff.; Hamadi/Manzo, Corporate Digital Responsibility, 2021, S. 3ff.; einen Überblick zum noch geringen juristischen Literaturbestand zu CDR gibt Dürr ZGE 2021, 165 (166 Fn. 2).

1. Umgang mit Daten

Zentrales Handlungsfeld von CDR ist der verantwortungsvolle Umgang mit Daten.[87] Dies ist Ausdruck der immensen Relevanz von Daten für digitale Anwendungen und Geschäftsmodelle sowie des großen Schutzbedürfnisses von personenbezogenen Daten, aus denen sich zB detaillierte Profile von Personen erstellen lassen.

Der unternehmerische Umgang mit Daten reicht vom Sammeln und Abspeichern (Stufe 1) über das Aufbereiten und Analysieren (Stufe 2) bis hin zum Zugänglichmachen, Weitergeben und ihrer Verwendung in Geschäftsentscheidungen (Stufe 3).[88] Verantwortungsvoller Umgang mit Daten lässt sich in den einzelnen Stufen in verschiedene Fragen und Zielsetzungen übersetzen, welche vielfach untrennbar mit datenschutzrechtlichen Fragestellungen verwoben sind:[89]

In der *ersten Stufe* kann CDR zB das Ziel verfolgen, Personen selbstbestimmte Einwilligungsentscheidungen zu ermöglichen, indem mithilfe von Symbolen oder Grafiken über die Datenschutzpolitik informiert wird oder Wahlmöglichkeiten eröffnet werden, wie und welche Daten verwendet werden.[90] Mit Blick auf die Speicherung von Daten ist auch die IT-Sicherheit von betrieblichen Infrastrukturen relevant, um Daten vor Diebstahl oder Manipulation zu schützen.[91]

In der *zweiten Stufe* kann CDR darauf abzielen, beim Einsatz von algorithmischen Systemen die *„Verzerrung von Datenanalysen"* durch sog. „Biases" zu mitigieren,[92] die Erstellung von Profilen (Profiling) *„transparent*

87 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 4f.; Bahreini/Charton/Lukas RDi 2021, 548 (548f.); Esselmann/Brink Ökologisches Wirtschaften 33, 2 (2020), 11 (12); Cooper/Siu/Wei, Corporate Digital Responsibility, 2015, S. 2f.; Dörr Praxisleitfaden CDR S. 109f., 111f., 115; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (19ff.); Richter PinG 6 (2018), 237 (238).

88 Vgl. Dörr Praxisleitfaden CDR S. 17f.

89 Zu den Schnittstellen zum Datenschutz sogleich → § 2 D. III. 4. und → § 3 B.

90 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 4; Maßnahmenvorschläge im Feld „Umgang mit Daten" beim Handlungsfeld „Verbrauchersouveränität und Autonomie sicherstellen", vgl. dazu https://cdr-initiative.de/kodex (Stand 1.12.2023).

91 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 5; Nietsch CSR Compliance/Anzinger § 27 Rn. 65ff.

92 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 4; speziell für künstliche Intelligenz Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (20).

und fair [zu] gestalten" und zB die Analyse von Daten nach persönlichkeitsbezogenen Merkmalen zu unterlassen.[93]

Schließlich kann sich verantwortungsvoller Umgang mit Daten in der *dritten Stufe* daran zeigen, dass solches Verhalten auch über das eigene Unternehmen hinaus bei Geschäftspartnern, ggf. mit entsprechenden Verhaltenskodizes, eingefordert wird.[94] Digitale Verantwortung kann sich auch in der Bereitschaft äußern, bestimmte Daten im rechtlich zulässigen Rahmen ggü. Dritten (bspw. Forschende) bereitzustellen[95] oder auf bestimmte Formen manipulativen Marketings zu verzichten.[96]

Den genannten Zielen können sich Unternehmen durch vielfältige technische und organisatorische Maßnahmen nähern, die hier nur allgemein angedeutet werden können.[97] So kann die Gestaltung von Benutzeroberflächen oder die Programmierung der dahinterstehenden Systemarchitektur auf CDR-Kriterien hin angepasst werden und hierfür zB die Mitarbeitenden geschult und sensibilisiert werden. Relevant sind auch Schutzmaßnahmen vor physischen Einwirkungen auf Serverinfrastrukturen iRd Corporate Cyber Security.

Im Sinne einer vollständigen Darstellung von CDR werden nachfolgend weitere Handlungsfelder beschrieben, die nicht unmittelbar den Umgang mit Daten betreffen, aber eine teils enge bzw. systeminhärente Verbindung zu Daten aufweisen.

2. Digitale Bildung, Inklusion, Wandel der Arbeitswelt

Die Handlungsfelder der digitalen Bildung und Inklusion adressieren Wissens- und Kompetenzdisparitäten, die mit Blick auf neue digitale Technolo-

93 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 4; Dörr Praxisleitfaden CDR S. 110.

94 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 4f.; zur „Datenermächtigung" im Einzelnen auch Dörr Praxisleitfaden CDR S. 111.

95 Dörr Praxisleitfaden CDR S. 109.

96 Dörr Praxisleitfaden CDR S. 115f.

97 Im Detail Dörr Praxisleitfaden CDR S. 101ff. mit Hinweisen zu möglichen Engagements; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (18ff.); zu weiteren konkreten Maßnahmenvorschlägen vgl. https://cdr-initiative.de/kodex (Stand 1.12.2023); beispielhaften Überblick über praktische Maßnahmen liefern die CDR-Berichte der an der Initiative teilnehmenden Unternehmen, vgl. dazu https://cdr-initiative.de/cdr-berichte (Stand 1.12.2023).

gien bei Nutzerinnen und Nutzern wie auch Mitarbeitenden in Unternehmen bestehen.

Die zunehmende Digitalisierung verändert die individuellen Lebenswelten und kann für Personen eine Zugangshürde zu bestimmten Produkten und Dienstleistungen darstellen, etwa wenn diese nur digital zugänglich sind.[98] Um Nutzer auf digitalisierungsspezifische Veränderungen vorzubereiten und einer schleichenden Exklusion aus der (digitalisierten) Gesellschaft vorzubeugen, ist das Ziel von CDR, diese bedarfsgerecht im Umgang mit digitalen Technologien (fort) zu bilden, über Chancen und Risiken sowie ethische Fragen der Digitalisierung aufzuklären und zu einem souveränen Handeln zu befähigen sowie digitale Zugangshürden zu beseitigen.[99]

Auch für Mitarbeitende in digitalisierten Arbeitswelten besteht die Gefahr von Zugangshürden und Exklusion, zB durch eine zunehmende Automatisierung von Produktions- und Arbeitsprozessen, eine verstärkte Mensch-Maschine-Interaktion sowie neue Qualifikationsanforderungen.[100] Dass diesen Veränderungen der Arbeitswelt eine besondere Bedeutung auch für digitale Unternehmensverantwortung zukommt, zeigt sich daran, dass der CDR-Kodex des BMUV die „Mitarbeitenden-Einbindung" als eigenes Handlungsfeld aufführt.[101] Ziel ist hier, die Mitarbeitenden bei der Gestaltung von Transformationsprozessen zu beteiligen und zB durch Weiterbildungsmaßnahmen zu unterstützen.[102]

3. Umwelt-, Klima- und Ressourcenschutz

Schließlich hat CDR auch eine ökologische Dimension.[103] Digitale Technologien verbrauchen einerseits Energie und Ressourcen mit stark steigender Tendenz. So ist der digitale Sektor weltweit geschätzt für rund 2–4

98 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 6, 9; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (21).

99 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 6, 9; vgl. auch https://www.cdr-building-bloxx.com/digitale-befaehigung/ (Stand 1.12.2023).

100 Dazu Dörr Praxisleitfaden CDR S. 24ff.; vgl. auch https://www.cdr-building-bloxx.com/zukunft-arbeit/ (Stand 1.12.2023).

101 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 8.

102 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 8.

103 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 7; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (18f.) mwN; Lobschat et al. Journal of Business Research 122 (2021), 875 (879); vgl. dazu auch https://www.cdr-building-bloxx.com/umwelt-ressourcen/ (Stand 1.12.2023).

Prozent der globalen Treibhausgas-Emissionen verantwortlich.[104] Auch der Ressourceneinsatz für die Produktion von digitalen Produkten ist beträchtlich. Auf der Inputseite werden zahlreiche seltene Metalle und Mineralien benötigt, die unter hoch problematischen ökologischen, politischen und sozialen Bedingungen gefördert werden und auf der Output-Seite entstehen große Mengen an Elektronikschrott, von denen nur ein kleiner Teil recycelt wird.[105] Andererseits leisten digitale Technologien große Beiträge zur Lösung bzw. Abfederung von Umwelt-, Klima- und Ressourcenproblemen.[106] Sie sind also auch eine notwendige Voraussetzung für die Erreichung umfassender Nachhaltigkeitsziele.[107] Die ökologische Dimension digitaler Technologien ist damit ein eminent wichtiges Handlungsfeld von CDR. Unternehmen sollen dabei den durch die Herstellung und den Betrieb von technischen Geräten verursachten Verbrauch von Energie und Ressourcen reduzieren und gleichzeitig digitale Anwendungen entwickeln, die umweltfreundliches Verhalten unterstützen.[108]

104 Coalition for Digital Environmental Sustainability (CODES), Action Plan for a Sustainable Planet in the Digital Age, 2020, vgl. dazu https://doi.org/10.5281/zenodo.6573509, S. 20 (Stand 1.12.2023) betrachtet den digitalen Sektor insgesamt und kommt zur Einschätzung, dass er je nach Berechnungsmethode für ca. 1,8–3,9 Prozent der globalen Treibhausgas-Emissionen verantwortlich ist. Nach den Schätzungen von McKinsey ist Informationstechnik in Unternehmen weltweit für die jährliche Emission von 350–400 Megatonnen CO_2-Äquivalente verantwortlich. Das sind 1 Prozent der weltweiten jährlichen Treibhausgas-Emissionen. Der größte CO_2-Emittent sind dabei nicht die Rechenzentren vor Ort, sondern die Herstellung und Betrieb aller Endgeräte der Mitarbeiter wie Laptops, Tablets, Smartphones und Drucker. Diese Endnutzergeräte erzeugen weltweit 1,5 bis 2 Mal mehr CO_2 als Rechenzentren, vgl. dazu https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-green-it-revolution-a-blueprint-for-cios-to-combat-climate-change, S. 2f. (Stand 1.12.2023).

105 UNEP, Foresight Brief Nr. 27, The growing footprint of digitalisation, vgl. dazu https://wedocs.unep.org/handle/20.500.11822/37439, S. 4 (Stand 1.12.2023).

106 Laut World Economic Forum, Davos Agenda 2022, 3 ways digital technology can be a sustainability game changer, 19.1.2022, vgl. dazu https://www.weforum.org/agenda/2022/01/digital-technology-sustainability-strategy/ (Stand 1.12.2023) können digitale Technologien ua genutzt werden, um Fortschritte bei Nachhaltigkeit zu messen und verfolgen, die Nutzung von Ressourcen zu optimieren, Treibhausgasemissionen zu reduzieren und eine Kreislaufwirtschaft möglich machen; siehe auch Dörr Praxisleitfaden CDR S. 114ff.

107 Detailliert dazu Mittwoch JZ 2023, 376 (376, 381ff.).

108 Vgl. BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 7; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (18f.); Lobschat et al. Journal of Business Research 122 (2021), 875 (879).

4. Spannungsfeld zwischen gesetzlichen Regelungen und CDR

Mit Blick auf Inhalte von CDR und deren Zusammenwirken mit rechtlichen Anforderungen ist bemerkenswert, dass die Web-Version des CDR-Kodex des BMUV bei mehreren Maßnahmenvorschlägen auf die Voraussetzungen der Datenschutz-Grundverordnung (DSGVO)[109] verweist.[110] Für den Maßnahmenvorschlag, *„Kundinnen und Kunden [zu] informieren, wenn Kundendaten genutzt werden, um Profile über sie zu erstellen"* wird zB darauf verwiesen, dass dies *„bei personenbezogenen Daten der Informationspflicht aus Art. 13 Abs. 2 Buchstabe f, Art. 14 Abs. 2 Buchstabe g DSGVO [entspricht]."*[111] Der Vorschlag, dass Unternehmen *„sicherstellen, dass persönliche Daten nur von Personen verwendet werden, die über entsprechende Berechtigungen verfügen"*, entspräche *„bei personenbezogenen Daten den TOMs (Technische und Organisatorische Maßnahmen) im Sinne des Art. 32 DSGVO."*[112] Auch in der CDR-Literatur wird die DSGVO wiederholt als wichtiges Instrument für den Datenschutz angeführt.[113]

Hier zeigt sich ein durchaus problematisches Spannungsfeld von CDR zum gesetzlichen Regelungsrahmen. Zwar kann die Aufnahme von wichtigen gesetzlichen Anforderungen in ein freiwilliges Verantwortungsregime einerseits ihre besondere Bedeutung hervorheben und andererseits auf *„die verbraucherfreundliche Umsetzung gesetzlicher Anforderungen"*[114] abzielen, wie es der CDR-Kodex des BMUV formuliert. Die genügende Erfüllung

109 VO (EU) 2016/679.

110 Maßnahmenvorschläge im Feld „Umgang mit Daten" in der Webversion des Corporate Digital Responsibility-Kodex, vgl. dazu https://cdr-initiative.de/kodex (Stand 1.12.2023). Weiterhin finden sich Verweise auf ein Gutachten der Datenethikkommission (DEK). In der PDF-Version des CDR-Kodex finden sich keine entsprechenden Verweise.

111 Maßnahmenvorschlag um *„Profilanalysen („Profiling") verantwortlich, transparent und fair gestalten"* und dazugehörige Fußnote 2 im Feld „Umgang mit Daten" in der Webversion des Corporate Digital Responsibility-Kodex, vgl. dazu https://cdr-initiative.de/kodex (Stand 1.12.2023).

112 Maßnahmenvorschlag um *„Verantwortlichen Umgang mit Daten im Unternehmen sicherstellen"* und dazugehörige Fußnote 10 im Feld „Umgang mit Daten" in der Webversion des Corporate Digital Responsibility-Kodex, vgl. dazu https://cdr-initiative.de/kodex (Stand 1.12.2023).

113 Nietsch CSR Compliance/Anzinger § 27 Rn. 55; Esselmann/Golle/Thiel/Brink, Corporate Digital Responsibility, 2020, S. 10, 12; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (17f., 22); Lobschat et al. Journal of Business Research 122 (2021), 875 (878f., 883); Mueller Bus Inf Syst Eng 64 (2022), 689 (692); Panzer-Heemeier/Nemat CCZ 2022, 223 (227); Richter PinG (2018) 6, 237 (238).

114 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 4.

der geltenden gesetzlichen Anforderungen ist jedoch die Pflicht eines jeden Unternehmens und Ausdruck ihrer Regelkonformität. Es kann sich dabei nicht um ein freiwilliges unternehmerisches Engagement handeln. Besonders problematisch erscheint, dass eine staatliche Initiative damit dem ersten Anschein nach die gesetzlichen Anforderungen zu „Maßnahmenvorschlägen" herabstuft und die Unternehmen im Mantel der Freiwilligkeit *„über das gesetzlich Vorgeschriebene hinaus[gehende]"* Aktivitäten berichten können, obwohl diese Aktivitäten die gesellschaftlich erwartete Regeleinhaltung widerspiegeln.

Aus diesem Spannungsfeld ergibt sich die Notwendigkeit, CDR in den bestehenden und zukünftigen rechtlichen Kontext einzubetten und ihre Wechselwirkung zum Recht zu bestimmen. Der regulatorische Kontext ist für den Anwendungsbereich und Inhalt einer freiwilligen Unternehmensverantwortung gerade konstitutiv, da dieser den Spielraum bestimmt, in dem Unternehmen tatsächlich freiwillig tätig werden können und eigene, nicht hoheitlich vorgegebene „Sollens-" und „Müssens-Sätze" formulieren können. Dies ist Gegenstand des nachfolgenden Kapitels.

§ 3 Corporate Digital Responsibility im Kontext eines entstehenden Datenrechts

Digitale Unternehmensverantwortung ist inhaltlich vielfältig und bewegt sich infolgedessen in einem ebenso vielseitigen Regulierungsrahmen: Für die Handlungsfelder der digitalen Bildung und Inklusion sowie des Wandels der Arbeitswelt bilden zB das Sozial- und Arbeitsrecht mögliche rechtliche Anknüpfungspunkte. Für das Handlungsfeld Umwelt- und Klimaschutz spielt dagegen das Umwelt- und Produktrecht ua eine Rolle.[115] Die vorliegende Arbeit fokussiert den Umgang mit Daten und den dazugehörigen rechtlichen Rahmen.

Die Regulierung von digital- und datenbezogenen Sachverhalten hat in der jüngeren Zeit an Fahrt aufgenommen, insb. auf europäischer Ebene.

115 Etwa wenn es um die Gestaltung nachhaltiger Produkte geht, vgl. Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Schaffung eines Rahmens für die Festlegung von Ökodesign-Anforderungen für nachhaltige Produkte und zur Aufhebung der Richtlinie 2009/125/EG vom 30.3.2022, COM(2022) 142 final.

Die Europäische Kommission stellte im Februar 2020 eine Digitalstrategie zur Gestaltung von Europas digitaler Zukunft vor.[116] Parallel legte sie auch eine Datenstrategie vor, in welcher sie die Herausforderungen einer datenzentrierten Wirtschaft und Gesellschaft skizziert und strategische Leitlinien formuliert.[117] Zudem hat sie im Januar 2022 mit der politischen „Erklärung zu den digitalen Rechten"[118] wichtige Rechte und Grundsätze proklamiert, die sich auch Unternehmen zu eigen machen sollen, weil diese *„im digitalen Raum Verantwortung tragen"*.[119] Hierzu gehören zB die Menschzentrierung und Inklusivität des digitalen Wandels, die Entscheidungsfreiheit und Befähigung der Nutzenden wie auch die Sicherheit im digitalen Raum und die digitale Nachhaltigkeit. Dieser strategische Rahmen wird durch ein breites Spektrum an bereits geltender oder gerade im Gesetzgebungsprozess befindlicher Regulierung zu digitalen Plattformen, Technologien und Daten ausgefüllt.

Wichtige Bausteine dieser Gesetzgebung sind das 2022 verabschiedete Gesetz über digitale Märkte und das Gesetz über digitale Dienste (A.), mit denen die Regulierung von großen digitalen Plattformen und Unternehmen forciert wird.[120] Datenrechtlich kommt dem europäischen Datenschutzrecht eine zentrale Bedeutung zu (B.). Des Weiteren ist der freie Zugang zu Daten bzw. ihre gemeinsame Nutzung ein Regelungsanliegen des europäischen Gesetzgebers (C.), das durch das im Mai 2022 verabschiedete Daten-Governance-Gesetz und das im November 2023 verabschiedete Datengesetz adressiert wird. Weiterhin soll die Sicherheit von digitalen Technologien und Daten erhöht werden, indem zB Hard- und Softwareprodukte durch einen „Cyber Resilience Act" strenger reguliert werden (D.). Der

116 Gestaltung der digitalen Zukunft Europas vom 19.2.2020, COM(2020) 67 final; daran anknüpfend wurden die Zielvorstellungen im „Digitalen Kompass 2030" weiter ausformuliert, vgl. Digitaler Kompass 2030: der europäische Weg in die digitale Dekade vom 9.3.2021, COM(2021) 118 final.

117 Eine europäische Datenstrategie vom 19.2.2020, COM(2020) 66 final, 2ff., 13ff.

118 Europäische Erklärung zu den digitalen Rechten und Grundsätzen für die digitale Dekade vom 26.1.2022, COM(2022) 28 final; Nüßing MMR 2022, 341 (341f.) erblickt in der Erklärung wenig neue Forderungen bzw. Grundsätze.

119 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Eine europäische Erklärung zu den digitalen Rechten und Grundsätzen für die digitale Dekade vom 26.1.2022, COM(2022) 27 final, 7.

120 Beide Rechtsakte sind Schlüsselmaßnahmen, die die Kommission bereits in ihrer Digitalstrategie formulierte, vgl. COM(2020) 67 final, 11, 14; zum Regelungsziel Gielen/Uphues EuZW 2021, 627.

datengetriebene Einsatz von KI-Systemen wird derzeit ebenfalls rechtlich eingefasst, ua durch eine EU-Verordnung über Künstliche Intelligenz (E.).

Im Folgenden wird der (entstehende) regulatorische Rahmen aufgezeigt und in Bezug zu den Zielen und Inhalten der CDR gesetzt. Hierbei wird eine Makro-Perspektive gewählt, um der Regelungs- und Detailfülle des regulatorischen Rahmens, dem begrenzten Umfang dieser Arbeit und dem weiten Handlungsspielraum der CDR zum Umgang mit Daten gerecht zu werden.

A. Gesetze über digitale Märkte und digitale Dienste

Das Gesetz über digitale Märkte (DMA)[121] und das Gesetz über digitale Dienste (DSA)[122] betreffen einerseits die wettbewerbliche Ausrichtung digitaler Märkte und andererseits die Moderation von illegalen Inhalten in digitalen Plattformen und Diensten. Beide Rechtsakte traten im November 2022 in Kraft.

Das Gesetz über digitale Märkte reguliert ausgewählte „Torwächter"-Unternehmen, die über eine besonders dominante Stellung in digitalen Märkten verfügen und erlegt ihnen verschiedene Verhaltenspflichten auf.[123] Damit soll sichergestellt werden, dass digitale Märkte fair und für andere Wettbewerber „bestreitbar" sind.[124] So dürfen Torwächter ua keine personenbezogenen Daten miteinander zusammenführen, die aus dem Anbieten verschiedener Plattformdienste resultieren (zB Daten von WhatsApp und Instagram, die beide zu Meta gehören).[125] Demgegenüber ist das Ziel des Gesetzes über digitale Dienste, rechtswidrige Inhalte wie Hassrede und Desinformationen im Internet unionsweit wirksamer zu bekämpfen

121 VO (EU) 2022/1925.

122 VO (EU) 2022/2065.

123 Zur Definition siehe Art. 3 DMA, der Kriterien für Torwächter nennt (Abs. 1) und diese um quantitative Vermutungsregeln ergänzt (Abs. 2); zentrale Verpflichtungen für Torwächter finden sich in Art. 5 und 6 DMA, im Detail dazu Gielen/Uphues EuZW 2021, 627 (629ff.); Podszun/Bongartz/Kirk NJW 2022, 3249 (3250ff.).

124 Siehe Art. 1 Abs. 1 DMA; zur Einordnung des DMA als Wettbewerbsrecht oder Binnenmarkt-Regulierung mit eigenen Zielen, siehe Gielen/Uphues EuZW 2021, 627 (628); Podszun/Bongartz/Kirk NJW 2022, 3249 (3249f.).

125 Siehe Art. 5 Abs. 2 lit. b DMA, der insoweit Ähnlichkeit zu dem 2021 einführten deutschen § 19a GWB aufweist; problematisierend zu einer Normkollision Gielen/Uphues EuZW 2021, 627 (631f.).

und insofern bereits bestehende Regelungsregime zu harmonisieren.[126] Dafür werden Vermittlungsdienste abgestimmten Haftungsprivilegierungen (Art. 4–6 DSA) und Sorgfaltspflichten (Art. 11ff. DSA) unterworfen.[127]

Auch wenn wettbewerbliche Ziele keinen Kerninhalt von CDR darstellen, ist „faires" Verhalten gegenüber Mitbewerbern bzw. Nutzern sowie ein sensibler Umgang mit rechtswidrigen Inhalten generell einer verantwortungsvollen Unternehmensführung zuzuordnen. Zudem handelt es sich bei DMA und DSA um zentrale digitalpolitische Rechtsakte,[128] die in der Darstellung der digital- und datenrechtlichen Landschaft auf EU-Ebene nicht fehlen dürfen. Für Unternehmen mit digitalen Geschäftsmodellen werden bestehende Rechtspflichten aus dem Kartell- und Wettbewerbsrecht und zur Moderation von Inhalten also unionsweit (weiter) harmonisiert bzw. ausgestaltet.

B. Datenschutz

Die Datenschutz-Grundverordnung (DSGVO)[129] bestimmt als unmittelbar geltendes Unionsrecht seit Mai 2018 maßgeblich die Regeln zum Schutz personenbezogener Daten in der EU.[130] Die DSGVO formuliert dabei insb. Grundsätze für die Verarbeitung von personenbezogenen Daten (I.) und verschiedene Rechte von betroffenen Personen (II.). Darüber hinaus werden denjenigen diverse Pflichten auferlegt, die für die Datenverarbeitung verantwortlich bzw. mit dieser beauftragt sind (III.).

126 So führten mehrere EU-Mitgliedstaaten bereits nationale Gesetze zur Bekämpfung rechtswidriger oder strafbarer Inhalte im Internet ein, zB Deutschland mit dem Netzwerkdurchsetzungsgesetz (NetzDG), vgl. Gielen/Uphues EuZW 2021, 627 (632f.).

127 Art. 1 Abs. 2 DSA; zu den verschiedenen Arten von Vermittlungsdiensten und den dazugehörigen Sorgfaltspflichten Gielen/Uphues EuZW 2021, 627 (634ff.).

128 Beide Rechtsakte sind für die EU-Kommission „Schlüsselmaßnahmen" ihrer Digitalstrategie, vgl. COM(2020) 67 final, 11, 14.

129 VO (EU) 2016/679.

130 Neben der DSGVO gibt es weitere spezialgesetzliche Vorschriften zum Datenschutz, die Vorschriften der DSGVO ggf. verdrängen. Hierzu gehört in Deutschland ua der Datenschutz bei Telekommunikation und Telemedien (§§ 1ff. TTDSG), besondere Regelungen im Bundesdatenschutzgesetz (§§ 1ff. BDSG) oder zu digitalen Gesundheitsanwendungen (§ 4 Digitale Gesundheitsanwendungen-Verordnung).

I. Grundsätze der DSGVO

In Art. 5 Abs. 1 DSGVO finden sich die grundsätzlichen Anforderungen an die Verarbeitung von personenbezogenen Daten. Zu den Grundsätzen gehört, dass die Daten erstens rechtmäßig, also auf Grundlage einer Einwilligung oder einer anderen gesetzlichen Befugnis, und transparent verarbeitet werden müssen (lit. a). Zweitens unterliegen die Daten einer Zweckbindung, dürfen also nicht für andere als die festgelegten bzw. legitime Zwecke verwendet werden (lit. b). Weiterhin gilt der Grundsatz der Datenminimierung, also dass Daten für den jeweiligen Zweck angemessen und erheblich sind und nicht über das notwendige Maß hinaus verarbeitet werden (lit. c). Auch dürfen Daten nur solange nicht-anonymisiert gespeichert werden, wie es für die Zwecke der Verarbeitung „erforderlich" ist (lit. e) und müssen durchgängig sicher und vertraulich verarbeitet werden (lit. f).

Die Verarbeitung von personenbezogenen Daten nach der DSGVO unterliegt damit kurz gefasst ua den Grundsätzen der Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung sowie Integrität und Vertraulichkeit.[131] Das Datenschutzrecht der DSGVO ist also „prinzipiengeleitet"[132] und weist damit Ähnlichkeiten zu den Prinzipien auf, die sich im CDR-Kodex des BMUV, aber auch anderen Leitlinien zum verantwortungsvollen Umgang mit digitalen Anwendungen, finden.[133] Zudem gibt es inhaltliche Überschneidungen zwischen den Grundsätzen der DSGVO und den für

131 Siehe Art. 5 Abs. 1 DSGVO am Ende der jeweiligen Absätze. Weitere Grundsätze sind die Verarbeitung nach Treu und Glauben (lit. a), Richtigkeit (lit. d) und Speicherbegrenzung (lit. e); ob es sich dabei um rechtsverbindliche Grundsätze oder um Prinzipien i.S.v. Optimierungsgeboten handelt, ist umstritten: für verbindliche Grundsätze BeckOK DatenschutzR/Schantz DS-GVO Art. 5 Rn. 2; Ehmann/Selmayr/Heberlein DS-GVO Art. 5 Rn. 1; für Optimierungsgebote wohl: Paal/Pauly/Frenzel DS-GVO Art. 5 Rn. 9; ebenfalls dazu Nietsch CSR Compliance/Anzinger § 27 Rn. 56.

132 Zu den Prinzipien des Datenschutzrechts und ihrer Bedeutung: BeckOK DatenschutzR/Wolff DS-GVO Grundlagen Rn. 1ff.; Ehmann/Selmayr/Heberlein DS-GVO Art. 5 Rn. 2; mit Blick auf CDR vgl. Nietsch CSR Compliance/Anzinger § 27 Rn. 55.

133 Siehe Prinzipien im BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 3; für den Code of Digital Ethics der Merck KGaA ausführlich Bahreini/Charton/Lukas RDi 2021, 548 (550f.); andere sprechen von „Werten", vgl. idigiT, Leitlinien zu digitaler Ethik in Europa, 2022, S. 13.

die CDR formulierten Prinzipien, so mit Blick auf Transparenz,[134] Integrität und Vertraulichkeit[135] oder Autonomie[136].

II. Rechte von betroffenen Personen

Die Art. 12–23 DSGVO verleihen Personen verschiedene Rechte, wenn ihre personenbezogenen Daten verarbeitet werden. Die Rechte umfassen den gesamten Prozess der Datenverarbeitung und beginnen mit einer Information über die Datenerhebung *„in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache"* (Art. 12 Abs. 1 DSGVO). Es bestehen sodann Auskunftsrechte, ein Recht auf Berichtigung von unrichtigen Daten, ein Recht auf Löschung bzw. „Vergessenwerden" und auf Datenübertragbarkeit (Art. 15–18 DSGVO). Beachtenswert ist außerdem das *„Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden"* in Art. 22 Abs. 1 DSGVO.[137]

Mit diesen Rechten ermöglicht die DSGVO betroffenen Personen umfassend über die eigenen personenbezogenen Daten sowie Art und Umfang ihrer Verarbeitung zu entscheiden. Die souveräne und autonome Entscheidung über eigene Daten von Nutzern wird als wichtiger Bestandteil der CDR gesehen.[138] Aufgrund der weitreichenden gesetzlichen Gewährleistungen ist der Spielraum einer freiwilligen CDR für die „Rechtsstellung" von Nutzern aber begrenzt.

---

134 Der Grundsatz „Transparenz" (Art. 5 Abs. 1 lit. a DSGVO) ist ebenfalls ein Prinzip im CDR-Kodex und anderen europäischen Leitlinien, vgl. BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 3; idigiT, Leitlinien zu digitaler Ethik in Europa, 2022, S. 13.

135 Der Grundsatz „Integrität und Vertraulichkeit" (Art. 5 Abs. 1 lit. f DSGVO) könnte dem Prinzip „Schaden vermeiden" und „Verantwortlichkeit" im CDR-Kodex zugeordnet werden, vgl. BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 3; in anderen europäischen Leitlinien findet sich der Wert „Sicherheit", vgl. idigiT, Leitlinien zu digitaler Ethik in Europa, 2022, S. 13.

136 Das Prinzip „Autonomie" aus dem CDR-Kodex könnte den Grundsätzen der Rechtmäßigkeit und Zweckbindung in Art. 5 Abs. 1 lit. a und lit. b DSGVO entsprechen, vgl. BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 3.

137 Auch wenn dieses Recht nicht ausnahmslos gilt (Abs. 2), ist der für die Datenverarbeitung Verantwortliche dennoch zu „angemessene[n] Maßnahmen" verpflichtet, um die Rechte, Freiheiten und berechtigten Interessen der betroffenen Person zu schützen; dazu Ehmann/Selmayr/Hladjk DS-GVO Art. 22 Rn. 11ff.

138 BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 4; Dörr Praxisleitfaden CDR S. 11f.; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (22).

III. Verantwortung für die Datenverarbeitung

Das vierte Kapitel der DSGVO (Art. 24–43) enthält vielgestaltige Pflichten für datenverarbeitende Instanzen bzw. Personen.[139] Zunächst ist mehreren Pflichten gemein, dass diese *„geeignete technische und organisatorische Maßnahmen"* des für die Datenverarbeitung Verantwortlichen erfordern.[140] Bei der Auswahl der Maßnahmen sind idR der Stand der Technik, Implementierungskosten sowie Umstände der Verarbeitung und die mit ihr verbundenen Risiken zu berücksichtigen und abzuwägen.[141]

Solche technischen und organisatorischen Maßnahmen hat der Verantwortliche ua zu treffen, um zB durch Pseudonymisierung *„die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen"* oder um *„sicher[zu]stellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden"* (Art. 25 Abs. 1 und Abs. 2 S.1 DSGVO). Bei diesen Pflichten handelt es sich um sog. Datenschutz „by design" bzw. „by default".[142]

Ebenfalls ist die Sicherheit der Datenverarbeitung durch technische und organisatorische Maßnahmen zu gewährleisten, um ein für das jeweilige Risiko *„angemessenes Schutzniveau zu gewährleisten"* (Art. 32 Abs. 1 DSGVO). Hierzu werden beispielhaft mögliche Maßnahmen aufgeführt, wie Pseudonymisierung und Verschlüsselung von Daten.

Ein Datenschutz „by design" bzw. „by default" und informationstechnisch sichere Systeme werden auch als Gestaltungsaufgaben einer CDR gesehen.[143] Ihrem Grundsatz nach sind dies jedoch Pflichten unter der DSGVO, sofern personenbezogene Daten betroffen sind. Diese Pflichten gelten uneingeschränkt auch für neue digitale Technologien. So orientieren sich die technischen und organisatorischen Maßnahmen idR am Stand der

139 Die DSGVO spricht von für die Verarbeitung „Verantwortliche" und von „Auftragsverarbeitern", vgl. nur Art. 24 und 28 DSGVO.

140 So in Art. 24 Abs. 1, Art. 25 Abs. 1, Art. 32 Abs. 1, Art. 34 Abs. 3 lit. a DSGVO; zum Begriff der technischen und organisatorischen Maßnahmen: Paal/Pauly/Martini DS-GVO Art. 24 Rn. 20ff.

141 Siehe Art. 24 Abs. 1, Art. 25 Abs. 1, Art. 32 Abs. 1 DSGVO.

142 BeckOK DatenschutzR/Paulus DS-GVO Art. 25 Rn. 4f., 8; Ehmann/Selmayr/Baumgartner DS-GVO Art. 25 Rn. 1f.

143 Dörr Praxisleitfaden CDR S. 111; Maßnahmenvorschlag 2 beim Ziel *„Verantwortliche Technikgestaltung im Umgang mit Daten fördern"* im Feld „Umgang mit Daten" in der Webversion des Corporate Digital Responsibility-Kodex, vgl. dazu https://cdr-initiative.de/kodex (Stand 1.12.2023).

Technik, sodass Unternehmen fortlaufend zu einer (Re-)Evaluation der ergriffenen Schutzmaßnahmen angehalten sind. Für neuartige Technologien, die bei der Datenverarbeitung zu einem hohen Risiko für die Rechte und Freiheiten von Personen führen,[144] sind zudem gemäß Art. 35 Abs. 1 DSGVO die Folgen für den Datenschutz abzuschätzen.[145] Die DSGVO unterwirft Unternehmen damit verschiedenen Pflichten zum Schutz von personenbezogenen Daten, welche insb. auch präventiven Charakter haben und ihrem Inhalt und Umfang nach im Einzelfall ausfüllungsbedürftig sind. Deshalb ist der Spielraum für freiwillige Maßnahmen im Rahmen einer digitalen Unternehmensverantwortung hier ebenfalls überschaubar.

IV. Zwischenfazit

Für den Schutz von personenbezogenen Daten gibt die DSGVO einen weitreichenden Regulierungsrahmen vor, der umfassend Rechte von betroffenen Personen festlegt und verantwortliche Unternehmen verpflichtet. Deshalb sind die Möglichkeiten für Unternehmen, über ihre Verpflichtungen aus der DSGVO hinaus wesentliche eigene Schutzmaßnahmen im Rahmen einer CDR zu ergreifen, begrenzt.[146]

Daraus folgt erstens, dass es aufgrund des hohen Schutzniveaus der DSGVO unsachgemäß wäre, diese im Hinblick auf digitale Unternehmensverantwortung als „bloß" grundlegenden rechtlichen Maßstab einzuordnen.[147] Diese ist vielmehr der Ausgangspunkt und *„important guideline[s]"*[148] für eine unternehmensinterne Auseinandersetzung mit CDR, auf

144 Die DSGVO verweist insb. auf Fälle des systematischen und umfassenden Profilings und der Verarbeitung von besonders sensiblen Daten, Art. 35 Abs. 3 lit. a und b DSGVO.

145 Zur Anwendung der Datenschutz-Folgeabschätzung gemäß Art. 35 DSGVO beim Einsatz von personenbezogenen Trainingsdaten für ein KI-System: Schürmann ZD 2022, 316 (317ff.); im Einzelnen ferner Paal/Pauly/Martini DS-GVO Art. 35 Rn. 44ff.

146 In diese Richtung ebenfalls: Nietsch CSR Compliance/Anzinger § 27 Rn. 55ff.; Mueller Bus Inf Syst Eng 64 (2022), 689 (696); Pauly/Wichert DB-Beil. Heft 21/2023, 44 (45); Richter PinG 6 (2018), 237 (238); für Esselmann/Golle/Thiel/Brink, Corporate Digital Responsibility, 2020, S. 10 überwiegt im Bereich Privacy bislang die DSGVO-Compliance mit wenigen darüberhinausgehenden Unternehmensaktivitäten.

147 Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (17f.; 22); in diese Richtung wohl auch Mueller Bus Inf Syst Eng 64 (2022), 689 (692).

148 Lobschat et al. Journal of Business Research 122 (2021), 875 (879); wohl auch Panzer-Heemeier/Nemat CCZ 2022, 223 (227).

dessen Grundlage eine entsprechende CDR-Kultur und dazugehörige Normen im Unternehmen entwickelt werden können.[149] Dass der CDR-Kodex seine Ziele bzw. Maßnahmenvorschläge teils analog zu Pflichten in der DSGVO formuliert (→ § 2 D. III. 4.), kann einerseits als Ausdruck ihres hohen Schutzniveaus und ihrer Leitfunktion und andererseits als mögliche regulatorische „Sättigung" im Bereich des Datenschutzes gesehen werden. Vor diesem Hintergrund bleibt zu konstatieren, dass in Veröffentlichungen zur CDR kaum eine Auseinandersetzung mit den Regelungen der DSGVO stattfindet. Zweitens ist die DSGVO ein Ergebnis von zurückliegenden Regulierungsdebatten und -prozessen zum Datenschutz,[150] die für andere digitale Technologien gerade geführt werden bzw. bevorstehen. Entsprechend ist die DSGVO eine Blaupause dafür, dass Freiräume einer freiwilligen Unternehmensverantwortung abhängig vom Regelungsumfeld sind.

Dies soll nicht darüber hinwegtäuschen, dass zwischen der DSGVO und freiwilliger digitaler Unternehmensverantwortung Verknüpfungen bestehen: So beruht ihr Schutzanspruch auf teils gleichen und teils ähnlichen Grundprinzipien (insb. Transparenz, Sicherheit von Daten und Autonomie der Nutzenden). Daneben ermöglicht die DSGVO gewisse Selbstregulierung durch sog. Verhaltensregeln. Diese Regeln können Verbände und andere Vereinigungen ausarbeiten und damit die Anwendung der gesetzlichen Vorschriften konkretisieren (Art. 40 DSGVO).[151]

Neben der DSGVO gibt es auf unionsrechtlicher Ebene weitere datenschutzrechtliche Regeln, insb. für elektronische Kommunikationsdienste, die in der E-Privacy-Richtlinie bzw. nationalem Recht reguliert werden.[152] Die E-Privacy-Richtlinie sollte 2018 zeitgleich zum Inkrafttreten der DSGVO durch eine E-Privacy-Verordnung ersetzt werden, um die Vor-

149 Lobschat et al. Journal of Business Research 122 (2021), 875 (879); Panzer-Heemeier/Nemat CCZ 2022, 223 (228); Pauly/Wichert DB-Beil. Heft 21/2023, 44 (45); Richter PinG 6 (2018), 237 (238).

150 Lobschat et al. Journal of Business Research 122 (2021), 875 (885); Econsense, Umsetzung digitaler Verantwortung in Unternehmen, 2020, S. 7, 12.

151 Detailliert dazu Dürr ZGE 2021, 165 (175f.); mit Beispielen Wittmann/Haidenthaler MMR 2022, 8 (10ff.).

152 RL 2002/58/EG; in Deutschland aktuell umgesetzt durch das Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) vom 23.6.2021 (BGBl. I 1982); im Detail zum Verhältnis zur DSGVO: BeckOK DatenschutzR/Holländer DS-GVO Art. 95 Rn. 2ff.; Paal/Pauly/Pauly DS-GVO Art. 95 Rn. 2f.

schriften der DSGVO zu ergänzen.[153] Das Gesetzgebungsverfahren läuft aktuell noch.[154] Aufgrund des besonderen Anwendungsbereichs und der Anknüpfung an das Schutzniveau der DSGVO wird an dieser Stelle auf eine nähere Darstellung beider Rechtsakte verzichtet.[155]

C. Datenzugang und -nutzung

Die EU-Kommission hat 2020 in ihrer Datenstrategie die hohe wirtschaftliche und gesellschaftliche Bedeutung von Daten hervorgehoben und gefordert, dass diese *„Quelle für Wachstum und Innovation"* in einer europäischen Datenwirtschaft genutzt werden solle.[156] Um einen EU-Binnenmarkt für Daten zu schaffen, wurden in der Strategie verschiedene politische Maßnahmen angekündigt,[157] die nun in zwei Gesetzesinitiativen mündeten:

Das Daten-Governance-Gesetz (DGG)[158] trat am 23.6.2022 in Kraft und zielt darauf ab, die Verfügbarkeit von Daten zu erhöhen, in dem datenvermittelnde Akteure reguliert und Möglichkeiten für die gemeinsame Datennutzung in der EU gestärkt werden.[159] Komplementär zur seit 2019 bestehenden Richtlinie über offene Daten, die die Weiterverwendung von Daten öffentlicher Stellen, von Unternehmen und von Forschungsdaten betrifft,[160] regelt das DGG die Weiterverwendung von „geschützten" Daten, die Rechten Dritter unterliegen.[161] Hierzu werden insbesondere sog. Da-

153 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) vom 10.1.2017, COM(2017) 10 final; dazu Paal/Pauly/Pauly DS-GVO Art. 95 Rn. 4f.

154 Der letzte Stand ist eine Diskussion im Rat der Europäischen Union am 10.02.2021, vgl. dazu https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=COM:2017:10:FIN (Stand 1.12.2023).

155 Im Detail dazu BeckOK DatenschutzR/Holländer DS-GVO Art. 95 Rn. 1, 4; Ehmann/Selmayr/Klabunde/Selmayr DS-GVO Art. 95 Rn. 8ff.; Paal/Pauly/Pauly DS-GVO Art. 95 Rn. 2f.

156 COM(2020) 66 final, 1ff.

157 COM(2020) 66 final, 5, 13ff.

158 VO (EU) 2022/868, welche gemäß Art. 38 DGG ab dem 24.9.2023 gilt.

159 Siehe Erwägungsgründe 3 und 5 VO (EU) 2022/868; näher Schildbach ZD 2022, 148 (148f.); Tolks MMR 2022, 444.

160 RL (EU) 2019/1024.

161 Art. 3 Abs. 1 lit. d und Erwägungsgrund Nr. 6 der RL (EU) 2019/1024; vgl. auch Tolks MMR 2022, 444 (445); Schildbach ZD 2022, 148 (149).

tenvermittlungsdienste reguliert, die *„Geschäftsbeziehungen zwischen einer unbestimmten Anzahl von betroffenen Personen oder Dateninhabern einerseits und Datennutzern andererseits"* anbahnen, um *„die gemeinsame Datennutzung [...] zu ermöglichen"* (Art. 2 Nr. 11 DGG). Diese spezielle Form der unternehmerischen Tätigkeit unterliegt einem verpflichtenden Anmeldeverfahren (Art. 10f. DGG) und weiteren Verhaltenspflichten nach Art. 12 DGG.[162] Weiterhin werden sog. „datenaltruistische Organisationen" durch das DGG geregelt, die entgeltlos die gemeinsame Datennutzung für Ziele von allgemeinem Interesse (zB Gesundheitsversorgung, Bekämpfung des Klimawandels) ermöglichen.[163] In Folge seines spezifischen Anwendungsbereichs ist das Daten-Governance-Gesetz nur selektiv für die Ausgestaltung von digitaler Unternehmensverantwortung relevant, namentlich wenn Datenintermediäre und ihre Tätigkeiten betroffen sind.

Größerem Interesse kommt dem im November 2023 verabschiedeten Data Act bzw. Datengesetz (DaG)[164] zu, das sich mit konkreten Rechten und Verfahren für den Datenzugang und damit notwendigen Bedingungen der Datenwertschöpfung befasst.[165] Das Datengesetz zielt also darauf, Daten – unabhängig von ihrem Personenbezug[166] – einfacher zugänglich und nutzbar zu machen.[167]

Dazu regelt das zweite Kapitel des Datengesetzes die Grundmodalitäten der Datenweitergabe und die Rechte und Pflichten der daran Beteiligten. Zunächst müssen Hersteller und Entwickler ihre vernetzten Produkte und verbundenen Dienste so gestalten, dass die bei ihrer Nutzung erzeugten

162 Hierzu gehören zB ein Diskriminierungsverbot, ein Neutralitäts- und Transparenzgebot, das Verbot von Kopplungsgeschäften, Anforderungen an die Umwandlung von Datenformaten oder die Interoperabilität von Daten, vgl. Hennemann/Ditfurth NJW 2022, 1905 (1908ff.), Tolks MMR 2022, 444 (446).

163 Für diese regeln die Art. 18ff. DGG ua Anforderungen für ihre Eintragung, die Transparenz und zum Schutz der Rechte und Interessen betroffener Personen und Dateninhaber; kritisch Schildbach ZD 2022, 148 (151f.).

164 VO (EU) 2023/2854.

165 COM(2022) 68 final, 5f.; vgl. auch Wiebe GRUR 2023, 1569; Tolks MMR 2022, 444 (449).

166 Siehe Art. 1 Abs. 5 Datengesetz und Erwägungsgrund Nr. 7: *„[Das Datengesetz] ergänzt das Unionsrecht zum Schutz personenbezogener Daten und zum Schutz der Privatsphäre, insbesondere die Verordnungen (EU) 2016/679 und (EU) 2017/1725 und die Richtlinie 2002/58/EG, und lässt es unberührt"*; die Grenze für die Datenverwendbarkeit ist also der Datenschutz, vgl. Bomhard/Merkle RDi 2022, 168 (169); Specht-Riemenschneider MMR 2022, 809 (810); Assion/Willecke MMR 2023, 805 (809f.).

167 COM(2022) 68 final, 3.

Daten für die Nutzenden *„einfach, sicher, unentgeltlich und [...] direkt zugänglich*" sind (Art. 3 DaG), sog. „Access by Design".[168] Hierauf aufbauend sollen Nutzer den Zugang zu Daten, die bei der Nutzung eines Produktes oder Dienstes erzeugt werden, verlangen können (Art. 4 DaG). Auch sollen Nutzer verlangen können, dass ihre Daten direkt an Dritte weitergegeben werden, die in diesem Fall besonderen Pflichten unterliegen (Art. 5 und 6 DaG). Das dritte Kapitel enthält die Pflichten der Dateninhaber, welche Daten bereitstellen müssen. Diese betreffen die Modalitäten, wie eine Datenbereitstellung (vertraglich) zu vereinbaren ist (Art. 8 DaG) und Vergütungsfragen (Art. 9 DaG). Im fünften Kapitel bestimmt das Datengesetz, dass Daten aufgrund einer außergewöhnlichen Notwendigkeit für öffentliche Stellen bereitgestellt werden müssen, zB bei einem öffentlichen Notstand.[169] Im sechsten Kapitel finden sich weitreichende Vorschriften für (cloud-basierte) Datenverarbeitungsdienste, die insb. den Wechsel des Anbieters erleichtern und etwaige *„gewerbliche, technische, vertragliche und organisatorische Hindernisse*" beseitigen sollen (Art. 23 DaG).[170] Schließlich werden im achten Kapitel umfangreiche Regelungen zur Interoperabilität für Anbieter von Datenräumen und Datenverarbeitungsdiensten getroffen. Damit knüpft das Datengesetz an die Verordnung über den freien Verkehr nicht personenbezogener Daten[171] von 2018 an, gemäß der einerseits nichtpersonenbezogene Daten frei in der EU verwendet werden können und die Selbstregulierung des erleichterten Wechsels von insb. Cloud-Anbietern durch Verhaltensregeln (wohl erfolglos)[172] forciert wurde.

Das europäische Datengesetz führt damit zu einer umfassenden rechtlichen Einfassung des Zugangs zu Daten aus der Nutzung von vernetzten Produkten und verbundenen Diensten, auch wenn es im Einzelnen ver-

168 Assion/Willecke MMR 2023, 805 (806f.); detailliert Wiebe GRUR 2023, 1569 (1570f.); Bomhard/Merkle RDi 2022, 168 (173) sprechen insofern von *„erheblich[en] Auswirkungen auf die technische Gestaltung von Produkten und Leistungen*".

169 Vgl. Wiebe GRUR 2023, 1569 (1575f.); Specht-Riemenschneider MMR 2022, 809 (812, 824ff.).

170 Vgl. Wiebe GRUR 2023, 1569 (1576); kritisch Bomhard/Merkle RDi 2022, 168 (175).

171 VO (EU) 2018/1807.

172 So hebt die EU-Kommission im Entwurf ihres Datengesetzes hervor: *„[I]n Bezug auf Cloud-Dienste scheint der Selbstregulierungsansatz [der Verordnung über den freien Verkehr nicht personenbezogener Daten] die Marktdynamik nicht wesentlich beeinflusst zu haben; daher enthält dieser Vorschlag [zu einem Datengesetz] einen Regulierungsansatz für das Problem*", COM(2022) 68 final, 5.

schiedener Kritik ausgesetzt ist.[173] Für CDR heißt dies, dass die Autonomie bzw. Selbstbestimmung über den Umgang mit Daten („Datenermächtigung"[174]) perspektivisch über regulatorische Datenzugangsansprüche und korrespondierende unternehmerische Pflichten verwirklicht wird.

D. Cybersicherheit

Auf EU-Ebene wird mit der Cybersicherheit ein weiteres Handlungsfeld der CDR adressiert. Mit der sog. NIS-Richtlinie[175] von 2016 existieren Regelungen, um die Sicherheit von Netz- und Informationssystemen sektorbezogen zu erhöhen und kritische (Digital-)Infrastrukturen besser zu schützen. Hierzu werden insb. die EU-Mitgliedstaaten verpflichtet, entsprechende nationale Strategien zu erarbeiten und Sicherheits- und Meldevorschriften für Betreiber kritischer Digitalinfrastrukturen definiert.[176] Dieser Rechtsrahmen wurde durch die 2023 in Kraft getretene NIS2-Richtlinie modernisiert und ihr Anwendungsbereich ausgeweitet und verschärft.[177] Weiterhin wurde 2019 der „Rechtsakt zur Cybersicherheit" verabschiedet.[178] Dieser harmonisierte ua den Rahmen für freiwillige Zertifizierung der Cybersicherheit von Produkten, Diensten und Prozessen der Informations- und Kommunikationstechnik, der Unternehmen betrifft, die sich entsprechend zertifizieren lassen.[179]

173 Assion/Willecke MMR 2023, 805 (810) kritisieren viele unbestimmte Rechtsbegriffe; detailliert auch Wiebe GRUR 2023, 1569 (1577f.); für die Entwurfsfassung kamen Bomhard/Merkle RDi 2022, 168 (176) bereits zum Ergebnis, dass *„[z]entrale Tatbestandsmerkmale und Anforderungen des Data Act aktuell derart unklar sind, dass sie sich kaum rechtssicher umsetzen ließen"* und für Specht-Riemenschneider MMR 2022, 809 (826) waren für die Erreichung der Regelungsziele noch *„mehr als vorsichtige Korrekturen"* erforderlich.

174 Zum Begriff und Einzelaspekten Dörr Praxisleitfaden CDR S. 111f.; Herden et al. NachhaltigkeitsManagementForum 29 (2021), 13 (22); ebenfalls zur „Verbrauchersouveränität und Autonomie": BMUV, Corporate Digital Responsibility-Kodex, 2021, S. 4.

175 RL (EU) 2016/1148; in Deutschland umgesetzt mit dem Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 vom 23.6.2017 (BGBl. I 1885).

176 Siehe Art. 7, 14, 16 RL (EU) 2016/1148.

177 RL (EU) 2022/2555; detailliert Schmidt K&R 2023, 705 (706ff.); vgl. dazu auch https://digital-strategy.ec.europa.eu/de/policies/nis2-directive (Stand 1.12.2023).

178 VO (EU) 2019/881.

179 Siehe Art. 46ff. der VO (EU) 2019/881.

Für Unternehmen, die Hard- und Softwareprodukte entwickeln und vertreiben, könnte jedoch das im September 2022 vorgeschlagene Gesetz über Cyberresilienz (GCR-E)[180] einschneidende Bedeutung bekommen. Dieses soll Sicherheitsvorschriften für sicherere Hard- und Softwareprodukte schaffen und damit die jährlich durch Cyberangriffe und -kriminalität entstehenden Kosten und Schäden für Nutzer und die Gesellschaft senken.[181] Für dieses Ziel legt der Gesetzesentwurf ua *„grundlegende Anforderungen an die Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen sowie Pflichten der Wirtschaftsakteure in Bezug auf diese Produkte hinsichtlich der Cybersicherheit"* fest und enthält Vorschriften zum Inverkehrbringen solcher Produkte (Art. 1 lit. a und b GCR-E). Auch für Sicherheitsupdates während des Lebenszyklus eines Produkts werden grundlegende Anforderungen an Hersteller festgelegt (Art. 1 lit. c GCR-E). Hersteller sollen ihre Produkte mit digitalen Elementen so gestalten, dass *„sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten"*[182] und dafür eine Bewertung der Sicherheitsrisiken durchführen, zu der sie ggf. in einem Anhang aufgezählte Maßnahmen treffen müssen (zB Authentifizierungssysteme oder Verschlüsselung), Art. 10 Abs. 1 und 2 GCR-E.[183]

Auch wenn das Gesetzgebungsverfahren noch nicht abgeschlossen ist, lässt der Entwurf zum Gesetz über Cyberresilienz erwarten, dass die EU in den kommenden Jahren einen strengen Rechtsrahmen für die sichere Gestaltung von digitaler Hard- und Software schaffen wird. Dieser könnte viele der Ziele und Maßnahmen, die bislang einer freiwilligen Digitalverantwortung von Unternehmen zugeordnet werden (→ § 2 D. III.), in rechtliche Pflichten transformieren.

180 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020 vom 15.9.2022, COM(2022) 454 final.

181 COM(2022) 454 final, 1.

182 Anhänge des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020 vom 15.9.2022, COM(2022) 454 final, 1.

183 Anhang zu COM(2022) 454 final, 1.

E. Künstliche Intelligenz

Im April 2021 stellte die EU-Kommission ihren Vorschlag für ein Gesetz über künstliche Intelligenz (KIG-E) vor.[184] Ziel des Vorschlags ist es, zur *„Entwicklung einer sicheren, vertrauenswürdigen und ethisch vertretbaren künstlichen Intelligenz"* beizutragen und Vorteile sowie Risiken von KI-Systemen angemessen zu regeln.[185] In der Vorbereitungsphase wurden die Eingaben von zahlreichen Stakeholdern einbezogen, auch um im Hinblick auf bestehende Ethik-Kodizes einen gemeinsamen, wertorientierten Ansatz zu finden.[186] Die gesetzliche Haftung für KI-Systeme ist nicht Bestandteil des KIG-E und soll in einer Richtlinie harmonisiert werden.[187]

Im Mittelpunkt des Kommissionsentwurfs steht ein risikobasierter Ansatz, der KI-Systeme anhand ihres Risikos einstuft und ihren Einsatz mit abgestuften Anforderungen und Pflichten belegt.[188] Verboten werden sollen KI-Systeme mit einem „unannehmbaren Risiko" für die Werte der Union bzw. für Grundrechte.[189] Hierzu gehören Systeme mit hohem Manipulationspotential, mit denen Behörden die Vertrauenswürdigkeit von Personen benachteiligend bewerten oder klassifizieren könnten (sog. Social Scoring) oder die zur „biometrischen Echtzeit-Fernidentifizierung" im öffentlichen Raum dienen.[190] Grundsätzlich erlaubt werden sollen Systeme mit einem „hohen Risiko".[191] Diese sollen jedoch besonderen rechtlichen

184 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union vom 21.4.2021, COM(2021) 206 final.

185 COM(2021) 206 final, 2.

186 Der Vorschlag beruht ua auf den Arbeiten der Hochrangigen Expertengruppe für KI, die wichtige Anforderungen in Ethik-Leitlinien für vertrauenswürdige KI integriert hat, vgl. COM(2021) 206 final, 9f.

187 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (Richtlinie über KI-Haftung) vom 28.9.2022, COM(2022) 496 final.

188 COM(2021) 206 final, 8, 15ff.; siehe auch Geminn ZD 2021, 354 (356ff.); Orssich EuZW 2022, 254 (257ff.).

189 COM(2021) 206 final, 15.

190 COM(2021) 206 final, 15, 50ff. (Art. 5); im Detail Orssich EuZW 2022, 254 (257f.).

191 COM(2021) 206 final, 15; die Einstufung als „Hochrisiko-KI-System" hängt von seiner Funktion, ihrem konkreten Anwendungszweck und -modalitäten ab. Der Entwurf unterscheidet zwischen KI-Systemen als „Sicherheitskomponenten von Produkten" und „eigenständigen KI-Systemen", die in einem Anhang zum Entwurf explizit genannt werden, siehe COM(2021) 206 final, 15, 52f. (Art. 6, 7); dazu Geminn ZD 2021, 354 (357ff.); Orssich EuZW 2022, 254 (258ff.).

Anforderungen unterliegen, sodass qualifizierte „Risikomanagementsysteme" eingerichtet (Art. 9 KIG-E) und die in das System eingespeisten Daten besonders ausgewählt und verwaltet werden müssen (Art. 10 KIG-E). Weiterhin sollen ua Pflichten zur Dokumentation, zur Aufzeichnung, zur Transparenz und menschlichen Aufsicht sowie zur Resilienz und Sicherheit der Systeme gelten (Art. 11–15 KIG-E). Bei KI-Systemen mit spezifischen Manipulationsrisiken soll der Einsatz einer KI offengelegt werden.[192] Für KI-Systeme mit einem geringen oder minimalen Risiko sieht der KIG-E keine besonderen regulatorischen Anforderungen vor, sodass sie im bestehenden Rechtsrahmen betrieben werden können. Ein Großteil der aktuell in der EU eingesetzten KI-Systeme dürfte in diese Kategorie fallen.[193] Gleichzeitig soll der KIG-E für den verantwortungsvollen Einsatz von künstlicher Intelligenz nicht abschließend sein und fördert daher die freiwillige Erfüllung bzw. Übererfüllung der gesetzlichen Regeln (Art. 69 KIG-E). So soll die Aufstellung von Verhaltenskodizes erleichtert werden, um die Anforderungen an Hochrisiko-Systeme auf Systeme mit geringen Risiken zu übertragen (Art. 69 Abs. 1 KIG-E) oder um freiwillig weitere Anforderungen zu erfüllen, die sich zB *„auf die ökologische Nachhaltigkeit, die barrierefreie Zugänglichkeit für Personen mit Behinderungen, die Beteiligung von Interessenträgern an der Konzeption und Entwicklung von KI-Systemen [...] beziehen*" (Art. 69 Abs. 2 KIG-E).

Aufgrund des laufenden Gesetzgebungsverfahrens sind sowohl der Beschluss als auch die finalen Regelungsinhalte eines europäischen KI-Gesetzes noch offen.[194] Der ursprüngliche Kommissionsentwurf ist aufgrund von sich verändernden politischen Agenden und verstärkten Forderungen nach weniger Bürokratie und Regelungslast infolge von gesamtwirtschaftlichen Entwicklungen zuletzt zunehmend unter Druck geraten. In jedem Fall wird der unionsrechtliche Rechtsrahmen darüber entscheiden, welche Handlungsspielräume einer CDR in Bezug auf Anwendungen künstlicher Intelligenz zukommen.

Nach derzeitigem Stand würden diese Spielräume korrespondierend zu dem abgestuften Regulierungsregime des KIG-E variieren. Für Systeme mit geringen Risiken verbliebe ein wesentlicher Handlungsspielraum für digi-

192 Art. 52 KIG-E nennt KI-Systeme, die mit natürlichen Personen interagieren (Abs. 1), die Emotionen erkennen oder biometrisch kategorisieren (Abs. 2) oder die Bild-, Ton- oder Videoinhalte als „Deepfakes" erzeugen (Abs. 3), COM(2021) 206 final, 78.

193 Orssich EuZW 2022, 254 (255).

194 Zum derzeitigen Stand vgl. https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0106(OLP) (Stand 1.12.2023).

tale Unternehmensverantwortung, in dem entweder (ausgewählte) gesetzliche Vorgaben freiwillig erfüllt werden, diese als Orientierung für unternehmensinterne Leitlinien dienen oder jenseits dessen eine eigene Auseinandersetzung mit verantwortungsvollem KI-Einsatz erfolgt. Für Hochrisiko-Systeme unterlägen Unternehmen dagegen diversen gesetzlichen Pflichten, die Handlungsspielräume einer CDR einschränken. Die in Art. 69 KIG-E genannten Ziele wie der ökologisch bewusste Technologieeinsatz, die Barrierefreiheit oder Stakeholder-Beteiligung – gleichzeitig zentrale Ziele einer CDR (→ § 2 D. III.) – würden aber weiterhin freiwilligem Unternehmensengagement überlassen bleiben. Damit verbliebe der verantwortungsvolle Einsatz von KI auch bei Inkrafttreten des KIG-E für eine digitale Unternehmensverantwortung weiterhin hochrelevant.

F. Zwischenfazit

Die europäische Regulierungslandschaft prägt zum einen, dass für bestimmte Bereiche bereits ein grundlegender bis weitreichender Rechtsrahmen besteht wie zB im Bereich des Datenschutzes, der Cybersicherheit oder der Regulierung von digitalen Plattformen und Vermittlungsdiensten. Bereits länger bestehende Regulierungen wurden in den vergangenen Jahren ausgeweitet, zB durch die DSGVO (2018) oder den DMA (2022). Zum anderen forciert der europäische Gesetzgeber intensiv die Regulierung weiterer digital- und datenbezogener Sachverhalte durch diverse Gesetzesinitiativen. So werden Eckpfeiler für eine europäische Datenwirtschaft gelegt (DGG, DaG) und Schlüsseltechnologien wie algorithmische Systeme (ua KIG-E) reglementiert. Damit zeigt sich die zunehmende Entstehung eines europäischen Datenrechts bzw. „Datenwirtschaftsrechts“[195].

Für digitale Unternehmensverantwortung folgt daraus, dass die Spielräume freiwilliger Regelsetzung kleiner werden und eine zunehmende Verrechtlichung einsetzt. Hierbei gewinnt die „rechtliche Verantwortung“ iSd vollständigen Beachtung und Umsetzung gesetzlicher Regeln an Bedeutung. Die gesetzliche Normbildung erfolgt dabei nicht im „luftleeren Raum“, sondern in Wechselwirkung mit Stakeholdern – der Entwurf zum KIG belegt eindrücklich, dass Grundsätze aus Ethik-Kodizes von privaten

195 Hennemann/Ditfurth NJW 2022, 1905; Specht-Riemenschneider MMR 2022, 809 (811); Steinrötter RDi 2021, 480 (482ff.).

und öffentlichen Initiativen in gesetzliche Anforderungen einfließen.[196] In die legislative Willensbildung werden über unternehmerische und weitere Interessenvertreter zukünftig auch Erwägungen der CDR einfließen. Als Triebfeder könnte sich dabei erweisen, dass sich die Ziele von europäischer Regulierung und von CDR an mehreren Stellen (ua Datenschutz, Datenzugang) überschneiden und somit einem gleichförmigen Zielbild folgen.

Weiterhin fördert der europäische Gesetzgeber an verschiedenen Stellen die Erarbeitung von Verhaltenskodizes, die gesetzliche Pflichten konkretisieren (→ Art. 40 Abs. 2 DSGVO) oder freiwillige Selbstverpflichtungen betreffen (→ Art. 69 Abs. 2 KIG-E). Hier verbleiben also nicht nur rechtliche „Lücken", sondern explizite Spielräume für selbstregulierende Normbildung iRd Corporate Digital Responsibility.[197]

G. Ausblick ins nationale Recht

Auch EU-Mitgliedstaaten regeln digital- und datenbezogene Sachverhalte, entweder in Vorgriff oder als Ergänzung etwaiger EU-Vorschriften. In Deutschland existiert insb. für öffentliche Datenbereitsteller bereits ein Datennutzungsgesetz.[198] Im aktuellen Koalitionsvertrag werden ua ein Datengesetz, Datentreuhandgesetz und ein Forschungsdatengesetz angekündigt.[199] Von Interesse ist auch ein Blick nach Dänemark: in das dortige Gesetz über Jahresabschlüsse wurde 2020 eine Pflicht für große Unternehmen aufgenommen, nach dem „Comply or Explain"-Prinzip über ihre Arbeit und ihre Politik in Bezug auf datenethische Fragen zu berichten.[200]

196 Vgl. COM(2021) 206 final, 9f.; zur Durchführung von Folgeabschätzungen und Beteiligung von Stakeholdern bei EU-Initiativen, siehe https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/impact-assessments_de (Stand 1.12.2023).

197 Dazu auch Dürr ZGE 2021, 165 (174ff.); Pauly/Wichert DB-Beil. Heft 21/2023, 44 (47).

198 Gesetz für die Nutzung von Daten des öffentlichen Sektors (Datennutzungsgesetz) vom 16.07.2021, BGBl. I 2941, 2946.

199 Koalitionsvertrag 2021–2025 zwischen der SPD, Bündnis 90 / Die Grünen und der FDP, Mehr Fortschritt wagen, Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, abrufbar unter: https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf (Stand 1.12.2023), S. 14, 18.

200 Siehe § 99d im Gesetz zur Änderung des Jahresabschlussgesetzes vom 26.05.2020, Nr. L 124 B, abrufbar unter: https://www.ft.dk/ripdf/samling/20191/lovforslag/l124b/20191_l124b_som_vedtaget.pdf (Stand 1.12.2023).

Es bleibt abzuwarten, ob solche oder ähnliche Berichterstattungspflichten in anderen Mitgliedstaaten oder auf EU-Ebene eingeführt werden. Der bestehende deutsche und unionsrechtliche Rahmen sieht bislang keine spezifische Berichterstattungspflicht von Unternehmen zu digitalethischen oder CDR-bezogenen Fragen vor.[201]

§ 4 Fazit

Auf Grundlage der vorangegangenen Untersuchung ergeben sich für die Rolle der Corporate Digital Responsibility im Kontext eines entstehenden Datenrechts und mögliche zukünftige Wege einer rechtlichen Implementierung von CDR derzeit folgende Schlussfolgerungen.

In der Europäischen Union bewegt sich das Konzept der CDR in einem dynamischen rechtlichen Kontext, der sich durch einen zunehmenden digital- und datenrechtlichen Regulierungsdruck auszeichnet. Die zu erwartende und voranschreitende Verrechtlichung kann die Aktionsräume einer freiwilligen digitalen Unternehmensverantwortung reduzieren. Dadurch kann sich unternehmerisches CDR-Engagement perspektivisch verändern und sich der Fokus auf rechtliche Compliance verlagern. Gleichzeitig zeigt der Gesetzgebungsprozess zur europäischen KI-Verordnung beispielhaft, dass digitalrechtliche Gesetzesvorhaben und ihre Regulierungstiefe kontrovers diskutiert werden und sich die verfolgten Regulierungsansätze dynamisch verändern können. Letzteres vor allem vor dem Hintergrund von sich verändernden politischen Agenden und gesamtwirtschaftlichen Entwicklungen, die mit verstärkten Forderungen nach weniger Bürokratie und Regelungslast einhergehen.

Damit kommen CDR zwei wichtige rechtliche Funktionen zu: Einerseits ermöglicht CDR proaktive Selbstregulierung und kann Orientierung in einem hoch dynamischen Handlungsfeld sichern, in dem viele Fragen gesetzlich noch nicht reguliert sind oder unternehmerischer Eigenverantwortung überlassen werden. Andererseits können Unternehmen bestehende oder entstehende Lücken und Unsicherheiten in der rechtlichen Regulierung[202] mit CDR-Strategien und -Maßnahmen proaktiv ausfüllen. Wäh-

201 Ausführlich dazu → § 2 C. I.; vgl. RL (EU) 2022/2464 und § 289c HGB; detailliert auch Merbecks BB 2021, 2159 (2161ff.).

202 Zu diesem Aspekt ausführlich: Bahreini/Charton/Lukas RDi 2021, 548 (549); Dürr ZGE 2021, 165 (182f.).

rend gesetzliche Vorschriften vor allem regeln, „was" gemacht oder befolgt werden muss, kann CDR dies ins unternehmerische „wie" übersetzen.

Passend dazu lässt sich im CDR-Diskurs eine starke Fokussierung auf die unternehmenspraktische Integration von digitalverantwortlichen Verhaltensweisen konstatieren. Aus wissenschaftlicher Perspektive ist dabei eine teils nur oberflächliche Auseinandersetzung mit dem gesetzlichen Regulierungsumfeld und eine noch flexible und dogmatisch nicht in sich geschlossene Konzeptualisierung der CDR festzustellen. Die Vielfalt der CDR-Initiativen und eine mögliche heterogene Implementierung in verschiedenen Sektoren und Unternehmen birgt gleichzeitig das Risiko einer desintegrierten Entwicklung von CDR. Eine verstärkte Zusammenführung der unterschiedlichen CDR-Konzeptionen wäre daher wünschenswert, insbesondere auch im Hinblick auf das Potenzial der CDR, zur Transformation von digital- und datenbezogenen Pflichten in „hartes" Recht beizutragen.

Anders als es sich im Bereich der CSR beobachten lässt, scheint das CDR-Konzept als solches bislang (noch) keine Triebfeder für gesetzliche Regulierung zu sein oder ihre inhaltliche Ausgestaltung zu befruchten. So könnten Zielsetzungen der CDR zu verantwortungsvollem digitalen Unternehmenshandeln in gesetzlicher Regulierung implementiert werden, indem beispielsweise Berichterstattungspflichten der CDR-Initiative perspektivisch und in Anlehnung an die digital-ethischen Berichterstattungspflichten in Dänemark ins Recht aufgenommen würden.

Auf der Basis der in dieser Arbeit durchgeführten Bestandsaufnahme zur CDR ergeben sich für zukünftige Wege einer rechtlichen Implementierung von CDR drei Hypothesen:

Erstens werden sich CDR und entstehende Rechtsakte verstärkt gegenseitig sensibilisieren und stimulieren und darüber Zielsetzungen der CDR in die rechtliche Regulierung von digital- und datenbezogenen Sachverhalten einfließen.

Zweitens wird zunehmendes CDR-Engagement in Unternehmen auf andere Marktteilnehmer ausstrahlen, sodass sich für bislang freiwillige Handlungsoptionen der CDR eine wahrgenommene oder faktische Verbindlichkeit[203] ergibt. Die dadurch entstehenden quasi-verbindlichen Handlungsstandards können die Auslegung von gesetzlichen Anforderungen beein-

203 Zu einer faktischen Bindungswirkung Dürr ZGE 2021, 165 (182); Hoffmann-Riem Recht im Sog der digitalen Transformation S. 114; für den Bereich der CSR Spießhofer NZG 2018, 441 (442f.).

flussen oder durch Gesetzgeber aufgegriffen und in „hartes" Recht transformiert werden.

Drittens wird digitale Verantwortung von Unternehmen in einem dynamischen (europäischen und nationalen) Regulierungsumfeld wichtige Beiträge für eine proaktive Selbstregulierung im (entstehenden) Rechtskontext leisten. Zugleich ermöglichen und fördern bestimmte Rechtsakte eine „regulierte Selbstregulierung" (vgl. DSGVO, KIG-E). Beides läuft hoheitlicher Regulierung voraus bzw. parallel und kann deren Normbildung beeinflussen.

Insgesamt zeigen diese Ergebnisse und Schlussfolgerungen, dass CDR für die rechtswissenschaftliche Forschung, das Unternehmenshandeln und die gesellschaftliche Diskussion zu Technologiefolgen ein komplexes und dynamisches Forschungs- und Praxisfeld eröffnet.

Literatur- und Quellenverzeichnis

Assion, Simon/Willecke, Lukas, Der EU Data Act, Die neuen Regelungen zu vernetzten Produkten und Diensten, MMR 2023, 805–810.

Bahreini, Dariush/Charton, Jean Enno/Lucas, Simon, Unternehmensethik 4.0, Eine Darstellung von Zielen, Entwicklung und Inhalt eines Prinzipien-basierten Code of Digital Ethics sowie eine Analyse der normativen Wirkung dieser Leitlinien, RDi 2021, 548–554.

Bertelsmann Stiftung, Wittenberg-Zentrum für Globale Ethik (Hrsg.), Unternehmensverantwortung im digitalen Wandel, Ein Debattenbeitrag zu Corporate Digital Responsibility, Gütersloh 2020, abrufbar unter https://www.bertelsmann-stiftung.de/fileadmin/files/user_upload/UN_Verantwortung_im_digitalen_Wandel.pdf (Stand 1.12.2023).

Boehme-Neßler, Volker, Unscharfes Recht: Überlegungen zur Relativierung des Rechts in der digitalisierten Welt, Berlin 2008.

Bomhard, David/Merkle, Marieke, Der Entwurf eines EU Data Acts, Neue Spielregeln für die Data Economy, RDi 2022, 168–176.

Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) (Hrsg.), Corporate Digital Responsibility-Kodex, Freiwillige Selbstverpflichtung mit Bericht, 2021, abrufbar unter https://cdr-initiative.de/uploads/files/2022-02_Kodex_CDR-Initiative.pdf (Stand 1.12.2023).

Brandenburg, Anne/Waurick, Steffen, Corporate Digital Responsibility – freiwillig zu mehr digitaler Verantwortung?, RDi 2023, 365–368.

Cooper, Tim/Siu, Jade/Wei, Kuangyi, Corporate digital responsibility, Doing well by doing good, in: Accenture Outlook, 2015, abrufbar unter https://www.criticaleye.com/inspiring/insights-servfile.cfm?id=4431 (Stand 1.12.2023).

Dörr, Saskia, Praxisleitfaden Corporate Digital Responsibility, Unternehmerische Verantwortung und Nachhaltigkeitsmanagement im Digitalzeitalter, Berlin 2020.

Dürr, Paul, Corporate Digital Responsibility, Digitale Unternehmensverantwortung zwischen Rechtsverbindlichkeit und Selbstregulierung, ZGE 2021, 165–187.

Econsense – Forum Nachhaltige Entwicklung der Deutschen Wirtschaft e.V. (Hrsg.), econsense-Blueprint zur Umsetzung digitaler Verantwortung in Unternehmen, November 2020, abrufbar unter https://econsense.de/wp-content/uploads/2020/11/201119_econsense_Blueprint_D.pdf (Stand 1.12.2023).

Ehmann, Ansbach/Selmayer, Martin, Datenschutz-Grundverordnung, Kommentar, 2. Auflage 2018.

Esselmann, Frank/Brink, Alexander, Digitalverantwortung als Chance, Ökologisches Wirtschaften 33, 2 (2020), 11–13, abrufbar unter https://doi.org/10.14512/OEW350211 (Stand 1.12.2023).

Esselmann, Frank/Golle, Dominik/Thiel, Christian/Brink, Alexander, Corporate Digital Responsibility, Unternehmerische Verantwortung als Chance für die deutsche Wirtschaft, in: Zentrum Digitalisierung.Bayern (Hrsg.), ZD.B Digital Dialogue, Positionspapier, 2020, abrufbar unter https://zentrum-digitalisierung.bayern/wp-content/uploads/ZD.B-Positionspapier_Final_web.pdf (Stand 1.12.2023).

Floridi, Luciano/Taddeo, Mariarosaria, What is data ethics?, Philosophical Transactions of the Royal Society A, 374: 20160360, 2016, abrufbar unter https://doi.org/10.1098/rsta.2016.0360 (Stand 1.12.2023).

Geminn, Christian, Die Regulierung Künstlicher Intelligenz, Anmerkungen zum Entwurf eines Artificial Intelligence Act, ZD 2021, 354–359.

Gielen, Nico/Uphues, Steffen, Digital Markets Act und Digital Services Act, Regulierung von Markt- und Meinungsmacht durch die Europäische Union, EuZW 2021, 627–637.

Hamadi, Hassan/Manzo, Claudia, "Corporate Digital Responsibility", A Study on Managerial Challenges for AI integration in Business, 2021, abrufbar unter https://lup.lub.lu.se/student-papers/search/publication/9052507 (Stand 1.12.2023).

Hennemann, Moritz/von Ditfurth, Lukas, Datenintermediäre und Data Governance Act, NJW 2022, 1905–1910.

Herden, Christina/Alliu, Ervin/Cakici, André/Cormier, Thibaut et al., "Corporate Digital Responsibility", New corporate responsibilities in the digital age, NachhaltigkeitsManagementForum 29 (2021), 13–29, abrufbar unter https://link.springer.com/article/10.1007/s00550-020-00509-x (Stand 1.12.2023).

Hoffmann-Riem, Wolfgang, Recht im Sog der digitalen Transformation, Tübingen 2022.

idigiT – Institute for Digital Transformation in Healthcare (Hrsg.), Zwischen Unternehmenswerten und Operationalisierung – Digital-ethischer Umgang mit neuen Technologien, idigiT Studie: Leitlinien zu digitaler Ethik in Europa, August 2022, abrufbar unter https://www.transforming-healthcare.com/insights/ (Stand 1.12.2023).

Kettner, Sara Elisa/Thorun, Christian, Corporate Digital Responsibility, Ergebnisse eine repräsentativen Verbraucherbefragung, in: ConPolicy Institut für Verbraucherpolitik (Hrsg.), 27.4.2021, abrufbar unter https://cdr-initiative.de/uploads/files/210503_Umfrage_FInal_Faktenblatt_CDR.pdf (Stand 1.12.2023). (zitiert: Kettner/Thorun, Corporate Digital Responsibility-Verbraucherbefragung)

Lobschat, Lara/Mueller, Benjamin/Eggers, Felix/Brandimarte, Laura et al., Corporate digital responsibility, Journal of Business Research 122 (2021), 875–888, abrufbar unter https://doi.org/10.1016/j.jbusres.2019.10.006 (Stand 1.12.2023).

Merbecks, Ute, Corporate Digital Responsibility: neue Herausforderungen für die nichtfinanzielle Berichterstattung, BB 2021, 2159–2163.

Mihale-Wilson, Cristina/Hinz, Oliver/van der Aalst, Wil/Weinhardt, Christof, Corporate Digital Responsibility, Relevance and Opportunities for Business and Information Systems Engineering, Business & Information Systems Engineering 64 (2022), 127–132, abrufbar unter https://doi.org/10.1007/s12599-022-00746-y (Stand 1.12.2023).

Mittwoch, Anne-Christin, Digitalisierung und Nachhaltigkeit – Praktische Konvergenzen zweier Leitdiskurse im Unternehmensrecht, JZ 2023, 376–384.

Mittwoch, Anne-Christin, Nachhaltigkeit und Unternehmensrecht, Tübingen 2022.

Möslein, Florian, Corporate Digital Responsibility: Eine aktienrechtliche Skizze, in: Grundmann, Stefan/Merkt, Hanno/Mülbert, Peter O. (Hrsg.), Festschrift für Klaus J. Hopt zum 80. Geburtstag am 24. August 2020, Berlin/Boston 2020, 805–823.

Mueller, Benjamin, Corporate Digital Responsibility, Business & Information Systems Engineering 64 (2022), 689–700, abrufbar unter https://doi.org/10.1007/s12599-022-00760-0 (Stand 1.12.2023).

Nietsch, Michael, Corporate Social Responsibility Compliance, München 2021.

Noack, Ulrich, Organisationspflichten und -Strukturen kraft Digitalisierung, ZHR 183 (2019), 105–144.

Nüßing, Christoph, Eine digitale Magna Carta? Die Europäische Erklärung zu digitalen Rechten, MMR 2022, 341–342.

Orssich, Irina, Das europäische Konzept für vertrauenswürdige Künstliche Intelligenz, EuZW 2022, 254–261.

Paal, Boris/Pauly, Daniel, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 3. Auflage, München 2021.

Panzer-Heemeier, Andrea/Nemat, André T., Digitale Ethik – Eine neue Chance für ESG-Compliance, CCZ 2022, 223–230.

Panzer-Heemeier, Andrea/Nemat, André T./Meckenstock, Cordula, ESG 2.0 – Digitale Ethik als neue Dimension der Nachhaltigkeit, ESG 2022, 104–109.

Pauly, Daniel/Wichert, Felix, Corporate Digital Responsibility, digitale Ethik & Co., Datenverarbeitungen und digitale Technologie in der ESG-Strategie, DB-Beil. Heft 21/2023, 44–47.

Podszun, Rupprecht/Bongartz, Philipp/Kirk, Alexander, Digital Markets Act – Neue Regeln für Fairness in der Plattformökonomie, NJW 2022, 3249–3254.

Richter, Frederick, Aus Sicht der Stiftung Datenschutz: CDR – More Than Just a Hype?, Privacy in Germany (PinG) 2018 Nr. 6, 237–238.

Schildbach, Roman, Zugang zu Daten der öffentlichen Hand und Datenaltruismus nach dem Entwurf des Daten-Governance-Gesetzes, ZD 2022, 148–153.

Schliesky, Utz, Digitale Ethik und Recht, NJW 2019, 3692–3697.

Schmidt, Stephan, Neue europäische Anforderungen im Cybersicherheitsrecht – die NIS2-Richtlinie im Überblick, Kommunikation & Recht (K&R) 2023, 705–710.

Schürmann, Kathrin, Datenschutz-Folgenabschätzung beim Einsatz Künstlicher Intelligenz, ZD 2022, 316–321.

Schweitzer, Heike, Digitale Plattformen als private Gesetzgeber: Ein Perspektivwechsel für die europäische „Plattform-Regulierung", ZEuP 2019, 1–12.

Specht-Riemenschneider, Louisa, Der Entwurf des Data Act, Eine Analyse der vorgesehenen Datenzugangsansprüche im Verhältnis B2B, B2C und B2G, MMR 2022, 809–826.

Spießhofer, Birgit, Compliance und Corporate Social Responsibility, NZG 2018, 441–447.

Spießhofer, Birgit, Unternehmerische Verantwortung, Zur Entstehung einer globalen Wirtschaftsordnung, Baden-Baden 2017.

Steinrötter, Björn, Gegenstand und Bausteine eines EU-Datenwirtschaftsrechts, RDi 2021, 480–486.

Teicke, Tobias, CSR meets Compliance – Über die zunehmende Verrechtlichung der Corporate Social Responsibility, CCZ 2018, 274–275.

Tolks, Daniel, Die finale Fassung des Data Governance Act, Erste Schritte in Richtung einer europäischen Datenwirtschaft, MMR 2022, 444–449.

Thorun, Christian/Kettner, Sara Elisa/Merck, Johannes, Ethik in der Digitalisierung, Der Bedarf für eine Corporate Digital Responsibility, in: Friedrich-Ebert-Stiftung (Hrsg.), WISO Direkt, 17/2018, abrufbar unter https://library.fes.de/pdf-files/wiso/14691.pdf (Stand 1.12.2023).

Wiebe, Andreas, Der Data Act – Innovation oder Illusion?, GRUR 2023, 1569–1578.

Wittmann, Jörn/Haidenthaler, Gregor, IT-Compliance in der Cloud – Rechtssicherheit durch Codes of Conduct?, Anerkannte Verhaltensregeln als Garantie und Nachweis bei der DS-GVO-konformen Cloud-Nutzung, MMR 2022, 8–18.

Wolff, Heinrich Amadeus/Brink, Stefan/von Ungern-Sternberg, Antje (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht, 45. Edition (Stand: 1.8.2023), München 2023.

Datenschutzrechtliche Aspekte bei der Umsetzung der Whistleblower-Richtlinie in Unternehmen

Lucia Neumayer

§ 1 Einführung: Definition

Der Begriff ‚*Whistleblower*' lässt sich von der englischen Redewendung ‚to blow the whistle' ableiten und bedeutet übersetzt so viel wie ‚in die Pfeife blasen'. Im deutschen Sprachraum ist damit ein ‚Enthüller' oder ‚Hinweisgeber' gemeint, der Informationen aus einem vertraulichen oder geheimen Umfeld an die Öffentlichkeit bringt, da diese von allgemeinem Interesse sind. Diese Meldungen betreffen meist Missstände wie Insiderhandel, Korruption oder Datenmissbrauch und verweisen auf Vorgänge in der Politik, in Behörden oder privatwirtschaftlichen Unternehmen. Im beruflichen Kontext schwingt hier oft auch ein negativer Beigeschmack des Denunzierens, ‚Verpetzens' oder ‚Anlastens' mit. Personen wie Julian Assange, der Gründer von WikiLeaks, sowie Edward Snowden, der einen der größten Datenschutzskandale der US-Geschichte mit der Veröffentlichung des PRISM-Überwachungsprogramms der National Security Agency (NSA) auslöste, sind mittlerweile weltweit bekannt und gaben dem Terminus ‚Whistleblower' ein Gesicht.[1]

Bei der Beschäftigung mit Hinweisgebern und deren gesetzlichen Schutz ist ein Blick in die USA unvermeidlich. Der Schutz von Whistleblowern wurde dort im Wesentlichen von drei Bundesgesetzen geformt.

1863 war es der US-Präsident Abraham Lincoln, der mit dem ‚US False Claims Act'[2] die erste Whistleblowing-Bestimmung erließ. Diese Regelung gab Privatpersonen, die im Auftrag des Staates eine Klage einbrachten, einen Anspruch auf einen Teil des Schadenersatzes. In den Vereinigten Staaten ist Whistleblowing daher bereits ein in der Gesellschaft verankertes Instrument zur Aufdeckung von Verbrechen oder Missständen.

1 Ehrbar NetV 2016, 20 (20).

2 United States Department of Justice, The False Claims Act, abrufbar unter: https://www.justice.gov/civil/false-claims-act (Stand 15.12.2023).

Im Jahr 2001 wurde – als Reaktion auf die Bilanzskandale des Energiekonzerns ENRON sowie des Telefonkonzerns WorldCom – der ‚Sarbanes-Oxley Act'[3] (SOX) erlassen.[4] Somit wurden alle US-börsennotierten Unternehmen zur Implementierung von unternehmensinternen Whistleblowing-Hotlines verpflichtet. Auf Grund der exterritorialen Wirkung des SOX sind davon auch ausländische Unternehmen betroffen, wenn deren Aktien an der US-Börse gehandelt werden.[5] Mit der Schaffung des ‚Dodd-Frank Wall Street Reform and Consumer Protection Act'[6], der in Folge der Auswirkungen der Finanzmarktkrise 2007 ein Belohnungssystem für Meldungen von Verstößen gegen US-Wertpapiergesetze etablierte, ging folgende Änderung einher: Whistleblower erhalten seither bei Hinweisen zu Verstößen gegen das amerikanische Wertpapiergesetz einen Teil der Schadenssumme als Belohnung.[7]

Der Begriff ‚Whistleblowing' hat in den letzten zehn Jahren aber auch im öffentlichen Diskurs in Europa stark an Bedeutung gewonnen.[8] Einer der wohl bekanntesten Whistleblower ist Edward Snowden, ein ehemaliger Mitarbeiter der CIA, dem amerikanischen Geheimdienst. Er veröffentlichte im Sommer 2013 geheime Dokumente aus dem PRISM-Programm der National Security Agency (NSA) zur weltweiten Internetüberwachung durch den US-Militärgeheimdienst. Den Hinweis gab er erst anonym, später legte er seine Identität aber offen, weil er sich dadurch mehr Schutz vor den Strafverfolgungen durch die US-Regierung erhoffte. Aufgrund der internationalen medialen Berichterstattung der NSA-Affäre geriet auch Snowden in den Fokus der breiten Öffentlichkeit.[9] Ein weiterer Whistleblower, der mit der Veröffentlichung und Aufklärung von Missständen in amerikanischen Behörden weltweite Bekanntheit erlangte, ist Julian Assange, der Gründer von Wikileaks. Im Sommer 2022 beschloss die Regierung Groß-

3 Vgl. dazu https://www.congress.gov/bill/107th-congress/house-bill/3763/text/enr (Stand 15.12.2023).
4 *Fidler/Winner* in *Kalss/Oppitz/U. Torggler/Winner*, BörseG/MAR § 124 BörseG Rn. 41.
5 Pollirer Dako 2020, 38 (38).
6 https://www.congress.gov/bill/111th-congress/house-bill/4173 (Stand 07.12.2023).
7 *Fleischer/Schmolke* NZG, 361 (368).
8 Hastenrath CB 2022, 58 (58).
9 Ehrbar NetV 2016, 20 (20).

britanniens jedoch, ihn an die Vereinigten Staaten auszuliefern, wo ihm ein Prozess wegen Spionagevorwürfen droht.[10]

Bei diesen Beispielen handelt es sich zwar um besonders schwere Skandale, die aufgedeckt wurden, jedoch nicht um Einzelfälle. Durch den unzureichenden Schutz und die daraus resultierenden teils lebenslangen Nachteile durch die Offenlegung von rechtswidrigen Praxen oder geheimen Unterlagen könnten potenzielle Hinweisgeber jedoch abgeschreckt werden. In Österreich, aber auch in den meisten anderen Mitgliedsstaaten der europäischen Union ist der rechtliche Schutz von Whistleblowern bisher nur unzureichend vorhanden gewesen. Genau dies soll sich mit der EU-Richtlinie zum Hinweisgeberschutz künftig ändern.[11]

§ 2 Tätigwerden der Kommission

Das Ziel der Erarbeitung einer Richtlinie zum unionsweit einheitlichen Schutz von Whistleblowern verfolgte die Europäische Kommission bereits seit 2017. Zu diesem Zeitpunkt hatten nur zehn Mitgliedstaaten einen ausreichenden Schutz für Hinweisgeber gesetzlich verankert. Dazu gehörten: Irland, Italien, Litauen, Malta, die Niederlande, Schweden, die Slowakei, Ungarn und das Vereinigte Königreich. Die anderen Staaten sahen nur teilweise Schutzmechanismen vor bzw. schützten nur bestimmte Gruppen.[12] Am 16.12.2019 trat dann die finale EU-Richtlinie zum Hinweisgeberschutz gem. RL (EU) 2019/1937 in Geltung, die sogenannte Whistleblower-Richtlinie (WBRL).

Bis zu diesem Zeitpunkt war die Erarbeitung der Richtlinie jedoch stark von politischen Auseinandersetzungen umkämpft.[13] Das Drängen zu einer umfassenden Regelung zum unionsweiten Hinweisgeberschutz ging nicht von der Kommission, sondern vom Europäischen Parlament aus. Mit seinen beiden Entschließungen[14] war das Parlament die treibende Kraft, die die Kommission zur Erarbeitung eines Gesetzgebungsvorschlags für einen umfassenden, unionsweiten Schutz von Whistleblowern aufforderte. Am

10 tagesschau, Gründer von WikiLeaks: London bestätigt Auslieferung von Assange an die USA (Stand: 17.06.2022) Vgl. dazu https://www.tagesschau.de/ausland/europa/auslieferung-assange-107.html.
11 Teichmann/Weber CB 2022, 157 (157).
12 Peitsch NetV, 60 (60).
13 Schmolke NZG 2020, 5 (5).
14 2016/2055(INI)); (2016/2224(INI)).

23.4.2018 wurde sodann der erste Vorschlag zur Richtlinie vorgelegt.[15] Dieser war inhaltlich an die Empfehlungen des Europarates zum Schutz von Whistleblowern angelehnt.[16]

Eine von der Europäischen Kommission in Auftrag gegebene Studie im Zuge der Erarbeitung der Richtlinie geht bezüglich der jährlichen Einnahmeausfälle auf EU-Ebene durch Korruption und Betrug von 179 bis 256 Milliarden Euro aus.[17] Nur im Bereich des öffentlichen Auftragswesens sind die Ertragsausfälle, wegen eines nicht ausreichenden Schutzes von Hinweisgebern, jährlich auf 5,8 bis 9,6 Milliarden Euro zu schätzen.[18]

Der erste Vorschlag war dem Europäischen Parlament aber nicht weitreichend genug. Der zuständige Rechtsausschuss legte in einer Entschließung des Parlaments legislative Änderungen vor, die den Schutz der möglichen Hinweisgeber in weitgehender Weise gewährleisten sollte. Zu den umstrittensten Punkten zählten das dreigliedrige Meldesystem (interne Meldung, externe Meldung und Offenlegung) sowie der Schutz von anonymen Hinweisgebern, die erst später identifiziert werden, und der Schutz von Personen, die den Hinweisgeber unterstützen (‚Mittler').[19]

Mitte März des Jahres 2019 gelang es dem Rat und dem Parlament, sich schließlich über die neue Richtlinie zu einigen. Im April des gleichen Jahres gab dann das Parlament seine Zustimmung, im Oktober schließlich auch der Rat. Am 26.11.2019 wurde die EU-Richtlinie dann im Amtsblatt veröffentlicht. Sie ist seit Dezember 2019 in Kraft.

§ 3 Die Whistleblower-Richtlinie

Die Mitgliedstaaten hatten mit einer Frist bis zum 17.12.2021 Zeit, um die neuen Vorgaben der Richtlinie in nationales Recht nach RL (EU) 2019/1937 umzusetzen. Die Realisierung in Österreich erfolgte jedoch nicht fristgerecht, weshalb im Jänner 2022 ein Vertragsverletzungsverfahren durch die Kommission gegen die Republik Österreich eingeleitet wurde.[20] Der erste

15 COM(2018) 218 final.
16 CM/Rec (2014)7).
17 COM(2018) 218 final, 11.
18 COM(2018) 218 final, 3.
19 COM(2018)0218 – C8-0159/2018 – 2018/0106(COD).
20 INFR(2022)0004.

Entwurf zur Umsetzung wurde mit einer Begutachtungsfrist vom 03.6.2022 bis zum 15.7.2022 vom Arbeitsministerium veröffentlicht.[21]

Am 25.02.2023 trat das HinweisgeberInnenschutzgesetz (HSchG)[22] in Österreich schlussendlich in Kraft. Mit über einem Jahr Verspätung wurde damit die WBRL in innerstaatliches Recht umgesetzt.[23]

Im folgenden Kapitel werden die relevantesten Inhalte der Richtlinie näher beleuchtet. Der wesentliche Fokus liegt hierbei auf der datenschutzrechtlichen Umsetzung der WBRL in Unternehmen unter Bezugnahme auf das österreichische Gesetzt, zur Umsetzung der Richtlinie sowie dessen Begutachtungsverfahren.

A. Inhalt und Zweck der Richtlinie

Der Art. 1 der Richtlinie steckt die Ziele der WBRL ab: Diese liegen gem. Art. 1 WBRL in erster Linie darin, die bessere Durchsetzung von Unionsrecht zu gewährleisten sowie das Schutzniveau für Whistleblower zu vereinheitlichen und zu erhöhen.

Der vorgesehene Schutz vor Repressalien soll Beschäftigte gem. Erwgr. 1 WBRL von privaten sowie öffentlichen Organisationen dazu ermutigen, Gesetzesverstöße zu melden, die das öffentliche Interesse betreffen.

B. Anwendungsbereich

I. Persönlicher Anwendungsbereich

Der persönliche Anwendungsbereich der WBRL wird in Art. 4 WBRL weit gefasst, damit möglichst alle Personen, die Informationen über Verstöße offenlegen möchten, ebenfalls geschützt sind.

Vom persönlichen Anwendungsbereich der Richtlinie umfasst werden daher alle Arbeitnehmer, die in den unionsrechtlichen Arbeitnehmerbegriff nach Art. 45 Abs.1 Vertrag über die Arbeitsweise der Europäischen Union fallen. Im Erwägungsgrund 38 zur WBRL wird außerdem festgehalten, dass diese sowohl Personen „*in atypischen Beschäftigungsverhältnissen, Teilzeitbeschäftigte, Personen in befristeten Beschäftigungsverhältnissen und*

21 ME HSchG 2022, 210/ME 27. GP.
22 ÖBGBl. 2023 I 6.
23 Irresberger/Stangl-Krieger/Bruchbacher/Kercz/Wasinger GRCaktuell 2023, 28.

Leiharbeiter" (Erwgr. 38 WBRL) einschließt als auch für Beamte und Vertragsbedienstete im öffentlichen Dienst gelte. Erfasst sind darüber hinaus ehemalige sowie künftige Beschäftigte.

Neben den Arbeitnehmern werden vom persönlichen Anwendungsbereich auch Selbständige gem. Art. 49 AEUV sowie Anteilseigner und Personen eingeschlossen, die dem Verwaltungs-, Leitungs- oder Aufsichtsorgan eines Unternehmens angehören. Des Weiteren sind ebenfalls Berater, Auftraggeber und Lieferanten geschützt.

Aber nicht nur die Person des Hinweisgebers ist abgesichert, vielmehr gilt dies gleichermaßen für natürliche Personen, die den Hinweisgeber unterstützen oder ermutigen, den Hinweis abzugeben, natürliche Personen, die dem Hinweisgeber nahestehen und dadurch auch von Repressalien betroffen sein könnten, wie etwa Kollegen oder Verwandte, sowie des Weiteren ebenfalls juristische Personen, die im Eigentum des Hinweisgebers sind oder für die er arbeitet, so gem. Art. 4 WBRL .

II. Sachlicher Anwendungsbereich

Der sachliche Anwendungsbereich erstreckt sich auf Verstöße gegen das Unionsrecht, die in eine der im Anhang zur Richtlinie angeführten Unionsrechtsakte der Union fallen und in Art. 2 Abs. 1 lit. a WBRL enumerativ aufgelistet sind. Dazu gehören das öffentliche Auftragswesen, Finanzdienstleistungen, Geldwäsche, Terrorismusfinanzierung, Verkehrssicherheit, Umweltschutz, Produktsicherheit, Verbraucherschutz und Datenschutz.

Die Legaldefinition des ‚Verstoßes' findet sich in Art. 5 Ziff. 1 WBRL. Davon umfasst werden rechtwidrige Handlungen sowie Unterlassungen gegen die in Art. 2 WBRL angeführten Rechtsgebiete wie in Art. 5 Z1 WBRL ausgeführt.

Nicht eingeschlossen ist ein unethisches, dem öffentlichen Interesse widerstrebendes Verhalten.[24]

Explizite Ausnahmen des sachlichen Anwendungsbereichs finden sich in Art. 3 Abs. 2–4 WBRL. Dazu zählen etwa Angelegenheiten der nationalen Sicherheit, der Schutz von Verschlusssachen oder jener der anwaltlichen und ärztlichen Verschwiegenheitspflicht, wenn sie durch einen Mandanten oder Patienten einen Verstoß erfahren.

24 Schmolke NZG 2020, 5 (6).

Dies bedeutet aber auch, dass Fälle wie jener von Edward Snowden nicht in den Anwendungsbereich der WBRL fallen würden.[25]

Die Richtlinie gibt den Mitgliedstaaten darüber hinaus die Befugnis, den sachlichen Anwendungsbereich ebenfalls auf Bereiche des jeweiligen nationalen Rechts zu erweitern, so geregelt in Art. 2 WBRL. Eine Ausdehnung auf Verstöße gegen das nationale Recht hätte auf der einen Seite den Vorteil, dass der Hinweisgeber vor der Meldung nicht erst kontrollieren muss, ob der Verstoß tatsächlich europäisches und nicht innerstaatliches Recht betrifft. Eine solche Prüfung wird den Rechtsunterworfenen in vielen Fällen nicht zumutbar sein.[26] Dies kann außerdem dazu führen, dass der Whistleblower seine Meldung aus Angst, doch nicht geschützt zu sein, schlichtweg unterlässt.[27] Auf der anderen Seite trifft dies auch auf die Meldestellen zu, da diese nach Eingang einer Meldung ebenso erst feststellen müssen, ob ein Verstoß gegen das Unionsrecht vorliegt.[28]

C. Das Meldesystem

Die Ausgestaltung und die Umsetzung des Meldesystems gehörten bei der Entstehung der WBRL wohl zu den essenziellsten Streitgegenständen. Erst war die Ausgestaltung als ein dreistufiges System mit den Stufen intern – extern – öffentlich geplant. Letzten Endes wurde jedoch die Entscheidung für ein zweistufiges System getroffen. Die Richtlinie sieht nun ein Meldesystem mit einem internen und einem externen Meldekanal vor und erst danach steht dem Hinweisgeber die Möglichkeit der Offenlegung frei.[29]

In Art. 7 Abs. 2 WBRL wird eindeutig festgehalten, dass die Staaten bei der Umsetzung der Richtlinie in nationales Recht sich verstärkt für interne anstatt externe Meldekanäle einsetzen sollen, wenn dadurch die Wirksamkeit des Vorgehens gegen den gemeldeten Verstoß höher ist und der Hinweisgeber keine Repressalien fürchten muss.

Für Hinweisgeber muss es gem. Art. 9 Abs. 2, Art. 12 Abs. 2 WBRL möglich sein, einen Verstoß sowohl mündlich als auch schriftlich oder durch ein persönliches Treffen zu melden. Dem Whistleblower muss nach der

25 Schmolke NZG 2020, 5 (8).
26 Arnold GesRZ 2020, 153 (154).
27 Kröll/Stumpf RdW 2020, 161 (162).
28 *Falter*, Whistleblower (un)erwünscht? in *Roters/Gräf/Wollmann* (Hrsg), Zukunft Denken und Verantworten (2020) 353 (366).
29 Reppelmund EuZW 2019, 307.

Meldung innerhalb von sieben Tagen eine Bestätigung des Eingangs zugehen. In weiterer Folge muss ihm innerhalb von drei Monaten (in besonderen Fällen sechs Monaten) nach Erhalt der Eingangsbestätigung Rückmeldung über den Stand der Meldung und Folgemaßnahmen erstattet werden, so geregelt in Art. 9 Abs. 1 lit. f WBRL. Zu Letzteren zählen die Schlüssigkeitsprüfung der Hinweise und in weiterer Folge die Einleitung von Ermittlungen, Strafverfolgungsmaßnahmen oder der Abschluss des Verfahrens wie in Art. 5 Ziff. 12 WBRL festgesetzt.

I. Interne Meldekanäle

Mit der Umsetzung der Richtlinie in nationales Recht haben die Mitgliedsstaaten für die Errichtung von internen Kanälen zur Meldung und für verfahrensgerechte Folgemaßnahmen zu sorgen. Meldekanäle sind gem. Art. 8 Abs. 1 WBRL gleichermaßen bei juristischen Personen sowohl im privaten als auch im öffentlichen Sektor einzurichten, was im Einklang mit den Sozialpartnern geschehen sollte.

Von der Pflicht der Errichtung sind juristische Personen des Privatrechts ab 50 Arbeitnehmern betroffen. Unabhängig davon sind nach Art. 8 Abs. 4 WBRL ebenso juristische Personen zur Einrichtung eines Meldekanals verpflichtet, auf die die im Anhang in den Teilen I. B sowie II angeführten Unionsrechtsakten einschlägig sind. Hierbei geht es um Akte des Finanzsektors, der Verhinderung von Geldwäsche und der Bekämpfung von Terrorismus, der Verkehrssicherheit und des Umweltschutzes.[30]

Darüber hinaus besteht für die Mitgliedstaaten gem. Abs. 7 WBRL die Möglichkeit der Mitgliedstaaten, nach Durchführung einer geeigneten Risikobewertung zugleich juristische Personen mit weniger als 50 Arbeitnehmern zur Errichtung von Meldekanälen und Verfahren zu verpflichten. Die Betriebe werden dabei auf ein bestehendes Risiko für die Umwelt oder die öffentliche Gesundheit überprüft. Davon sind Unternehmen betroffen, die insbesondere in den Sektoren der Lebensmittelindustrie, der Pharmazie, der Chemie oder dem Baugewerbe tätig sind.[31] Trifft ein Mitgliedsstaat eine solche Entscheidung, so hat er dies gem. Art. 8 Abs. 8 WBRL der Kommission mitzuteilen, die die anderen Mitgliedsstaaten darüber informieren wird.

30 Novacek FJ 2019, 222 (223).
31 Kröll/Stumpf RdW 2020, 161 (162).

Außerdem sind auch juristische Personen des öffentlichen Rechts von der Pflicht zur Errichtung interner Meldekanäle betroffen. Eine Mitarbeitergrenze wie bei juristischen Personen des privaten Sektors ist hier nicht vorgesehen. Die Richtlinie gibt den Mitgliedstaaten den Handlungsspielraum, Gemeinden mit weniger als 10.000 Einwohnern oder weniger als 50 Arbeitnehmern von der Pflicht zur Implementierung interner Meldekanäle ausnehmen zu können, so geregelt in Art. 8 Abs. 9 WBRL.

Die Art des Meldekanals, der eingerichtet werden muss, unterliegt gem. Art. 8 Abs. 5 WBRL der Entscheidung der juristischen Person des Privatrechts bzw. des öffentlichen Rechts selbst. Zudem muss der Meldekanal nicht im Unternehmen intern betrieben werden, sondern kann ebenfalls an Dritte ausgelagert werden, die damit beauftragt werden, das Hinweisgebersystem für das Unternehmen zu betreiben. Im Erwägungsgrund 53 der Richtlinie werden Beispiele für interne Meldekanäle genannt. Diese können gem. Erwgr. 53 WBRL unter anderem sein: ein Beschwerde-Briefkasten, eine Plattform im Intra- oder Internet oder eine Telefonhotline. Da neben den Beschäftigten aber auch dritte Personen wie Lieferanten oder Subunternehmen in den persönlichen Anwendungsbereich der WBRL fallen und demnach einen Hinweis abgeben können, muss der interne Meldekanal auch für unternehmensfremde Person geöffnet und zugänglich sein.

Das Betreiben der internen Meldestelle muss gem. Erwgr. 54 WBRL nicht durch die juristische Person selbst erfolgen, sondern ist ebenso durch Dritte möglich, wie externe Berater, Prüfer oder spezielle Anbieter von Meldeplattformen sowie Arbeitnehmer- und Gewerkschaftsvertreter. Essenziell ist, dass die Vertraulichkeit und die Identität des Hinweisgebers gewahrt bleiben.

II. Externe Meldekanäle

Grundsätzlich steht es den Hinweisgebern frei, die Meldung an eine interne oder externe Meldestelle zu erstatten. Die Richtlinie hält in Art. 7 Abs. 2 WBRL die Mitgliedsstaaten jedoch dazu an, interne Meldekanäle zu priorisieren.

Behörden sollen von den Mitgliedstaaten als externe Meldestellen benannt und für die Einrichtung einer unabhängigen und autonom handelnden externen Meldestelle sowie für das Setzen geeigneter Folgemaßnahmen zuständig werden. Im Erwägungsgrund 64 werden entsprechende Behörden genannt, die hierfür in Betracht gezogen werden können: Justiz- oder Strafverfolgungsbehörden, Regulierungs- und Aufsichtsstellen, Stellen zur

Korruptionsbekämpfung oder Ombudspersonen, - so geregelt in Erwgr. 64 WBRL.

Bei externen Meldekanälen gelten gem. Art. 11 Abs. 2 lit. b WBRL die gleichen Fristen zur Verständigung von Whistleblowern wie bei internen Kanälen: Innerhalb von sieben Tagen nach einer Meldung muss eine Eingangsbestätigung erfolgen. Nach drei Monaten sowie in besonderen Fällen nach sechs Monaten hat dann gem. Art. 11 Abs. 2 lit. d WBRL die Rückmeldung über den Stand der Meldung und Folgemaßnahmen zu erfolgen. Nach Ende der Ermittlungstätigkeit muss ihm dann gem. Art. 11 Abs. 2 lit. e WBRL ein endgültiges Ergebnis mitgeteilt werden. Speziell geschulte Mitarbeiter der externen Meldestelle sind laut Art. 12 Abs. 4 - 5 WBRL für die Entgegennahme der Meldung, die Einleitung von Folgemaßnahmen und die Kommunikation mit dem Hinweisgeber zuständig. Sollten Mitarbeiter die Meldung auf anderem Weg als über den Meldekanal erhalten, so ist gem. es ihnen Art. 12 Abs. 3 WBRL untersagt, Informationen offenzulegen, durch die die Geheimhaltung der Identität des Hinweisgebers gefährdet werden könnte.

Wird eine Meldung an eine unzuständige Behörde erstattet, so ist diese Behörde verpflichtet, unter Inkenntnissetzung des Hinweisgebers, die Meldung an die jeweils zuständige Behörde weiterzuleiten. Wird es durch das nationale Recht oder das Unionsrecht vorgesehen, so haben die Behörden gem. Erwgr. 71 WBRL darüber hinaus eine Übermittlung der Meldung an die zuständigen Stellen der Union durchzuführen, etwa an das Europäische Amt für Betrugsbekämpfung oder die Europäische Staatsanwaltschaft.

In Art. 13 WBRL heißt es weiters, dass die Behörden leicht verständliche und zugängliche Informationen über die Entgegennahme von Hinweisen und die Vorgehensweise bezüglich Folgemaßnahmen auf ihrer Website zu veröffentlichen haben.

III. Offenlegung

Die Offenlegung ist die letzte Stufe des Meldesystems. Unter einer ‚Offenlegung' versteht die Richtlinie *„das öffentliche Zugänglichmachen von Informationen über Verstöße"* (Art. 5 Ziff. 6 WBRL). Der Weg der Offenlegung nach Art. 15 WBRL steht dem Hinweisgeber jedoch nur frei, wenn einer der folgenden Fälle vorliegt: Die Meldungserstattung ist intern und extern bereits erfolgt, aber keine geeigneten Folgemaßnahmen wurden ergriffen. Weiters erlaubt die Richtlinie die Offenlegung von Meldungen, wenn der Hinweisgeber gem. Art. 8 Abs. 1 WBRL den hinreichenden Grund zur An-

nahme hat, dass eine offenkundige Gefährdung des öffentlichen Interesses existiert, Repressalien befürchtet werden müssen oder die Gefahr der Beweismittelunterdrückung sowie -vernichtung besteht oder die zuständige Behörde am Verstoß selbst beteiligt sein könnte.

IV. Anonyme Meldekanäle

Die Zulassung anonymer Meldungen an Meldestellen wird gem. Art. 6 Abs. 2 WBRL dem nationalen Gesetzgeber überlassen. Einerseits soll damit den Zweifeln gegenüber anonymen Hinweisen entgegengekommen werden, da hier häufig Skepsis bezüglich der Motive sowie ihrer Lauterbarkeit besteht. Andererseits wird die Bereitwilligkeit, Verstöße zu melden, bei künftigen Hinweisgebern auch von der Möglichkeit abhängen, die eigene Identität nicht preiszugeben, sondern anonym zu bleiben.[32]

In der Praxis wird eine gänzliche Anonymität des Hinweisgebers trotzdem oft nicht gegeben sein, weil durch die Meldung und die darin enthaltenen Informationen oftmals ein Rückschluss auf eine Person oder einen einzugrenzenden Personenkreis möglich ist.[33]

V. Konzerninterne Meldekanäle

Für Unternehmensgruppen und Konzerne kann es aus Effizienz- und Kostengründen erstrebenswert sein, ein gemeinsames Whistleblowing-System einzurichten, anstatt jede juristische Person innerhalb des Konzerns mit einem eigenen Meldekanal auszustatten. Grundsätzlich sieht die WBRL auch vor, dass juristische Personen des Privatrechts gemeinsam eine Whistleblowing-Stelle betreiben können. Diese Möglichkeit ist jedoch gem. Art. 8 Abs. 6 WBRL auf Unternehmen mit 50 bis 249 Arbeitnehmern limitiert. Für Konzerne, die in der Mutter- und den Töchtergesellschaften jeweils über 250 Personen beschäftigen, würde dies bedeuten, dass die Konzerne keinen gemeinsamen internen Meldekanal einrichten können. Nach Ansicht der europäischen Kommission genügt ein konzernweites Whistleblowing-System den Anforderungen der WBRL nicht. Dies geht aus zwei Stellungnahmen der Kommission hervor, die den Anfragen von europäischen Großkonzernen folgten. Demnach sei ein zentral im Kon-

32 Schmolke NZG 2020, 5 (9).
33 Artikel 29 Gruppe WP 117, 11.

zern angesiedeltes System contra legem und jede Tochtergesellschaft müsse ein eigenständiges, dezentrales Hinweisgebersystem betreiben. Art. 8 Abs. 6 WBRL wird von der Kommission so ausgelegt, dass auch Tochtergesellschaften die zentrale Meldestelle des Konzerns wählen dürfen, allerdings müssen gleichzeitig eigene Meldekanäle angeboten werden. Zusätzlich muss der Hinweisgeber seine Zustimmung geben, die Ermittlung an der zentralen Stelle erfolgen zu lassen. Verweigert er, die Übertragung der Ermittlung an die konzernzentrale Stelle zu bewilligen, ist der gemeldete Verstoß ausschließlich auf der Ebene der Tochtergesellschaft zu untersuchen. Das Ergebnis dieser Ermittlung darf dann jedoch nach Ansicht der Kommission konzernintern übermittelt werden.

Für Großkonzerne mit Töchtergesellschaften von über 250 Mitarbeitern würde dies zudem bedeuten, dass der Art. 8 Abs. 6 WBRL nicht einschlägig ist und jede Gesellschaft allein für die Einrichtung der Meldekanäle und Ermittlungen zuständig ist.[34]

D. Schutzmaßnahmen

Kapitel VI der WBRL enthält einen Katalog von Maßnahmen zum Schutz der Hinweisgeber und betroffener Personen. Es werden ebenso Sanktionen festgelegt, die auf der einen Seite die Wirksamkeit der Schutzregelungen garantieren sowie andererseits einen abschreckenden Effekt gegen böswillige Meldungen und Repressalien erzielen sollen gem. Erwgr. 102 WBRL.

I. Schutz für Hinweisgeber

Anspruch auf Schutz besitzen in einem ersten Schritt nur jene Hinweisgeber, die vom persönlichen Schutzbereich der Richtlinie umfasst werden. Das Recht auf Schutz eines Hinweisgebers besteht nach Art. 6 Abs. 1 lit. a WBRL weiters nur, wenn der Hinweisgeber hinreichende Gründe zur Annahme hatte, dass der Verstoß in den Anwendungsbereich der WBRL fällt und die Informationen der Zuwiderhandlung zum Zeitpunkt der Meldung der Wahrheit entsprachen.

Für den Schutz des Whistleblowers reicht es aus, dass Letzterer zum Zeitpunkt der Meldung im guten Glauben ist, dass ein Verstoß erfolgt

34 Block/Kremer, Whistleblowing im Konzern: Eine zentrale Stelle ist zu wenig! abrufbar unter: https://www.cmshs-bloggt.de/compliance/whistleblowing-im-konzern-eine-zentrale-stelle-ist-zu-wenig/. (Stand 15.12.2023).

ist. Dieser muss nicht nachweislich vorliegen. Die Richtlinie gibt keine Kriterien für eine Bewertung vor, wann eine Meldung ‚hinreichend' ist. Gemäß Erwägungsgrund 32 ist dies *„eine Schutzvorkehrung gegen böswillige oder missbräuchliche Meldungen, da sie gewährleistet, dass Personen keinen Schutz erhalten, wenn sie zum Zeitpunkt der Meldung willentlich und wissentlich falsche oder irreführende Informationen gemeldet haben."* (Erwgr. 32 S. 3 WBRL)

Wie in Erwgr. 32 S. 5 WBRL festgelegt, sind die subjektiven Motive des Whistleblowers, die ihn zu einer Meldung veranlassen, bei der Frage der Schutzwürdigkeit nicht relevant.

Durch die Voraussetzung der Gutgläubigkeit wird den Whistleblowern der Weg zu einer Meldung oder Offenlegung erleichtert, da es für Laien vermutlich in vielen Fällen schwierig zu erkennen ist, ob der Verstoß nun konkret in den Anwendungsbereich der Richtlinie fällt oder nicht.[35]

Gemäß Art. 6 Abs. 1 lit. b WBRL ist der Schutz des Whistleblowers darüber hinaus an die Voraussetzung geknüpft, dass er intern einen Verstoß meldet oder eine Offenlegung vorgenommen hat. Bei Meldungen, die ein Whistleblower anonym erstattet und bei denen jedoch im Nachhinein seine Identität bekannt wird, erhält er ebenso Schutz vor Repressalien nach Art. 6 Abs. 3 WBRL.

II. Untersagung von Repressalien

Der Begriff der Repressalien wird in Art. 5 Ziff. 11 WBRL legaldefiniert. Darunter zu verstehen sind direkte oder indirekte ungerechtfertigte Handlungen sowie Unterlassungen in einem beruflichen Kontext, die nach einer Meldung oder Offenlegung i. S. d. Richtlinie erfolgen. Für einen umfassenden Schutz des Hinweisgebers ist auch der Begriff der Repressalien äußerst weit gefasst.

Die Mitgliedstaaten müssen nach Art. 19 WBRL jegliche Form von Repressalien, die sich gegen schützenswerte Whistleblower richtet, und deren Androhung verbieten. Beispiele für Repressalien werden außerdem in Art. 19 aufgelistet. Dies können etwa eine Kündigung, Suspendierung, Herabstufung, negative Leistungsbeurteilung oder Mobbing und Diskriminierung sein (Art. 19 WBRL).

35 Kröll/Stumpf RdW 2020, 161 (162).

Den Hinweisgebern sind nach Art. 20 Abs. 2 WBRL unterstützende Maßnahmen anzubieten. Dazu gehört unter anderem eine kostenlose, öffentlich zugängliche Beratung über Abhilfemöglichkeiten und Rechte der betroffenen Person. Die zuständigen Behörden haben außerdem die Hinweisgeber bei der Kommunikation mit anderen Behörden zu unterstützen, die am Schutz vor Repressalien beteiligt sind. Des Weiteren ist eine Prozesskostenhilfe in Strafverfahren für jene Whistleblower bereitzustellen, die sich gerichtlich gegen Repressalien wehren möchten. Ebenso liegt es laut Art. 20 Abs. 2 WBRL in der Hand der Mitgliedstaaten, weitere unterstützende Maßnahmen für Hinweisgeber, wie beispielsweise eine psychologische Beratung, anzubieten, denn in vielen Fällen können die erlittenen Repressalien beim Whistleblower zu finanziellen Schwierigkeiten sowie zu psychischen Auswirkungen führen.[36]

Die Mitgliedstaaten werden nach Art. 21 Abs. 1 WBRL verpflichtet, erforderliche Maßnahmen zu treffen, um die gutgläubig handelnden Hinweisgeber vor Repressalien zu schützen. Die Schutzmaßnahmen gegen Repressalien werden demonstrativ in Art. 21 Abs. 2–8 WBRL gelistet. In Art. 21 Abs. 2 WBRL wird beinahe eine straf- und zivilrechtliche Immunität für Whistleblower festgelegt, demnach können sie für die Verletzung von Berufsgeheimnissen nicht verantwortlich gemacht werden. Noch weitergehender ist der Art. 21 Abs. 7 WBRL: So haben Hinweisgeber in Gerichtsverfahren wegen Verleumdung, Urheberrechts- und Geheimhaltungspflichtverletzungen sowie Verstößen gegen Datenschutzvorschriften, Geschäftsgeheimnisse und Schadensersatzverfahren nicht belangt zu werden. Sie haben zudem die Möglichkeit, eine Klageabweisung zu beantragen.

Nach Art. 21 Abs. 3 WBRL kann ein Hinweisgeber nicht für die Beschaffung der Informationen, die gemeldet werden sollen, belangt werden. Wird beim Erwerb dieser Informationen durch Hinweisgeber jedoch eine Straftat begangen – Erwgr. 92 WBRL nennt hier etwa Hacking oder Hausfriedensbruch –, so greift der Haftbarkeitsausschluss nicht.

Ein weiterer hervorzuhebender Schutzmechanismus ist die in Art. 21 Abs. 5 WBRL geregelte Beweislastumkehr. Legt der Hinweisgeber dar, dass er aufgrund einer getätigten Meldung oder Offenlegung Repressalien erfahren hat, so hat die Partei, die die Repressalien veranlasst hat (zB der Arbeitgeber) entsprechend Art. 21 Abs. 5 WBRL, den Beweis zu erbringen, dass diese auf anderen Gründen als der Meldung basieren.

36 Dilling CZZ 2019, 214 (216).

III. Schutz der betroffenen Person

Neben dem Schutz von Hinweisgebern wird auch jenem der betroffenen Personen in der Richtlinie Rechnung getragen, um eine Rufschädigung und weitere negative Folgen in der Sphäre des Beschuldigten zu vermeiden (Erwgr. 100 WBRL). Demnach müssen die Mitgliedstaaten nach Art. 22 Abs. 1 WBRL sicherstellen, dass die betroffenen Personen gem. der Grundrechte-Charta den Zugang zu wirksamen Rechtsbehelfen, ein faires Verfahren und die Wahrung der Unschuldsvermutung haben. Weiters müssen in einer Meldung beschuldigte Personen ihre Verteidigungsrechte sowie die Rechte auf Anhörung und auf Akteneinsicht vollumfänglich ausüben können. Die Identität der betroffenen Person ist außerdem während der gesamten Dauer einer Meldung durch die zuständigen Behörden und dadurch eingeleitete Folgemaßnahmen zu schützen (Art. 22 Abs. 2 WBRL).

IV. Sanktionen

Gemäß Art. 23 Abs. 1 WBRL wird der Schutz der Hinweisgeber auf der einen Seite noch verstärkt, indem die Richtlinie vorschreibt, dass Mitgliedsstaaten *„wirksame, angemessene und abschreckende Sanktionen"* gegen juristische oder natürliche Personen verhängen, welche Repressalien gegen schutzwürdige Personen ergreifen, Meldungen behindern oder dies versuchen, mutwillig gerichtliche Verfahren anstreben oder gegen den Vertraulichkeitsgrundsatz der Richtlinie in Art. 14 WBRL verstoßen.

Demgegenüber wird in Abs. 2 darüber hinaus festgelegt, dass Hinweisgeber, die wissentlich falsche oder irreführende Informationen gemeldet haben, aus dem Schutzbereich der Richtlinie fallen und dass ihnen **Sanktionen** sowie Schadenersatzpflichten auferlegt werden können.[37] Im Weiteren haben die Mitgliedstaaten entsprechend Art. 23 Abs. 2 WBRL Maßnahmen zur Wiedergutmachung der durch eine Meldung entstandenen Schäden im nationalen Recht umzusetzen.

Zu einem Streitfall können Hinweisgeber werden, die leicht oder grob fahrlässig handeln. In solchen Fällen kann die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) zum Kriterium der Authentizität der Informationen herangezogen werden. Demnach hat ein

37 Dilling CZZ 2019, 214 (216).

Whistleblower vor der Meldung sorgfältig zu prüfen, ob die Informationen zum Verstoß zutreffend und ernstzunehmend sind.[38]

§ 4 Umsetzung der Whistleblower-Richtlinie in Unternehmen

Die Implementierung eines Hinweisgebersystems im Unternehmen sollte möglichst so erfolgen, dass die gemeldeten Verstöße effektiv und nach transparenten internen Leitlinien bearbeitet werden können. Damit werden viele Unternehmen vor neue Aufgaben und Schwierigkeiten gestellt – teils, wenn es darum geht, erstmalig Meldekanäle einzurichten, oder wenn bereits bestehende Hinweisgebersysteme auf die neue Rechtslage auszurichten sind. Hinzu kommen bei der Einführung und im Betrieb von Whistleblowing-Systemen datenschutzrechtliche und arbeitsrechtliche Herausforderungen.[39] Das folgende Kapitel widmet sich speziell den daraus resultierenden datenschutzrechtlichen Fragestellungen, im Groben werden auch mit dem Arbeitsrecht in Verbindung stehende Berührungspunkte skizziert.

A. Datenschutzrechtliche Aspekte im Rahmen von Hinweisgebersystemen

Die Datenschutz-Grundverordnung (DSGVO)[40] gilt seit dem 25.5.2018. Als EU-Verordnung ist sie, anders als die WBRL, die erst in nationales Gesetz gegossen werden muss, in allen Mitgliedsstaaten der Europäischen Union unmittelbar anwendbar. Die DSGVO sieht für die Mitgliedsstaaten einige Öffnungsklauseln vor, die durch den nationalen Gesetzgeber ausgestaltet werden können. Diese Möglichkeit hat Österreich mit der Verabschiedung des Datenschutzgesetzes (DSG) teils genutzt. Das DSG ist gleichzeitig mit dem Datenschutzgesetz in Kraft getreten.[41]

Der sachliche Anwendungsbereich der DSGVO ist nach Art. 2 Abs. 1 eröffnet, wenn „*personenbezogene Daten für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nicht automatisierte*

38 EGMR 16.2.2021, 23922/19.
39 Kröll/Stumpf RdW 2020, 161 (165).
40 VO (EU) 2016/679.
41 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 188.

Verarbeitung personenbezogener Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen."

Unter dem Begriff ‚*personenbezogene Daten*' wird nach Art. 4 Abs. 1 DSGVO die Verarbeitung von Informationen verstanden, die sich auf identifizierte oder identifizierbare natürliche Personen beziehen. Dabei kann die Verarbeitung der Daten ganz oder teilweise automatisiert oder auch nicht automatisiert vorgenommen werden. So fallen ebenfalls rein manuelle Verarbeitungen in den sachlichen Anwendungsbereich, wenn die Verarbeitung in einer strukturierten Sammlung erfolgt.[42]

Bei einem Hinweisgebersystem wird bei nahezu allen eingehenden Meldungen ein Personenbezug bestehen. Der Inhalt einer Meldung wird jedenfalls den Namen des Beschuldigten und bei einer nicht anonymen Meldung den Namen des Hinweisgebers inkludieren. Darüber hinaus werden meist zusätzliche Informationen mit Personenbezug über den Verstoß enthalten sein, wie die Position im Unternehmen oder weitere Umstände der Beobachtungen des Whistleblowers. In einem weiteren Schritt muss die Meldung auf ihre Plausibilität geprüft werden. Dazu wird es notwendig sein, verschiedene personenbezogene Daten aus Datenbanken oder IT-Systemen auszuwerten. Bei einer Bestätigung des Verdachts werden vermutlich weitere Daten aus E-Mail-Postfächern analysiert. In einem weiteren Schritt wird es auch notwendig sein, abschließend Befragungen durchzuführen, um den Sachverhalt aufzuklären. Bewahrheitet sich die Meldung, so werden die Daten schlussendlich in einem Report an den Vorstand oder die Geschäftsführung übermittelt.

Damit wird eine Vielzahl an personenbezogenen Daten – von der Entgegennahme des Hinweises bis hin zur Übermittlung einer sachverhaltsklärenden Stellungnahme – verarbeitet, während der Anwendungsbereich der DSGVO als eröffnet gilt.[43] Jede Verarbeitung von personenbezogenen Daten stellt aber einen Eingriff in das Grundrecht auf Datenschutz des Einzelnen dar. Bei der DSGVO handelt es sich um ein Verbotsgesetz mit Erlaubnisvorbehalten. Demnach ist eine Verarbeitung von personenbezogenen Daten nur erlaubt, wenn die Verarbeitung auf Grundlage der Grundsätze der DSGVO nach Art. 5 stattfindet und die Datenverarbeitung auf Basis einer legitimen Rechtsgrundlage nach Art. 6 erfolgt.[44]

42 Kühling/Raab/Buchner DS-GVO BDSG (2020) Art. 2 Rn. 19.
43 Fehr ZD 2022, 256.
44 Petsche Whistleblowing & Internal Investigations S. 225.

Vor diesem Hintergrund ist es für Unternehmen in der Praxis entscheidend, die Bestimmungen der DSGVO auch bei der Implementierung und im Betrieb eines internen Meldekanals angemessen zu beachten. Schließlich können Unternehmen aus datenschutzrechtlicher Sicht für alle Handlungen im Rahmen des Hinweisgebersystems verantwortlich gemacht werden sowie in Folge Adressat von Bußgeldern oder Schadenersatzforderungen sein.[45]

B. Die rechtmäßige Verarbeitung personenbezogener Daten nach Artikel 6 DSGVO

Personenbezogene Daten können nach Art. 6 DSGVO nur verarbeitet werden, wenn es hierfür eine datenschutzrechtliche Grundlage gibt. Der Verantwortliche – bei Hinweisgebersystemen also in den meisten Fällen das Unternehmen – ist für dessen Einhaltung zuständig. Bei der Abgabe einer Meldung an eine interne Meldestelle werden personenbezogene Daten verarbeitet. Infolgedessen braucht es eine konkrete Rechtsgrundlage, auf die sich die Einrichtung eines Whistleblowing-Systems stützt. Hierfür muss eine der in Art. 6 Abs. 1 lit. a – f aufgezählten Voraussetzungen vorliegen. In einem weiteren Schritt sollen die Rechtgrundlagen, die Einwilligung (lit. a), die Befolgung eines Vertrages (lit. b), die Erfüllung einer rechtlichen Verpflichtung (lit. c) sowie die berechtigten Interessen des Verantwortlichen (lit. f) näher betrachtet werden.

Die Rechtsgrundlage des lebensnotwendigen Interesses (lit. d) sowie die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt (lit. e), können bei der Verarbeitung von personenbezogenen Daten durch das Betreiben eines Hinweisgebersystems wohl ausgeschlossen werden.

I. Die Einwilligung lit. a

Dabei wäre die Einwilligung aller Mitarbeiter des Unternehmens in die Verarbeitung ihrer personenbezogenen Daten durch das Betreiben eines Whistleblowing-Systems der unkomplizierteste Weg. Letzterer ist jedoch aus mehreren Gründen als äußerst kritisch anzusehen. Die Einwilligung muss freiwillig und in informierter sowie unmissverständlicher Weise abgegeben werden. Hier stellt sich die Frage, ob die Einwilligung überhaupt

45 Fehr ZD 2022, 256.

freiwillig erfolgen kann oder ob Mitarbeiter, aufgrund der bestehenden Weisungsgebundenheit und des Abhängigkeitsverhältnisses, das Gefühl haben, sie müssten der Implementierung eines Hinweisgeberschutzsystems zustimmen, da sie sonst beruflich benachteiligt werden könnten. Der Beweis, dass die Einwilligung aus freien Stücken abgegeben wurde, wird für den Verantwortlichen oft schwer zu erbringen sein. Ebenso kann die Einwilligung nicht in informierter Weise erfolgen, sollte eine allgemeine Einwilligungserklärung eingeholt werden. Schließlich ist vor der Abgabe einer Meldung unklar, wer von der Verarbeitung personenbezogener Daten betroffen sein wird. Die Einwilligung kann außerdem nicht pauschal für die Verarbeitung der personenbezogenen Daten im Rahmen des Whistleblowings gegeben werden, der Art. 4 Ziff. 11 DSGVO verlangt nämlich, dass die Einwilligung für den bestimmten Fall erfolgen muss.

Eine Einwilligung für Letzteren kann auch nur vom Hinweisgeber selbst erfolgen und hier nur für die Verarbeitung seiner eigenen personenbezogenen Daten. Er kann nicht in die Verarbeitung der Daten des Beschuldigten oder Dritter einwilligen. Spätestens hier ist die Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO gescheitert und damit keine legitime Rechtgrundlage.[46]

II. Die Erfüllung eines Vertrages lit. b

Art. 6 Abs. 1 lit. b DSGVO wird als taugliche Rechtsgrundlage für die Datenverarbeitung bei Whistleblowing-Systemen ebenso ausscheiden, weil diese wohl nicht mehr mit der Erfüllung des Arbeitsvertrages gerechtfertigt werden kann.[47] Die Datenverarbeitung dient schlussendlich nicht den Beschäftigungsverhältnissen an sich, sondern der Durchsetzung von internen Compliance-Interessen.[48]

46 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 194.

47 Datenschutzkonferenz, Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf (Stand: 15.12.2023).

48 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 196.

III. Die Erfüllung einer rechtlichen Verpflichtung lit. c

Bisher konnten sich nur Unternehmen in ausgewählten Branchen wie dem Bankwesen, wo die Pflicht zur Einrichtung von Meldekanälen bereits gesetzlich vorgeschrieben ist, auf die Rechtgrundlage nach Art. 6 Abs. 1 lit. c stützen.[49] Mit der Umsetzung der WBRL wird sich dies jedoch ändern, da alle Unternehmen mit mehr als 49 Mitarbeitern Hinweisgeberkanäle einrichten müssen. Hiervon erfasst sind jedoch nur Meldungen von Verstößen, die ebenfalls in den sachlichen Anwendungsbereich fallen. Werden darüber hinaus weitere Meldungen abgegeben, die Verstöße gegen weitere Gesetze oder die unternehmensinterne Compliance-Richtlinie aufzeigen sollen, sind diese von der Erfüllung einer rechtlichen Verpflichtung nicht abgedeckt. Auch Unternehmen, die nicht dem Anwendungsbereich der WBRL angehören, weil sie etwa weniger als 50 Arbeitnehmer beschäftigten, können sich nicht auf diese Rechtsgrundlage berufen.[50]

IV. Das berechtigte Interesse des Verantwortlichen lit. f

Für alle Meldungen, die nicht von der Erfüllung einer rechtlichen Verpflichtung umfasst werden, müssen Unternehmen den Erlaubnistatbestand gem. Art. 6 Abs. 1 lit. f DSGVO heranziehen. Die Verarbeitung personenbezogener Daten ist demnach nur zulässig, wenn diese zur Wahrung des berechtigten Interesses des Verantwortlichen erforderlich sind und schwerer wiegen als der Schutz der Grundrechte des Betroffenen.[51] In der Praxis wird es daher erforderlich sein, eine Prüfung des berechtigten Interesses vorzunehmen, ob im Einzelfall die Datenverarbeitung notwendig ist, um das angestrebte Ziel zu erreichen. Ein solches berechtigtes Interesse wird zu bejahen sein, wenn es um die Prävention von Strafverfolgungen, Imageschäden oder massiven wirtschaftlichen Schäden geht. Anders zu bewerten ist die Interessenabwägung, wenn sich der Verstoß gegen den Compliance- oder Ethik-Kodex richtet.[52]

49 Fehr ZD 2022, 256 (257).
50 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 197
51 Altenbach/Dierkes CCZ 2020, 126 (127).
52 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 198.

Bei der Etablierung von Meldekanälen in Unternehmen ist daher ein Augenmerk, darauf zu legen, welche Art und Schwere von Verstößen gemeldet werden. Jede Verarbeitung von personenbezogenen Daten durch Verstöße, die nicht in den gesetzlich definierten Anwendungsbereich fallen, muss vom berechtigten Interesse gedeckt sein. Je weitgehender der Inhalt der Meldung in einem Unternehmen ist, desto schwieriger wird es aus datenschutzrechtlicher Sicht für den Verantwortlichen, gegen den Schutz und die Wahrung der Grundrechte des Betroffenen zu argumentieren. Aus diesem Grund sollten die Beschäftigten ebenfalls dazu angehalten werden, lediglich jene Verstöße zu melden, die strafrechtlich relevant sind, und keine Banalitäten, die voraussichtlich auch von internen Meldestellen nicht verfolgt werden.[53]

Für kleine Unternehmen wurde hier keine Abhilfe geschaffen. Sie stehen vor der gleichen Situation wie vor der Umsetzung der WBRL und können sich derzeit nur auf das berechtigte Interesse stützen.

Eine mögliche Alternative wäre es jedoch, sich auf Art. 88 DSGVO zu berufen. Dieser sieht vor, dass der nationale Gesetzgeber anhand von *„Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext"* festlegen kann. Da es sich bei Art. 88 DSGVO allerdings um eine Öffnungsklausel handelt, haben nicht alle Mitgliedstaaten diese Möglichkeit genutzt. Dies gilt auch für den österreichischen Gesetzgeber[54], weshalb der datenschutzrechtliche Aspekt von Whistleblowing-Systemen für österreichische Unternehmen auf Grund fehlender spezifischerer Vorschriften im Beschäftigungskontext gesetzlich nicht vorgesehen ist und die Möglichkeit der Kollektivvereinbarung, anders als etwa in Deutschland[55], damit keinen gangbaren Weg darstellt.

Arbeitsverfassungsrechtliche Aspekte zur Umsetzung von internen Hinweisgebersystemen in Unternehmen werden im Folgenden in Kap. 4 skizziert.

53 Schmidl in Hauschka/Moosmayer/Lösler Corporate Compliance § 28 Rn. 340.

54 Brodil ecolex 2018, 486 (488).

55 Datenschutzkonferenz Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf. (Stand 15.12.2023).

V. Verarbeitung von personenbezogenen Daten nach Artikel 10 DSGVO

Basiert die Verarbeitung von personenbezogenen Daten auf einer tauglichen Grundlage nach Art. 6 DSGVO, muss geprüft werden, ob auch Daten nach Art. 10 DSGVO über strafrechtliche Verurteilungen und Straftaten verarbeitet werden. Art. 10 DSGVO wird in Zusammenhang mit der Verarbeitung von personenbezogenen Daten durch Hinweisgebersysteme, je nach Art und Schwere des gemeldeten Verstoßes, eine Rolle spielen. Die Verarbeitung der Daten ist demnach unter behördlicher Aufsicht erlaubt oder *„wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten [gestattet ist], das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht.* (Art. 10 DSGVO)

Wird davon ausgegangen, dass auch der Verdacht auf eine begangene Straftat von der Bestimmung des Art. 10 umfasst wird, so ist es für Unternehmen nur dann zulässig, ein Whistleblowing-System einzurichten, wenn sie nach dem nationalen Recht oder dem Unionsrecht der gesetzlichen Pflicht dazu unterliegen. Laut dem DSG ist gem. § 4 Abs. 3 Ziff. 2 ebenfalls die Verarbeitung von personenbezogenen Daten über gerichtliche oder verwaltungsbehördlich strafbare Handlungen und über den Verdacht der Begehung einer Straftat unter Einhaltung der DSGVO gestattet, sofern sich die Zulässigkeit der Datenverarbeitung aus gesetzlichen Sorgfaltspflichten ergibt oder diese zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten laut Art. 6 Abs. 1 lit. f DSGVO erforderlich ist. Hierbei müssen bei der Art der Verarbeitung der Daten die Interessen des Betroffenen nach der DSGVO und dem DSG garantiert werden. Daraus ist zu schließen, dass das berechtigte Interesse eines Unternehmens gleichsam als Rechtsgrundlage für die Verarbeitung von Daten nach Art. 10 DSGVO herangezogen werden kann.[56]

C. Die datenschutzrechtliche Rollenverteilung

Die DSGVO richtet sich an differente Akteure, die auf Grund ihrer Verpflichtungen zu unterscheiden sind. Die Klärung dieser Rollenverteilung ist daher eine grundlegende Frage im Datenschutzrecht, weil von dieser Frage wesentliche Rechts- und Haftungsfragen abhängig gemacht werden.

56 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 200.

Das Ziel der verschiedenen Rollen liegt darin, dass auch beim Zusammenwirken mehrerer Akteure und komplexer Strukturen die Wahrung des Datenschutzes und damit der Schutz personenbezogener Daten garantiert werden können.[57]

In der Praxis müssen sich Unternehmer bei Einführung eines Hinweisgebersystems entscheiden, ob dies ein innerhalb des Unternehmens geführtes Meldesystem ist oder ob dieses an eine externe, nicht direkt im Unternehmen angesiedelte Person oder Organisation ausgelagert wird. Dies kann etwa ein Call-Center oder eine plattformbasierte Whistleblowing-Stelle sein. Daraus ergibt sich in weiterer Folge auch die Rollenverteilung. Ebenso ist für Unternehmensgruppen und Konzerne zu prüfen, inwieweit die datenschutzrechtliche Möglichkeit besteht, für alle juristischen Personen gemeinsam ein Hinweisgebersystem zu betreiben.

I. Die Auftragsverarbeitung nach Artikel 28 DSGVO

Bei einem intern geführten Meldesystem ist der Unternehmer demnach gem. Art. 4 Ziff. 7 DSGVO der Verantwortliche. Letzterer trägt die Entscheidungsfunktion und bestimmt damit über Mittel und Zweck der Verarbeitung personenbezogener Daten. Damit ist er sowohl für die Mehrheit der Pflichten nach der DSGVO als auch für das wesentliche Haftungsobjekt verantwortlich.

Fällt die Wahl auf ein ausgelagertes Hinweisgebersystem, werden durch die Meldung personenbezogener Daten des Hinweisgebers, der betroffenen Person und Dritten wie Zeugen durch einen externen Empfänger verarbeitet. In diesem Fall muss geklärt werden, ob der externe Dritte in einem Auftragsverarbeitungsverhältnis zum Verantwortlichen steht oder ob dieser selbst die Rolle des Verantwortlichen innehat.

Wird der externe Empfänger damit beauftragt, die Meldung zu empfangen, aufzuarbeiten und die Informationen an eine vom Unternehmen benannte Person weiterzuleiten, die dann über Folgemaßnahmen zu entscheiden hat, so wird er klar als Auftragsverarbeiter anzusehen sein. Dementsprechend muss nach Art. 28 DSGVO ein Auftragsverarbeitungsvertrag abgeschlossen werden, wodurch der Datentransfer legitimiert wird und keine zusätzliche Rechtsgrundlage nötig ist. Der Rolle des Auftragsverarbeiters liegt zu Grunde, dass dieser die Verarbeitung ausschließlich auf Weisung des Verantwortlichen vornehmen darf.

57 Artikel-29-Datenschutzgruppe WP 117, 1.

Eine andere Verteilung der Rollen ist gegeben, wenn der Betreiber des externen Meldesystems auch mit der eigenständigen Entscheidung über Folgemaßnahmen, die Ermittlungen und die Nachforschung der Meldung oder der Befragung beauftragt wird. Auf Grund der mangelnden Weisungs- sowie Kontrollmöglichkeiten des Unternehmers gegenüber dem externen Empfänger liegt dann kein Auftragsverarbeitungsverhältnis vor. Der Externe wird in dieser Konstellation zu einem Verantwortlichen. Dies wiederum bedeutet, dass die Datenübermittlung nicht durch einen Auftragsverarbeitungsvertrag legitimiert werden kann, sondern die Datenübermittlung auf einer eigenen Rechtsgrundlage beruhen muss.

Hier kommen einerseits der Art. 6 Abs. 1 lit. c DSGVO und damit die Erfüllung einer gesetzlichen Pflicht zum Tragen. Da aber der externe Empfänger nicht gesetzlich dazu verpflichtet ist, ein Whistleblowing-System für ein fremdes Unternehmen zu betreiben, ist fraglich, ob der lit. c überhaupt eine geeignete Grundlage darstellt. In diesem Fall wird auf Grundlage des Vertrages zwischen dem Unternehmen und der Whistleblowing-Stelle wohl die Rechtsgrundlage der Erfüllung einer vertraglichen Verpflichtung nach lit. b zum Tragen kommen. Andererseits wird die Rechtsgrundlage des berechtigten Interesses des Unternehmens im Sinne des Art. 6 Abs. 1 lit. f in Betracht gezogen werden können.[58]

Sollte zudem ein Unternehmen mit Sitz im Europäischen Wirtschaftsraum (EWR) einen externen Dritten außerhalb des EWR mit der Entgegennahme der Meldungen beauftragen, so muss geprüft werden, ob es sich hierbei um ein ‚sicheres Drittland' handelt. Dies ist der Fall, wenn nach Art. 45 DSGVO ein Angemessenheitsbeschluss der Europäischen Kommission existiert. Liegt ein solcher nicht vor, handelt es sich um ein sogenanntes ‚unsicheres Drittland' und es müssen geeignete Garantien nach Art. 46 DSGVO getroffen werden. Dies kann der Abschluss der Standardvertragsklauseln der Europäischen Kommission oder von Binding Corporate Rules gem. Art. 47 DSGVO sein.[59]

58 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 204.

59 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 206.

II. Die Gemeinsame Verantwortlichkeit nach Artikel 26 DSGVO

Unter dem Aspekt der datenschutzrechtlichen Rollenverteilung muss auch ein Blick auf die Datenübermittlung durch Whistleblowing-Systeme innerhalb eines Konzerns geworfen werden. Schließlich sieht die DSGVO kein Konzernprivileg bei der Übermittlung von Daten vor. Verbundunternehmen sind untereinander wie Dritte iSd. Art. 4 Ziff. 10 zu sehen. Deshalb bedarf die Datenübermittlung zwischen konzernverbundenen Unternehmen einer tauglichen Rechtgrundlage, anzudenken ist hier das berechtigte Interesse nach Art. 6 Abs. 1 lit. f DSGVO.[60]

So könnte ein berechtigtes Interesse des Mutterunternehmens an gemeldeten Verstößen in den Konzerntöchtern argumentiert werden. Die Weiterleitung von ausnahmslos allen gemeldeten Verstößen in einem konzernangehörigen Unternehmen kann sich jedoch nicht auf berechtigte Interessen stützen. Hier sollte der Fokus auf jene Meldungen gelegt werden, die Personen beschuldigen, die durch ihre Funktion eine weitreichende Einflussnahme im Unternehmen haben. Alternativ sollte der Schwerpunkt auf Mitarbeiter gelegt werden, denen zwar nur ein geringer Einfluss innerhalb des Konzerns zukommt, deren Verstoß aber derart schwerwiegend ist, dass ein überwiegendes berechtigtes Interesse der Konzernmutter an der Datenübermittlung besteht. Der Erlaubnistatbestand des Art. 6 Abs.1 lit. f DSGVO wird damit nicht pauschal als Grundlage dienen können, sondern erfordert im Einzelfall eine Interessenabwägung zwischen dem Interesse des Verantwortlichen und den Rechten und Freiheiten der Betroffenen.[61]

Eine weitere Möglichkeit, die bei der Datenübermittlung innerhalb eines Konzernes vorliegen kann, ist die gemeinsame Verantwortlichkeit gem. Art. 26 DSGVO. Dies wäre der Fall, wenn mehrere Unternehmen eines Konzerns gemeinsam einen Meldekanal betreiben. Hierfür müsste eine Vereinbarung über die gemeinsame Verantwortlichkeit geschlossen werden.[62]

Nach Meinung der Art.-29-Datenschutzgruppe soll die Bearbeitung von Hinweisen grundsätzlich von dem Unternehmen des Mitgliedsstaates vorgenommen werden, in dem die Meldung erfolgte. Umfasst ein Konzern

60 Moos/Schefzig/Arning Praxishandbuch DSGVO 56.
61 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 207.
62 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 205

Gesellschaften in verschiedenen EU-Ländern, so sollen die Hinweise nicht automatisch an die Unternehmensgruppe weitergeleitet werden. Hiervon kann eine Ausnahme erfolgen, wenn die Art oder die Schwere des Verstoßes oder auch die Konzernstruktur eine Weiterleitung erforderlich machen.[63]

Sollte bei einem länderübergreifenden Konzern die Übermittlung von Hinweisen ebenfalls in Ländern außerhalb des EWR und damit in ein Drittland erfolgen, so ist wiederum zu beachten, dass die Bestimmung des Kapitels V der DSGVO zur Übermittlung personenbezogener Daten an Drittländer zu erfüllen ist.[64]

D. Spannungsfeld Hinweisgeberschutz und Betroffenenrechte

Bei gemeldeten Verstößen durch Whistleblowing-Systeme ist meist nur ein kleiner Personenkreis unmittelbar für deren Überprüfung und Aufklärung zuständig, um die Verdunklungsgefahr und das Vernichten von Beweisen zu verhindern. Demgegenüber stehen nun die Aufklärungs- und Unterrichtungspflichten nach der DSGVO, die die Aufklärung des Verstoßes und den Schutz des Hinweisgebers gefährden können. Anhand des folgenden Beispiels soll das Spannungsverhältnis zwischen der WBRL und der DSGVO kurz angerissen werden.

Der Verantwortliche hat nach Art. 13 und 14 DSGVO gegenüber Betroffenen seine Informationspflichten zu erfüllen und muss diese darüber in Kenntnis setzen, wenn er deren personenbezogene Daten verarbeitet. Demnach muss eine Person auch darüber informiert werden, wenn sie in einer Meldung beschuldigt wird, ein Fehlverhalten gesetzt zu haben. Zusätzlich stehen den Betroffenen – also den Beschuldigten – ebenfalls die Betroffenenrechte nach Kapitel IIIDSGVO offen. Bekommt diese Person nun Kenntnis von den Ermittlungen gegen sie, so kann diese nach Art. 15 DSGVO bei der Meldestelle eine Kopie der Daten verlangen, die Gegenstand der Ermittlungen sind. Somit könnte der Beschuldigte versuchen, sich gegen die Vorwürfe zu wehren oder Beweise zu vernichten, womit die Aufklärung des Verstoßes gefährdet wäre.[65]

63 Artikel 29 Gruppe WP 117, 18
64 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 192
65 Fehr ZD 2022, 256 (259).

Weiters kann der Beschuldigte auch die Löschung dieser Daten verlangen oder behaupten, die verarbeiteten Daten seien unrichtig, und diese berichtigen lassen.

Nachfolgend soll aufgezeigt werden, wie ein solches Spannungsverhältnis in der Praxis aufgelöst werden könnte.

I. Informationspflicht nach Artikel 13 und 14 DSGVO im Verhältnis zum Hinweisgeberschutz

Der Hinweisgeber selbst kann bei der Abgabe seiner Meldung über die Verarbeitung gem. Art. 13 DSGVO unterrichtet werden. Eine Ausnahme besteht bei der Einreichung einer anonymen Meldung, da in diesem Fall keine personenbezogenen Daten des Betroffenen verarbeitet werden. Sollte im Zuge der Übermittlungen oder durch die abgegebenen Informationen in der Hinweismeldung die Identität des Whistleblowers bekannt werden, so ist die Informationspflicht nach Art.13 zu wahren und der Hinweisgeber über die Verarbeitung zu informieren.[66]

Bei fast allen gemeldeten Verstößen wird der Beschuldigte in der Regel aber nicht wissen, dass seine personenbezogenen Daten durch die Abgabe des Hinweises verarbeitet werden und ihm vom Hinweisgeber ein Vergehen vorgeworfen wird.

Werden die Daten nicht direkt bei den Betroffenen selbst erhoben, so muss nach Art. 14 DSGVO über sämtliche Umstände wie die Speicherung der Daten, die Art dieser Daten, Zwecke der Datenverarbeitung, den Namen und die Kontaktdaten des Verantwortlichen innerhalb eines Monats ab Erhebung der Daten informiert werden. Dies gilt ebenso für Betroffene, die in einer Hinweisgebermeldung eines Verstoßes beschuldigt werden. Im Sinne der Aufklärung von Verstößen und dem Hinweisgeberschutz ist es jedoch kontraproduktiv, den Beschuldigten gem. Art. 14 DSGVO zu unterrichten, weil dies eine Verdunklungsgefahr birgt und der Beschuldigte Beweise vernichten könnte. Diesem Umstand kann mit der Ausnahmebestimmung des Art. 14 Abs. 5 lit. b DSGVO entgegengewirkt werden. Demnach kann die Informationserteilung aufgeschoben werden, wenn dadurch die Verwirklichung der Ziele der Verarbeitung unmöglich gemacht oder ernsthaft beeinträchtigt wird. Diese Ausnahme ist jedoch nicht dauerhaft.

66 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 208.

Sobald der Grund für die Aufschiebung wegfällt, muss die Unterrichtung des Betroffenen unverzüglich nachgeholt werden. Dies wäre der Fall, sobald alle notwendigen Informationen zur Überprüfung des gemeldeten Verstoßes zusammengetragen worden sind. Aus der Sicht der Verantwortlichen besteht ein Risiko, die Erforderlichkeit für die Legitimation des Ausnahmetatbestandes nicht richtig einzuschätzen und den Betroffenen zu spät über die Verarbeitung seiner personenbezogenen Daten zu informieren. Eine Verletzung der Informationspflicht kann für das Unternehmen nach Art. 83 Abs. 5 lit. b DSGVO auch zu einem Bußgeld von bis zu 20.000.000 EUR oder von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs führen.[67]

Auf der Seite des Hinweisgebers erscheint es zudem problematisch, dass laut Art. 14 Abs. 2 lit. f DSGVO ebenfalls die Quelle offenzulegen ist, aus der die personenbezogenen Daten stammen. Das heißt, sofern die Meldung nicht anonym abgegeben wurde, muss die Identität des Whistleblowers offengelegt werden. Die Preisgabe der Identität eines Hinweisgebers nach der DSGVO steht jedoch in einem eindeutigen Widerspruch zum Schutz des Hinweisgebers nach der WBRL. Nach Ansicht der Art.-29-Datenschutzgruppe[68] ist, sofern dies nicht unmöglich ist, die genaue Datenquelle anzugeben. Die Unmöglichkeit nimmt dabei Bezug auf die Rückführbarkeit der personenbezogenen Daten auf die Datenquelle. Bei einer nicht namentlichen Offenlegung der Quelle muss dem Betroffenen jedoch die Art der Quelle genannt werden. Die Art.-29-Datenschutzgruppe vertritt hier die Ansicht, dass in diesem Fall eine rein kategorische Bezeichnung, wie Arbeitnehmer oder Auftragnehmer, ausreicht, um dem Art. 14 Abs. 2 lit. f nachzukommen. Damit ist aber kein völliger Ausschluss der Identifizierbarkeit des Hinweisgebers garantiert. Auch mit der Nennung einer Personenkategorie können Rückschlüsse auf konkrete Personen als Whistleblower gezogen werden, womit der vollumfängliche Schutz von Hinweisgebern nicht gegeben ist.[69]

Diese Pattsituation kann jedoch nach Art. 14 Abs. 5 lit. c DSGVO umgangen werden, wenn durch Rechtsvorschriften der Union oder der jeweiligen Mitgliedstaaten die Erlangung oder Offenlegung ausdrücklich geregelt ist und zudem Maßnahmen zum Schutz der berechtigten Interessen des Be-

67 Altenbach/Dierkes CCZ 2020, 126 (129).
68 Artikel-29-Datenschutzgruppe WP 260 rev.01, 51.
69 Brunner/Nagel Datenschutz Konkret 2020, 32 (33).

troffenen festgehalten werden.[70] Der Art. 23 Abs. 1 lit. i DSGVO gibt den nationalen Gesetzgeber hier in Form einer Öffnungsklausel Handlungsspielraum, wonach die Informationspflicht im Rahmen einer Interessensabwägung beschränkt werden kann, um Rechte und Freiheiten anderer Personen zu schützen.

In Deutschland wurde eine solche Regelung, die die Geheimhaltung der Identität des Hinweisgebers schützt, im § 29 Abs. 1 S. 1 Bundesdatenschutzgesetz (BDSG) verankert. Eine Pflicht zur Unterrichtung liegt demnach nicht vor, wenn durch die Information nach Art. 14 DSGVO Auskünfte offenbart würden, die auf Grund des überwiegenden berechtigten Interesses eines Dritten, wie eines Hinweisgebers, geheim gehalten werden müssen. Eine ähnliche Bestimmung wurde durch den österreichischen Gesetzgeber jedoch nicht vorgesehen. Dies würde bedeuten: Sobald die Ausnahmebestimmung zur Informationspflicht wegfällt, müssen diese nachgeholt und der Beschuldigte über die Identität des Hinweisgebers unterrichtet werden.[71]

Wenn die Meldung daher nicht anonym, sondern unter Offenlegung des Namens des Hinweisgebers erfolgt, sollte dieser beim ersten Kontakt des Systems darauf hingewiesen werden, dass seine Identität zwar geschützt wird, der Beschuldigte aber grundsätzlich einen Monat nach der Meldung bzw. sobald die Voraussetzungen für das Aufschieben der Informationspflicht weggefallen sind, informiert werden muss und damit auch die Identität des Hinweisgebers preisgegeben wird. Sollte Letzterer die Meldung trotz dieser Information nicht anonym abgeben, kommt nach Art. 7 Abs. 2 DSGVO die Einwilligung der Person in Frage und es hat die Information über den Widerruf der Einwilligung zu erfolgen. Ein solcher Widerruf wird jedoch nur bis zu einem Monat nach der getätigten Meldung wirksam sein.[72]

II. Die Auskunftspflicht nach Artikel 15 DSGVO im Verhältnis zum Hinweisgeberschutz

Gemäß Art. 15 DSGVO hat ein Betroffener das Recht, eine Bestätigung vom Verantwortlichen zu erhalten, ob und welche personenbezogenen Daten von ihm verarbeitet werden. Der Betroffene hat laut Erwgr. 52

70 Altenbach/Dierkes CCZ 2020, 126 (130).
71 Brunner/Nagel Datenschutz Konkret 2020, 32 (33).
72 Fassbach/Hülsberg GWR 2020, 255 (257).

DSGVO Anspruch auf eine Kopie seiner personenbezogenen Daten, die Gegenstand der Verarbeitung sind. Darüber hinaus muss es der betroffenen Person möglich sein, das Recht auf Auskunft in angemessenen Abständen auszuüben. Der Verantwortliche muss den Betroffenen ebenfalls über die Datenerhebung in Kenntnis setzen. Bei einer indirekten Datenerhebung, wenn die personenbezogenen Daten nicht bei der betroffenen Person selbst gesammelt werden, wie dies bei Hinweisgebersystemen der Fall ist, stellt sich nun wieder die Frage der Offenlegung der Identität des Whistleblowers. Schließlich hat nach Art. 15 DSGVO auch die beschuldigte Person ein Recht auf Auskunft bezüglich der über sie gespeicherten Daten und deren Herkunft.

Art. 15 Abs. 4 sieht hier eine Ausnahmeregelung vor. Das Recht auf Datenkopie kann demnach beschränkt werden, wenn die Rechte und Freiheiten anderer Personen dadurch beeinträchtigt werden. Nach dem Wortlaut des Art. 15 gilt dieser Ausnahmetatbestand zum Schutz der Rechte und Freiheiten anderer Personen, sofern eine Kopie der Daten nach Abs. 3 angefragt wird.

Nachdem mit dem Recht auf Erhalt einer Kopie auch die nach Abs. 1 zu erteilende Auskunft der Verarbeitung personenbezogener Daten gemeint ist, wird damit die Möglichkeit einer Interessensabwägung für das Recht auf Auskunft eröffnet.[73]

Eine pauschale Verweigerung der Auskunft an den Beschuldigten wird durch diese Ausnahme jedoch nicht gerechtfertigt werden können. Im Einzelfall muss das Interesse des Beschuldigten am Auskunftsanspruch gegen das betriebliche Interesse des Verantwortlichen an der Auskunftsverweigerung und gegen das berechtigte Interesse von Dritten, wie dem Hinweisgeber, dessen Identität tunlichst zu schützen ist, abgewogen werden.

Mit dieser Frage beschäftigte sich das deutsche Landesarbeitsgericht (LAG) Baden-Württemberg[74] im Jahr 2018. Im angesprochenen Fall handelte es sich um die erste Entscheidung im deutschsprachigen Raum, die sich mit Auskunftsverlangen in Bezug auf Hinweisgebersysteme befasste. Konkret ging es um eine interne Whistleblowing-Meldung, deren Ermittlung bereits abgeschlossen war, weshalb eine Verdunklungsgefahr oder Beeinträchtigung des Ermittlungserfolgs ausgeschlossen werden konnte.

Für die datenschutzrechtliche Interessensabwägung kam das LAG zur folgenden Erwägung: Die Geheimhaltung einer Informationsquelle kann

73 Paal/Pauly/Paal DS-GVO Art. 15 Rn. 40-43.
74 LAG Baden-Württemberg 17 Sa 11/18.

ein legitimes Interesse darstellen, wenn der Arbeitgeber als Verantwortlicher dem Whistleblower zum Zwecke der internen Aufklärung des gemeldeten Fehlverhaltens Anonymität zusichert. Nach Ansicht des LAG bestehen jedoch auch Fälle, in denen das Geheimhaltungsinteresse hinter das Auskunftsinteresse tritt, etwa wenn der Hinweisgeber eine Meldung wider besseres Wissen abgibt oder leichtfertig unrichtige Informationen weitergibt. In einer solchen Konstellation dürfte das Auskunftsverlangen der beschuldigten Person unter Berücksichtigung eines erhöhten Schutzbedarfes schwerer wiegen.

Die Zusage der Anonymität des Hinweisgebers kann aber nicht schlichtweg als Grund für eine zulässige Auskunftsversagung herangezogen werden. Besteht keine gesetzlich verankerte Geheimhaltungspflicht, sondern wurde diese lediglich vereinbart, ist im Einzelfall eine Interessensabwägung vorzunehmen.

Das LAG verurteilte den Arbeitgeber in seiner Entscheidung dazu, dem beschuldigten Mitarbeiter *„eine Kopie seiner personenbezogenen Leistungs- und Verhaltensdaten, die Gegenstand der vorgenommenen Verarbeitung sind, bereitzustellen"*.[75]

In Deutschland besteht nach § 29 Abs. 1 BDSG, wie bereits beschrieben wurde, keine Auskunftsverpflichtung, sofern dadurch Informationen offengelegt werden, die wegen des überwiegenden berechtigten Interesses eines Dritten geheim zu halten sind. In Österreich kann jedoch auf eine vergleichbare Norm nicht zurückgegriffen werden. Unter Beachtung des Art. 15 Abs. 4 DSGVO sind jedoch auch in Österreich im Einzelfall eine Interessensabwägung vorzunehmen und damit die Vertraulichkeit der Identität des Hinweisgebers sicherzustellen.[76]

Für Unternehmen, die der WBRL unterliegen, schafft hier Art. 16 WBRL Abhilfe und statuiert das Vertraulichkeitsgebot für die Identität des Whistleblowers sowie von Dritten. Unbefugte dürfen keinesfalls Zugang zu den Daten der Meldungen haben. Anzumerken ist jedoch, dass damit nicht alle Dokumente und Unterlagen des Meldekanals umfasst werden, sondern nur jene, aus denen indirekt oder direkte die Identität des Hinweisgebers hervorgeht.[77] Eine Ausnahme bildet der Abs. 2, sofern es sich um eine nach dem nationalen Recht oder dem Unionsrecht *„notwendige und verhältnismäßige Pflicht im Rahmen der Untersuchungen durch nationale Be-*

75 Altenbach/Dierkes CCZ 2020, 126 (129).
76 Brunner/Nagel Datenschutz Konkret 2020, 32 (33).
77 Altenbach/Dierkes CCZ 2020, 126 (129).

hörden oder von Gerichtsverfahren" handelt. Trifft dies zu, darf die Identität des Hinweisgebers offengelegt werden. Davor muss Letzterer jedoch nach Art. 16 Abs. 3 WBRL darüber informiert werden. Auch ist ihm dazu eine schriftliche Begründung zu übermitteln.

Mit dem Spannungsfeld zwischen dem Schutz der Identität des Whistleblowers und der Einhaltung des Datenschutzrechtes beschäftigen sich ebenso die Erwägungsgründe 84 und 85 der WBRL. Die Mitgliedstaaten sollen demnach, um die Wirksamkeit der WBRL zu gewährleisten, die DSGVO und die Rechte der Betroffenen mit gesetzgeberischen Maßnahmen einschränken, soweit und solange dies notwendig ist (Erwgr. 84-85 WBRL). Damit wird es auf die Ausgestaltung der Umsetzungsakte der Mitgliedstaaten ankommen, die DSGVO einzuschränken, um den Schutz von Hinweisgebern zu gewährleisten.

III. Recht auf Berichtigung nach Artikel 16 DSGVO

Art. 16 DSGVO regelt das Recht auf Berichtigung durch den Betroffenen. Demnach hat Letzterer das Recht, vom Verantwortlichen eine unverzügliche Berichtigung seiner inkorrekten personenbezogenen Daten sowie eine Komplettierung von unvollständigen personenbezogenen Daten zu verlangen.[78] Im Zusammenhang mit Hinweisgebersystemen kann dies von Relevanz sein, wenn der Betroffene von der Meldung erfährt, in der er beschuldigt wird, und die Informationen zu seinen personenbezogenen Daten inhaltlich unwahr sind oder der Beschuldigte behauptet, dass diese inkorrekt sind. Für die ermittelnde Meldestelle wird zu diesem Zeitpunkt oft noch nicht klar sein, ob es sich tatsächlich um eine falsche Meldung handelt oder der Betroffene dies nur angibt. Die Berichtigung hat nach Art. 16 S. 1 jedoch unverzüglich zu erfolgen.

Gemäß S. 2 besteht für den Betroffenen zudem die Möglichkeit, die Ergänzung seiner unvollständigen Daten zu verlangen. Personenbezogene Daten gelten als fragmentarisch, wenn diese in Bezug auf die konkrete Verarbeitung so lückenhaft sind, dass der mit der Verarbeitung verfolgte Zweck nicht (mehr) erreicht wird.[79]

Dies wäre der Fall, wenn der Betroffene behauptet, dass die in der Meldung offengelegten personenbezogenen Daten so unvollständig seien,

78 Paal/Pauly/Paal DS-GVO Art. 16 Rn. 13-14.
79 Paal/Pauly/Paal DS-GVO Art. 16 Rn. 18.

dass eine sachverhaltsaufklärende Überprüfung des Verstoßes nicht erzielt werden kann.

Eine derartige Anwendung des Art. 16 DSGVO würde aber gegen den Zweck der WBRL sprechen. Dem Beschuldigten sollte im Sinne der Aufklärung des Verstoßes und der Reduktion der Verdunklungsgefahr nicht schon in einem frühen Stadium der Ermittlungen die Möglichkeit gegeben werden, seine Perspektive darzulegen.

Das Verwaltungsgericht Köln entschied zum Berichtigungsanspruch nach Art. 16 DSGVO, dass es sich bei dem Tatbestandsmal der ‚Unrichtigkeit' nach der unionsrechtlichen Auslegung um ein objektives Kriterium handelt und dieses nur auf Tatsachenangaben anwendbar ist. Demnach kann sich ein Berichtigungsanspruch aus Art. 16 DSGVO nur dann ergeben, wenn feststeht, dass die Daten, die der Verantwortliche verarbeitet, objektiv nicht mit der Realität übereinstimmen, und gleichzeitig sicher ist, dass die vom Betroffenen als richtig erklärten Daten auch tatsächlich mit der Wirklichkeit übereinstimmen.[80]

Eine dahingehende Gewissheit in Zusammenhang mit einem Verlangen auf Berechtigung bei Whistleblowing-Meldungen wird bei der verantwortlichen Meldestelle wohl nicht vorliegen können, weshalb die gespeicherten Informationen eines Hinweises demnach nicht unverzüglich berichtigt werden müssen.

IV. Widerspruchsrecht nach Artikel 21 DSGVO

Art. 21 DSGVO schützt den Betroffenen gegen eine Verarbeitung, die nicht in seinem Willen ist. Nach Abs. 1 kann sich der Betroffene mit dem Widerspruchsrecht jedoch nur gegen eine Verarbeitung wehren, die zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung öffentlicher Gewalt nach Art. 6 Abs. 2 lit. e DSGVO erforderlich ist oder zur Wahrung des berechtigen Interesses des Verantwortlichen dient, soweit das Interesse des Berechtigten gegenüber der Grundfreiheit des Betroffenen gem. Art. 6 Abs. 1 lit. f DSGVO überwiegt. Die Beschränkung auf die Rechtsgrundlage ergibt sich daraus, dass dem Betroffenen bei der Einwilligung nach lit. a ohnedies die Möglichkeit des jederzeitigen Widerrufs offensteht. Bei Erfüllung eines Vertrages nach lit. b würde der Widerruf wohl einen Vertragsbruch darstellen. Im Falle der Verarbeitung gestützt auf die

80 VG Köln 25 K 2138/19.

Rechtsgrundlage des Art. 6 Abs. 1 lit. c geht das Widerspruchsrecht ebenso vor wie das lebenswichtige Interesse nach lit. d.[81]

Besteht die gesetzliche Verpflichtung zur Führung eines Hinweisgebersystems, so wird der Widerspruch nach Art. 21 DSGVO demnach nicht von praktischer Relevanz sein. Wird der interne Meldekanal freiwillig betrieben und wird hierfür die Rechtsgrundlage nach dem berechtigten Interesse des Verantwortlichen gem. Art. 6 Abs. 1 lit. f herangezogen, ist es im Einzelfall die Aufgabe des Verantwortlichen, eine umfassende Interessenabwägung durchzuführen. Dabei ist das besondere Interesse des Betroffenen gegen das eigene zwingend schutzwürdige Interesse des Verantwortlichen oder einer anderen dritten Person abzuwiegen. Bei einer Datenverarbeitung nach lit. f wird dies schon daraus resultierten, dass sowohl das Interesse des Verantwortlichen als auch des Dritten die Verarbeitung der personenbezogenen Daten des Betroffenen legitimieren. Als schutzwürdig sind hierbei alle Gründe zu sehen, die vom Unionsrecht oder von nationalen Gesetzen anerkannt sind. Der Widerspruch des Betroffenen kann durch den Verantwortlichen damit rechtmäßig verweigert werden, wenn er beweisen kann, dass die Datenverarbeitung auf Grund von zwingendem schutzwürdigem Interesse des Verantwortlichen oder eines Dritten gegenüber den Grundrechten und Freiheiten des Betroffenen überwiegt.[82]

E. Durchführung einer Datenschutz-Folgenabschätzung nach Artikel 35

Eine Datenschutz-Folgenabschätzung ist durchzuführen, wenn die Verarbeitung der personenbezogenen Daten aufgrund der Art, des Umfanges, der Umstände und des Zwecks der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten von natürlichen Personen zur Folge hat. Diese Voraussetzungen sind bei einem Hinweisgebersystem zu bejahen, da mit der Meldung Informationen von potenziellen Gesetzesverstößen verarbeitet werden. Dies kann mit zum Teil schwerwiegenden Folgen für den Beschuldigten, den Hinweisgeber und die in der Meldung genannten dritten Personen einhergehen. Damit existiert ein hohes Risiko für die Rechte und Freiheiten der Betroffenen.[83] Dass ein Hinweisgebersystem dem

81 Knyrim/Haidinger DatKomm Art. 21 Rn. 27.
82 Knyrim/Haidinger DatKomm Art. 21 Rn. 42.
83 Datenschutzkonferenz, Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendaten-

Art. 35 DSGVO unterliegt, zeigt auch eine Entscheidung der italienischen Datenschutzbehörde Garante per la Protezione dei Dati Personali (GPDP). Gegen die Flughafenbetreibergesellschaft Aeroporto Guglielmo Marconi di Bologna S.p.A. sowie den externen Betreiber des Whistleblowing-Systems wurde wegen einer fehlenden Datenschutzfolgeabschätzung für den Meldekanal und -prozess für beide insgesamt Parteien eine Geldbuße iHv 60.000 Euro verhängt.[84]

Eine Ausnahme besteht nach der Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V). Dieses sieht gem. § 2 Abs. 2 letzter Satz vor, dass eine Datenschutz-Folgenabschätzung nicht zu realisieren ist, wenn die Verarbeitung im Zusammenhang mit dem Arbeitsverhältnis erfolgt und bereits eine Betriebsvereinbarung abgeschlossen wurde. Besteht jedoch kein Betriebsrat, ist es demnach erforderlich, eine Datenschutz-Folgenabschätzung durchzuführen, da die Daten von Arbeitnehmern und damit besonders schutzwürdigen Personen nach § 2 Abs. 3 Ziff. 4 DSFA-V verarbeitet werden und die Verarbeitung der personenbezogenen Daten gem. § 2 Abs. 3 Ziff. 1 DSFA-V umfangreich ist. Zwar bietet die DSGVO keine Definition, was unter einer ‚umfangreichen Verarbeitung' zu verstehen ist, im Sinne eines ordentlichen Risikomanagements sollte allerdings eine Datenschutz-Folgenabschätzung in betriebsratlosen Betrieben realisiert werden.[85]

F. Erstellung eines Löschkonzeptes

Ein weiteres Spannungsverhältnis der WBRL und der DSGVO manifestiert sich zwischen den Dokumentationserfordernissen nach Art. 18 WBRL und den Löschpflichten nach Art. 17 Abs. 1 DSGVO.[86]

Aus dem Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e DSGVO sind Daten zu löschen, sobald diese nicht mehr benötigt werden.

schutz, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf (Stand: 15.12.2023).

84 Garante per la Protezione dei dati personali 9685922, abrufbar unter: https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9685922 (Stand: 15.12.2023).

85 Schweiger RdW 2020, 533 (535).

86 Fehr ZD 2022, 256 (260).

Sowohl die Datenschutzkonferenz[87] als auch die Art.-29-Datenschutzgruppe[88] sehen eine Frist von zwei Monaten nach Abschluss der Ermittlungen vor, nach der die personenbezogenen Daten zu löschen sind. Sind jedoch weitere rechtliche Schritte wie die Einleitung eines Strafverfahrens oder eines Disziplinarverfahrens notwendig, so kann die Speicherdauer ausgeweitet werden, während die Löschung nach Ende der Rechtsmittelfristen des Verfahrens durchzuführen ist.

In der Praxis kann dies problematisch werden, wenn es zu einem späteren Zeitpunkt, etwa durch eine weitere Meldung eines Hinweisgebers oder neue Informationen bekannt werden. Die DSGVO sieht hierfür eine einzige Ausnahme im Art. 17 Abs. 3 lit. e vor, sofern erst weitere rechtliche Schritte wie Disziplinarverfahren oder die Einleitung von Strafverfahren abgeklärt werden müssen. Dies gilt der Sicherung zur Geltendmachung eigener Rechtsansprüche sowie der Verteidigung gegen Rechtsansprüche von Dritten.[89]

Auf Basis dieser Ausnahme können personenbezogene Daten jedoch nicht immer bis zur Verjährungsfrist aufbewahrt werden. Um sich zulässigerweise auf die Ausnahme des Art. 7 DSGVO stützen zu können, wird dies mit einem bereits laufenden Verfahren zu begründen sein oder ein solches mit hinreichender Wahrscheinlichkeit zu erwarten sein. Wird mit keinen Verfahren in absehbarer Zeit gerechnet, sondern will das Unternehmen die Löschung nur aufschieben, weil es möglicherweise zu einem Rechtsstreit kommen könnte, wird im Einzelfall eine Interessensabwägung durchzuführen sein. Eine längere Speicherung der Daten wird demnach nur möglich sein, wenn konkrete Anhaltspunkte vorliegen, dass die Geltendmachung von Rechtsansprüchen oder deren Schwere gegenüber dem Eingriff in die Grundrechte des Betroffenen, der mit der Aufbewahrung verbunden ist, überwiegt.[90]

Eine Abhilfe für die Praxis bietet die Pseudonymisierung und Verschlüsselung der Daten nach Art. 32 Abs. 1 lit. a DSGVO. Die bereits abgearbeiteten Meldungen können von einer Art ‚Löschgruppe' mit den zuständigen Akteuren des Unternehmens aus den Compliance-, Datenschutz- und Per-

87 Datenschutzkonferenz, Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf (Stand: 15.12.2023).

88 Artikel-29-Datenschutzgruppe WP 117, 14.

89 Fehr ZD 2022, 256 (260).

90 Altenbach/Dierkes CCZ 2020, 126 (129).

sonalabteilungen pseudonymisiert werden. In einem weiteren Schritt kann die pseudonymisierte Meldung archiviert werden, wobei eine Löschung zu einem späteren Zeitpunkt zwingend notwendig sein wird.[91]

Anstelle der Löschung können die Daten, wenn möglich und sinnvoll, auch anonymisiert werden, da die DSGVO auf diese nicht anwendbar ist und damit ein Wissensverlust von bisherigen Meldungen vermieden wird.[92]

§ 5 Arbeitsverfassungsrechtliche Aspekte bei der Umsetzung

Mit dem Einsatz von Hinweisgebersystemen kommt es zu einer weitreichenden Verarbeitung personenbezogener Daten der Beschäftigten. Diese Daten bergen das Risiko eines Eingriffs in die Persönlichkeitsrechte der Arbeitnehmer. Aus diesem Grund sind Whistleblowing-Systeme nicht nur auf ihre datenschutzrechtliche, sondern ebenso auf ihre arbeitsverfassungsrechtliche Zulässigkeit zu prüfen.[93]

Aus der Sicht des Arbeitsrechts stellt sich bei der Einrichtung interner Whistleblowing-Kanäle die Frage, ob diese die Zustimmung des Betriebsrates durch eine Betriebsvereinbarung erfordern – oder jene der Arbeitnehmer, sofern kein Betriebsrat besteht.

A. Zustimmung des Betriebsrates

Nach der Bestimmung des § 96 Abs. 1 Ziff. 3 des Arbeitsverfassungsgesetzes (ArbVG) brauchen Kontrollmaßnahmen und technische Systeme, die auf die Kontrolle der Arbeitnehmer abzielen und die Menschenwürde berühren, zu ihrer Rechtswirksamkeit die Zustimmung des Betriebsrates.

In ihrer Spruchpraxis ging die Datenschutzbehörde davon aus, dass bei der Einrichtung von Whistleblowing-Kanälen zwingend immer eine Betriebsvereinbarung abgeschlossen werden muss. Während *Thiele/Wagner*[94] dieser Linie folgen und den Abschluss einer Betriebsvereinbarung als zwingend ansehen, da es sich um eine Kontrollmaßnahme handelt, die die

91 Fehr ZD 2022, 256 (260).
92 Petsche/Abd El Malak/Feiler/Rieken/Romandy Whistleblowing & Internal Investigations 212.
93 Knyrim/Haidinger Praxishandbuch Datenschutzrecht S. 114.
94 Thiele/Wagner Umsetzung der DSGVO in der Personalpraxis S. 48.

Menschenwürde berührt, sind Teile der Lehre anderer Ansicht und üben scharfe Kritik an dieser Spruchpraxis. Demnach müsse bei der Einführung von Hinweisgebersystemen differenziert werden, ob diese die gesetzlichen Mindestinhalte überschreiten oder nicht. Hier kommt es bezüglich der Frage, ob eine Betriebsvereinbarung abgeschlossen werden muss, darauf an, ob die vorausgesetzten Tatbestandsmerkmale vorliegen. Im Falle der Einrichtung von Whistleblowing-Systemen sind hier die Tatbestände der Betriebsvereinbarung von Relevanz: einerseits der bereits angesprochene § 96 Abs. 1 Ziff. 3 ArbVG und andererseits § 96 a Abs. 1 Ziff. 1 ArbVG.[95]

Für personenbezogene Daten des Arbeitnehmers, die über die Ermittlung von allgemeinen Angaben zur Person und zu fachlichen Voraussetzungen hinausgehen, gilt Folgendes: Nach der genannten Bestimmung braucht die Einführung von Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung solcher Daten nur dann den Abschluss einer Betriebsvereinbarung, wenn die tatsächliche oder vorgesehene Verwendung dieser Daten über die Erfüllung von Verpflichtungen nicht hinausgeht (§ 96a Abs. 1 Z 1 ArbVG).

Hier wird jedoch die Ansicht der Datenschutzbehörde, dass es sich bei Hinweisgebersystemen um Kontrollmaßnahmen nach § 96 Abs. 1 Ziff. 3 ArbVG handelt und nicht um Systeme zur Personaldatenverarbeitung, außen vorgelassen. Erfolgt die Subsumtion eines Hinweisgebersystems nämlich unter § 96 Abs. 1 Ziff. 3 ArbVG, so ist jedenfalls der Abschluss einer Betriebsvereinbarung verpflichtend – selbst dann, wenn die Errichtung des Meldesystems auf Grundlage einer gesetzlichen Verpflichtung erfolgt. Die Rechtsansicht der Datenschutzbehörde wird auch in diesem Punkt als inhaltlich zu undifferenziert kritisiert. Sofern nur bestimmte Verstöße, wie jene gegen das Unionsrecht, zu melden sind und nicht jegliches Fehlverhalten bekanntzugeben ist, das durch einen Arbeitnehmer gesetzt wird (zB eine Arbeitszeitverletzung oder Mobbing am Arbeitsplatz), erfüllt ein Hinweisgebermeldesystem wohl nicht die Voraussetzungen eines Kontrollsystems bzw. erlangt es nicht eine derartige Intensität, die bei Beschäftigten das Gefühl einer ständigen Überwachung auslöst.[96]

Schweiger[97] vertritt aufgrund der Tatsache einer gesetzlich verankerten Mindestausgestaltung eines Hinweisgebersystems die Ansicht, dass sich Unternehmen bei der Einführung interner Meldekanäle für Whistleblower auf

95 Zankl/Kühteubl/Pusch Rechtshandbuch der Digitalisierung Rn 69.
96 Zankl/Kühteubl/Pusch, Rechtshandbuch der Digitalisierung Kap. 13.
97 Schweiger RdW 2020, 533.

die Bestimmung des § 96 a Abs. 1 Ziff. 1 ArbVG berufen können. Damit bedarf ein Whistleblowing-System, das nur die gesetzlich vorgeschriebenen Mindestinhalte umsetzt und von Unternehmen auf Grund der Anzahl der Mitarbeiter oder der Branche eingerichtet werden muss, nicht der Mitwirkung des Betriebsrates.

Anderes gilt, wenn sich ein Unternehmen, das nicht der gesetzlichen Verpflichtung zur Einrichtung eines Whistleblowing-Systems unterliegt, die Entscheidung trifft, ein solches einzuführen. Dann wird jedenfalls die Mitwirkung des Betriebsrates benötigt. Wenn sich das Unternehmen jedoch hierbei nach den gesetzlichen Mindestmaßen richtet und nicht darüber hinausgeht, so ist nach Ansicht von *Schweiger* auch eine fakultative Betriebsvereinbarung nach § 97 Abs. 1 Ziff. 20 ArbVG in Betracht zu ziehen.[98]

Ob eine Betriebsvereinbarung abzuschließen ist, wird daher oft vom konkreten Einzelfall und den Ausgestaltungen des Systems abhängen. Wird im Betrieb ein Zustand der ständigen Kontrolle erreicht, weil die Beschäftigten vertraglich dazu verpflichtet sind, jegliches Fehlverhalten und jegliche Verstöße gegen interne Compliance-Richtlinien zu melden, und kommt es so zu einem „dauernden Spitzelwesen", so wird eine Betriebsvereinbarung zwingend notwendig sein.[99]

Bei einer Ausgestaltung der Hinweisgeberkanäle über die gesetzliche Mindestverpflichtung hinaus ist damit in allen Betrieben davon auszugehen, dass es sich hierbei um Kontrollmaßnahmen iSd § 96 Abs. 1 Ziff. 3 ArbVG handelt und eine zwingende Betriebsvereinbarung abzuschließen ist.

Aufgrund der verschiedenen Auswertungs- und Verknüpfungsmöglichkeiten wird jedoch teils auch die Meinung vertreten, dass es unwahrscheinlich ist, dass das Meldesystem sich stets innerhalb des gesetzlichen Rahmens bewegt, womit die Einrichtung des Whistleblowing-Systems immer auch die verpflichtende Mitwirkung des Betriebsrates braucht.[100] In ähnlicher Weise äußert sich ebenfalls die Judikatur des Obersten Gerichtshofes[101]. Demnach besteht eine Kontrollmaßnahme nach § 96 Abs. 1 Ziff. 3 ArbVG bereits, wenn die denkbare Möglichkeit eines Eingriffs in die Sphäre der Menschenwürde gegeben ist.

98 Schweiger RdW 2020, 533 (534).
99 Stella/Winter ZAS 2021/22, 124 (126).
100 Schweiger RdW 2020, 533 (534).
101 OGH 8 ObA 288/01p.

Stella/Winter[102] vertreten jedoch die Annahme, dass auch dann, wenn ein Hinweisgebersystem, das nur die Mindestanforderungen des Gesetzes erfüllt, dazu genutzt werden könnte, die Menschenwürde zu berühren, für den Betriebsinhaber die Möglichkeit der Einrichtung eines Meldesystems besteht – auch ohne die Zustimmung bzw. das Veto des Betriebsrates. Der Zweck der zwingenden Mitbestimmung des Betriebsrates besteht darin, die Gestaltungsmöglichkeiten von Arbeitgebern bei sensiblen Themen an die nur in bestimmten Fällen ersetzbare Zustimmung des Betriebsrates zu koppeln. Hat der Arbeitgeber jedoch gar nicht die Freiheit zur Gestaltung der Arbeitsbedingungen, sondern ist er durch den Gesetzgeber zu einem bestimmten Handeln verpflichtet, kann diese Pflicht nicht durch das Mitwirkungsrecht eines Betriebsrates umgangen werden. Durch die WBRL und die nationalen Umsetzungsakte der Mitgliedsstaaten werden Unternehmen ab einer bestimmten Mitarbeiteranzahl dazu verpflichtet, Hinweisgebersysteme mit gewissen Mindeststandards umzusetzen. Mit diesem Gesetz als lex specialis wird die betriebsverfassungsrechtlich verankerte Mitwirkung verdrängt.

Damit wird eine Betriebsvereinbarung nur dann notwendig sein, wenn das Unternehmen nicht gesetzlich dazu verpflichtet ist, ein internes Hinweisgebersystem einzurichten oder wenn dieses über die gesetzlich erforderliche Mindestausgestaltung hinausgeht.

Schweiger[103] nennt eine weitere Möglichkeit, um bei der Einführung von Whistleblowing-Systemen von einer die Menschwürde berührenden Maßnahme hin zu einem Personaldatensystem zu rücken: die Auslagerung des internen Meldekanals an einen Dienstleister, der sich gegenüber dem Unternehmen vertraglich dazu verpflichtet, die aus den Meldungen stammenden Informationen nicht zur Kontrolle der Mitarbeiter heranzuziehen, sondern sich rein im gesetzlichen Mindestmaß eines Hinweisgebersystems zu bewegen und Meldungen, die nicht in den sachlichen Anwendungsbereich fallen, nicht weiterzuverfolgen.

Als weitere Maßnahme, um das Berühren der Menschwürde der Arbeitnehmer zu verhindern, bietet sich das System der stufenweisen Kontrollverdichtung an. Hier wird der Zugriff auf die inhaltlichen Informationen einer Meldung in einer ersten Stufe auf eine technische Auswertung wie zB auf Schlagworte beschränkt. In einem nächsten Schritt erfolgt die Auswertung

102 Stella/Winter ZAS 2021/22, 124 (126).
103 Schweiger RdW 2020, 533 (534).

mit Bezug auf vorab festgelegte Zwecke, die in den Anwendungsbereich des Gesetzes fallen. Erst in der dritten Stufe sollen inhaltliche Ermittlungen in der Meldung unter der Verarbeitung von personenbezogenen Informationen möglich sein.[104]

B. Zustimmung der Arbeitnehmer

Sofern kein Betriebsrat vorhanden ist, muss bei der Einführung von internen Hinweisgebersystemen die schriftliche Zustimmung jedes einzelnen Arbeitnehmers gem. § 10 Abs. 1 Arbeitsvertragsrechts-Anpassungsgesetz (AVRAG) eingeholt werden, wenn keine gesetzliche Pflicht zur Errichtung besteht oder die Ausgestaltung über die gesetzlichen Mindestanforderungen hinausgeht.[105] Nach § 10 Abs. 2 des AVRAG kann die Zustimmung des Beschäftigten, soweit eine schriftliche Vereinbarung mit dem Arbeitgeber über deren Dauer nicht vereinbart wurde, jederzeit ohne Einhaltung einer Frist schriftlich gekündigt werden. Im Fall der Verweigerung der Zustimmung oder deren Rücknahme dürfte das Whistleblowing-System nicht mehr auf diesen Arbeitnehmer anwendbar sein. Er darf also weder Hinweise geben noch dürfen diese in einer Meldung genannt werden.

§ 6 Der österreichische Umsetzungsakt der WBRL

Obwohl die Umsetzungsfrist zur WBRL am 17.12.2021 endete, ist die EU-Richtlinie erst im Februar 2023 dem Nationalrat zur Beschlussfassung vorgelegt worden und trat mit 25. Februar 2023 in Kraft.

A. Der Anwendungsbereich

Die WBRL lässt den Mitgliedsstaaten die Möglichkeit offen, den sachlichen Anwendungsbereich auf nationale Gesetze auszudehnen (vgl. Kap. 2.2). Diesen Spielraum hat Österreich in gewissem Ausmaß auch genutzt und Meldungen über Korruptions- sowie Amtsdelikte (§§ 302–309 StGB) in § 3 Abs 3 HSchG aufgenommen.

104 Kotschy/Reimer ZAS 2004, 167.
105 Neumayr/Reissner Zellkomm Rn 3.

Der § 28 Abs. 3 HschG schreibt eine Beurteilung der Wirkung des HSchG ab 2026 vor. Ziel dieser Regelungen ist es, auf Basis der Erfahrungen der folgenden Jahre die Ausdehnung der Geltungsbereiche im innerstaatlichen Recht zu erweitern.[106]

Auch laut dem allgemeinen Teil der Erläuterungen zum Gesetz sind spätere Erweiterungen des sachlichen Geltungsbereichs vorgesehen. Dies wird nach den künftigen Erfahrungen mit dem HSchG zu entscheiden sein. Weshalb dies aber erst zu einem späteren Zeitpunkt beschlossen werden soll, wird damit begründet, dass kleine und mittlere Unternehmen mit der Einrichtung eines neuen Hinweisgebersystems nicht zu stark belastet werden sollten.[107]

Bezüglich der Frage, welche Betriebe ein Whistleblowing-System verpflichtend einführen müssen, findet sich eine Präzisierung in § 11 Abs. 2 HSchG. Bei Unternehmen mit (saisonal) fluktuierenden Mitarbeiterzahlen wird laut § 3 Abs. 2 HSchG die durchschnittliche Anzahl der Mitarbeiter der drei personalstärksten Monate des vergangenen Kalenderjahres herangezogen, um festzulegen, ob diese einen internen Meldekanal einrichten müssen oder nicht.

B. Die Rechtsgrundlage

Das Gesetz bildet in § 8 Abs. 2 DSGVO die Rechtgrundlage für die Verarbeitung von personenbezogenen Daten aus Hinweisgebersystemen. Demnach kommt für Unternehmen, die in den Anwendungsbereich der Richtlinie fallen, die Rechtsgrundlage des Art. 6 Abs. 1 lit. c zum Tragen.

C. Anonyme Meldungen

Die WBRL verpflichtet die Mitgliedsstaaten nicht dazu, anonyme Hinweise zuzulassen (vgl. Kap. 2.3.4), doch wird die Möglichkeit der Anonymität für Hinweisgeber im Gesetz vorgesehen. Sollte deren Identität dennoch offengelegt werden, so sieht § 6 Abs. 3 HSchG vor, dass dem Hinweisgeber trotzdem der Schutz nach den Bestimmungen des HSchG garantiert ist.

Im Falle einer anonymen Meldung werden jedoch die Information an den Hinweisgeber über Folgemaßnahmen nach § 11 Abs. 9 HSchG oder

106 210/ME 27. GP Erläut 14.
107 210/ME 27. GP Erläut 1.

auch die Bestätigung des Gesprächsprotokolls mit Unterschrift gem. § 9 HSchG nicht möglich sein.

D. Konzerninterne Meldekanäle

Nach § 13 Abs. 4 HSchG besteht für Konzerne und Unternehmensgruppen die Möglichkeit, ein Whistleblowing-System gemeinsam zu betreiben und dieses auch einem externen Dienstleister auszulagern. Soweit ein gemeinsames Hinweisgebersystem betrieben wird, sieht das § 8 Abs. 3 HSchG vor, dass die Betriebe gemeinsam verantwortlich sind, gem. Art. 4 Ziff. 7 in Verbindung mit Art. 26 DSGVO.

Anders als in der WBRL sowie in den dazu verfassten Stellungnahmen der Europäischen Kommission (vgl. Kap. 2.3.5) gibt es jedoch keine gesetzlich vorgeschriebene Maximalanzahl von Beschäftigten, die das Betreiben einer gemeinsamen internen Whistleblowing-Stelle einschränkt. Damit wäre es auch für Großkonzerne mit Tochtergesellschaften über 250 Mitarbeiter möglich, gemeinsam ein Hinweisgebersystem zu betreiben. Zudem schreiben das nationale Gesetz sowie auch die WBRL ausdrücklich die Möglichkeit vor, Dritte mit dem Betrieb eines internen Meldekanals zu betrauen. Damit könnte ebenfalls eine Tochtergesellschaft im Konzernverbund mit dem Betrieb eines Whistleblowing-Systems für die anderen Gesellschaften beauftragt werden. Dies widerspricht jedoch der Ansicht der Art.-29-Datenschutzgruppe, wonach die Meldung vorrangig in jenem Mitgliedsstaat bearbeitet werden soll, in dem diese getätigt wurde (vgl. Kap. 3.3.2).[108]

Hier verabsäumte der Gesetzgeber es, mit einer ausreichend klaren Bestimmung Rechtsunsicherheiten völlig auszuräumen. Zu hoffen bleibt, dass im finalen Gesetzesentwurf oder in den Erläuterungen klargestellt wird, ob für Konzerne die zentrale Einrichtung einer Meldestelle ausreichend ist.

E. Datenschutzrechtliche Einschränkungen

In § 8 HSchG werden Einschränkungen des Datenschutzrechts zu Gunsten des Betriebs von Hinweisgebersystemen vorgesehen. Nach § 8 Abs. 1 HSchG dient die Verarbeitung der personenbezogenen Daten den Zwecken

108 Artikel-29-Datenschutzgruppe WP 117, 18.

des HSchG nach § 1 und § 8 Abs. 2 Ziff. 1. Hier wird jedoch offengelassen, welche Art der Datenverarbeitung vorgesehen werden kann.

Der § 8 Abs. 9 HSchG legt eine weitgehende Beschränkung der Betroffenenrechte nach Kapitel III DSGVO fest. Demnach muss ein Unternehmen den Betroffenen nach Art. 13 und 14 DSGVO nicht darüber informieren, dass eine Meldung über ihn eingegangen ist, und auch nicht seiner Auskunftspflicht gegenüber dem Betroffenen nach Art. 15 DSGVO nachkommen.

In den Gesetzesmaterialien finden sich jedoch keine Erläuterungen dazu, welcher Rechtsgrund des Art. 23 Abs. 1 lit. a bis j DSGVO die konkrete Beschränkung erfordert. Dies wurde im Begutachtungsverfahren vom Datenschutzrat als auch dem Bundesministerium für Justiz kritisiert, demnach sei eine Prüfung dahingehend notwendig, in welchem Ausmaß sowie für welche Zeitspanne die Beschränkung der Betroffenenrechte zur Zweckerreichung tatsächlich erforderlich ist. Die Beschränkungen konkretisiert und befristet werden.[109] Der Kritik dieser ausufernden Beschränkung der Betroffenenrecht wurde im HinSchG durch den Gesetzgeber nicht Rechnung getragen.

F. Datenschutz-Folgenabschätzung

Nach Art. 35 Abs. 10 DSGVO müssen Verantwortliche mit der gesetzlichen Verpflichtung nach dem Unionsrecht oder dem Recht des Mitgliedstaats zur Einrichtung eines Hinweisgebersystems keine eigene Datenschutz-Folgenabschätzung durchführen, sofern im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass des Gesetzes eine Datenschutz-Folgenabschätzung bereits erfolgte und es nach dem Ermessen des Mitgliedstaates nicht erforderlich ist. Demnach ist eine konkrete Datenschutz-Folgeabschätzung für die Einrichtung und den Betrieb eines Hinweisgebersystems ist vom Verantwortlichen nach § 8 Abs. 13 HSchG nicht durchzuführen, weil im Rahmen des Gesetzgebungsverfahren bereits eine allgemeine Datenschutz-Folgeabschätzung erfolgte.[110]

109 Datenschutzrat, Stellungnahme abrufbar unter, https://www.parlament.gv.at/PAKT/VHG/XXVII/SNME/SNME_221151/index.shtml (Stand: 15.12.2023); Bundesministerium für Justiz, Stellungnahme abrufbar unter https://www.parlament.gv.at/gegenstand/XXVII/SNME/221188/ (Stand: 15.12.2023).

110 210/ME 27. GP Erläut 9.

Auf diese Ausnahme kann sich eine Person jedoch nur berufen, wenn die Verarbeitung der personenbezogenen Daten auf der Rechtsgrundlage des Art. 6 Abs. 1 lit. c (Erfüllung einer rechtlichen Verpflichtung) oder lit. e (Wahrnehmung einer Aufgabe im öffentlichen Interesse) aufbaut. Erfolgt die Datenverarbeitung im Rahmen eines internen Meldekanals jedoch auf lit. f (berechtigtes Interesse), so ist demnach eine Datenschutz-Folgenabschätzung durchzuführen.

Kritik zu dieser beigelegten Datenschutz-Folgenabschätzung wurde im Rahmen des Begutachtungsverfahrens des Ministerialentwurfs unter anderem durch die Datenschutzbehörde und den Datenschutzrat kundgetan. Demnach sei die allgemeine Datenschutz-Folgenabschätzung zu pauschal gehalten, um den Vorgaben der DSGVO zu entsprechen. Besonders die Maßnahmen zur Datensicherheit sind zu wenig konkret und dürften vor allem für Verantwortliche, die nun ein Hinweisgebersystem einführen müssen, kaum eine Hilfe darstellen. Hier wird jedoch nur auf Art. 32 DSGVO verwiesen. Die Sicherheit der Verarbeitung, die in dieser Bestimmung geregelt wird, ist jedoch bei jeder Datenverarbeitung einzuhalten. Hier wäre es vielmehr sinnvoll gewesen, dem Stand der Technik entsprechende Maßnahmen anzuführen, um den verantwortlichen Stellen im Unternehmen einen Weg aufzuzeigen. Denkbar wäre hier etwa die Schulung der Mitarbeiter, die Hinweise bearbeiten, oder eine entsprechende Verschlüsselung der Meldekanäle.[111]

G. Die Aufbewahrungsfrist

Die Aufbewahrungsfrist, welche im Ministerialentwurf des Gesetzes vorgesehen war, stand in einem klaren Spannungsverhältnis zur DSGVO und konfligierte mit den Grundsätzen der DSGVO der Zweckbindung, der Datenminimierung und der Speicherbegrenzung von personenbezogenen Daten nach Art. 5 DSGVO.

Die vormals vorgesehen Aufbewahrungsfrist war mit dreißig Jahren ab der letztmaligen Verarbeitung und bei Protokolldaten sogar dreiunddreißig Jahre ab der letztmaligen Verarbeitung vorgesehen gewesen (§ 8 Abs. 9 -10 ME HSchG). Diese Aufbewahrungsfrist wicht damit vom Unionsrecht ab. Zwar können Einschränkungen der DSGVO nach Art. 23 DSGVO zulässig

111 Datenschutzbehörde, Stellungnahme abrufbar unter https://www.parlament.gv.at/PtWeb/api/s3serv/file/cb34b15b-dc74-4c93-90fb-b377813afb9b (Stand: 15.12.2023).

sein, diese müssen aber notwendig und verhältnismäßig sein, was bei Speicherfristen von bis zu dreiunddreißig Jahren fraglich ist.

Ausführungen in den Erläuterungen zum Gesetz, weshalb eine so lange Aufbewahrungsdauer gewählt wurde, gab es dazu nicht. Eine derart lange Frist wurde auch vom EU-Gesetzgeber nicht initiiert. Art. Art. 18 WBRL sieht vor, dass Meldungen nicht länger aufbewahrt werden sollten, als dies erforderlich und verhältnismäßig ist. Eine Verkürzung der Aufbewahrungsfrist scheint in Anbetracht dessen angemessen.

In den im § 3 Abs. 3 HSchG angeführten Bereichen, die in den sachlichen Anwendungsbereich des Gesetzes fallen, findet sich sogar nur selten eine Verjährungsfrist von bis zu zehn Jahren, wie bspw. die Geldwäschebestimmung gem. § 21 FM-GwG oder die Aufbewahrung ärztlicher Aufzeichnungen und Dokumentationen nach § 51 Abs. 3 ÄrzteG. Bei gemeldeten Verstößen, die sich gegen das Verwaltungsstrafrecht richten, gilt nach § 31 VStG lediglich eine Verjährungsfrist von drei Jahren.

Die lange Verjährungsfrist von dreißig Jahren nach § 1489 S. 2 ABGB, wenn dem Betroffenen der Schaden oder der Schädiger nicht bekannt wurden oder der Schaden aus einem Verbrechen entstanden ist, wird zumeist weder erforderlich noch verhältnismäßig sein.

Bei Meldungen, die sich als unrichtig herausstellen, wird eine Aufbewahrung zudem gar nicht notwendig sein. Eine Begründung zu dieser überaus langen Speicherfrist findet sich lediglich in der Datenschutz-Folgeabschätzung und lautet wie folgt: *„Diese Frist orientiert sich an der längsten für Verfahren der Rechtsdurchsetzung relevanten Verjährungsfrist.“*[112]

Diese Begründung wird für die meisten Meldungen aus internen Hinweisgebersystemen, wie soeben dargelegt, nichtzutreffend sein und lässt außerdem die Ansicht der österreichischen Datenschutzbehörde außer Acht, wonach der Verantwortliche darlegen muss, *„welche konkreten zukünftigen Verfahren auf welcher Grundlage anhängig gemacht werden könnten und inwiefern durch derartige Verfahren eine Notwendigkeit zur weiteren Speicherung der personenbezogenen Daten begründet wird“*.[113]

In der Praxis würde dies aber mit einem äußerst hohen administrativen Arbeitsaufwand einhergehen. Der § 10 Abs. 6 sieht schließlich vor, dass diese Daten unter hohen Sicherheitsstandards *„in einem vertraulichen und sicheren System zu speichern“* (§ 10 Abs. 6 ME HSchG) sind. Eine so lange

112 210/ME XXVII. GP - Ministerialentwurf - Datenschutz-Folgenabschätzung.
113 DSB-D123.085/0003-DSB/2018, 27.08.2018.

Aufbewahrungsfrist pauschal festzulegen, würde zudem auch gegen den Sinn und Zweck eines Löschkonzeptes sprechen.

Aus diesem Grund folgte der Gesetzgeber in diesem Punkt den kritischen Stellungnahmen, welche während des Begutachtungszeitraums eingingen und die Aufbewahrungsfrist wurde unter § 8 Abs. 11 HSchG neu geregelt. Die vorgeschriebene Frist für personenbezogene Daten aus Hinweisgebersystemen beträgt fünf Jahre ab der letztmaligen Verarbeitung. Zudem sind personenbezogene Daten so lange aufbewahrt werden, wie es für laufende Verwaltungs-, Zivil- oder strafrechtliche Ermittlungsverfahren erforderlich ist.

Protokolldaten über Verarbeitungsvorgänge, wie etwa Änderungen, Abfragen und Übermittlungen, unterliegen einer gesonderten Aufbewahrungsfrist von drei Jahren über die übliche Aufbewahrungsdauer hinaus. Nach Ablauf dieser Aufbewahrungsfrist sind personenbezogene Daten zu löschen (§ 8 Abs. 12 HSchG). Personenbezogene Daten, die nicht für die Verarbeitung von Hinweisen erforderlich sind, dürfen nicht erhoben werden und müssen, sollten diese versehentliche erfasst werden unverzüglich gelöscht werden wie § 8 Abs. 10 HSchG festlegt.

H. Sanktionen

Die WBRL regelt in Art. 23, dass die Mitgliedstaaten bei der Umsetzung in nationales Recht wirksame Sanktionen festzulegen haben (vgl. Kap. 2.4.4). Dies findet sich im Entwurf des HSchG, wobei jedoch nicht über die Richtlinie hinausgegangen wird. Der § 24 HSchG sieht Strafbestimmungen für Personen vor, die Maßnahmen der Vergeltung gegen Hinweisgeber setzen, den Schutz der Vertraulichkeit verletzen und ebenso für Personen, die wissentlich einen falschen oder irreführenden Hinweis geben. Hierbei handelt es sich um eine Verwaltungsübertretung, die mit einer Geldstrafe von bis zu 20.000 Euro und im Wiederholungsfall bis zu 40.000 Euro zu ahnden ist. Eine Strafe für Unternehmen, die zwar der gesetzlichen Pflicht zur Einrichtung eines Whistleblowing-Systems unterliegen, dieser aber nicht nachkommen, gibt es lt. § 24 HSchG. nicht.

I. Übergangsfristen

Verpflichtet nach dem HSchG sind Unternehmen und juristische Personen des öffentlichen Bereichs ab mindestens 50 Mitarbeitenden. Unternehmen sind juristische Personen des Privatrechts sowie rechtsfähige Personengesellschaften. Damit sind auch Vereine und gemeinnützige Organisationen verpflichtet Meldekanäle zu implementieren und betreiben. Die Gesellschaft bürgerlichen Rechts sowie der der Einzelunternehmer sind damit ausgenommen. Ebenfalls in die Pflicht miteinbezogen sind juristische Personen des öffentlichen Sektors, wie Bund, Länder und Gemeinden.[114]

In § 28 HSchG hat der Gesetzgeber jedoch Übergangsfristen für die Einführungen der Hinweisgebersysteme vorgesehen.

Ab dem Inkrafttreten des Gesetzes gilt eine Übergangsfrist von sechs Monaten, somit bis zum 25.8.2023 für juristische Personen mit mindestens 250 Beschäftigten (§ 28 Abs. 1 HSchG).

Unternehmen mit weniger als 250 Arbeitnehmern wird eine Übergangsfrist bis zum 18.12.2023 gewährt (§ 28 Abs. 2 HSchG). Damit ist die Umsetzung der WBRL in Österreich zwei Jahre nach der Umsetzungsfrist der Europäischen Kommission für die Mitgliedstaaten, die am 17.12.2021 endete, vollzogen.

§ 7 Conclusio

Mit der Umsetzung der WBRL in innerstaatliches Recht durch das HSchG kann in Österreich der Anreiz zur Abgabe von Hinweisen und zum Schutz der Hinweisgeber geschaffen werden. Aber nicht nur für die hinweisgebende Personen bietet der Schutz vor Repressalien Vorteile, auch für Unternehmen hat die Einführung von integren Whistleblowing-Systemen einen klaren Mehrwert. Zwar mag die Sorge vor Denunzianten und einer Flucht von Hinweisen groß sein, die noch größere Chance, dadurch möglichen Verstößen intern aufzuklären und sich dadurch zu verbessern, bevor sich Hinweisgeber damit an externe Meldestelle oder die Öffentlichkeit wenden, sollte nicht verkannt werden.

Auch wenn der Handlungsspielraum, den die WBRL den Mitgliedstaaten in Bezug auf den sachlichen Anwendungsbereich offen lässt vom österreichischen Gesetzgeber, teils genutzt wurde und nationales Recht mit einbe-

114 Irresberger/Stangl-Krieger/Bruchbacher/Kercz/Wasinger GRCaktuell 2023, 28.

zogen wurde (vgl. Kap.5.1), so ist bei der Umsetzung in Unternehmen der Rahmen für mögliche Meldungen nicht zu streng nach dem Gesetz auszulegen. Vielmehr sollten weitere Hinweise zu nationalen Gesetzen oder internen Compliance-Policys zugelassen werden. Einerseits ist für den Hinweisgeber in manchen Fällen gar nicht abschätzbar, ob der Verstoß, den er melden will, nun beispielsweise das europäische oder nationale Vergaberecht betrifft. Andererseits ist es im Interesse des Unternehmens, Kenntnis über mögliches Fehlverhalten und Verstöße zu haben und dagegen intern vorgehen zu können.

Meines Erachtens wäre es daher sinnvoll, das Gesetz in Zukunft auf innerstaatliches Recht auszudehnen. Schließlich sind hier auch einzelne Bundesländer bei der Umsetzung der WBRL weitergegangen: Das Burgenländische Hinweisgeberschutzgesetz (Bgld. HSchG) erstreckt den sachlichen Anwendungsbereich auf alle Verstöße gegen Landesrecht (§ 3 Bgld. HSchG). So resultiert die Situation, dass erstens Beschäftigte bei einem Rechtsträger der öffentlichen Hand wie der burgenländischen Landesregierung einen viel umfassenderen Rechtsrahmen bei der Meldung von Verstößen haben als Arbeitnehmer im privaten Sektor im Burgenland. Zweitens kommt es damit in neun verschiedenen Landesgesetzen zum Hinweisgeberschutz und zusätzlich zu einem bundesweiten Gesetz, wobei alle nicht aufeinander ausgerichtet sind.

Für Unternehmen birgt der aktuell vorliegende Gesetzesentwurf zur Umsetzung der WBRL außerdem das Potential zu Konflikten mit dem Datenschutzrecht. Dies betrifft einerseits Unternehmen, die nun erstmalig einen internen Meldekanal einrichten, und andererseits Unternehmen, die ein bereits bestehendes zu adaptieren haben, um dieses gesetzeskonform zu betreiben.

Für Konzerne ist derzeit noch offen, ob ein zentraler gemeinsamer Meldekanal immer geführt werden kann oder ob jede Tochtergesellschaft dies dezentral zu organisieren hat. Hinzu kommt die Frage, wie mit Tochtergesellschaften umzugehen ist, die etwa weniger als 50 Mitarbeiter beschäftigen. Diese würden nicht in den Anwendungsbereich des Gesetzes fallen. Dabei gibt es für jeden Betrieb auch die Möglichkeit, freiwillig ein Whistleblowing-System zu führen. In diesem Fall gelten jedoch nicht die datenschutzrechtlichen Erleichterungen, die im Gesetz vorgesehen sind, wie die Beschränkungen der Betroffenenrechte nach Kapitel III der DSGVO. In einer Unternehmensgruppe würde dies bedeuten, dass kleine Tochtergesellschaften nicht an zentralen Meldekanälen teilnehmen dürften bzw. deren Meldungen datenschutzrechtlich anders zu behandeln wären.

Ein weiteres Problem bei der Umsetzung für Unternehmensgruppen stellt sich in der zu Aufbewahrungsfrist. Diese wird nicht von der WBRL vorgegeben, was heißt, dass jeder Mitgliedstaat diese im nationalen Gesetz festlegt. Bei länderübergreifenden Unternehmensgruppen würde dies eine unterschiedlich lange Aufbewahrungsfrist je nach Sitz der Gesellschaft bedeuten.

Sitzt die Konzernmutter etwa in Deutschland und die Tochter in Österreich, so müsste eine Meldung, die von einem Mitarbeiter in der österreichischen Gesellschaft getätigt wird, nach dem HSchG fünf Jahre ab der letzten Verarbeitung aufbewahrt werden. In Deutschland, wo sich die Konzernmutter befindet, ist die Meldung jedoch laut Gesetz für einen besseren Schutz hinweisgebender Personen Hinweisgeberschutzgesetz (HinSchG) bereits drei Jahre nach Abschluss des Verfahrens zu löschen, besagt § 11 (5) HinSchG. Dies stellt besonders bei gemeldeten Verstößen, die Konzerne in verschiedenen Mitgliedstaaten betreffen, eine Herausforderung dar und gilt auch für den Fall, dass die Ermittlungen nicht nur in jenem Land, in dem die Meldung erfolgte, aufgenommen werden, sondern ebenso in anderen Ländern. Werden die Fristen für die Aufbewahrung nach den unterschiedlichen innerstaatlichen Ländern alle beachtet, so muss dies auch bei der Erarbeitung des Löschkonzeptes und der Strukturierung des Berechtigungsmanagements beachtet werden. Aufbauend auf dem bereits genannten Beispiel müsste die Dokumentation zum Hinweis und zu den eingeleiteten Ermittlungen demnach bei der Konzernmutter in Deutschland nach drei Jahren gelöscht werden. Bei der österreichischen Tochter könnte der Hinweis aber noch zwei weitere Jahre gespeichert werden.

Ob die Einrichtung von zentralen Meldekanälen in einer Konzerngruppe gesetzlich möglich ist und falls ja, bis zu welcher Beschäftigtenanzahl dies vorgesehen ist, wurde auch mit Inkrafttreten des Gesetzes noch nicht abschließend geklärt. Die Europäische Kommission und die Art.-29-Datenschutzgruppe haben sich bereits gegen den Betrieb einer zentralen Meldestelle ausgesprochen, die auch in allen Verstößen die Ermittlungen durchführen sollte. In der Praxis hat der Betrieb einer zentralen Meldestelle in Konzernen viele Vorteile. Einerseits werden mit der Bündelung Kosten und Ressourcen gespart, andererseits kann sich eine Tochtergesellschaft auf den Betrieb des Hinweisgebersystems spezialisieren, sodass alle Verbundunternehmen den Meldekanal an eine Gesellschaft auslagern. Dort kann sich eine eigene Compliance-Abteilung mit der Aufklärung und der Prüfung der Meldungen beschäftigen. Darüber hinaus ist es in der Praxis oftmals bereits der Fall, dass Unternehmensgruppen ein gemeinsames

Whistleblowing-System betreiben. Sollte diese Möglichkeit gesetzlich nicht ausreichend sein, so müssten diese auf dezentrale Kanäle umgestellt werden oder es sind neben dem bereits bestehenden zentralen Meldesystem noch zusätzliche Kanäle einzuführen.

Kompliziert kann es vor allem werden, wenn ein Mitgliedstaat den sachlichen Anwendungsbereich im Umsetzungsakt, wie dies die WBRL erlaubt, auf nationales Gesetz ausweitet. Diesen Handlungsspielraum hat der österreichische Gesetzgeber teilweise genutzt und auch Korruptions- sowie Amtsdelikte in das HSchG aufgenommen.

Dies würde jedoch zu folgendem Szenario führen: Ein Konzern mit Sitz der Muttergesellschaft in Deutschland hat Töchtergesellschaften in verschiedenen EU-Ländern, darunter ebenfalls in Österreich und Italien. Die italienische Tochtergesellschaft wurde damit beauftragt, einen zentralen Meldekanal für den gesamten Konzern zu implementieren und die Ermittlungen durchzuführen. Erfolgt nun aber eine Meldung von Beschäftigten der österreichischen Tochtergesellschaft über ein Korruptionsdelikt nach StGB, so müsste die italienische Schwesterngesellschaft eine sachverhaltsaufklärende Überprüfung nach dem Recht eines anderen Mitgliedstaates realisieren.

Neben den soeben beschriebenen Rechtsunsicherheiten für Konzerne kann es mit der Umsetzung der WBRL in nationales Recht auch für Kleinunternehmen, die nicht durch die gesetzliche Pflicht gebunden sind, ein Hinweisgebersystem zu implementieren, weil sie etwa weniger als 50 Mitarbeitende beschäftigte, dies aber freiwillig umsetzen möchten, zu Stolpersteinen kommen. Da sie nicht dem HSchG unterliegen, kommen ebenfalls die im Gesetz vorgesehenen Erleichterungen im Datenschutzrecht für die Einführung der Meldekanäle für sie zur Anwendung. Dies bedeutet, juristische Personen, welche nicht in den Anwendungsbereich des HSchG fallen, sollten bei der Einführung eines Whistleblowing-Systems jedenfalls eine Datenschutz-Folgenabschätzung durchführen, sofern kein Betriebsrat vorhanden ist und eine Betriebsvereinbarung nach der DSFA-V vorliegt. Ein Berufen auf die Beschränkung der Betroffenenrechte der DSGVO ist demnach auch nicht möglich.

Auf Grund des abgesteckten sachlichen Anwendungsbereichs auf das Unionsrecht und in Österreich ebenfalls auf das Korruptionsstrafrecht können sich Meldestellen bei Verstößen, die über die in § 3 HSchG genannten Rechtsbereiche hinausgehen, nicht auf das Gesetz stützen und würden für diese Bereiche wiederum freiwillig ein Hinweisgebersystem betreiben. Dies würde bedeuten, die Datenverarbeitung muss auf Art. 6 Abs. 1 lit. f DSGVO

gestützt werden. Für alle Verstöße, die nicht unter § 3 HSchG fallen, gelten damit auch nicht die datenschutzrechtlichen Erleichterungen nach dem HSchG.

Damit werden österreichische Unternehmen zudem vor Herausforderungen gestellt, wenn es um die Frage der Betroffenenrechte nach Kapitel III der DSGVO geht. In Folge wäre der Beschuldigte also nach Art. 14 und 15 DSGVO von der Verarbeitung seiner personenbezogenen Daten durch den gemeldeten Verstoß zu informieren und die Identität des Whistleblowers müsste somit offengelegt werden. Dies würde wiederum gegen Ziel und Zweck der WBRL sprechen und für Unternehmen mit einem hohen Verwaltungsaufwand einhergehen.

Hier werden sehenden Auges zwei verschiedene datenschutzrechtliche Regime geschaffen: einerseits jenes, für das die gesetzliche Deckung durch das HSchG gilt, und andererseits für alle Betriebe sowie Rechtsbereiche, die nicht dem Gesetz unterliegen. Diese Zweigleisigkeit ist aus praktischer und datenschutzrechtlicher Sicht bedenklich und könnte darüber hinaus zu einer Art ‚Zwei-Klassengesellschaft von Hinweisgebern' führen, wenn ein Hinweisgeber nicht unter den Schutz fallen würde, den das Gesetz bietet.

Um diese Pattsituation aufzulösen, könnte der Gesetzgeber vorsehen, die Möglichkeit der freiwilligen Unterwerfung in das HSchG zu integrieren. Damit wäre einerseits für die Kleinunternehmen mit bis zu 50 Mitarbeitern Abhilfe geschaffen, die interne Meldekanäle einführen wollen, und ebenso für eingehende Meldungen, die nicht Verstöße nach § 3 HSchG betreffen.

Aus arbeitsrechtlicher Sicht wird für Betriebe mit Betriebsrat bei der Umsetzung von Whistleblowing-Systemen wohl eine positive Zusammenarbeit notwendig sein. Nicht zuletzt kann die Aufklärung von Verstößen nicht nur für die Unternehmensführung, sondern ebenso für die Belegschaft Vorteile mit sich bringen, weshalb mit einer Sensibilisierung und Aufklärung aller Mitarbeiter schon vor der Einführung eines Meldekanals versucht werden sollte, in allen Unternehmensebenen Akzeptanz für Hinweisgebersysteme zu schaffen.

Tatsächlich lässt sich festhalten, dass auf die datenschutzrechtlichen Aspekte bei der Umsetzung der WBRL und der zukünftigen Einführung der internen Meldekanäle in Unternehmen nicht ausreichend Rücksicht genommen wurde und sich dadurch Spannungsverhältnisse ergeben.

Letztendlich ist abzuwarten, wie die Umsetzung mit der längsten Frist 17.12.2023 in österreichischen Unternehmen gelingt und neuen praktischen Erfahrungswerten und Erkenntnisse diese in die Evaluierung der Bestimmungen des HSchG durch den Gesetzgeber im Jahr 2026 einbezogen wer-

den, um hier vorhersehbaren Problemen durch gesetzliche Lösungen einen Riegel vorzuschieben.

Literaturverzeichnis

Altenbach/Dierkes EU-Whistleblowing-Richtlinie und DSGVO, CCZ 2020, 126.

Arnol, Whistleblower-Richtlinie und Gold Plating, GesRZ 2020, 153.

Artikel-29-Datenschutzgruppe Leitlinien für Transparenz gem. VO 2016/679 (WP 260 rev.01).

Artikel-29-Datenschutzgruppe Stellungnahme 1/2006 zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität. WP 117.

Block/Kremer Whistleblowing im Konzern: Eine zentrale Stelle ist zu wenig! https://www.cmshs-bloggt.de/compliance/whistleblowing-im-konzern-eine-zentrale-stelle-ist-zu-wenig/. (15.8.2022).

Brodil Arbeitnehmerdatenschutz und Datenschutz-Grundverordnung (DSGVO), ecolex 2018, 486.

Brunner/Nagel Whistleblowing - Sicherstellung des Hinweisgeberschutzes, Datenschutz Konkret 2020, 32.

Council of Europe Protection of Whistleblowers, Recommendation CM/Rec (2014)7 and explanatory memoran-dum, https://rm. coe.int/16807096c7 (15.8.2022).

Datenschutzkonferenz Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz, https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf.

Dilling Der Schutz von Hinweisgebern und betroffenen Personen nach der EU-Whistleblower-Richtlinie, CZZ 2019, 214.

Ehrbar Whistleblowing - das Hinweisgebersystem im österreichischen Recht, NetV 2016, 20.

Europäisches Parlament Entwurf einer legislativen Entschließung des europäischen Parlaments, https://www.europarl.europa.eu/doceo/document/A-8-2018-0398_DE.html#title1 (15.8.2022).

Falter Whistleblower (un)erwünscht? in *Roters/Gräf/Wollmann* (Hrsg), Zukunft Denken und Verantworten. Herausforderungen Für Politik, Wissenschaft und Gesellschaft Im 21. Jahrhundert (2020) 353.

Fassbach/Hülsberg Beschäftigtendatenschutz im Hinweisgeberverfahren: Interessenkonflikt zwischen Hinweisgeberschutz und Auskunftsrecht des Beschuldigten, GWR 2020, 255.

Fehr Whistleblowing und Datenschutz – ein unlösbares Spannungsfeld? ZD, 256–261.

Feiler/Rieken/Romandy Kapitel 3: Datenschutzkonforme Gestaltung von Hinweisgebersystemen, in *Petsche* (Hrsg), Whistleblowing & Internal Investigations. Praxiskommentar zur Whistleblowing-Richtlinie (2021).

Fleischer/Schmolk Finanzielle Anreize für Whistleblower im Europäischen Kapitalmarktrecht? NZG, 361.

Haidinger Kap 16, in *Knyrim* (Hrsg), Praxishandbuch Datenschutzrecht[4] (2020).

Hastenrath ZHAW-Studie: Auswirkungen der Whistleblowing-Richtlinie, CB 2022, 58.

Fidler/Winner in Kalss/Oppitz/U. Torggler/Winner, BörseG/MAR § 124 BörseG (Stand 1.8.2019, rdb.at)

Irresberger, Stangl-Krieger, Bruchbacher, Kercz, Wasinger, Spezialfragen zur gesetzeskonformen Einrichtung von HinweisgeberInnensystemen, GRCaktuell 2023, 28.

Kotschy/Reimer Die Überwachung der Internet-Kommunikation am Arbeitsplatz, ZAS 2004, 167.

Kröll/Stumpf Die EU-Richtlinie zum Schutz von Whistleblowern - Handlungsbedarf für Unternehmen, RdW 2020, 161.

Kühling/Buchner Datenschutz-Grundverordnung BDSG. Kommentar[4] (2024).

Kühteubl/Pusch Kap 13, in Rechtshandbuch der Digitalisierung (2021).

Moos Kapitel 8: Verarbeitungen in gemeinsamer, getrennter und alleiniger Verantwortlichkeit, in Moos/Schefzig/Arning/Baumgartner/Braun/Cornelius/Gardyan-Eisenlohr/Gausling/Hansen-Oest/Heinemann (Hrsg), Praxishandbuch DSGVO. Einschließlich BDSG und spezifischer Anwendungsfälle[2] (2021).

Neumayr/Reissner, Zeller Kommentar zum Arbeitsrecht[3] (2018).

Novacek, EU-RL zum Schutz der Hinweisgeber auf Verstöße gegen Unionsrecht ("Whistleblower") EU-RL zum Schutz der Hinweisgeber auf Verstöße gegen Unionsrecht ("Whistleblower")- Auswirkungen im Steuerrecht, FJ 2019, 222.

Paal/Pauly/Ernst, DS-GVO BDSG // Datenschutz-Grundverordnung. Bundesdatenschutzgesetz[3] (2021).

Peitsch, Whistleblowing-Hotlines spätestens 2021 verpflichtend. Bislang keine Pflicht zur Einrichtung von Whistleblowing-Hotlines, NetV 2020, 60.

Petsche, Kapitel 2: Rechtlicher Rahmen für Internal Investigations, in *Petsche* (Hrsg), Whistleblowing & Internal Investigations. Praxiskommentar zur Whistleblowing-Richtlinie (2021) 220.

Pollirer, Checkliste Whistleblowing, Dako 2020, 38.

Reppelmund, Whistleblowing-Richtlinie: Vorläufige Einigung zwischen Europäischem Parlament und den Mitgliedstaaten, EuZW 2019, 307.

Schmolke, Die neue Whistleblower-Richtlinie ist da! Und nun? NZG 2020, 5.

Schweiger, Die Richtlinie zum Schutz von Hinweisgebern - arbeitsrechtliche Konsequenzen (Teil II), RdW 2020, 533.

Stella/Winter, Whistleblowing-RL: Ungelöste Rechtsfragen für die betriebliche Umsetzung, ZAS 2021, 124.

tagesschau, Gründer von WikiLeaks: London bestätigt Auslieferung von Assange an die USA (17.6.2022).

Teichman/Weber, Die Whistleblowing-Richtlinie, ihr Missbrauchspotential und Implikationen für Compliance-Beauftragte, CB 2022, 157.

Thiele/Wagner, Umsetzung der DSGVO in der Personalpraxis. Fragen, Antworten, Muster (2019).

Zankl, Rechtshandbuch der Digitalisierung (2021).

Rechtsquellenverzeichnis

Arbeitsverfassungsgesetz BGBl 1974/22

Arbeitsvertragsrechts-Anpassungsgesetz BGBl 1993/459

Burgenländisches Hinweisgeberschutzgesetz LGBl. 26/2022

Bundesgesetz über das Verfahren und den Schutz bei Hinweisen auf Rechtsverletzungen in bestimmten Rechtsbereichen (HinweisgeberInnenschutzgesetz – HSchG) BGBl. I Nr. 6/2023

Ministerialentwurf betreffend Bundesgesetz, mit dem ein Bundesgesetz über das Verfahren und den Schutz bei Hinweisen auf Rechtsverletzungen in bestimmten Rechtsbereichen (HinweisgeberInnenschutzgesetz – HSchG) erlassen wird

Richtlinie des Europäischen Parlaments und des Rates v. 23.10.2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, ABl L 305/17.

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 2016/119.

The False Claims Act

Dodd-Frank Wall Street Reform and Consumer Protection Act

Sarbanes-Oxley Act of 2002

Judikaturverzeichnis

OGH 13.6.2002, 8 ObA 288/01p.

DSB-D123.085/0003-DSB/2018, 27.8.2018.

LAG Baden-Württemberg, 20.12.2018, 17 Sa 11/18.

EGMR 16. 2. 2021, 23922/19, *Gawlik/Liechtenstein.*

VG Köln, 25.3.2022, 25 K 2138/19.

Plattformregulierung 2.0: Die (un-)mittelbare Grundrechtsbindung Privater im Digital Services Act

Ina Kapusta

A. Einleitung[*]

I. Einleitende Bemerkungen[**]

Immer mehr Menschen sind von Drohungen, Beleidigungen und Hassrede im Internet betroffen. Eine Studie der Universität Leipzig ergab, dass die Zahl der Betroffenen binnen kurzer Zeit von 18 % im Jahre 2020 auf 24 % im Jahre 2022 anstieg.[1] Darüber hinaus gaben 50 % der Befragten an, aus Angst, Opfer von Hassrede zu werden, einen Beitrag im Internet bewusst vorsichtiger formuliert oder gar gänzlich auf dessen Veröffentlichung verzichtet zu haben. In Österreich sind nach Angaben der Statistik Austria sogar 31 % der Bevölkerung mit feindseligen oder erniedrigenden Inhalten konfrontiert.[2] Aber wie kann Hassrede im Internet effektiver reguliert oder gar bestraft werden?

Diese Frage stellte sich auch die ehemalige Nationalratsabgeordnete, Klubobfrau und Bundessprecherin der Grünen im Parlament, *Eva Glawischnig-Piesczek*, die in einem öffentlich zugänglichen Kommentar auf Facebook u.a. als „*miese Volksverräterin*" bezeichnet wurde.[3] Dieser Kommentar eines namentlich nicht bekannten Nutzers wurde unter einem Artikel eines

---

* Zur besseren Lesbarkeit wird in diesem Beitrag das generische Maskulinum verwendet. Die in diesem Beitrag verwendeten Personenbezeichnungen beziehen sich jedoch – sofern nicht anders kenntlich gemacht – ohne Unterschied auf alle Geschlechter.

** Der Beitrag entspringt der im September 2023 eingereichten Abschlussarbeit der *Verfasserin* iRd Bachelorstudiums Wirtschaftsrecht an der Leopold-Franzens-Universität Innsbruck und befindet sich inhaltlich auf dem Stand der Einreichung und formal hinsichtlich der Quellen auf dem Stand von Februar 2024. Für die Ermöglichung und Unterstützung bei der Veröffentlichung wird Herrn Univ.-Prof. Dr. Thomas Müller, LL.M. herzlichst gedankt.

1 Hoven/Forschungsgruppe g/d/p, Hass im Netz, 2022 (Stand 12.2.2024).

2 Statistik Austria, Österreichischer Zahlenspiegel, 2023 (Stand 12.2.2024).

3 Zankl RHdB Digitalisierung/Kresbach Rn. 22.1 (22.42).

österreichischen Online-Nachrichtenmagazins mit einem sie darstellenden Lichtbild veröffentlicht und trotz Aufforderung zur zeitnahen Löschung von Facebook nicht entfernt.[4] Im Dezember 2016 beantragte sie daher vor dem Handelsgericht (HG) Wien den Erlass einer einstweiligen Verfügung gegen Facebook Ireland Ltd.[5] Neben Schadenersatz gem. § 1330 öABGB,[6] beantragte sie, gestützt auf § 78 öUrhG,[7] dass Facebook schuldig zu erkennen sei, „*die Veröffentlichung und/oder Verbreitung von die Klägerin zeigenden Lichtbildern zu unterlassen, wenn im Begleittext die wörtlichen und/oder sinngleichen Behauptungen*" verbreitet werden.[8]

Da das HG Wien dem Unterlassungsbegehren stattgab, sperrte Facebook daraufhin zunächst in Österreich den Zugang zu diesem Beitrag.[9] Das in der Folge von Facebook angerufene Oberlandesgericht (OLG) Wien bestätigte den erstinstanzlichen Beschluss hinsichtlich der wortgleichen (nicht jedoch sinngleichen) Äußerungen und sprach der Klägerin unabhängig davon, ob der unmittelbare Täter den Kommentar vom Inland oder Ausland aus verbreitet habe, einen Anspruch auf Unterlassung zu.[10] Dies mit der Begründung, dass der Ort der Verletzung der Persönlichkeitsrechte im sozialen Netzwerk am Ort des gewöhnlichen Aufenthalts der Klägerin liege und daher jedenfalls österreichisches Recht zur Anwendung käme.[11] Facebook sei jedoch nicht für Inhalte in Österreich verantwortlich, die in Österreich nicht angezeigt werden.[12]

4 Ein besonderes Merkmal von Plattformen wie bspw. Facebook liegt aufgrund der Plattformökonomie sowie der vorherrschenden Machtasymmetrie (s. A.II.) in der Schnelligkeit und Globalität der Verbreitung von unzulässigen Inhalten, woraus sich die Dringlichkeit des Unterlassungsbegehrens ergibt; vgl. hierzu Eifert/Metzger/Schweitzer/Wagner CMLR 2021, 987 (1018); Struth Hassrede S. 3.

5 Janisch jusIT 2019, 225 (225 ff.).

6 Allgemeines bürgerliches Gesetzbuch für die gesammten [sic!] deutschen Erbländer der Oesterreichischen Monarchie, öJGS 1811/946 idF. öBGBl I 2024/11.

7 Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (Urheberrechtsgesetz), öBGBl. 1936/111 idF. öBGBl. I 2023/182.

8 HG Wien 7.12.2016, 11 Cg 65/16w-17 (nicht veröffentlicht); Kettemann/Kraml/Rachinger/Rauchegger/Tiedeke CR 2021, 154 (155 f.); Witzeneder Glawischnig-Piesczek vs. Facebook S. 6 ff.

9 Die einstweilige Verfügung bezog sich mangels ausdrücklicher Festlegung eines geographischen Geltungsbereichs sowie ausdrücklichen Antrags *Glawischnig-Piesczeks* auf Erweiterung desselben, ausschließlich auf das österreichische Staatsgebiet; vgl. Kettemann/Kraml/Rachinger/Rauchegger/Tiedeke CR 2021, 154 (155).

10 OLG Wien 5 R/17t-23, S. 21 f., ZIIR-Slg 2017, 268 (268).

11 Windhager ZIIR 2017, 349 (355).

12 Kettemann/Kraml/Rachinger/Rauchegger/Tiedeke CR 2021, 154 (155).

Auch der in der Folge von beiden Parteien angerufene Oberste Gerichtshof (OGH) bestätigte das Unterlassungsbegehren der Klägerin betreffend die „*Veröffentlichung und/oder Verbreitung von die Klägerin zeigenden Lichtbildern im Zusammenhang mit den inkriminierten Äußerungen*".[13] Unklar war hingegen die Frage, ob der Betreiber nach einem rechtswidrigen, gegen Persönlichkeitsrechte verstoßenden Verhalten auch dazu verpflichtet werden kann, (i) „*andere wortgleiche Informationen*" jedes oder nur des jeweiligen Nutzers, (ii) weltweit oder nur im jeweiligen Mitgliedstaat zu entfernen und ob dies (iii) auch für „*sinngleiche Informationen gilt, sobald dem Betreiber dieser Umstand zur Kenntnis gelangt*".[14] Aus diesem Grund suchte der OGH den EuGH im Rahmen eines Vorabentscheidungsverfahrens iSd Art. 267 AEUV um Auslegung der Art. 14 und 15 E-Commerce-RL[15] im Hinblick auf jede denkbare Art von Unterlassungsanordnung an.[16]

Der EuGH entschied schließlich, dass Plattformbetreiber zur Sperrung des Zugangs bzw. zur Entfernung der betreffenden einzelnen Information des konkreten Nutzers sowie aller wort- und sinngleichen Inhalte verpflichtet werden könne.[17] Darüber hinaus bestätigte der EuGH, dass Löschungspflichten von nationalen Gerichten mit weltweiter Geltung auferlegt werden können.[18]

Dieser Fall verdeutlicht die Schwierigkeiten, die derzeit mit der Bekämpfung von rechtswidrigen Inhalten auf sozialen Netzwerken einhergehen. Hierzu gehört insbesondere die Anonymität bzw. Unsichtbarkeit des Urhebers eines Beitrags sowie die nahezu unbegrenzte Macht der Plattformen,

13 OGH 6 Ob 116/17b, ZIIR 2018, 104 (104 f.). Der OGH akzeptierte hiermit Facebooks Handeln im Hinblick auf die Verunmöglichung des Zugriffs auf den ursprünglichen Kommentar in Österreich und bestätigte zugleich indirekt, dass kein „*Take-down im globalen Maßstab gefordert war*"; Kettemann/Kraml/Rachinger/Rauchegger/Tiedeke CR 2021, 154 (155).

14 Vorabentscheidungsersuchen des OGH vom 10.1.2018 (2018/C 104/26).

15 RL 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), ABl. 2000 L 178/1.

16 Unter Ausnutzung eines möglichst weiten Ermessensspielraums (vgl. hierzu auch EuGH Urt. v. 16.12.1981 – C-244/80, ECLI:EU:C:1981:302 Rn. 16 = BeckRS 1981, 107971 – Foglia/Novello) bei der Formulierung der Vorlagefrage ersuchte der OGH den EuGH, jede denkbare, sohin auch weltweite, Art von Unterlassungsanordnung zu prüfen.

17 Casolari/Gatti Application of EU Law/Lonardo S. 9 (20 f.).

18 EuGH Urt. v. 3.10.2019 – C-18/18, ECLI:EU:C:2019:821 Rn. 53 = BeckRS 2019, 23113 – Glawischnig-Piesczek; Peifer GRUR-Prax 2019, 534 (534).

darüber zu entscheiden, welcher Inhalt veröffentlicht wird (bzw. bleibt) und durch den verwendeten Algorithmus Verbreitung findet.[19] Hieraus folgt auch die große Bedeutung dieser Plattformen für die Gesellschaft, denn die sozialen Netzwerke wirken auf eine Vielzahl von Prozessen ein, welche die Meinungsbildung substanziell beeinflussen.[20] Im Folgenden wird daher zunächst die Bedeutung der Plattformökonomie analysiert.[21]

II. Soziale Netzwerke als Gatekeeper von Informationen – Bedeutung der Plattformökonomie

Auf die Aufmerksamkeitsökonomie spezialisierte Plattformen, wie bspw. Facebook, Instagram oder TikTok, folgen einer kommerziellen Logik im „*Matchmaking*"[22] zwischen Inhalten und Publikum.[23] Dabei untersagen sie durch ihre Nutzungsbedingungen bestimmte Inhalte sowie Formen von Äußerungen auf ihren Plattformen.[24] Diese Bedingungen[25] sind darauf ausgerichtet, die Plattform möglichst attraktiv sowohl für Nutzer als auch für Werbekunden zu gestalten,[26] denn Meinungsplattformen finanzieren sich regelmäßig über Werbeeinnahmen und die Weitergabe von Nutzerdaten an Dritte (sog. „*Dienst gegen Daten*").[27]

Die sozialen Netzwerke, die auch als „*private Gesetzgeber*" bezeichnet werden,[28] legen in Nutzungsbedingungen, AGB oder sog. „*Gemeinschafts-*

19 Grabenwarter/Holoubek/Leitl-Staudinger Kommunikationsplattformen/Oswald S. 67 (70 f.).
20 Paal/Hennemann ZRP 2017, 76 (76 ff.).
21 Zu sozialen Netzwerken als Gatekeeper von Informationen und der Bedeutung der Plattformökonomie s. A.II.
22 Der große Mehrwert eines solchen Geschäftsmodells liegt darin, den Austausch von Waren, Dienstleistungen und Informationen zu erleichtern, indem unter Nutzung der auf der Plattform generierten Informationen die besten „*Matches*" bspw. zwischen Käufer und Verkäufer gemacht werden; vgl. Eifert/Metzger/Schweitzer/Wagner CMLR 2021, 987 (988).
23 Engert AcP 218 (2018), 304 (331 ff.); Denga EuR 2021, 569 (570); Tommasi ERPL 2021, 925 (925 ff.).
24 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (153); Heldt Drittwirkung S. 254 ff.
25 S. bspw. Facebook, Gemeinschaftsstandards, 2015 (Stand 12.2.2024).
26 Denga EuR 2021, 569 (573 f.).
27 Zum Begriff „*Dienst gegen Daten*" s. Denga EuR 2021, 569 (571); Metzger AcP 216 (2016), 817 (833 ff.).
28 Legner ZUM 2024, 99 (100); Schweitzer ZEuP 2019, 1 (1).

standards" fest,[29] welche Arten von Inhalten sie tolerieren und unter welchen Voraussetzungen Beiträge gelöscht oder Nutzerkonten gesperrt werden.[30] In den Nutzungsbedingungen untersagt werden insbesondere Gewaltaufrufe, Darstellungen von Nacktheit, bestimmte Formen der Desinformation und die Veröffentlichung von Inhalten, die von den Plattformen als „*Hate Speech*"[31] qualifiziert werden.[32] Darunter werden direkte Verbalangriffe auf einzelne Personen oder Personengruppen verstanden, wenn die Äußerung an der Zugehörigkeit zu einer geschützten Kategorie[33] anknüpft. Diese Anknüpfung an bestimmte Kategorien ermöglicht es dem Plattformbetreiber auf eine abstrakt-generelle Regelungstechnik sowie auslegungsbedürftige Begriffe zurückzugreifen.[34]

Um die gewünschten Nutzungsbedingungen durchzusetzen, können die Diensteanbieter einschlägige Beiträge löschen sowie Nutzerkonten vorübergehend oder unbefristet sperren.[35] So sperrte Meta bspw. die Konten des ehemaligen Präsidenten der USA, Donald Trump, wegen wiederholter Verbreitung von Desinformationen für beinahe zwei Jahre.[36] Alternativ können die Diensteanbieter auch die Reichweite unerwünschter Inhalte einschränken, indem anderen Nutzern diese Inhalte in deren „*algorithmus-gesteuerten Newsfeed*" seltener oder überhaupt nicht mehr angezeigt werden.[37]

An der privaten Regelungsmacht der Plattformen[38] wird insbesondere kritisiert, dass ein fundamentales Demokratieproblem entstehe,[39] wenn private Unternehmen über unregulierte „*Entscheidungshoheit […] über die Regeln und Voraussetzungen der Individual- und Massenkommunikation*"

29 Aus zivilrechtlicher Sicht üben sie damit ihr (virtuelles) Hausrecht aus und werden dadurch zu privaten Regelsetzern für demokratierelevante Kommunikationsprozesse; s. Kettemann/Schulz/Fertmann ZRP 2021, 138 (138 f.).

30 Ammann/Bottega/Bukovac/Lehner/Meier/Piskóty/Rausch/Rehmann/Schneider/Weder/Wilhelm Verantwortung und Recht/Karg S. 67 (86).

31 Grabenwarter/Holoubek/Leitl-Staudinger Kommunikationsplattformen/Oswald S. 67 (81 ff.).

32 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (153).

33 Hierzu zählen bspw. Ethnie, Religion, Geschlecht, Nationalität und sexuelle Orientierung.

34 Friehe NJW 2020, 1697 (1697 ff.).

35 Goldman MTLR 2021, 1 (23 ff.); Kahl/Horn K&R 2021, 703 (704); Friehe NJW 2020, 1697 (1700 f.).

36 Grabenwarter/Holoubek/Leitl-Staudinger Kommunikationsplattformen/Kettemann/Rachinger/Sekwenz S. 55 (55).

37 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (154).

38 Mendelsohn MMR 2021, 857 (858 ff.).

39 Denga EuR 2021, 569 (570 ff.).

verfügen.[40] Die Kontrolle über den Zugang zu Informationen und die Ausformung der weltweiten Redefreiheit dürfe nicht jener geringen Anzahl an Diensteanbietern obliegen, die eine marktmächtige Stellung innehaben[41] und dürfe nicht zu einer Form der privaten Zensur werden.[42] Schließlich obliege es den Diensteanbietern, ob die Moderation ex-ante beruhend auf der Kennzeichnung bestimmter Inhalte oder ex-post, dh durch „*notice and take down-Verfahren*" erfolge.[43] Doch ist zu beachten, dass Diensteanbietern im Falle einer Unterlassung der Content Moderation ein Haftungsrisiko droht, welches – vorbeugend ausgeübt – zu präventivem Sperren oder Löschen von Inhalten im bloßen Verdachtsfall führen kann (sog. „*Overblocking*").[44]

Der Grund für dieses zentrale Demokratieproblem liegt in den steigenden Nutzerzahlen sozialer Netzwerke, die dafür sorgen, dass sich Teile der Meinungsbildungsmacht vom öffentlichen in den privaten Sektor verschieben.[45] Die Diensteanbieter profitieren dabei von meinungsstärkenden digital-öffentlichen Kommunikationsräumen,[46] die von den Nutzern teilweise mehrfach täglich sowie ausschließlich anstelle von Medien wie Fernsehen oder Rundfunk verwendet werden.[47] Dies führt schließlich dazu, dass die Diensteanbieter die Rolle vormals meinungskontrollierender, stark regulierter Medienunternehmen einnehmen.[48] Die Meinungskontrolle erfolgt dabei insbesondere durch den Einsatz von Algorithmen, die das Informationsangebot filtern und entsprechend den Präferenzen des Nutzers anpas-

40 Schwartmann, Trump, 2021 (Stand 12.2.2024).
41 Helberger/Pierson/Poell TIS 2018, 1 (5 ff.).
42 Schiek StudZR-WissOn 2021, 61 (62).
43 Denga EuR 2021, 569 (575).
44 Die Gefahr des "*Overblocking*" wird durch transnationale Intermediäre, die Filter- und Sperrsysteme verwenden, noch weiter verstärkt, da die urheberrechtlichen Schranken nicht harmonisiert sind und hierdurch „*das System nicht hinreichend zwischen einem unzulässigen und einem zulässigen Inhalt unterscheiden kann, so dass sein Einsatz zur Sperrung von Kommunikationen mit zulässigem Inhalt führen könnte*"; vgl. EuGH Urt. v. 24.11.2011 – C-70/10, ECLI:EU:C:2011:771, Rn. 52 = BeckRS 2011, 81685 – Scarlet Extended; s. auch Wielsch RW 2019, 84 (101).
45 Di Fabio Grundrechtsgeltung S. 23 ff.
46 Ladeur MMR 2001, 787 (791); Schiek StudZR-WissOn 2021, 61 (63) mwN.
47 Erwgr. 1 DSA (VO [EU] 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), ABl. 2022 L 277/1).
48 Paal/Hennemann ZRP 2017, 76 (76 f.).

sen, was dazu führen kann, dass Inhalte unterschiedlich starke Verbreitung finden.[49]

Durch diese bedeutende Rolle privater Unternehmen bei der öffentlichen Meinungsbildung[50] schwindet die staatliche Regulierungsmacht zunehmend.[51] Zugleich begünstigt die Kommunikationsstruktur sozialer Medien Grundrechtsverletzungen,[52] wie bspw. Eingriffe in das Recht der Meinungsäußerungsfreiheit und Informationsfreiheit gem. Art. 11 Grundrechtecharta (GRC).[53] Gefördert wird dies v.a. durch die erschwerte gerichtliche Verfolgung aufgrund von Ortsunabhängigkeit, Anonymität[54] sowie Asynchronität im Netz, welche die psychologische Hemmschwelle zur Verbreitung von *Hate Speech* senken.[55] Dies liegt wiederum an der mangelnden Wahrnehmung und Durchsetzung von Korrektiven.[56] Darüber hinaus wird die Eingriffsintensität der Grundrechtsverletzungen dadurch verstärkt, dass das Internet als kollektives Gedächtnis Inhalte auf unbegrenzte Zeit speichern sowie wiedergeben kann.[57]

III. Untersuchungsgegenstand

Die Regulierung großer Plattformen durch spezifische präventive Maßnahmen basiert auf einer Dreiecksbeziehung zwischen der Rechtsetzung im Mehrebenensystem, den Plattformbetreibern und den Nutzern.[58] Dabei

49 Hermstrüwer/Lüdemann Schutz der Meinungsbildung/Lüdemann S. 1 (2).
50 Schulz/Dankert Informationsintermediäre S. 8 ff.
51 Eifert/Gostomzyk Netzwerkrecht/Ladeur S. 169 (170 ff.).
52 Bayer/Holznagel/Korpisaari/Woods Platform Regulation/Koivukari/Korpisaari S. 473 (475 ff.) Das spezifische Problem transnationaler Kommunikationsnetzwerke liegt in den Worten *Wielschs* darin, *„dass im digitalen Kontext ein autonomes, dezentrales Handeln des Einzelnen erst durch Intermediäre ermöglicht wird, deren Funktionalität somit über die Verwirklichungsbedingungen von Freiheitsrechten aller Beteiligten entscheidet";* vgl. Wielsch RW 2019, 84 (88 f.).
53 Bajlicz/Bohnert/Ganglbauer/Gärner/Petermair/Ponader/Tilzer/Werderitsch Tagung ÖffR XI/Achleitner S. 3 (3 f.).
54 Zur „*Anonymität als Dilemma*", das es zu gleich zu gewährleisten wie zu überwinden gilt, s. Heckmann NJW 2012, 2631 (2631 ff.) und Palzer AfP 48 (2017), 199 (200 f.).
55 Schiek StudZR-WissOn 2021, 61 (63 f.); Heckmann NJW 2012, 2631 (2632).
56 Schneiders UFITA 85 (2021), 269 (286).
57 EuGH Urt. v. 13.5.2014 – C-131/12, ECLI:EU:C:2014:317, Rn. 89 ff. = BeckRS 2014, 80862 – Google Spain und Google.
58 Grabenwarter/Holoubek/Leitl-Staudinger Kommunikationsplattformen/Holoubek S. 29 (32 ff.).

kommt den Plattformbetreibern – wie die einleitenden Bemerkungen ebenso wie aktuelle Entwicklungen[59] gezeigt haben – eine zentrale Rolle im Hinblick auf die Freiheit und die Wirkungen der Kommunikation im digitalen Raum zu.[60] Die Plattformen regulieren selbständig, ob und welche Inhalte sie beschränken oder deren Verbreitung mindern und ob schädliche Informationen durch Algorithmen in entscheidender Weise verstärkt bzw. eingeschränkt werden.[61] Indem die Plattformbetreiber damit eine Funktion einnehmen, in welcher sie in Grundrechtskonflikten Abwägungen treffen können bzw. müssen,[62] kommt ihnen eine rechtssetzende Rolle zu, dh jene Rolle, die nach herkömmlichem Verständnis im Mehrebenensystem dem nationalen, europäischen[63] oder völkerrechtlichen Gesetzgeber zukommen würde.[64]

Um den hieraus resultierenden Gefahren für die Grundrechte der Nutzer entgegenzuwirken, bestand zwar bislang auf europäischer Ebene[65] mit der E-Commerce-RL ein einschlägiges Rechtsinstrument.[66] Dieses wurde allerdings als nicht mehr zeitgemäß angesehen,[67] sodass die nationalen Gesetzgeber[68] die Problematik selbst regelten.[69] Um eine derartige Fragmentie-

59 Dies bestätigten u.a. die veröffentlichten Transparenzberichte zur Entfernung von Inhalten bspw. betreffend Hassreden, offensichtlicher Desinformation und Deplatforming-Maßnahmen in sozialen Netzwerken; s. auch Achleitner ZTR 2021, 1 (2).

60 Vereinigung der Deutschen Staatsrechtslehrer Veröffentlichungen LXXIV/Pöschl S. 405 (412 ff.).

61 Grabenwarter/Holoubek/Leitl-Staudinger Kommunikationsplattformen/Holoubek S. 29 (33 f.).

62 Adelberg K&R 2022, 19 (23).

63 Gielen/Uphues EuZW 2021, 627 (632).

64 Grabenwarter/Holoubek/Leitl-Staudinger Kommunikationsplattformen/Holoubek S. 29 (32 f.).

65 Hiermit ist der europäische Gesetzgeber dem amerikanischen Vorbild der Section 230 des Communication Decency Acts aus dem Jahr 1996 gefolgt, wonach es heißt „„*No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.*“; s. hierzu Gielen/Uphues EuZW 2021, 627 (632) mit Verweis auf Langvardt Geo. L. Tech. Rev. 2018, 1353 (1373).

66 Zur Haftungsprivilegierung der Art. 12 ff. E-Commerce-RL s. auch Specht-Riemenschneider/F. Hofmann, Gutachten, 2021, S. 35 ff mwN (Stand 12.2.2024).

67 Vgl. hierzu auch Kumarasamy, DSA, 2022 (Stand 12.2.2024).

68 Korpisaari J. Media Law 2022, 352 (352 ff.).

69 In Öst. bspw. das Bundesgesetz, mit dem Maßnahmen zur Bekämpfung von Hass im Netz getroffen werden (Hass-im-Netz-Bekämpfungs-Gesetz – HiNBG), öBGBl. I 2020/148 oder in Deutschland das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) dBGBl. 2017 I 3352 idF dBGBl. 2022 I 1182. Zum NetzDG s. auch Kohl J. Media Law 2022, 25 (35 ff.)

rung durch einzelstaatliche Regulierung der Mitgliedstaaten zu verhindern, wurde schließlich der europäische Gesetzgeber mit einem gänzlich neuen „*Plattformgrundgesetz*", dem Digital Services Act (DSA), tätig.[70] Dieser legt die Rahmenbedingungen für die Bereitstellung grenzüberschreitender digitaler Dienste fest[71] und kommt hierdurch dem Bedürfnis nach einem klaren Leitbild und einer normativen Einordnung der Natur von „*Dienst gegen Daten*"-Verträgen nach.[72]

Die im DSA geregelten Rahmenbedingungen sollen „*das Risiko irrtümlicher oder ungerechtfertigter Sperrungen […] mindern, die abschreckenden Wirkungen auf die freie Meinungsäußerung verringern, die Informations- und Meinungsfreiheit fördern und die Rechtsbehelfsmöglichkeiten der Nutzer stärken*".[73] Der DSA macht den Diensteanbietern dabei nicht nur verfahrensrechtliche, sondern auch materiellrechtliche Vorgaben, wonach diese bei der Durchsetzung inhaltsbeschränkender Community-Standards[74] „*sorgfältig, objektiv und verhältnismäßig*" vorzugehen und die „*Rechte und berechtigten Interessen aller Beteiligten sowie die Grundrechte der Nutzer, die in der Charta verankert sind*"[75] zu achten haben.[76]

Der vorliegende Beitrag untersucht daher die Frage, ob die privatrechtlichen Betreiber sozialer Plattformen entweder sekundärrechtlich – insbesondere durch Art. 14 Abs. 4 DSA – an die primärrechtlichen Unionsgrundrechte der GRC gebunden werden können oder ob die Grundrechte „aus sich heraus" wirken; und in der Folge, in welchem Verhältnis die eigene Grundrechtsposition der Diensteanbieter zu ihrer Bindung an die Grundrechte der Nutzer steht.[77]

---

sowie Schroeder/Reider, Online Antisemitism, 2023 (Stand 12.2.2024). Zum HiNBG s. auch Ristic/Frybert JAP 2020/2021, 239 (239 ff.).

70 Schiek StudZR-WissOn 2021, 61 (98).

71 Erwgr. 2 DSA; EPRS Liability S. 7 ff.

72 Mendelsohn MMR 2021, 857 (860).

73 COM(2020) 825 final, 14.

74 Die grundrechtliche Problematik verdeutlicht sich insbesondere auch im Vergleich mit den staatlichen Lösch- und Sperrpflichten im Hinblick auf die Meldung von Inhalten. Nach dem NetzDG werden von dem betreffenden Netzwerk genaue Angaben bis zur Nennung des verletzten Straftatbestandes verlangt, während hingegen bei Community Standards soziale Netzwerke auch auf Basis unsubstantiierter Meldungen prüfen. Ein Eingriff oder gar eine Verletzung des Grundrechts droht jedoch erst, wenn diese Prüfung nicht sorgfältig erfolgt; vgl. Skobel Regulierung S. 365 f.

75 Art. 14 Abs. 4 DSA.

76 Schiek StudZR-WissOn 2021, 61 (98 ff.).

77 Grabenwarter/Holoubek/Leitl-Staudinger Kommunikationsplattformen//Holoubek S. 29 (38 f.).

IV. Gang der Untersuchung

Zur Beantwortung dieser Fragen wird einleitend auf den DSA, insbesondere die Ausgangslage, das Ziel und den Zweck des DSA, sowie dessen Systematik und Durchsetzung in seinen Grundzügen eingegangen.[78] Anschließend wird allgemein der Begriff der mittelbaren und unmittelbaren Drittwirkung erörtert. Darauf folgt die eigentliche Frage, ob der DSA als europäische VO, sohin Sekundärrecht, eine solche mittelbare oder gar unmittelbare Drittwirkung vorsehen kann und will. Dies bspw., indem der Anwendungsbereich der primärrechtlichen GRC erweitert wird oder ob sich die Bindung an die GRC aus den Unionsgrundrechten selbst heraus ergibt und durch den DSA ausschließlich deklaratorisch angeordnet wird.[79] Zu diesem Zweck wird insbesondere Art. 14 Abs. 4 DSA untersucht, auf dessen Grundlage sich eine entsprechende Drittwirkung ergeben könnte.[80]

B. Einführung in den Digital Services Act

I. Ausgangslage

In den vergangenen Jahren hat sich ein deutlicher Paradigmenwechsel, oder in den Worten des EU-Kommissars *Thierry Breton* ein „*9/11 moment of social media*"[81] vollzogen, bei welchem digitale Plattformen zur neuen Form der demokratischen Kommunikation geworden sind.[82] Gleichwohl Hass und Desinformation keine ausschließlich im Internet auftretenden Phänomene darstellen, können sie auf großen digitalen Plattformen einfacher, effizienter und schneller eine bedeutsame Reichweite bei gleichzeitiger Anonymität des Verfassers erlangen.[83] Dies kann zum einen dazu führen, dass Nutzer ihre Kommunikation aus Angst vor möglichen Hasskommentaren einschränken und zum anderen, dass sich Informationen verbreiten, die eine alternative, nicht existierende Welt zugunsten der Verbreiter (sog. „*Fake News*") abbilden.[84]

78 Die Einführung in den Digital Services Act erfolgt unter B.
79 Zur Frage der Grundrechtsdogmatik s. unter C.
80 Zur Analyse einer möglichen Drittwirkung aus dem DSA s. unter D.
81 Breton, Capitol Hill, 2021 (Stand 12.2.2024).
82 Gielen/Uphues EuZW 2021, 627 (627 ff.).
83 Steinebach/Bader/Rinsdorf/Krämer/Roßnagel Desinformation/Bader S. 15 (22 f.).
84 Bohlen NJW 2020, 1999 (2000); Gielen/Uphues EuZW 2021, 627 (632 f.).

Diese ausgeprägte Problematik verstärkte sich aus historischer Sicht mit der Einführung der Haftungsprivilegierung in Art. 14 E-Commerce-RL, weil diese das Entstehen derart großer und mächtiger Plattformen begünstigte.[85] Die Haftungsprivilegierung befreite die Plattformbetreiber grundsätzlich von der Haftung für Inhalte, die Nutzer auf ihre Plattformen hochgeladen haben, es sei denn, die Plattformen unterließen es trotz Kenntniserlangung von rechtswidrigen Inhalten, diese unverzüglich zu entfernen oder den Zugang zu sperren.[86] Die Regelungen der E-Commerce-RL waren jedoch nicht in der Lage, die mit neuen technologischen Entwicklungen, insbesondere der algorithmischen Entscheidungsfindung, rechtswidrigen Inhalten im Internet und Online-Desinformation,[87] einhergehenden Gefahren hintanzuhalten.[88] Da die von der EU erlassenen Mitteilungen,[89] Empfehlungen[90] und Verhaltenskodizes[91] nicht verbindlich waren, trieben einige Mitgliedstaaten nationale Gesetzesvorhaben voran.[92] Dieser Fragmentierung wollte die EU durch die Erlassung einer ggü. dem nationalen Recht vorrangig anzuwendenden VO iSd Art. 288 Abs. 2 AEUV entgegenwirken, die neben einem allgemeinen Haftungsregime ein abgestuftes Regulierungsmodell vorsieht.[93]

Der Unionsgesetzgeber sah sich diesbezüglich jedoch mit mehreren Herausforderungen konfrontiert. Zum einen galt es, das Interesse der Nutzer

85 „*Grundpfeiler der Internetwirtschaft*", s. Berberich/Seip GRUR-Prax 2021, 4 (6); Ammann/Bottega/Bukovac/Lehner/Meier/Piskóty/Rausch/Rehmann/Schneider/Weder/Wilhelm Verantwortung und Recht/Karg S. 67 (84 f.).

86 Achleitner ecolex 2021, 512 (513); Gielen/Uphues EuZW 2021, 627 (632 f.).

87 F. Hofmann/Raue/F. Hofmann/Raue DSA Einleitung Rn. 2.

88 Gielen/Uphues EuZW 2021, 627 (632).

89 Zu den Mitteilungen s. bspw. Gemeinsame Mitteilung an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen betreffend den „Aktionsplan gegen Desinformation", JOIN(2018) 36 final und die Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen betreffend den „Umgang mit illegalen Online-Inhalten. Mehr Verantwortung für Online-Plattformen", COM(2017) 555 final.

90 Zu den Empfehlungen der Kommission s. Empfehlung (EU) 2018/334 der Kommission vom 1. März 2018 für wirksame Maßnahmen im Umgang mit illegalen Online-Inhalten, ABl. 2018 L 63/50.

91 Bspw. Code of Conduct on Countering Illegal Hate Speech Online, den die Europäische Kommission im Mai 2016 mit Facebook, Microsoft, Twitter und Youtube vereinbart hat und dem sich später auch Instagram, Snapchat und weitere anschlossen, s. Europäische Kommission, Code of Conduct, 2016 (Stand 12.2.2024).

92 Gielen/Uphues EuZW 2021, 627 (632 f.).

93 Berberich/Seip GRUR-Prax 2021, 4 (4 ff.).

an Innovation zu wecken, den Handel im Binnenmarkt der EU zu erleichtern und kleinen Unternehmen die Teilnahme an der Plattformökonomie[94] zu ermöglichen.[95] Zum anderen bestand die Regulierungsaufgabe darin, die Ausschaltung des Wettbewerbs, die strukturelle Missachtung von Rechtsnormen und die Ausnutzung von Verhaltensanomalien[96] zu verhindern.[97] Unter Berücksichtigung dieser Herausforderungen veröffentlichte die Europäische Kommission am 15.12.2020 einen Vorschlag für ein Gesetz über Digitale Dienste (DSA).[98] Am 16.11.2022 trat der DSA schließlich in Kraft,[99] wobei die vollständige Anwendbarkeit aller Verpflichtungen stufenweise[100] bis 17.2.2024 umgesetzt wurde.[101] Nur zwei Tage nach dem Inkrafttreten aller Verpflichtungen, leitete die Europäische Kommission bereits das erste förmliche Verfahren auf der Grundlage des DSA gegen TikTok ein.[102]

II. Regulierungsziele

Der europäische Gesetzgeber verfolgt mit dem DSA im Wesentlichen den Ansatz, den bestehenden Rechtsrahmen der E-Commerce-RL zu aktualisieren bzw. einen neuen Rechtsrahmen zu schaffen, der verhindert, dass die stärksten Marktteilnehmer ihre Spielregeln durchsetzen.[103] Basierend auf

94 Zum Begriff der Plattformökonomie auf digitalen Plattformen im Generellen s. Engert AcP 218 (2018), 304 (307).
95 F. Hofmann/Raue/F. Hofmann/Raue DSA Einleitung Rn. 1.
96 Wagner/Eidenmüller ZfPW 2019, 220 (230 ff.).
97 F. Hofmann/Raue/F. Hofmann/Raue DSA Einleitung Rn. 1; Podszun NJW-Beil. 2022, 56 (57 ff.).
98 COM(2020) 825 final; s. auch Achleitner ZTR 2021, 1 (1 f.).
99 Art. 93 Abs. 1 DSA; Achleitner MR-Int 2022, 114 (114 f.).
100 Ab dem 25.8.2023 gelten die Bestimmungen des DSA für die 19 von der Kommission designierten VLOP und VLOSE: Europäische Kommission, DSA, 2023 (Stand 12.2.2024). Darüber benannte die Kommission am 20.12.2023 drei weitere VLOP; s. Europäische Kommission, VLOP, 2023 (Stand 12.2.2024).
101 Art. 93 Abs. 2 DSA.
102 TikTok wurde am 25.4.2023 als sehr großes Unternehmen benannt, weshalb TikTok bereits vier Monate nach seiner Benennung verpflichtet war, damit zu beginnen, eine Reihe gesetzlich festgelegter Pflichten zu erfüllen. Die Europäische Kommission untersucht nun, ob TikTok in den Bereichen Jugendschutz, Transparenz der Werbung, Datenzugang für Forschende sowie Risikomanagement in Bezug auf suchterzeugendes Design und schädliche Inhalte gegen den DSA verstoßen hat; vgl. Europäische Kommission, Verfahren gegen TikTok, 2024 (Stand 12.2.2024).
103 Podszun NJW-Beil. 2022, 56 (60).

diesem Regulierungsansatz strebt der DSA verschiedene Ziele zu Gunsten unterschiedlicher Akteure an.

Aus Sicht der digitalen Dienste sind ausweislich des Kommissionsentwurfs *„klare und harmonisierte evidenzbasierte Regeln […] erforderlich […], die den Internet-Mittlern ein angemessenes Maß an Rechtssicherheit garantieren*".[104] Gleichzeitig sollen mit dem DSA Wettbewerbsbedingungen entstehen, die Innovation, Wachstum und Wettbewerbsfähigkeit fördern.[105] Damit dient der DSA auch der Verwirklichung des Binnenmarkts,[106] indem durch die einheitliche Regulierung eine Fragmentierung des Binnenmarkts vermieden wird und kleineren, innovativen Diensteanbietern durch die Konkretisierung der Haftungsprivilegierungen Expansions- und Wachstumschancen eröffnet werden.[107]

Demgegenüber soll aus Sicht der Nutzer digitaler Dienste ein sicherer, vorhersehbarer und vertrauenswürdiger digitaler Raum geschaffen werden, in welchem die Grundrechte der Nutzer v.a. durch ein vermehrtes Maß an Information sowie Transparenz im Hinblick auf die Durchsetzung effektiver[108] geschützt werden.[109] Insbesondere das Grundrecht auf freie Meinungsäußerung ist durch ungerechtfertigte Sperrmaßnahmen gefährdet.[110] Durch die Einschränkung systemischer Risiken, die in der Digitalwirtschaft von Plattformen ausgehen, wird ein rechtlich normierter Rahmen in digi-

104 COM(2020) 825 final, 2.

105 Vgl. hierzu auch Europäische Kommission, DSA Paket, 2022 (Stand 12.2.2024).

106 Erwgr. 4 und 34 DSA; COM(2020) 825 final, 6.

107 COM(2020) 825 final, 12; s. auch F. Hofmann/Raue/F. Hofmann/Raue DSA Einleitung Rn. 6 ff.; Kraul HdB digitale Dienste/Nathanail Ziele Rn. 2; Weidlinger ecolex 2023, 186 (186 ff.). Im Unterschied zum DSA verfolgt der DMA – VO (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte), ABl. 2022 L 265/1 – das Ziel, dass „*Plattformen ihr Potenzial voll entfalten können und sowohl Endnutzer als auch gewerbliche Nutzer die Vorteile der Plattformwirtschaft und der digitalen Wirtschaft in einem bestreitbaren und fairen Wettbewerbsumfeld nutzen können*"; COM(2020) 842 final, 3. Zum Zusammenspiel des regulatorischen Rahmens von DMA und DSA s. auch Eifert/Metzger/Schweitzer/Wagner CMLR 2021, 987 (994 ff.).

108 F. Hofmann/Raue/F. Hofmann/Raue DSA Einleitung Rn. 8.

109 Art. 1 Abs. 1 DSA iVm Erwgr. 2 DSA; Legner ZUM 2024, 99 (99 f.). Vgl. auch Europäische Kommission, Impact assessment, 2020 (Stand 12.2.2024).

110 Kraul HdB digitale Dienste/Kraul Einführung Rn. 18 ff.

talen Räumen geschaffen, der nicht mehr dem alleinigen Ermessen der Diensteanbieter obliegt.[111]

III. Regelungsgegenstände

Der DSA befasst sich im Wesentlichen mit zwei materiellen Regelungsgegenständen: der Haftung der Vermittlungsdienste einerseits sowie den ihnen auferlegten Sorgfaltspflichten andererseits. Für digitale Vermittlungsdienste, auch Intermediäre iSd Art. 3 lit. g DSA genannt, ist charakteristisch, dass sie Inhalte Dritter, dh die Inhalte ihrer Nutzer, bereitstellen. Da die Anzahl der Nutzerinhalte, die Online-Desinformationen, andere gesellschaftliche Risiken oder sonstige Rechtswidrigkeiten enthalten – wie zunächst dargestellt – zunehmend steigt, sollen die Sorgfaltspflichten der Vermittlungsdienste zur Schaffung eines sicheren, berechenbaren und vertrauenswürdigen Umfelds beitragen.[112] Der DSA knüpft diesbezüglich inhaltlich an den Begriff des rechtswidrigen Inhalts an, der „*alle Informationen [meint], die als solche oder durch ihre Bezugnahme auf eine Tätigkeit […] nicht im Einklang mit dem Unionsrecht oder dem Recht eines Mitgliedstaats stehen*".[113] Diesbezüglich gilt grundsätzlich weiterhin, dass die Vermittlungsdienste für auf ihren Plattformen verbreitete, rechtswidrige Inhalte nicht haften.[114] Die Haftungsprivilegierung greift allerdings nur insoweit, als der Vermittlungsdienst keine Kenntnis von diesem (nicht ohnehin bereits offensichtlich) rechtswidrigen Inhalt hat und nach Kenntniserlangung in Form eines "*notice and take down Verfahrens*" zeitnah tätig wird.[115] Im konkreten Einzelfall kann es jedoch schwer sein zu beurteilen, ob ein vom

111 BVerfGE 152, 152 = NJW 2020, 300 Rn. 88; Kraul HdB digitale Dienste/Nathanail Ziele Rn. 14 f.

112 Erwgr. 2 und 3 DSA.

113 Art. 3 lit. h DSA ohne Unterscheidung im Hinblick auf strafrechtliche Verstöße, Urheberrechts- oder Persönlichkeitsrechtsverletzung; s. auch Ammann/Bottega/Bukovac/Lehner/Meier/Piskóty/Rausch/Rehmann/Schneider/Weder/Wilhelm Verantwortung und Recht/Karg S. 67 (87).

114 Wie ein rechtswidriger Inhalt definiert ist, ergibt sich nicht aus dem DSA selbst; s. hierzu COM(2020) 825 final, 23; F. Hofmann/Raue/F. Hofmann/Raue DSA Einleitung Rn. 10 f.

115 Art. 6 Abs. 1 lit. a DSA spricht insoweit von „*Tatsachen oder Umstände[n], […] aus denen eine rechtswidrige Tätigkeit oder [ein] rechtswidrige[r] Inhalt offensichtlich hervorgeht*".

Intermediär vermittelter Inhalt rechtmäßig oder rechtswidrig ist.[116] Erfolgt eine Entscheidung zu Unrecht, so müssen Mechanismen zur Richtigkeitsgewähr von Lösch- und Sperrentscheidungen vorgesehen werden sowie ein Mechanismus zur Korrektur derselben, weil nicht nur die Interessen der Inhaber der Rechte, sondern auch die Informations- und Meinungsfreiheit der Nutzer berührt wird.[117]

Darüber hinaus kann sich eine Haftung der Diensteanbieter aus der konkreten Ausgestaltung der Plattform, bspw. der Transparenz von Empfehlungssystemen gem. Art. 27 und Art. 38 DSA,[118] ergeben.[119] Diensteanbietern ist es weiters verboten, sog. „*dark patterns*"[120] einzusetzen, um Nutzer zu täuschen, zu manipulieren oder anderweitig in ihrer Fähigkeit, freie und informierte Entscheidungen zu treffen, maßgeblich zu beeinträchtigen oder zu behindern.[121]

IV. Systematik

Damit ein Diensteanbieter vom regulatorischen Rahmen des DSA betroffen ist, muss dieser in territorialer Hinsicht eine „*wesentliche Verbindung zur Union*" aufweisen.[122] Diese gilt als gegeben, wenn der Diensteanbieter entweder seine Niederlassung in der Union hat, die Zahl von Nutzern in den Mitgliedstaaten im Verhältnis zu deren Bevölkerung erheblich ist oder

116 Dieses Prognoserisiko kann nicht zur Gänze auf die Diensteanbieter verlagert werden, weil anderenfalls die Problematik des „*Overblocking*" greift. Vielmehr bedarf es eines Haftungsregimes mit effektivem Rechtsschutz und Schutz rechtmäßiger Inhalte; vgl. Specht-Riemenschneider/F. Hofmann, Gutachten, 2021, S. 25 f. (Stand 12.2.2024).

117 Dass private Plattformen zur Regelung rechtmäßiger Inhalte durch AGB und Inhaltemoderation auf Basis unbestimmter Rechtsbegriffe staatlich verpflichtet werden („*staatlich-private-Ko-Regulierung*"), wird in der Lit. als grundrechtlich problematisch angesehen; s. F. Hofmann/Raue/F. Hofmann/Raue DSA Einleitung Rn. 17.

118 Rössel AfP 54 (2021), 93 (101 f.).

119 F. Hofmann/Raue/F. Hofmann/Raue DSA Einleitung Rn. 13.

120 Der Begriff „*dark patterns*" beschreibt die Tricks der Diensteanbieter, um den Nutzer zu einem von ihm nicht gewollten Handeln zu bewegen, bspw. eine Beeinflussung zur Einwilligung in eine eigentlich nicht gewollte Datenverarbeitung; s. Bering Grundrechtsbindung S. 41 f.; Rössel AfP 54 (2021), 93 (101 f.); Schäufele/Krück GRUR-Prax 2023, 120 (122).

121 F. Hofmann/Raue/F. Hofmann/Raue DSA Einleitung Rn. 26 ff.

122 Art. 2 Abs. 1 iVm Art. 3 lit. d und e DSA; Erwgr. 7 und 8 DSA.

die Tätigkeit des Diensteanbieters auf einen oder mehrere Mitgliedstaaten ausgerichtet[123] ist.[124]

Ist der Anwendungsbereich eröffnet, knüpft der DSA – bis auf wenige Ausnahmen wie bspw. die „*Gute-Samariter-Klausel*"[125] – an den Regelungsansatz der E-Commerce-RL an und behält insbesondere die Haftungsprivilegierung[126] für (Hosting-)Diensteanbieter bei.[127] Dies hat zur Folge, dass Diensteanbieter zwar auch in Zukunft grundsätzlich[128] nicht für die Vermittlung rechtswidriger Inhalte ihrer Nutzer haften, ihnen jedoch besondere Sorgfalts- und Transparenzpflichten auferlegt werden, die sich je nach der Art des Vermittlungsdienstes,[129] dessen Größe[130] und Funktion[131] unterscheiden.[132]

Auf Basis des risikobasierten Ansatzes wird ein regulatorischer Rahmen geschaffen, in welchem in Abhängigkeit von festgestellten Risiken ex-ante spezifische präventive Maßnahmen gesetzt werden.[133] Diese Maßnahmen sind in Form eines „*Pyramiden-Modells*" ausgestaltet, weshalb die grundlegenden Pflichten zwar mehr Adressaten betreffen, aber weniger eingriffsintensiv sind, währenddessen auf den darauffolgenden Stufen zwar weniger

123 Ob ein Diensteanbieter seine Tätigkeit auf einen Mitgliedstaat ausrichtet, bestimmt sich nach der Gesamtheit aller Umstände, insbesondere der technischen Bereitstellung, der Verwendung der gebräuchlichen Sprache des Mitgliedstaats oder der Verfügbarkeit im nationalen App-Store.

124 Gerdemann/Spindler GRUR 2023, 3 (4 f.).

125 Untersuchungen auf Eigeninitiative schließen die Anwendung der Haftungsprivilegien gem. Art. 7 DSA nicht aus, wodurch für die Anbieter digitaler Dienste der Anreiz geschaffen werden soll, proaktive Maßnahmen zur Entfernung von rechtswidrigen Inhalten zu ergreifen; s. auch Europäische Kommission, Empfehlung (EU) 2018/334 vom 1. März 2018 für wirksame Maßnahmen im Umgang mit illegalen Online-Inhalten, ABl. 2018 L 63/50, Erwgr. 26; Sesing-Wagenpfeil CR 2023, 113 (121).

126 Achleitner MR-Int 2022, 114 (114 f.).

127 Die Haftungsprivilegierung habe dazu geführt, dass „*im ganzen Binnenmarkt viele neuartige Dienste entstehen und expandieren konnten*", weshalb „*dieser Rahmen […] daher bestehen bleiben [sollte]*" (Erwgr. 16); s. auch F. Hofmann/Raue/F. Hofmann/Raue DSA Einleitung Rn. 2 ff.

128 Der DSA als Teil der europäischen Digitalrechtsstrategie kodifiziert den Rahmen für die bedingte Haftungsbefreiung anhand der Rspr. des EuGH und führt dies in den Erwgr. aus; vgl. Kraul HdB digitale Dienste/Kraul Einführung Rn. 27 ff.

129 Dabei unterscheidet der DSA zwischen Access- (reine Durchleitung), Caching- und Hosting-Diensteanbietern sowie Online-Plattformen und Online-Suchmaschinen.

130 Bspw. die Unterscheidung in VLOP und VLOSE in Art. 33 ff. DSA.

131 So zB Art. 29 ff. DSA für Transaktionsplattformen.

132 F. Hofmann/Raue/F. Hofmann/Raue DSA Einleitung Rn. 4.

133 Achleitner MR-Int 2022, 114 (116).

Adressaten, aber deutlich intensivere Verpflichtungen bestehen.[134] Diese Ausgestaltung in vier Stufen soll im Folgenden in Kürze erläutert werden.[135]

Die allgemeinen Sorgfaltspflichten der ersten Stufe (Kap. III, Abschnitt 1 DSA) gelten dabei für sämtliche Anbieter von Vermittlungsdiensten.[136] Vermittlungsdienste sind die Summe aller Dienstleistungen der Informationsgesellschaft,[137] die gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbracht werden.[138] Zu diesen allgemeinen Sorgfaltspflichten gehören bspw. die Pflicht zur Einrichtung einer Kontaktstelle für Nutzer gem. Art. 12 DSA[139] und die Transparenzanforderungen für AGB gem. Art. 14 DSA.[140]

Die Verpflichtungen der zweiten Stufe (Kap. III, Abschnitt 2 DSA) treffen Hosting-Diensteanbieter, einschließlich Online-Plattformen, jene der dritten Stufe (Kap. III, Abschnitt 3 DSA) ausschließlich Anbieter von Online-Plattformen, die als Untergruppe der Hosting-Diensteanbieter zu verstehen sind.[141] Als Hosting-Diensteanbieter werden jene Vermittlungsdienste qualifiziert, die von Nutzern bereitgestellte Informationen in deren Auftrag speichern, zB Cloud-Computing-Dienste und Web-Hosting-Dienste.[142] Als Sonderform des Hosting-Dienstes speichern Online-Plattformen von Nutzern bereitgestellte Informationen nicht nur, sondern verbreiten diese öffentlich.[143] Zudem ist es erforderlich, dass Online-Plattformen ihre

134 F. Hofmann/Raue/F. Hofmann/Raue DSA Einleitung Rn. 37 ff.; s. auch für eine umfassende graphische Darstellung Turillazzi/Taddeo/Floridi/Casolari Law Innov Technol 2023, 83 (87).

135 Für eine übersichtliche Darstellung der Pflichten s. auch Rohrßen ZVertriebsR 2021, 71 (75 f.).

136 Demschik ecolex 2023, 183 (183 ff.).

137 Art. 3 lit. a DSA iVm Art. 1 Abs. 1 lit. b RL (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft, ABl. 2015 L 241/3.

138 Gerdemann/Spindler GRUR 2023, 3 (4 f.).

139 Demnach ist der Diensteanbieter verpflichtet, eine elektronische Kontaktadresse für Nutzer vorzusehen, um eine direkte und schnelle Kommunikation auf elektronischem Weg zu ermöglichen; s. auch Kraul HdB digitale Dienste/Maamar Sorgfaltspflichten Rn. 24 ff.

140 F. Hofmann/Raue/Raue DSA Art. 14 Rn. 1 ff.

141 Eine Ausnahme sieht Art. 19 DSA für sog. Kleinst- und Kleinunternehmen vor; vgl. Demschik ecolex 2023, 183 (185).

142 Art. 3 lit. g Nr. iii DSA iVm Art. 6 DSA; s. auch Gerdemann/Spindler GRUR 2023, 3 (8).

143 Art. 3 lit. i DSA.

Dienste gegen Entgelt erbringen, was auch das Bezahlen mit Daten umfasst.[144]

Für Anbieter von Hosting-Diensten, einschließlich Online-Plattformen, gelten bspw. die Vorschriften zur Einrichtung besonderer Melde- und Abhilfeverfahren iSd Art. 16 DSA, wodurch es Nutzern erleichtert werden soll, gegen rechtswidrige Inhalte vorzugehen.[145] Darüber hinaus besteht für Anbieter von Online-Plattformen gem. Art. 20 DSA die Verpflichtung zur Errichtung eines internen Beschwerdemanagements, bei welchem sich Nutzer im Falle einer zu ihren Lasten ausfallenden Entscheidung wehren können.[146] Der DSA schützt jedoch nicht nur die Nutzer, sondern auch die Online-Plattformen selbst, indem zum Schutz vor missbräuchlicher Verwendung derselben der Intermediär durch Art. 23 DSA ermächtigt wird, seine Dienste gegenüber Nutzern, welche vermehrt und offensichtlich rechtswidrige Inhalte bereitstellen, temporär auszusetzen.[147] Diese Ermächtigung stellt eine sekundärrechtliche Verankerung des „*Deplatforming*"[148] dar.[149]

Sehr große Online-Plattformen (very large online platforms, kurz VLOP zB Amazon, Apple App Store, Booking.com, Google Maps und Google Shopping, Youtube, Instagram und TikTok) und sehr große Online-Suchmaschinen (very large online search engines, kurz VLOSE zB Google Search, Microsoft Bing) werden aufgrund ihrer besonderen Rolle und Reich-

144 Gerdemann/Spindler GRUR 2023, 115 (115 f.).

145 S. Art. 16 ff. DSA, zu dessen Auslegung Erwgr. 50 herangezogen werden kann.

146 Achleitner MR-Int 2022, 114 (115); Gielen/Uphues EuZW 2021, 627 (635 f.); Legner ZUM 2024, 99 (105 f.).

147 Achleitner MR-Int 2022, 114 (115).

148 Grabenwarter/Holoubek/Leitl-Staudinger Kommunikationsplattformen/Kettemann/Rachinger/Sekwenz S. 55 (58 ff.).

149 Da die Art und Weise, wie eine solche Rolle und Reichweite genutzt werden können, erhebliche Auswirkungen auf die Online-Sicherheit und die öffentliche Meinung haben, verfolgt der DSA einen risikobasierten Ansatz. Dieser zielt darauf ab, spezifische Risiken, die zu Schäden sozialer oder wirtschaftlicher Art führen können, zu identifizieren, zu vermeiden oder zumindest zu mindern; vgl. Achleitner MR-Int 2022, 114 (115). Ein solcher risikobasierter Ansatz wird bspw. auch im Datenschutzrecht (Art 35 Datenschutz-Grundverordnung (DSGVO) – VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. 2016 L 119/1) verfolgt, jedoch mit dem Unterschied, dass in der DSGVO das Risikomanagement unter Beteiligung der Aufsichtsbehörde als direkte Kontrollinstanz vorgesehen ist; s. Schröder ZD 2019, 503 (503 ff.).

weite, die als erhebliche Gefahrenquelle eingeschätzt werden,[150] einem besonderen Regulierungsregime samt detaillierten Regelungen zur Rechtsdurchsetzung unterworfen.[151] Die Pflichten dieser vierten und damit regulierungsintensivsten Stufe (Abschnitt 5 DSA)[152] beinhalten nicht nur Verschärfungen der Regulierungselemente der dritten Stufe, sondern zusätzlich Instrumente der Fremd- und Selbstregulierung.[153] Während der Begriff der Online-Plattform iSd Art. 3 lit. i DSA auf jenem der dritten Regulierungsstufe aufbaut, werden Online-Suchmaschinen gem. Art. 3 lit. j DSA als sämtliche Vermittlungsdienste definiert, die Nutzern auf Basis eines beliebigen Themas Suchanfragen auf allen Websites oder Websites in bestimmten Sprachen ermöglichen.[154] Als „*sehr groß*" ist eine Plattform oder Suchmaschine zu qualifizieren, wenn sie eine durchschnittliche monatliche Anzahl von 45 Mio. aktiven Nutzern in der EU erreicht.[155] Diese vierte Gruppe von Diensteanbietern ist bspw. von der Pflicht zur Durchführung einer Risikobewertung, der Umsetzung von Maßnahmen zur Risikominderung und Vorgaben für Empfehlungssysteme betroffen.[156]

V. Kontrolle und Durchsetzung

Durch Aussagen wie „*Recht ist nur so gut wie seine Durchsetzung*"[157] oder „*Enforcement is […] key*"[158] wird der Stellenwert der Durchsetzung des DSA deutlich. Aus diesem Grund erfolgt diese zeitgleich auf verschiedenen Ebenen:[159] Zunächst werden die Mitgliedstaaten in Kapitel IV Abschnitt 1 DSA dazu verpflichtet, einen hoheitlichen Aufsichts- und Durchsetzungs-

150 Kastor/Püschel K&R 2023, 20 (21 ff.).
151 Berberich/Seip GRUR-Prax 2021, 4 (5 f.).
152 F. Hofmann/Raue/F. Hofmann/Raue DSA Einleitung Rn. 45 f.
153 Gerdemann/Spindler GRUR 2023, 115 (121).
154 Sesing-Wagenpfeil CR 2023, 113 (118 ff.); Gerdemann/Spindler GRUR 2023, 115 (121 ff.).
155 Art. 33 Abs. 1 DSA, wobei die Erreichung des Schwellenwertes durch die Kommission mittels Beschl. auf Basis der von den Diensteanbietern halbjährlich gemeldeten Nutzerzahlen gem. Art. 24 Abs. 3 DSA oder bei konkreten Anzeichen der Überschreitung auch durch flexiblere Einstufung gem. Art. 33 Abs. 4 UAbs. 2-4 DSA erfolgt.
156 Art. 34 ff. DSA.
157 Kraul HdB digitale Dienste/Bartels Durchsetzung Rn. 1.
158 SWD(2020) 348 final, Part 1, S. 22 f. und S. 42 ff.
159 Müller MMR 2022, 1007 (1010 f.).

apparat zu schaffen und eine Behörde als Koordinator für digitale Dienste auszuweisen.[160] Zugleich erkennt Art. 54 DSA neben der behördlichen Rechtsdurchsetzung auch eine privatrechtliche Rechtsdurchsetzung vor den nationalen Gerichten ausdrücklich an.[161] In der zweiten Ebene sind die nationalen Behörden gem. Kapitel IV Abschnitt 2 DSA zur länderübergreifenden Zusammenarbeit, dh insbesondere zur gegenseitigen Amtshilfe und Koordination, verpflichtet.[162] Jeder Mitgliedstaat hat eine auf seinem Staatsgebiet zuständige Behörde als Koordinator für digitale Dienste (Digital Services Coordinator, kurz DSC) zu benennen, der grundsätzlich für alle Fragen im Zusammenhang mit der Überwachung und Durchsetzung zuständig ist. Darüber hinaus wird eine unabhängige Beratergruppe der Koordinatoren für digitale Dienste mit der Beaufsichtigung gem. Kapitel IV Abschnitt 3 DSA betraut.[163] Dieses Europäische Gremium für digitale Dienste (European Board for Digital Services, kurz EBDS) unterstützt bspw. die Koordination gemeinsamer Untersuchungen.[164] Schließlich obliegt der Kommission die Zuständigkeit gegenüber VLOP und VLOSE im Hinblick auf die Beaufsichtigung, Untersuchung, Durchsetzung und Überwachung gem. Kapitel IV Abschnitt 4 DSA.[165]

C. Grundrechtsdogmatik

I. Drittwirkung von Unionsgrundrechten[166]

Das Ziel der Schaffung von Grundrechten ist primär die Regelung des vertikalen Verhältnisses zwischen der Union und den Unionsbürgern auf der einen Seite sowie der Union und den Mitgliedstaaten andererseits.[167] Die GRC grenzt ihren Anwendungsbereich selbst derart ab, dass die Charta *„für die Organe, Einrichtungen und sonstigen Stellen der Union unter Wah-*

160 Kraul HdB digitale Dienste/Bartels Durchsetzung Rn. 8 ff.; Berberich/Seip GRUR-Prax 2021, 4 (6); Schäufele/Krück GRUR-Prax 2023, 120 (123).
161 F. Hofmann/Raue DSA Art. 54 Rn. 1 ff.; Kraul HdB digitale Dienste/Bartels Durchsetzung Rn. 117 f.
162 Art. 56 ff. DSA; s. auch Kraul HdB digitale Dienste/Bartels Durchsetzung Rn. 24 ff.
163 Art. 61 ff. DSA; vgl. Müller MMR 2022, 1007 (1010).
164 Kraul HdB digitale Dienste/Bartels Durchsetzung Rn. 19 ff.; Steinrötter RHdB Plattformregulierung/Achleitner Durchsetzung Rn. 1.
165 Art. 64 ff. DSA; Kraul HdB digitale Dienste/Bartels Durchsetzung Rn. 17 f.
166 Zur Drittwirkung von Grundrechten im Allg. s. Kulick Horizontalwirkung S. 43 ff.
167 Wischmeyer, Rechtsgutachten, 2023, S. 8 (Stand 12.2.2024).

rung des Subsidiaritätsprinzips und für die Mitgliedstaaten ausschließlich bei der Durchführung des Rechts der Union"[168] gilt.[169] Dies entspricht auch dem traditionellen Verständnis der Grundrechte als Abwehrrechte, wonach diese die Freiheitssphäre des Einzelnen vor den Eingriffen der öffentlichen Gewalt des Staats schützen.[170] Demgegenüber nicht geregelt ist die Frage,[171] ob die Grundrechte auch eine horizontale Wirkung entfalten.[172]

Die Horizontalwirkung von Grundrechten, die auch als Drittwirkung der Grundrechte bezeichnet wird, beschäftigt sich mit der Wirkung von Grundrechten zwischen zwei oder mehreren Privaten und sohin selbst grundrechtsberechtigten Parteien.[173] Diese Wirkung ist von Relevanz, weil es sich bei den Anbietern sozialer Netzwerke typischerweise um private Unternehmen handelt, die als solche grundsätzlich nicht zu den klassischen Grundrechtsverpflichteten zählen.[174] Damit also Schranken für die normative Gestaltungsmacht der Anbieter solcher Dienste aus den Unionsgrundrechten abgeleitet werden können, müssen diese entweder unmittelbar[175] oder zumindest mittelbar[176] an die GRC gebunden sein.[177]

168 Art. 51 Abs. 1 GRC; vgl. zur Bindung der Europäischen Union auch Meyer/Hölscheidt/Schwerdtfeger GRC Art. 51 Rn. 27 ff und zu jener der Mitgliedstaaten ebenda Rn. 36 ff.

169 Stöggl ZÖR 2019, 465 (466 ff.).

170 Badó/Belling Rechtsentwicklungen/Belling/Herold/Kneis S. 53 (53 f.).

171 EuGH Urt. v. 15.1.2014 – C-176/12, ECLI:EU:C:2014:2, Rn. 42 ff. = BeckRS 2014, 80030 – Association de médiation sociale.

172 Wischmeyer, Rechtsgutachten, 2023, S. 8 (Stand 12.2.2024).

173 Der Begriff „*Drittwirkung*" wurde 1954 geprägt von *Hans-Peter Ipsen*; vgl. Neumann/Nipperdey/Scheuner HdB Grundrechte II/Ipsen S. 111 (143). In diesem Beitrag nicht näher beleuchtet wird die Theorie der staatlichen Schutzpflicht. Dieser Ansatz vertritt, dass die Grundrechte einen Schutzauftrag des Staates enthalten, der den Staat bei fehlender Machtsymmetrie verpflichtet, den unterlegenen Bürger vor der Beeinträchtigung seiner Grundrechte durch den überlegenen Bürger zu wahren; vgl. Badó/Belling Rechtsentwicklungen/Belling/Herold/Kneis S. 53 (55).

174 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (155 ff.).

175 Zur Problematik der unmittelbaren Drittwirkung s. C.I.1.

176 Zur mittelbaren Drittwirkung s. C.I.2.

177 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (155 f.).

1. Problematik der unmittelbaren Drittwirkung

Die unmittelbare Drittwirkung sieht eine direkte Bindung Privater an die Grundrechte vor, sodass sich Bürger in privaten Rechtsverhältnissen auf die Einhaltung der Grundrechte berufen können.[178] Gegen diese Form der Drittwirkung spricht einerseits der Wortlaut des Art. 51 Abs. 1 GRC, der die GRC nur für Unionsorgane sowie für die Mitgliedstaaten bei der Durchführung von Unionsrecht anwendbar erklärt.[179] Weiters spricht gegen die unmittelbare Drittwirkung, dass die Anforderungen der Charta an die Rechtfertigung von Grundrechtseingriffen nicht auf ein privatautonomes Verhalten[180] ausgerichtet sind, weil sie insbesondere dem erforderlichen Gesetzesvorbehalt in Art. 52 Abs. 1 GRC nicht gerecht werden.[181]

2. Mittelbare Drittwirkung der Unionsgrundrechte

Die mittelbare Drittwirkung folgt in ihrem Ergebnis der unmittelbaren Drittwirkung,[182] weil auch sie eine Wirkung von Grundrechten zwischen Privaten entstehen lässt[183] und im Hinblick auf die Intensität ihrer Bindung nur graduell variiert,[184] sodass ein Rückgriff auf die dogmatische Figur der unmittelbaren Drittwirkung nicht zwangsläufig nötig ist.[185] Dabei wird der

178 Badó/Belling Rechtsentwicklungen/Belling/Herold/Kneis S. 53 (55); Schoditsch Grundrechte S. 192 ff.

179 Haratsch/Koenig/Pechstein EuropaR Rn. 723 f.; Kahl/Raschauer/Storr Grundsatzfragen GRC/Stangl S. 1 (6).

180 Beachte jedoch, dass auch die DSGVO in einzelnen Vorschriften die Grundrechte in die Privatrechtsverhältnisse einbringt; bspw. wird gem. Art. 6 Abs. 1 lit. f DSGVO bei der Rechtmäßigkeit einer Datenverarbeitung eine Abwägung mit den Grundrechten des Betroffenen durchgeführt.

181 Haratsch/Koenig/Pechstein EuropaR Rn. 723; Jarass Art 51 GRC Rn. 41 f.; s. zur Frage, ob Unionsgrundrechte aus sich heraus Geltung zwischen Privaten beanspruchen können, C.III.

182 Dies wird umso deutlicher, wenn die Gerichte grundrechtliche Wertungen nicht ausschließlich im Wege der verfassungskonformen Auslegung des Zivilrechts zum Ausdruck bringen, sondern darüber hinaus konkrete sachliche oder verfahrensrechtliche Pflichten aus den Grundrechten ableiten, sodass aus praktischer Sichtweise von einer quasi unmittelbaren Wirkung gesprochen werden kann; vgl. hierzu Wischmeyer, Rechtsgutachten, 2023, S. 20 f. (Stand 12.2.2024).

183 Bajlicz/Bohnert/Ganglbauer/Gärner/Petermair/Ponader/Tilzer/Werderitsch Tagung ÖffR XI/Achleitner S. 3 (14).

184 Wischmeyer, Rechtsgutachten, 2023, S. 20 f. (Stand 12.2.2024).

185 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (157).

Gefahr, die von privaten Akteuren bzw. im konkreten Fall von „*privaten Gesetzgebern*" ausgeht, derart entgegengewirkt,[186] dass die nationalen sowie europäischen Gerichte bei der Anwendung und Auslegung von Recht unmittelbar an die Unionsgrundrechte gebunden sind.[187]

Konkret hat dies zur Folge, dass der Private bei fehlender gesetzgeberischer Determinierung, durch grundrechtskonforme Auslegung unbestimmter Rechtsbegriffe[188] und Generalklauseln geschützt wird.[189] Je geringer die regulierende Wirkung des Markts ist, desto höher ist die grundrechtstypische Gefährdungslage des unterlegenen Vertragspartners, woraus sich ein höheres Schutzniveau ergibt.[190] Eine Wirkung zwischen Privaten ergibt sich dadurch, dass diese horizontal durch zivilrechtliche Bestimmungen berechtigt und verpflichtet werden, wobei die Auslegung derselben vor dem Hintergrund der Grundrechte durch die Judikative erfolgt.[191] Darüber hinaus leitet der EuGH aus den Unionsgrundrechten konkrete sachliche oder verfahrensrechtliche Pflichten ab, wodurch diese praktisch unmittelbar angewendet werden.[192] Diese Form der Drittwirkung wird sowohl vom EuGH[193] als auch von der herrschenden Lehre anerkannt.[194]

---

186 OGH 24.1.2019, 6 Ob 55/18 h; 15.4.1998, 3 Ob 2440/96m; Bajlicz/Bohnert/Ganglbauer/Gärner/Petermair/Ponader/Tilzer/Werderitsch Tagung ÖffR XI/Achleitner S. 3 (13 f.).

187 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (157).

188 VfGH 3.3.2003, V1/02 ua = VfSlg 16.821/2003.

189 Schiek StudZR-WissOn 2021, 61 (73).

190 Limbach JuS 1985, 10 (13 ff.); Schiek StudZR-WissOn 2021, 61 (73 f.).

191 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (157); Haratsch/Koenig/Pechstein EuropaR Rn. 723. Die Ausstrahlungswirkung der Grundrechte erfolgt z.B. in unbestimmten Rechtsbegriffen und Generalklauseln wie bspw. „*Sittenwidrigkeit*" und „*Treu und Glauben*".

192 EuGH Urt. v. 29.1.2008 – C-275/06, ECLI:EU:C:2008:54, Rn. 70 = BeckRS 2008, 70164 – Promusicae; Urt. v. 6.11.2018 – C-684/16, ECLI:EU:C:2018:874, Rn. 76 ff. = BeckRS 2018, 27414 – Max-Planck-Gesellschaft zur Förderung der Wissenschaften; Urt. v. 6.11.2018 – verb. Rs. C-569/16 u. C-570/16, ECLI:EU:C:2018:871, Rn. 92 = BeckRS 2018, 27416 – Bauer.

193 EuGH Urt. v. 24.11.2011 – C-70/10, ECLI:EU:C:2011:771, Rn. 41 ff. = BeckRS 2011, 81685 – Scarlet Extended; Urt. v. 16.2.2012 – C-360/10, ECLI:EU:C:2012:85, Rn. 39 ff. = BeckRS 2012, 80348 – SABAM; Urt. v. 18.7.2013 – C-426/11, ECLI:EU:C:2013:521, Rn. 30 = BeckRS 2013, 81519 – Alemo-Herron u.a.; Urt. v. 16.7.2015 – C-580/13, ECLI:EU:C:2015:485, Rn. 34 = BeckRS 2015, 80946 – Coty Germany; s. auch Meyer/Hölscheidt/Schwerdtfeger GRC Art. 51 Rn. 57 ff.

194 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (157) mwN.

II. Kann der DSA grundsätzlich eine Horizontalwirkung von Unionsgrundrechten begründen?

Um die Frage beantworten zu können, ob der DSA als Sekundärrechtsakt eine Horizontalwirkung von Unionsgrundrechten begründen kann, ist die normative Architektur des Unionsverfassungsrechts zu betrachten. Demnach ist der Unionsgesetzgeber an das primärrechtliche Unionsrecht gebunden, über welches ihm die Dispositionsbefugnis entzogen ist, sodass grundrechtliche Bindungen mit primärrechtlicher Wirkung nicht ohne entsprechende Grundlage im Primärrecht angeordnet werden können.[195]

Daraus folgt, dass der DSA als Sekundärrechtsakt keine konstitutive, sondern ausschließlich deklarative Qualität im Hinblick auf eine mögliche Horizontalwirkung der Unionsgrundrechte besitzt.[196] Daran ändert auch die Tatsache nichts, dass einzelne Grundrechte vom einfachen Gesetzgeber schon aufgrund ihrer „*Normprägung*" ausgestaltungsbedürftig sind.[197]

Denkbar wäre folglich eine Bekräftigung der sich aus der Charta selbst ergebenden Bindung der Diensteanbieter an die Unionsgrundrechte,[198] sodass Art. 14 Abs. 4 DSA einen gesetzlich normierten deklarativen – uU auch konkretisierenden[199] – Fall der mittelbaren Drittwirkung der primärrechtlich verankerten Unionsgrundrechte der GRC darstellt.[200]

195 Die Bindung der Mitgliedstaaten an Unionsgrundrechte bei Eröffnung des Anwendungsbereichs in Art. 51 Abs. 1 GRC ändert daran nichts, weil hiervon nicht das Verhältnis von Unionsverfassungs- und Unionsgesetzgeber betroffen ist; s. auch Wischmeyer, Rechtsgutachten, 2023, S. 9 (Stand 12.2.2024).

196 Brauneck NVwZ 2024, 377 (383); Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (162 ff.).

197 Michl Unionsgrundrechte S. 80 ff.; Wischmeyer, Rechtsgutachten, 2023, S. 9 (Stand 12.2.2024).

198 Wischmeyer, Rechtsgutachten, 2023, S. 9 f. (Stand 12.2.2024).

199 Der Unionsgesetzgeber darf Gewährleistungen des Primärrechts – sohin auch die Unionsgrundrechte – gem. Art. 3 Abs. 1 iVm Abs. 6 EUV sekundärrechtlich konkretisieren und ihnen hiermit Geltung verschaffen; s. Ammann/Bottega/Bukovac/Lehner/Meier/Piskóty/Rausch/Rehmann/Schneider/Weder/Wilhelm Verantwortung und Recht/Karg S. 67 (89).

200 Kraul HdB digitale Dienste/Maamar Sorgfaltspflichten Rn. 45 ff.

III. Können Unionsgrundrechte aus sich heraus Geltung zwischen Privaten beanspruchen?

Es bleibt jedoch die Frage, ob die primärrechtlich verankerten Unionsgrundrechte, deren Wirkung durch Sekundärrecht – wie zuvor erörtert – nur deklaratorisch angeordnet werden kann, aus sich heraus eine Bindung zwischen Privaten erwirken können. Dabei ist die Frage der Horizontalwirkung dem Unionsrecht nicht unbekannt, doch hat sich der Fokus von RL und Grundfreiheiten auf die Inhalte der GRC verlagert.[201] Es lässt sich diesbezüglich aus der Judikatur des EuGH zusammengefasst ableiten, dass die Horizontalwirkung einer Norm des Primärrechts insbesondere anhand des jeweiligen Normzwecks sowie im Hinblick auf die Effektivität bestimmt wird.[202]

Bereits 1974 erkannte der EuGH die Bindung eines privaten Sportverbandes an die Dienstleistungsfreiheit aufgrund von *effet utile*-Erwägungen an,[203] führte diese Rechtsprechung auch in der Rs. *Bosman* fort[204] und erstreckte sie schließlich auf die Niederlassungsfreiheit.[205] Dabei lassen die normstrukturellen Parallelen von Grundfreiheiten und Grundrechten zumindest eine Indizwirkung für die Existenz einer Horizontalwirkung von Unionsgrundrechten zu.[206] Über diese Horizontalwirkung der Grundfreiheiten hinaus, erkannte der EuGH auch der Vorgängervorschrift des Art. 157 AEUV über das gleiche Entgelt von Männern und Frauen[207] sowie der Altersdiskriminierung[208] Horizontalwirkung zu.[209]

---

201 So auch der GA Cruz Villalón in seinem SchlA (SchlA v. 18.7.2013 – C-176/12, ECLI:EU:C:2013:491, Rn. 34 = BeckRS 2014, 80206 – Association de médiation sociale): „*Dringt man zum Kern der Frage vor, könnte es angesichts einiger in dieser Hinsicht zum Ausdruck gebrachten Meinungen scheinen, dass die Idee der horizontalen Wirkung ein dem Unionsrecht fremder Begriff sei, mit der man sich zum ersten Mal wegen der Einfügung der Charta in das Primärrecht der Union befassen musste. Und doch ist die Idee, dass die Grundfreiheiten des Verkehrs […] oder bestimmte Grundsätze wie der des Verbots der Diskriminierung aufgrund des Geschlechts […] in privatrechtlichen Beziehungen eine Rolle spielen, ein alter und gefestigter Gedanke*".

202 Unseld Horizontalwirkung S. 139.

203 EuGH Urt. v. 12.12.1974 – C-36/74, ECLI:EU:C:1974:140, Rn. 16/19 ff. = BeckRS 1974, 107015 – Walrave und Koch/Association Union Cycliste Internationale u.a.

204 EuGH Urt. v. 15.12.1995 – C-415/93, ECLI:EU:C:1995:463, Rn. 82 ff = BeckRS 2004, 77129 – Bosman.

205 EuGH Urt. v. 11.12.2007 – C-438/05, ECLI:EU:C:2007:772, Rn. 33 mwN, 61 = BeckRS 2007, 71032 – The International Transport Workers' Federation und The Finnish Seamen's Union.

206 Wischmeyer, Rechtsgutachten, 2023, S. 10 f. (Stand 12.2.2024).

Der EuGH geht in seiner jüngeren Rechtsprechung weiters von einer unmittelbaren Drittwirkung einzelner sozialer Grundrechte der GRC aus, sofern bestimmte Voraussetzungen vorliegen.[210] Besonders hervorzuheben ist dabei die Entscheidung *Egenberger* aus dem Jahr 2018, in welcher der EuGH entschied, dass *„ein mit einem Rechtsstreit zwischen zwei Privatpersonen befasstes nationales Gericht, wenn es ihm nicht möglich ist, das einschlägige nationale Recht im Einklang mit […] der Richtlinie […] auszulegen, verpflichtet ist, im Rahmen seiner Befugnisse den dem Einzelnen aus den Art. 21 und 47 der Charta erwachsenden Rechtsschutz zu gewährleisten und für die volle Wirksamkeit dieser Bestimmungen zu sorgen, indem es erforderlichenfalls jede entgegenstehende nationale Vorschrift unangewendet lässt*".[211]

Auch in der Rs. *Bauer und Broßonn* (2018) war eine unionsrechtskonforme Auslegung des nationalen Rechts nicht möglich, sodass der EuGH das Recht auf Jahresurlaub gem. Art. 31 Abs. 2 GRC als wesentlichen Grundsatz der Sozialordnung der Union anerkannte, diesem *„zwingenden Charakter"* zusprach und das Bedürfnis einer weiteren Konkretisierung der Norm verneinte.[212] Darüber hinaus stellte der EuGH klar, dass Art. 51 Abs. 1 GRC einer unmittelbaren Drittwirkung nicht entgegenstehe, da dieser keine Aussage über die Grundrechtsbindung Privater treffe und nicht derart ausgelegt werden könne, dass eine Horizontalwirkung *„kategorisch ausgeschlossen wäre"*.[213] Diese Rechtsprechung folgte einer Entscheidung aus dem Jahr 1976, in welcher der EuGH entschied, dass die ausdrückliche Adressierung

207 EuGH Urt. v. 8.4.1976 – C-43/75, ECLI:EU:C:1976:56, Rn. 30/34 ff. = BeckRS 2004, 71181 – Defrenne/SABENA.

208 EuGH Urt. v. 22.11.2005 – C-144/04, ECLI:EU:C:2005:709, Rn. 30 ff. = BeckRS 2005, 70888 – Mangold; Urt. v. 19.1.2010 – C-555/07, ECLI:EU:C:2010:21, Rn. 56 = BeckRS 2010, 90051 – Kücükdeveci.

209 Wischmeyer, Rechtsgutachten, 2023, S. 11 (Stand 12.2.2024).

210 EuGH Urt. v. 6.11.2018 – verb. Rs. C-569/16 u. C-570/16, ECLI:EU:C:2018:871, Rn. 79 ff. = BeckRS 2018, 27416 – Bauer; Urt. v. 22.11.2005 – C-144/04, ECLI:EU:C:2005:709, Rn. 55 ff. = BeckRS 2005, 70888 – Mangold; Urt. v. 19.1.2010 – C-555/07, ECLI:EU:C:2010:21, Rn. 56 = BeckRS 2010, 90051 – Kücükdeveci; Urt. v. 22.1.2019 – C-193/17, ECLI:EU:C:2019:43, Rn. 77 = BeckRS 2019, 288 – Cresco Investigation; Urt. v. 17.4.2018 – C-414/16, ECLI:EU:C:2018:257, Rn. 77 ff = BeckRS 2018, 5386 – Egenberger.

211 EuGH Urt. v. 17.4.2018 – C-414/16, ECLI:EU:C:2018:257, Rn. 82 = BeckRS 2018, 5386 – Egenberger.

212 EuGH Urt. v. 6.11.2018 – verb. Rs. C-569/16 u. C-570/16, ECLI:EU:C:2018:871, Rn. 83 f. = BeckRS 2018, 27416 – Bauer.

213 EuGH Urt. v. 6.11.2018 – verb. Rs. C-569/16 u. C-570/16, ECLI:EU:C:2018:871, Rn. 87 = BeckRS 2018, 27416 – Bauer.

der Mitgliedstaaten nicht ausschließt, dass *„zugleich allen an der Einhaltung der so umschriebenen Pflichten interessierten Privatpersonen Rechte verliehen sein können*“[214].[215] Diesen beiden Entscheidungen gemeinsam ist, dass das Verbot der contra legem-Auslegung richtlinienwidrigen nationalen Rechts durch die Berufung auf die Horizontalwirkung der Grundrechte umgangen wird.[216]

Auch wenn sich aus diesen zuvor genannten Entscheidungen keine nähere Begründung für die Horizontalwirkung ergibt, lassen sich daraus doch die beiden notwendigen Voraussetzungen für die unmittelbare Wirkung von Unionsgrundrechten zwischen Privaten ableiten.[217] Diese liegen vor, wenn das Unionsgrundrecht aufgrund seines zwingenden Charakters nicht vertraglich abbedungen werden kann und die grundrechtlich normierte Rechtsposition nicht von weiteren Bedingungen bzw. Konkretisierungen abhängig ist.[218]

Eine unmittelbare Drittwirkung kommt demnach in Betracht, wenn das Grundrecht aufgrund seiner Eigenschaften zwingender Natur und eigenständig ist.[219] Schließlich folgert der EuGH aus der Horizontalwirkung weiter, dass die grundrechtlichen Interessen aller Beteiligten ebenso wie die Wertungen des Sekundärrechtsgesetzgebers einzubeziehen sind.[220] Es lässt sich daher festhalten, dass die Horizontalwirkung des Primärrechts als „*alter und gefestigter Gedanke*“[221] des Unionsrechts aufgrund des Effektivitätsprinzips einen breiten Anwendungsbereich findet.[222] Dies insbesondere vor

214 EuGH Urt. v. 8.4.1976 – C-43/75, ECLI:EU:C:1976:56, Rn. 30/34 = BeckRS 2004, 71181 – Defrenne/SABENA.

215 Bajlicz/Bohnert/Ganglbauer/Gärner/Petermair/Ponader/Tilzer/Werderitsch Tagung ÖffR XI/Achleitner S. 3 (19).

216 Wischmeyer, Rechtsgutachten, 2023, S. 12 f. (Stand 12.2.2024).

217 Wischmeyer, Rechtsgutachten, 2023, S. 12 ff. (Stand 12.2.2024).

218 Haratsch/Koenig/Pechstein EuropaR Rn. 723.

219 GA Bot, SchlA v. 29.5.2018 – verb. Rs. C-569/16 u. C-570/16, ECLI:EU:C:2018:337, Rn. 80 = BeckRS 2018, 9605 – Bauer.

220 EuGH Urt. v. 17.4.2018 – C-414/16, ECLI:EU:C:2018:257, Rn. 80 f. = BeckRS 2018, 5386 – Egenberger; dieser Fall ist Gegenstand eines laufenden (Stand Februar 2024) Verfahrens vor dem BVerfG, in welchem dessen Vereinbarkeit mit der Verfassungsidentität und dem *Ultra-vires*-Grundsatz überprüft wird (s. hierzu BVerfG 2 BvR 934/19), weil im Erg. das Verbot der contra legem-Auslegung richtlinienwidrigen Rechts der Mitgliedstaaten umgangen wird, indem man auf die Horizontalwirkung zurückgreift.

221 GA Cruz-Villalón, SchlA v. 18.7.2013 – C-176/12, ECLI:EU:C:2013:491, Rn. 34 = BeckRS 2014, 80206 – Association de médiation sociale.

222 Wischmeyer, Rechtsgutachten, 2023, S. 15 f. (Stand 12.2.2024).

dem Hintergrund, dass Diensteanbieter im Hinblick auf die Regulierung von Kommunikation auf ihren Plattformen eine nahezu staatsähnliche Stellung erlangt haben, sodass ein effektiver Grundrechtsschutz auch zwischen Privaten erforderlich ist.[223]

Vor dem Hintergrund der vorgenannten Kriterien hat der EuGH die Horizontalwirkung für Art. 26 und 27 GRC hingegen ausdrücklich verneint.[224] In Bezug auf Art. 27 GRC begründet der EuGH dies mit dem Wortlaut der Bestimmung, nach welcher diese „*durch Bestimmungen des Unionsrechts oder des nationalen Rechts konkretisiert werden muss*", um „*seine volle Wirksamkeit*" zu entfalten.[225] Das Argument der spezifischen Struktur des konkretisierungsbedürftigen Grundrechts[226] greift der EuGH in seiner Entscheidung zu Art. 26 GRC auf und führt weiters aus, dass Art. 26 GRC „*für sich allein dem Einzelnen kein subjektives Recht verleihen [kann], das als solches geltend gemacht werden kann*".[227] Nach der Literatur wird eine Horizontalwirkung ebenfalls für Art. 30 GRC[228] und Art. 34 GRC[229] verneint.[230]

Insoweit der EuGH eine solche Horizontalwirkung anerkannt hat, beschränkte er sie bis dato in dreierlei Hinsicht: auf RL, auf bestimmte Rechtsgebiete und auf Subordinationsverhältnisse. Es stellt sich daher die Frage, ob diese Rechtsprechung auch auf andere Unionsgrundrechte der GRC übertragbar ist.

223 Prechal RDCE 2020, 407 (417 ff.); Wischmeyer, Rechtsgutachten, 2023, S. 16 f. (Stand 12.2.2024); zu derart mächtigen Positionen von App Stores im Speziellen, s. auch V. Hofmann/Dinar/Kettemann/Böke/Gradulewski/Hinrichs, Governance by Geschäft, 2021 (Stand 12.2.2024).

224 Wischmeyer, Rechtsgutachten, 2023, S. 15 (Stand 12.2.2024).

225 EuGH Urt. v. 15.1.2014 – C-176/12, ECLI:EU:C:2014:2, Rn. 45 ff = BeckRS 2014, 80030 – Association de médiation sociale.

226 Wischmeyer, Rechtsgutachten, 2023, S. 15 (Stand 12.2.2024).

227 EuGH Urt. v. 22.5.2014 – C-356/12, ECLI:EU:C:2014:350, Rn. 78 = BeckRS 2014, 80909 – Glatzel.

228 Die Horizontalwirkung des Art. 30 GRC (Schutz bei ungerechtfertigter Entlassung) wird aufgrund des Vorbehalts „*nach dem Unionsrecht und den einzelstaatlichen Rechtsvorschriften und Gepflogenheiten*" abgelehnt.

229 Auch die Horizontalwirkung des Art. 34 GRC (Soziale Sicherheit und soziale Unterstützung) wird aufgrund des Vorbehalts „*nach Maßgabe des Unionsrechts und der einzelstaatlichen Rechtsvorschriften und Gepflogenheiten*" abgelehnt.

230 Diesen Bestimmungen fehle es an einem über das Sekundärrecht hinausgehenden primärrechtlichen Schutzgehalt bzw. einem genuinen Schutzgut; s. Michl Unionsgrundrechte S. 165 ff.; Wischmeyer, Rechtsgutachten, 2023, S. 16 f. (Stand 12.2.2024).

1. Ist die Judikatur des EuGH formell auf RL beschränkt?

Wie die obige Analyse zeigt, erkannte der EuGH die Horizontalwirkung bislang ausschließlich bei RL an, nahm jedoch zu jener bei VO keine Stellung.[231] Während RL ausschließlich hinsichtlich ihres zu erreichenden Ziels verbindlich sind, den innerstaatlichen Stellen jedoch die Wahl der Form und Mittel überlassen, haben VO allgemeine Geltung, sind in all ihren Teilen verbindlich und gelten unmittelbar in jedem Mitgliedstaat.[232] Daraus folgt, dass ein Rückgriff auf die dogmatische Figur der Drittwirkung nur bei RL erforderlich ist, denn nur bei diesen kann der nationale Gesetzgeber aufgrund der *contra legem*-Grenze für die richtlinienkonforme Auslegung des nationalen Rechts den Schutzanspruch der Unionsgrundrechte durch fehlerhafte, verspätete oder gänzlich unterlassene Umsetzung einer RL unterlaufen.[233] Der EuGH nutzt insofern die Horizontalwirkung zur Begründung der Ausnahme von der allgemeinen Regel,[234] wonach sich Private gegenüber Privaten nicht unmittelbar auf RL berufen können.[235] Da der EuGH jedoch trotz der Bedenken, die gegenüber einer Horizontalwirkung der Unionsgrundrechte bestehen, diese anerkennt, gilt diese bei VO, die zweifelsfrei unmittelbare Wirkung gegenüber Privaten entfalten, umso mehr.[236] Es erscheint daher auch plausibel, dass die Literatur betreffend die Horizontalwirkung vom Anwendungsbereich des Sekundärrechts spricht, ohne dabei zwischen RL und VO zu unterscheiden.[237]

231 Wischmeyer, Rechtsgutachten, 2023, S. 17 (Stand 12.2.2024).

232 Art 288 AEUV; vgl. Haratsch/Koenig/Pechstein EuropaR Rn. 398 ff.

233 Wischmeyer, Rechtsgutachten, 2023, S. 17 (Stand 12.2.2024).

234 Dies ergibt sich auch aus den SchlA des GA Bobek (SchlA v. 25.7.2018 – C-193/17, ECLI:EU:C:2018:614, Rn. 186 ff. = BeckRS 2018, 16329) in der Rs. Cresco (SchlA v. 22.1.2019 – C-193/17, ECLI:EU:C:2019:43 = BeckRS 2019, 288) sowie des SchlA des GA Tanchev (SchlA v. 9.11.2017 – C-414/16, ECLI:EU:C:2017:851, Rn. 119 = BeckRS 2017, 134211) in der Rs. Egenberger (EuGH Urt. v. 17.4.2018 – C-414/16, ECLI:EU:C:2018:257 = BeckRS 2018, 5386), in welchen diese die Lösung des Falles über die Staatshaftung entsprechend der AMS-Entscheidung vorschlugen, denen der EuGH jedoch nicht gefolgt ist.

235 Stattdessen wird in diesen Fällen auf die Staatshaftung verwiesen; s. hierzu EuGH Urt. v. 19.11.1991 – verb. Rs. C-6/90 u. C-9/90, ECLI:EU:C:1991:428, Rn. 31 ff. = BeckRS 2004, 77605 – Francovich u. Bonifaci/Italien; Colombi Ciacchi EuConst 2019, 294 (299 ff.).

236 Wischmeyer, Rechtsgutachten, 2023, S. 18 (Stand 12.2.2024).

237 Keine Unterscheidung wird bspw. getroffen in Calliess/Ruffert/Kingreen GRC Art. 51 Rn. 24 ff.; Wischmeyer/Meißner NJW 2023, 2673 (2676).

2. Ist die Judikatur des EuGH inhaltlich auf Arbeits- und Diskriminierungsrecht beschränkt?

Die bisherige Rechtsprechung beschränkte sich jedoch nicht nur auf RL, sondern auch inhaltlich auf die Gebiete des Arbeits- und Diskriminierungsrechts sowie vereinzelte Unionsgrundrechte.[238] Dies aufgrund der machtasymmetrischen Stellung des Arbeitnehmers gegenüber dem Arbeitgeber, wodurch ein besonderer Bedarf nach normativer Korrektur besteht.[239]

In seiner Rechtsprechung begründete der EuGH die Horizontalwirkung jedoch nur eingeschränkt mit den Spezifika des Rechtsgebiets und des jeweiligen Unionsgrundrechts, sodass die Argumentation grundsätzlich auf alle Unionsgrundrechte übertragbar ist,[240] welche die Voraussetzungen der unmittelbaren Geltung und des zwingenden, eigenständigen Charakters erfüllen.[241] Aus der Bestimmung muss sich demnach ihre Rechtswirkung unbedingt und zwingend ergeben.[242] Dementsprechend ist weder die Unterscheidung in ein „*Recht*" iSd Art. 52 Abs. 1 bis 4 GRC oder einen sog. „*Charta-Grundsatz*" iSd Art. 52 Abs. 5 GRC noch das Vorliegen eines allg. Rechtsgrundsatzes des Unionsrecht notwendig.[243]

Gegen diese Argumentation wird in der Literatur teilweise vorgebracht, dass eine Verallgemeinerung der Grundsätze auf alle Unionsgrundrechte zu massiver Rechtsunsicherheit führe, weil es vermehrt zur Abwägung von Grundrechtspositionen komme.[244] Darüber hinaus würde die Privatautonomie aufgrund der Rechtfertigungslast massiv eingeschränkt[245] und

238 Dabei handelt es sich namentlich um die Art. 21, Art. 31 und Art. 47 der GRC; vgl. hierzu Frantziou CYELS 2020, 208 (208 f.).

239 Wischmeyer, Rechtsgutachten, 2023, S. 18 f. (Stand 12.2.2024); darüber hinaus ist die direkte Horizontalwirkung im Kontext des Arbeitsrechts bspw. in Frankreich und Italien anerkannt.

240 Hingegen aA Denga EuR 2021, 569 (585 ff.), der für eine Horizontalwirkung nur im EU-Arbeitsrecht plädiert.

241 Bajlicz/Bohnert/Ganglbauer/Gärner/Petermair/Ponader/Tilzer/Werderitsch Tagung ÖffR XI/Achleitner S. 3 (20 ff.); Frantziou CYELS 2020, 208 (217 ff.); Kainer NZA 2018, 894 (899); Prechal RDCE 2020, 407 (419); Wischmeyer, Rechtsgutachten, 2023, S. 19 (Stand 12.2.2024).

242 Prechal RDCE 2020, 407 (420).

243 Vgl. BVerfGE 152, 216 = EuZW 2019, 1035 Rn. 96 betreffend Art. 7 und 8 GRC; Wischmeyer, Rechtsgutachten, 2023, S. 19 (Stand 12.2.2024).

244 Kainer NZA 2018, 894 (898 ff.); Schoditsch Grundrechte S. 192 ff. Zur Sicherheit als Chartagrundsatz s. auch Leuschner Sicherheit S. 187 ff.

245 Bajlicz/Bohnert/Ganglbauer/Gärner/Petermair/Ponader/Tilzer/Werderitsch Tagung ÖffR XI/Achleitner S. 3 (14).

Private wären der Unsicherheit einer richterlichen Grundrechtsabwägung ausgesetzt.[246] Diesem Einwand ist jedoch entgegenzuhalten, dass der EuGH grundsätzlich Einwendungen, die zu unspezifisch sind, um dogmatisch anschlussfähig zu sein, kaum folgt.[247]

Daraus folgt im Ergebnis, dass die Judikatur des EuGH inhaltlich nicht auf Arbeits- und Diskriminierungsrecht beschränkt ist, sondern diese – bei Vorliegen der Voraussetzungen – auf alle Unionsgrundrechte übertragbar ist.

3. Ist die Judikatur des EuGH nur auf Subordinationsverhältnisse anwendbar?

Zuletzt stellt sich die Frage, ob für die Horizontalwirkung von Unionsgrundrechten ein Subordinationsverhältnis notwendige Voraussetzung ist, wie dies in früherer Rechtsprechung zu den Grundfreiheiten[248] der Fall war.[249] In seiner Rechtsprechung die GRC betreffend sah der EuGH in Arbeitsverhältnissen eine Machtasymmetrie zwischen Arbeitnehmer und Arbeitgeber.[250] Auch in der Literatur wird vertreten, dass die Horizontalwirkung vorwiegend für Private in Frage kommt, die einen dem Staat vergleichbaren Einfluss auf die Ausübung von Unionsgrundrechten des Einzelnen haben, was auch als intermediäre Gewalt bezeichnet wird.[251] Bezogen auf Plattformen folgt daraus, dass ein etwaiges Subordinationsverhältnis anhand der Stellung auf dem Markt, der Ausrichtung der Plattform sowie dem Grad der Angewiesenheit auf diese Plattform zu bestimmen ist.[252] Die soziale Macht eines privaten Diensteanbieters ist jedoch keine unbedingte Voraussetzung der Horizontalwirkung von Unionsgrundrechten, sondern

246 Kainer NZA 2018, 894 (899 f.).

247 Dies zeigt sich insbesondere auch an den Entscheidungen des EuGH in den Rs. *Egenberger* (EuGH Urt. v. 17.4.2018 – C-414/16, ECLI:EU:C:2018:257, Rn. 82 = BeckRS 2018, 5386) und *Cresco* (EuGH Urt. v. 22.1.2019 – C-193/17, ECLI:EU:C:2019:43, Rn. 89 = BeckRS 2019, 288 – Cresco Investigation), in welchen der EuGH den von den GA vorgebrachten SchlA keine Folge leistete; vgl. Wischmeyer, Rechtsgutachten, 2023, S. 20 (Stand 12.2.2024).

248 EuGH Urt. v. 15.12.1995 – C-415/93, ECLI:EU:C:1995:463, Rn. 68 ff = BeckRS 2004, 77129 – Bosman.

249 Wischmeyer, Rechtsgutachten, 2023, S. 10 ff. (Stand 12.2.2024).

250 Bajlicz/Bohnert/Ganglbauer/Gärner/Petermair/Ponader/Tilzer/Werderitsch Tagung ÖffR XI/Achleitner S. 3 (21).

251 Wischmeyer, Rechtsgutachten, 2023, S. 22 (Stand 12.2.2024).

252 BVerfG NJW 2019, 1935 Rn. 15; Heldt Drittwirkung S. 41.

ein Gesichtspunkt, welcher im Rahmen der Grundrechtsabwägung zu berücksichtigen ist.[253]

IV. Zwischenfazit

Die Entwicklung der Rechtsprechung des EuGH zur Horizontalwirkung der Grundrechte der GRC scheint noch nicht abgeschlossen zu sein,[254] was insbesondere daran liegt, dass der EuGH bisher nur in Einzelfällen Stellung genommen hat.[255] Legt man jedoch die eben skizzierten Maßstäbe zugrunde, können die für die Anwendung des DSA sachlich einschlägigen Grundrechte auf ihre Fähigkeit zur Horizontalwirkung untersucht werden.[256] Im Rahmen der Abwägung der konkreten Grundrechte darf die Übermacht der Diensteanbieter gegenüber den Nutzern nicht außer Acht gelassen werden.[257] Im Folgenden werden daher zunächst die einschlägigen Rechtsgrundlagen des DSA ermittelt und anschließend die Grundrechte der Akteure analysiert.

D. Drittwirkung von Grundrechten im DSA

I. Rechtsgrundlage einer Horizontalwirkung im DSA

Art. 14 DSA stellt eine fulminante Neuerung bei der Anwendung der Grundrechte dar, welche durch die Content Moderation betroffen sind.[258] So regelt Abs. 4, dass die *„Anbieter von Vermittlungsdiensten […] bei der*

253 BVerfGE 89, 214 (232 ff.); 128, 226 (249 f.); 148, 267 Rn. 33; 152, 152 Rn. 77. Darauf Bezug nehmend auch BGH NJW 2021, 3179 Rn. 122; Wischmeyer, Rechtsgutachten, 2023, S. 22 (Stand 12.2.2024).

254 Prechal RDCE 2020, 407 (424 f.).

255 Bajlicz/Bohnert/Ganglbauer/Gärner/Petermair/Ponader/Tilzer/Werderitsch Tagung ÖffR XI/Achleitner S. 3 (21).

256 Krit. *Achleitner*, wonach die Frage, unter welchen Umständen die Voraussetzungen der unmittelbaren Drittwirkung eines Grundrechts, sohin der zwingende Charakter und die Eigenständigkeit, vorliegen, noch nicht zur Gänze ausdifferenziert ist; s. Bajlicz/Bohnert/Ganglbauer/Gärner/Petermair/Ponader/Tilzer/Werderitsch Tagung ÖffR XI/Achleitner S. 3 (21) mwN.

257 Wischmeyer, Rechtsgutachten, 2023, S. 22 f. (Stand 12.2.2024).

258 Quintais/Appelman/Fathaigh GLJ 2023, 881 (883 f.).; Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (158).

Anwendung und Durchsetzung der in Absatz 1 genannten Beschränkungen sorgfältig, objektiv und verhältnismäßig vor[gehen] und […] dabei die Rechte und berechtigten Interessen aller Beteiligten sowie die Grundrechte der Nutzer, die in der Charta verankert sind, etwa das Recht auf freie Meinungsäußerung, die Freiheit und den Pluralismus der Medien und andere Grundrechte und -freiheiten" berücksichtigen müssen.[259] Als Vorbild für diese Regelung gilt die Terroristische Inhalte-VO,[260] die in Art. 5 Abs. 1 UAbs. 2 S 1 und Abs. 3 lit. c Hosting-Diensteanbieter dazu verpflichtet, bei inhaltsbeschränkenden Maßnahmen die Grundrechte der Nutzer zu beachten.[261]

II. Betroffene Grundrechtspositionen

Art. 14 Abs. 4 DSA scheint auf den ersten Blick in der deutschen Sprachfassung bei den geltend zu machenden Rechtspositionen zwischen „*alle[n] Beteiligte[n]*", die sich auf „*Rechte und berechtigte Interessen*" berufen können, und Grundrechten, auf welche sich nur die Nutzenden des Dienstes berufen können, zu unterscheiden.[262] Dies ist jedoch ein zu vernachlässigendes Spezifikum der deutschen Sprachfassung, denn andere Sprachfassungen, wie bspw. die englische, sprechen von einschließlich („*including*").[263]

Unter den berechtigten Interessen sind in der Folge die jeweils einschlägigen Grundrechte des Urhebers des Beitrags,[264] des Diensteanbieters[265] und Dritter[266] zu verstehen sowie das allen Betroffenen zu gewährende Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht iSd Art. 47 GRC.[267]

---

259 Art. 14 Abs. 4 DSA.

260 VO (EU) 2021/784 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Bekämpfung der Verbreitung terroristischer Online-Inhalte, ABl. 2021 L 172/79.

261 F. Hofmann/Raue/Raue DSA Art. 14 Rn. 18.

262 Mast/Kettemann/Dreyer/Schulz DSA/DMA/Mast/Kettemann/Schulz Art. 14 DSA Rn. 73 (i.E.).

263 Quintais/Appelman/Fathaigh GLJ 2023, 881 (895 ff.).

264 Hierzu detaillierter D.II.1. Grundrechte des Urhebers des Beitrags; Erwgr. 47 S 2 DSA; vgl. F. Hofmann/Raue/Raue DSA Art. 14 Rn. 88 ff.; zur Auslegung der Beiträge s. Kahl/Horn NJW 2023, 639 (639 ff.).

265 F. Hofmann/Raue/Raue DSA Art. 14 Rn. 103 ff.; krit. hierzu Denga EuR 2021, 569 (593).

266 Erwgr. 52 S 2 DSA.

267 Der DSA verweist nur vereinzelt auf bes. wichtige Grundrechte oder pauschal auf die GRC, bspw. Erwgr. 3, 9, 47, 51, 52, 63, 81, 109, 153, 155 sowie Art. 1 Abs. 1,

Auf der Seite des Diensteanbieters[268] sind insbesondere die Berufsfreiheit iSd Art. 15 GRC, die unternehmerische Freiheit gem. Art. 16 GRC, das Eigentumsgrundrecht des Art. 17 Abs. 1 und 2 GRC, das auch das Recht auf geistiges Eigentum umfasst, sowie die Meinungs- und Medienfreiheit gem. Art. 11 Abs. 1 und 2 GRC relevant.[269]

Von besonderer Bedeutung für die Nutzer der Plattformen – womit sowohl der Urheber des jeweiligen Beitrages gemeint ist, als auch die von diesem Beitrag negativ betroffenen Nutzer – sind die Menschenwürde gem. Art. 1 GRC, das Recht auf Achtung des Privat- und Familienlebens iSd Art. 7 GRC,[270] das Recht auf den Schutz personenbezogener Daten gem. Art. 8 GRC, die Meinungs- und Informationsfreiheit des Art. 11 Abs. 1 GRC, das Recht auf (geistiges) Eigentum in Art. 17 GRC, das Recht auf Nichtdiskriminierung gem. Art. 21 GRC sowie die Rechte des Kindes iSd Art. 24 GRC.[271]

Art. 14 Abs. 4 DSA beinhaltet insofern eine unvollständige Aufzählung deklaratorischer Natur, sodass die grundrechtliche Prüfung weder auf ausdrücklich genannte Unionsgrundrechte noch Grundrechtspositionen beschränkt werden darf.[272]

Die nachfolgende Analyse soll sich jedoch spezifisch mit jenen Grundrechten des Urhebers des Beitrags beschäftigen.

Art. 34 Abs. 1 UAbs. 2 lit. b DSA u.v.m.; vgl. Wischmeyer, Rechtsgutachten, 2023, S. 23 f. (Stand 12.2.2024).

268 Soziale Netzwerke als juristische Personen sind vom Anwendungsbereich der Unionsgrundrechte der GRC „*nicht ausgeschlossen*", es sei denn einzelne Grundrechtspositionen sind ausdrücklich Menschen als Grundrechtsträgern vorbehalten, s. EuGH Urt. v. 22.12.2010 – C-279/09, ECLI:EU:C:2010:811, Rn. 39 = BeckRS 2010, 91492 – DEB; *Denga* kritisiert jedoch die strukturelle Vernachlässigung der Grundrechtsposition der Diensteanbieter im DSA, s. Denga EuR 2021, 569 (593).

269 Quintais/Appelman/Fathaigh GLJ 2023, 881 (897); Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (162 ff.); Kraul HdB digitale Dienste/Maamar Sorgfaltspflichten Rn. 46; EuGH Urt. v. 14.2.2019 – C-345/17, ECLI:EU:C:2019:122, Rn. 65 = BeckRS 2019, 1399 – Buivids.

270 Der EuGH erkannte auch für Art. 7 und 8 GRC eine Horizontalwirkung an; vgl. EuGH Urt. v. 13.5.2014, C-131/12, ECLI:EU:C:2014:317, Rn. 81 = BeckRS 2014, 80862 – Google Spain and Google; Ammann/Bottega/Bukovac/Lehner/Meier/Piskóty/Rausch/Rehmann/Schneider/Weder/Wilhelm Verantwortung und Recht/Karg S. 67 (89).

271 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (159 ff.); Wischmeyer, Rechtsgutachten, 2023, S. 23 (Stand 12.2.2024).

272 Wischmeyer, Rechtsgutachten, 2023, S. 24 (Stand 12.2.2024).

Die Rechte der Nutzer werden ausdrücklich in Art. 14 Abs. 4 DSA sowie ergänzend in Erwgr. 47 DSA adressiert.[273] Für den Urheber des Beitrags von besonderer Bedeutung ist im Hinblick auf eine mögliche Intervention der Diensteanbieter das Recht auf Nichtdiskriminierung gem. Art. 21 GRC sowie auf Meinungsfreiheit gem. Art. 11 GRC,[274] weshalb der Fokus dieses Beitrags auf diesen beiden Unionsgrundrechten liegt.

1. Nichtdiskriminierung gemäß Art. 21 GRC

Art. 21 Abs. 1 GRC normiert als „*besondere Ausprägung*"[275] des allgemeinen Gleichheitsgrundsatzes des Art. 20 GRC umfassende Diskriminierungsverbote.[276] Im Hinblick auf die Umsetzung des allgemeinen Ziels des Art. 3 Abs. 3 UAbs. 2 EUV sowie des Diskriminierungsverbots des Art. 18 AEUV und der Rechtsetzungsermächtigung des Art. 19 AEUV verbietet Art. 21 GRC all jene Diskriminierungen, die auf bestimmten personengebundenen Merkmalen oder der Staatsangehörigkeit beruhen, weil diese den Menschen unveränderlich anhaften oder nur mit großem Aufwand geändert werden können.[277] Dies erklärt auch den engen inneren Zusammenhang zwischen Art. 21 GRC und dem Schutz der Menschenwürde in Art. 1 GRC.[278]

Die Horizontalwirkung des Art. 21 GRC[279] wurde – wie oben dargelegt[280] – in den Grundsatzentscheidungen *Egenberger*,[281] *Mangold*[282] und *Kücükdeveci*[283] durch den EuGH bereits anerkannt.[284]

---

273 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (159).
274 Wischmeyer, Rechtsgutachten, 2023, S. 24 (Stand 12.2.2024).
275 EuGH Urt. v. 29.4.2015 – C-528/13, ECLI:EU:C:2015:288, Rn. 48 = BeckRS 2015, 80577 – Léger; Urt. v. 22.5.2014 – C-356/12, ECLI:EU:C:2014:350, Rn. 43 = BeckRS 2014, 80909 – Glatzel.
276 Calliess/Ruffert/Rossi GRC Art. 21 Rn. 8.
277 S. zu Art. 21 GRC auch allg. Holoubek/Lienbacher/Köchle GRC Art. 21 Rn. 1 ff.; Streinz/Streinz GRC Art. 21 GRC Rn. 4 ff.; Calliess/Ruffert/Rossi GRC Art. 21 Rn. 2 f.
278 Calliess/Ruffert/Rossi GRC Art. 21 Rn. 3; Jarass Art. 21 GRC Rn. 2.
279 Vgl. auch Horvath/Lebesmühlbacher/Lehne/Lütte/Murer Tagung ÖffRe III/Scholz S. 17 (23 ff.).
280 Zur Frage, ob Unionsgrundrechte aus sich heraus Geltung zwischen Privaten beanspruchen können, s. C.III.
281 EuGH Urt. v. 17.4.2018 – C-414/16, ECLI:EU:C:2018:257, Rn. 77 ff. = BeckRS 2018, 5386 – Egenberger.
282 EuGH Urt. v. 22.11.2005 – C-144/04, ECLI:EU:C:2005:709, Rn. 55 ff. = BeckRS 2005, 70888 – Mangold.

2. Kommunikationsfreiheit gemäß Art. 11 Abs. 1 GRC

Die Informationsfreiheit des Art. 11 Abs. 1 GRC umfasst in aktiver Hinsicht das „*selbständige Recht, andere zu informieren, unabhängig davon, ob dies in mündlicher, schriftlicher, in gedruckter oder elektronischer Form geschieht*" und in passiver Hinsicht das „*Recht auf Zugänglichkeit und Empfang von Informationen*" und „*das Bemühen des Einzelnen um Informationen*".[285] Demnach ist sowohl die Meinungsfreiheit als auch die Freiheit, Informationen und Ideen zu empfangen sowie weiterzugeben, umfasst.[286] Der umfangreiche Schutz bezieht sich dabei nicht nur auf Werturteile, sondern auch auf Tatsachenbehauptungen, die geäußert oder über jegliche Formen der Verbreitung – unter anderem auch die Online-Kommunikation, bspw. durch Reposten oder Hyperlinks[287] über soziale Netzwerke – ausgedrückt werden.[288] Da die Qualität des Inhalts unerheblich ist,[289] fallen auch verletzende, schockierende oder beunruhigende Äußerungen in den Schutzbereich des Art. 11 Abs. 1 GRC.[290] Vom Anwendungsbereich des Art. 11 GRC können jedoch bestimmte Formen der Hassrede ausgenommen sein, die unter das Missbrauchsverbot des Art. 54 GRC fallen.[291] Unter dem Begriff der Hassrede im Internet (sog. „*Hate Speech*") sind verbale oder non-verbale Äußerungen eines Individuums oder einer Gruppe von Individuen

283 EuGH Urt. v. 19.1.2010 – C-555/07, ECLI:EU:C:2010:21, Rn. 56 = BeckRS 2010, 90051 – Kücükdeveci.

284 Frantziou CYELS 2020, 208 (215); Wischmeyer, Rechtsgutachten, 2023, S. 11 (Stand 12.2.2024).

285 Geschützt ist der gesamte Prozess von der Entgegennahme einer Information bis zur Aufbereitung oder Speicherung derselben; s. SchlA der GA *Trstenjak* (SchlA v. 24.11.2010 – C-316/09, ECLI:EU:C:2010:712, Rn. 81 ff. = BeckRS 2010, 91345 – MSD Sharp & Dohme).

286 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (159 f.).

287 EuGH Urt. v. 8.9.2016 – C-160/15, ECLI:EU:C:2016:644, Rn. 45 = BeckRS 2016, 82181 – GS Media.

288 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (159 f.).

289 EuGH Urt. v. 6.3.2001 – C-274/99, ECLI:EU:C:2001:127, Rn. 62 ff. = BeckRS 2001, 31031657 – Connolly/Kommission.

290 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (160).

291 Art. 54 GRC sieht vor, dass „*keine Bestimmung dieser Charta so auszulegen [sei] als begründe sie das Recht, eine Tätigkeit auszuüben oder eine Handlung vorzunehmen, die in der Charta anerkannten Rechten und Freiheit abzuschaffen oder sie stärker einzuschränken, als dies in der Charta vorgesehen ist*"; s. auch Struth Hassrede S. 109 ff.

zu verstehen, die sich gegen die Rechte und Freiheiten Anderer richten, indem die Würde bspw. aufgrund der ethnischen Herkunft, Religion oder politischen Überzeugung abgesprochen wird oder die Lebens-, Existenz- und Aufenthaltsrechte anderer unter Missachtung der Gleichheit abgestritten werden.[292]

Während der EuGH die Horizontalwirkung des Art. 21 GRC bereits ausdrücklich anerkannt hat, besteht eine solch klare Rechtsprechung zu Art. 11 GRC nicht.[293] Dennoch wird in der Literatur bejaht, dass Art. 11 GRC im Rahmen einer grundrechtskonformen Auslegung des zwischen Privaten anzuwendenden Rechts herangezogen werden kann,[294] dies insbesondere aufgrund des besonderen Schutzbedürfnisses gegenüber wirtschaftlichen bzw. sozialen Mächten und intermediären Gewalten.[295] Darüber hinaus entfaltet Art. 11 GRC iSd zuvor erarbeiteten Kriterien der unmittelbaren Geltung und des zwingend eigenständigen Charakters auch „*aus sich heraus Wirkung*".[296] Demnach bedarf es keiner Konkretisierung durch den Gesetzgeber, weil Art. 11 GRC „*schon seinem Wesen nach*"[297] mit korrespondierenden Pflichten der Betroffenen einhergeht.[298]

Schließlich ist darauf zu verweisen, dass der EuGH in seiner Rechtsprechung die Meinungsfreiheit bereits vor dem Inkrafttreten der GRC im Jahre 2009 als Grundrecht anerkannte.[299] Bei der Auslegung derselben kann zudem grundsätzlich auch auf die Rechtsprechung des EGMR zurückgegriffen werden, weil die Europäische Menschenrechtskommission (EMRK[300])

292 Struth Hassrede S. 5 f. mwN.

293 Wischmeyer, Rechtsgutachten, 2023, S. 24 (Stand 12.2.2024).

294 Denga EuR 2021, 569 (595); F. Hofmann/Raue/Raue DSA Art. 14 Rn. 78 ff.; Wischmeyer, Rechtsgutachten, 2023, S. 24 (Stand 12.2.2024).

295 Vgl. BVerfGE 148, 267 = NJW 2018, 1667 Rn. 33; BGHZ 230, 347 = NJW 2021, 3179 Rn. 55; Knebel Drittwirkung S. 102.

296 Zur diesbezüglichen Rsp. des EuGH zu Art. 21 und Art. 47 GRC s. EuGH Urt. v. 17.4.2018 – C-414/16, ECLI:EU:C:2018:257, Rn. 78. = BeckRS 2018, 5386 – Egenberger.

297 Der EuGH judizierte zu Art. 31 Abs. 2 GRC, dass das Recht eines Arbeitnehmers auf bezahlten Jahresurlaub schon seinem Wesen nach mit einer entsprechenden Pflicht des Arbeitsgebers einhergeht; vgl. EuGH Urt. v. 6.11.2018 – verb. Rs. C-569/16 u. C-570/16, ECLI:EU:C:2018:871, Rn. 90 = BeckRS 2018, 27416 – Bauer.

298 Wischmeyer, Rechtsgutachten, 2023, S. 24 (Stand 12.2.2024).

299 Wischmeyer, Rechtsgutachten, 2023, S. 24 f. (Stand 12.2.2024).

300 Konvention zum Schutze der Menschenrechte und Grundfreiheiten, öBGBl. 1958/210 idF öBGBl. III 2023/171.

der GRC in weiten Teilen als Leitbild diente.[301] Dies bestätigt auch Art. 6 Abs. 3 EUV iVm Art. 52 Abs. 3 S 1 GRC, der den Grundrechten der GRC die „*gleiche Bedeutung und Tragweite*" beimisst wie ihren Pendants[302] in der EMRK.[303] Im Unterschied zum EuGH kann der EGMR jedoch aus prozessualen Gründen nur Menschenrechtsverletzungen der Staaten sanktionieren.[304] Dies hat zur Folge, dass die Rechtsprechung zur Horizontalwirkung auf die positiv-rechtlichen Staatsschutzverpflichtungen (sog. „*positive obligations*") beschränkt ist.[305] Aus dieser Rechtsprechung lässt sich jedoch ableiten, dass der EGMR die Horizontalwirkung der Meinungsfreiheit anerkannt hat, indem er den über privatrechtliche Streitigkeiten entscheidenden Gerichten ausdifferenzierte Kriterien für die Abwägung[306] zwischen dem Recht auf Achtung des Privat- und Familienlebens gem. Art. 8 EMRK und der Freiheit der Meinungsäußerung gem. Art. 10 EMRK vorgibt.[307]

Der Rückgriff auf die EMRK umfasst dabei „*nicht nur […] den Wortlaut der EMRK, sondern u. a. auch […] die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte*".[308] In Anlehnung an diese Rechtsprechung wird Art. 11 Abs. 1 GRC iVm Art 10 EMRK als eine wesentliche Grundlage einer demokratischen Gesellschaft (auch als „*European First Amendment*" bezeichnet) charakterisiert.[309] Daraus kann der Schluss gezogen werden, dass, wenn die Horizontalwirkung des Art. 31 Abs. 2 GRC mit der Norm

301 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (155 ff.); Stern/Sachs Grundrechte-Charta/Krämer Art. 52 Rn. 65.

302 Die Entsprechung eines Art. ist dabei auf tatsächlicher und nicht ausschließlich auf rechtlicher Ebene zu sehen; s. hierzu Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (155).

303 EuGH Urt. v. 4.5.2016 – C-547/14, ECLI:EU:C:2016:325, Rn. 147 = BeckRS 2016, 80849 – Philip Morris Brands u.a.; 14.2.2019 – C-345/17, ECLI:EU:C:2019:122, Rn. 65 = BeckRS 2019, 1399 – Buivids.

304 Wischmeyer, Rechtsgutachten, 2023, S. 25 (Stand 12.2.2024).

305 Calliess/Ruffert/Kingreen GRC Art. 51 Rn. 32 ff.

306 Auch nach der Rspr. des EuGH ist zwischen widerstreitenden Grundrechten ein angemessener Ausgleich herzustellen; s. EuGH Urt. v. 12.6.2003 – C-112/00, ECLI:EU:C:2003:333, Rn. 81 = BeckRS 2004, 74143 – Schmidberger; Urt. v. 13.5.2014 – C-131/12, ECLI:EU:C:2014:317, Rn. 81 = BeckRS 2014, 80862 – Google Spain und Google; vgl. auch Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (173 f.).

307 Wischmeyer, Rechtsgutachten, 2023, S. 25 (Stand 12.2.2024); Quintais/Appelman/Fathaigh GLJ 2023, 881 (898).

308 EuGH Urt. v. 30.6.2016 – C-205/15, ECLI:EU:C:2016:499, Rn. 41 = BeckRS 2016, 81416 – Toma.

309 Frosio/Geiger Eur. Law J. 2023, 31 (46 ff.) mwN.

als tragendem Grundsatz des Sozialrechts begründet wurde, dies auch für Art. 11 GRC im Hinblick auf die demokratische Gesellschaft gelten sollte.[310]

3. Medienfreiheit gemäß Art. 11 Abs. 2 GRC

Von der Medienfreiheit in Art. 11 Abs. 2 GRC werden zusätzlich zu klassischen Medien, wie der Presse oder dem Rundfunk, auch die modernen Formen der Massenkommunikation erfasst,[311] sofern die journalistisch tätigen Nutzer ihre Beiträge an die Allgemeinheit richten.[312]

Dies bedeutet, dass der Beitrag öffentlich zugänglich sein muss, sodass er grundsätzlich von einem unbestimmten Personenkreis[313] eingesehen werden kann[314] und dass die mit klassischen Medien vergleichbare medienspezifische Vermittlungsleistung und nicht der einzelne Beitrag im Vordergrund steht.[315] So knüpft die Sperrung eines Nutzerkontos zwar auch an eine inhaltliche Dimension an, entzieht aber dem Nutzer darüber hinaus die von der Medienfreiheit geschützte – und für den Nutzer der Publikation erforderliche – Infrastruktur.[316] Dennoch können sich nur jene Nutzer auf die Medienfreiheit berufen, welche die Plattform für journalistische Zwecke,[317] wie bspw. Blogging, verwenden.[318]

310 Wischmeyer, Rechtsgutachten, 2023, S. 25 (Stand 12.2.2024).
311 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (161 f.); Stern/Sachs, Europäische Grundrechtecharta/von Coelln Art. 11 Rn. 38.
312 EuGH Urt. v. 16.12.2008 – C-73/07, ECLI:EU:C:2008:727, Rn. 61 = BeckRS 2008, 71330 – Satakunnan Markkinapörssi und Satamedia; Urt. v. 14.2.2019 – C-345/17, ECLI:EU:C:2019:122, Rn. 53 = BeckRS 2019, 1399 – Buivids.
313 Dies bedeutet, dass der Beitrag zumindest all jenen Nutzern offenstehen muss, die ebenfalls registriert sind.
314 Giere Einordnung S. 82.
315 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (162).
316 Skobel Regulierung S. 166 ff.; Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (161 f.).
317 EuGH Urt. v. 14.2.2019 – C-345/17, ECLI:EU:C:2019:122, Rn. 52 = BeckRS 2019, 1399 – Buivids.
318 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (162).

III. Folgen der Horizontalwirkung für die Beschränkung der Rechte von Nutzern

Die Grundrechtsbindung der Diensteanbieter an die einschlägigen – oben dargestellten – Unionsgrundrechte folgt nicht aus der Bestimmung des Art. 14 Abs. 4 DSA, sondern aus den Unionsgrundrechten selbst. Diese Horizontalwirkung hat zur Folge, dass nationale Gerichte im Rahmen der Grundrechtsabwägung die Auslegung der einschlägigen Normen „*unter Achtung ihres Wortlauts und unter Wahrung ihrer praktischen Wirksamkeit mit den durch die Charta gewährleisteten Grundrechten*" vornehmen müssen.[319] Da im Falle des DSA aufgrund seiner Rechtsnatur als VO keine unzureichende staatliche Umsetzung in Frage kommt, muss die Horizontalwirkung nicht herangezogen werden, um das Staatshaftungsrecht zu umgehen.[320]

Das nationale Gericht hat im Rahmen der Abwägung der Unionsgrundrechte den Wertungen des Unionsgesetzgebers zu folgen, wobei es „*den durch den Unionsgesetzgeber [… im Sekundärrecht] geschaffenen Ausgleich zwischen diesen Interessen zu berücksichtigen*" hat.[321] Im Rahmen der grundrechtlichen Abwägung ist neben der Generalklausel des Art. 14 Abs. 4 DSA, die insbesondere zur Auslegung der konkreten Pflichten zu berücksichtigen ist, auch die Zielbestimmung des Rechtsakts in Art. 1 Abs. 1 DSA heranzuziehen.[322] In der Literatur wird diesbezüglich angezweifelt, ob der Unionsgesetzgeber mit dem Erlass dieser Generalklausel seiner Verpflichtung zum Schutz der Unionsgrundrechte nachgekommen ist oder ob er verpflichtet gewesen wäre, potenziell grundrechtliche Kollisionslagen selbst aufzulösen.[323] Dieser Gedanke entstammt dem Verhältnismäßigkeitsgebot, aus welchem der EuGH die Pflicht des Unionsgesetzgebers ableitet, dass eine „*Regelung, die einen Eingriff in Grundrechte enthält, außerdem klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen [muss], so dass die Personen, die in der Ausübung der genannten Rechte eingeschränkt wer-*

319 EuGH Urt. v. 29.7.2019 – C-516/17, ECLI:EU:C:2019:625, Rn. 59 = BeckRS 2019, 15825 – Spiegel Online.
320 Wischmeyer, Rechtsgutachten, 2023, S. 25 (Stand 12.2.2024).
321 EuGH Urt. v. 17.4.2018 – C-414/16, ECLI:EU:C:2018:257, Rn. 81 = BeckRS 2018, 5386 – Egenberger.
322 Wischmeyer, Rechtsgutachten, 2023, S. 26 (Stand 12.2.2024).
323 Ungern-Sternberg Content Regulation/Wendel S. 59 (78 ff.).

den, über ausreichende Garantien verfügen, die ihren wirksamen Schutz vor Missbrauchsrisiken ermöglichen".[324]

Um zu gewährleisten, dass der Eingriff auf das absolut Notwendige beschränkt wird, muss die Regelung weiters angeben, unter welchen Umständen und unter welchen Voraussetzungen die Maßnahme getroffen werden darf.[325] Wird gegen den Verhältnismäßigkeits- bzw. Bestimmtheitsgrundsatz verstoßen, so kann dies zur Unwirksamkeit des Rechtsakts führen.[326] Es ist jedoch zu berücksichtigen, dass jegliche Eingriffe im vorliegenden Kontext weder durch die Union und ihre Organe noch durch die Mitgliedstaaten, sondern durch die Entscheidungen privater Plattformbetreiber vorgenommen werden.[327] Entsprechend der Rechtsprechung des EuGH kann es sich „*sogar als notwendig erweisen, es den Diensteanbietern zu überlassen, die konkreten Maßnahmen festzulegen, die zur Erreichung des angestrebten Ergebnisses zu ergreifen sind*",[328] um zur Verfügung stehende Ressourcen und Möglichkeiten bestmöglich mit den Pflichten und Herausforderungen in Einklang zu bringen.[329]

Zusätzlich zur zuvor erwähnten Zielbestimmung und der Generalklausel sind im Rahmen der Grundrechtsabwägung die Erwgr. 3, 47 und 48 DSA heranzuziehen, denen zufolge große Plattformen die zentrale Infrastruktur gesellschaftlicher Kommunikation darstellen.[330] Auf Grund dessen wirken auf den Nutzer sog. Netzwerk- und Lock-In-Effekte ein, die dazu führen, dass Nutzer die Plattform nicht ohne hohe Transaktionskosten wechseln können und hierdurch sog. „*natürliche Monopole*"[331] entstehen.[332] Dies

---

324 EuGH Urt. v. 26.4.2022 – C-401/19, ECLI:EU:C:2022:297, Rn. 67 = BeckEuRS 2022, 754093 – Polen/Parlament und Rat.

325 Zum Erfordernis der Verhältnismäßigkeit s. auch EuGH Urt. v. 16.7.2020 – C-311/18, ECLI:EU:C:2020:559, Rn. 176 mwN = BeckEuRS 2020, 642528 – Facebook Ireland und Schrems.

326 EuGH Urt. v. 8.4.2014 – verb. Rs. C-293/12 und C-594/12, ECLI:EU:C:2014:238, Rn. 52 ff = BeckRS 2014, 80686 – Digital Rights Ireland und Seitlinger u.a.

327 Wischmeyer, Rechtsgutachten, 2023, S. 27 (Stand 12.2.2024).

328 EuGH Urt. v. 26.4.2022 – C-401/19, ECLI:EU:C:2022:297, Rn. 75 = BeckEuRS 2022, 754093 – Polen/Parlament und Rat.

329 EuGH Urt. v. 27.3.2014, C-314/12, ECLI:EU:C:2014:192, Rn. 52 = BeckRS 2014, 80615 – UPC Telekabel Wien.

330 Wischmeyer, Rechtsgutachten, 2023, S. 26 (Stand 12.2.2024).

331 Wird demnach eine kritische Masse an Nutzern erreicht, setzt sich ein Dienst auf dem Markt durch. Solche Märkte werden als „*Winner-takes-it-all*"-Märkte bezeichnet; vgl. auch Eifert/Metzger/Schweitzer/Wagner CMLR 2021, 987 (990 f.); Gielen/Uphues EuZW 2021, (627) 627 f.

332 Schulz/Dankert Informationsintermediäre S. 50.

ist auch der Grund dafür, dass gerade große Digitalkonzerne, die durch ihre AGB „*Recht*" setzen, in besonders starker Weise in die Verantwortung genommen werden. Dem folgend bringt der DSA, im Besonderen Art. 14 Abs. 4 DSA, zum Ausdruck, dass die im Rahmen der Inhaltemoderation[333] ergehenden Entscheidungen prozedurale, aber auch wie sich im Folgenden zeigen wird, materielle Anforderungen[334] erfüllen müssen.[335]

IV. Alternative eines prozeduralen Ansatzes?

Ein Teil der Lehre vertritt die Ansicht, dass es trotz weitreichender prozeduraler Sicherungsmechanismen gänzlich an inhaltlichen Vorgaben für Provider fehle, weshalb an der Unionsverfassungsmäßigkeit des DSA zu zweifeln sei.[336] *Wendel* rügt, dass der DSA nicht ausdrücklich von den Plattformbetreibern verlange, Beschränkungen nur bei Vorliegen eines sachlichen Grundes vornehmen zu dürfen und zweifelt daher an der Unionsverfassungsmäßigkeit des DSA.[337] Diese Ansicht übersieht jedoch, dass sich aus der Horizontalwirkung der Grundrechte, die über Art. 14 Abs. 4 DSA vermittelt wird, das Verbot ergibt, willkürlich einzelne Meinungsäußerungen zu untersagen und bestimmte Auffassungen zu diskriminieren.[338] Daraus folgt im Umkehrschluss, dass Entscheidungen sehr wohl nur anhand sachlicher Gründe getroffen werden dürfen. Auch im Hinblick auf die Abwägung der Grundrechte – insbesondere des Rechts auf Meinungsfreiheit gem. Art. 11 GRC – wird eine sachlich begründete Entscheidung vorausgesetzt.[339]

Bestätigt wird dies schließlich durch den Wortlaut des Art. 14 Abs. 4 DSA, der bei der „*Anwendung und Durchsetzung*"[340] von Inhaltsbeschränkungen ein sorgfältiges, objektives und verhältnismäßiges

333 Zur Vielfalt der Möglichkeiten einer Inhaltemoderation s. auch Heldt Drittwirkung S. 197 f.
334 Zur möglichen Alternative eines prozeduralen Ansatzes s. unter D.IV.
335 Frosio/Geiger Eur. Law J. 2023, 31 (67 f.).
336 Ungern-Sternberg Content Regulation/Wendel S. 59 (75 ff.).
337 Eifert/Metzger/Schweitzer/Wagner CMLR 2021, 987 (1013); Ungern-Sternberg Content Regulation/Wendel S. 59 (78 ff.).
338 Wischmeyer, Rechtsgutachten, 2023, S. 28 f. (Stand 12.2.2024).
339 Wischmeyer, Rechtsgutachten, 2023, S. 29 (Stand 12.2.2024).
340 Art. 14 Abs. 4 DSA spricht ausschließlich von der Anwendung und Durchsetzung der in Abs. 1 DSA genannten Beschränkungen, jedoch stellt Erwgr. 47 klar, dass damit die Gestaltung derselben den Kriterien der Objektivität, Sorgfältigkeit und

Vorgehen vorschreibt.[341] Eine sorgfältige Anwendung von Beschränkungen liegt nur vor, wenn die Interessen all jener identifiziert werden, die davon positiv wie negativ betroffen sind, und diese bei der Entscheidung umfassend berücksichtigt werden.[342] Das grundlegende Gebot einer objektiven Entscheidung setzt voraus, dass keine subjektiven Entscheidungsspielräume bestehen und in der Folge frei von Willkür[343] und in nicht diskriminierender Weise[344] entschieden wird.[345] Schließlich bedarf es der Verhältnismäßigkeit der Entscheidung, dh, dass Beschränkungen nur vorgenommen werden dürfen, wenn der Vermittlungsdienst hierdurch eine anerkannte Zielsetzung verfolgt, die Beschränkungen zur Erreichung dieses Zieles geeignet und erforderlich sind und nicht außer Verhältnis zu den angestrebten Zielen stehen.[346] Keine Aussage ist damit über das notwendige Gewicht des „*sachlichen Grundes*"[347] getroffen, damit die beschränkende Maßnahme gerechtfertigt ist. Der DSA nimmt hierzu nur insofern Stellung, als er von VLOP und VLOSE besonders triftige Gründe für Moderationsentscheidungen verlangt, insbesondere solche, die auf die „*gesellschaftliche Debatte*"[348] hin geprüft werden müssen.[349]

Die These, der DSA verfolge einen rein prozeduralen Regulierungsansatz, kann daher verworfen werden, weil eine ausschließlich prozedurale Kontrolle ohne den Schutz eines dahinterstehenden materiellen Interesses ohne Wirkung bleiben würde.

Verhältnismäßigkeit genügen muss; s. Ungern-Sternberg Content Regulation/Janal S. 119 (126 f.).

341 F. Hofmann/Raue/Raue DSA Art. 14 Rn. 78 ff.

342 Dabei unterscheidet sich die deutsche Sprachfassung von der französischen und englischen Sprachfassung insofern, als dass das Wort „angemessen" nicht enthalten ist; vgl. F. Hofmann/Raue/Raue DSA Art. 14 Rn. 78 ff. mit Verweis auf Rn. 88. Diese fehlende Vorgabe, die einem Redaktionsfehler zu Grunde liegt, ergibt sich jedoch auch aus der Vorgabe verhältnismäßig vorzugehen.

343 Erwgr. 45, 47; Art. 16 Abs. 6 sowie Art. 20 Abs. 4 DSA.

344 Erwgr. 47; Art. 20 Abs. 4 DSA.

345 F. Hofmann/Raue/Raue DSA Art. 14 Rn. 78 ff.; Wischmeyer, Rechtsgutachten, 2023, S. 29 ff. (Stand 12.2.2024).

346 EuGH Urt. v. 26.4.2022 – C-401/19, ECLI:EU:C:2022:297, Rn. 63 ff. = BeckEuRS 2022, 754093 – Polen/Parlament und Rat; Urt. v. 17.12.2020 – C-336/19, ECLI:EU:C:2020:1031, Rn. 64 = BeckRS 2020, 35714 – Centraal Israëlitisch Consistorie van België u.a.; s. auch F. Hofmann/Raue/Raue DSA Art. 14 Rn. 84 f.; Wischmeyer, Rechtsgutachten, 2023, S. 30 (Stand 12.2.2024).

347 Zu den materiellen Anforderungen an Moderationsentscheidungen s. Wischmeyer/Meißner NJW 2023, 2673 (2678).

348 Art. 34 Abs. 1 UAbs. 2 lit. c DSA.

349 Wischmeyer, Rechtsgutachten, 2023, S. 30 f. (Stand 12.2.2024).

Eine weitere Alternative ist jener verfahrensrechtliche Ansatz, wie ihn jüngst der deutsche BGH entwickelt hat.[350] Demnach stünde es dem sozialen Netzwerk frei, bestimmte Inhalte in ihren AGB zu verbieten, allerdings dürfe eine Sperrung nicht willkürlich, sondern ausschließlich beruhend auf einem sachlichen Grund und einem objektiv überprüfbaren Tatbestand erfolgen.[351] Darüber hinaus würden verfahrensrechtliche Mindestanforderungen von den Diensteanbietern erfordern, dass Nutzer umgehend über Maßnahmen informiert werden, eine Begründung erhalten und ihnen schließlich eine Möglichkeit zur Gegenäußerung mit anschließend neuer Entscheidung gewährt würde.[352] Der BGH fordert weiters zwingend eine Anhörung bei Maßnahmen mit sanktionierendem Charakter.[353]

Durch diese Kombination aus formellen Anforderungen einerseits sowie materiell gelagertem Willkürverbot andererseits, wird zwar die grundlegende Absicherung der Meinungsfreiheit der Nutzer gewährleistet, doch bliebe es den Diensteanbietern weitestgehend unbenommen, jede Meinung zu unterdrücken, für welche sich ein sachlicher Grund – im Falle der Diensteanbieter insbesondere ein wirtschaftliches Interesse – finden lässt.[354] Dem ist entgegenzuhalten, dass Diensteanbieter das Forum des Meinungsaustausches und der Meinungsbildung bereitstellen.[355] Indem sie dieses für die Allgemeinheit öffnen, sind sie auch dazu verpflichtet, die Kommunikationsfreiheit zu respektieren und zu garantieren, dh dass sie in einem gewissen Ausmaß auch die damit einhergehenden Kontroversen und Konflikte hinnehmen müssen.[356] Darüber hinaus regelt der DSA die Verfahrens- und Formvorschriften[357] bereits umfassend und entsprechend der praktischen

350 Bering Grundrechtsbindung S. 16 ff.; Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (176); Hellgardt JZ 2018, 901 (901 ff.).

351 BGHZ 230, 347 = NJW 2021, 3179 Rn. 78 ff.; BGH ZUM-RD 2021, 612 Rn. 90 ff.; s. hierzu Kahl/Horn K&R, 703 (705 f.).

352 BGH 29.7.2021 – III ZR 179/20, ZUM 2021, 953 Rn. 83 ff.; BGH 29.7.2021 – III ZR 192/20, ZUM-RD 2021, 612 Rn. 95 ff.; Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (176).

353 BGH NJW 2021, 3179 Rn. 85; Wischmeyer, Rechtsgutachten, 2023, S. 30 (Stand 12.2.2024).

354 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (176).

355 Wissenschaftliche Studien belegen die steigende Relevanz der Informationsintermediäre für Nutzer als Quellen der Meinungsbildung; vgl. Schulz/Dankert Informationsintermediäre S. 8; Heldt Drittwirkung S. 153 ff.

356 Raue JZ 2018, 961 (967); BVerfGE 128, 226 (253 ff.) = NJW 2011, 1201.

357 Insbesondere Melde- und Beschwerdemechanismen iSd Art. 16 ff. DSA.

Bedürfnisse im Hinblick auf eine Verfahrensbeschleunigung,[358] sodass der DSA mit der zusätzlichen Verpflichtung des Art. 14 Abs. 4 DSA von einem stärker materiell angebundenen Ansatz auszugehen scheint.[359]

V. Grenzen der Normdurchsetzung

Auf Basis der vorangegangenen Überlegungen stellt sich abschließend die Frage, welche Maßnahmen zur Durchsetzung der AGB im Einzelfall zulässig sind. Art. 14 Abs. 4 DSA enthält diesbezüglich keine weiteren Vorgaben für Diensteanbieter, welche Tragweite der Pflicht zur Berücksichtigung der Grundrechte zukommt, sodass die Ausgestaltung der Nutzungsbedingungen davon abhängt, wie die Grundrechtspositionen zueinander im Verhältnis stehen.[360] Aufgrund des in Art. 14 Abs. 4 DSA verankerten Kriteriums der Verhältnismäßigkeit darf die Maßnahme nicht überschreiten, was zur Erreichung des verfolgten Ziels geeignet sowie erforderlich ist und es dürfen die hierdurch „*verursachten Nachteile nicht außer Verhältnis zu den angestrebten Zielen stehen*".[361]

Die geringste Form des Eingriffs ist das sog. „*Labeling*".[362] Hierbei bleibt der Beitrag bzw. die Äußerung als solche unberührt, wird jedoch inhaltlich dadurch abgewertet, dass der Beitrag mit einer entsprechenden Kennzeichnung oder inhaltlichen Einordnung versehen wird.[363] Dieser Ansatz weist den Vorteil auf, dass die Offenlegung es dem Leser ermöglicht, eine differenzierte Entscheidung auf Basis glaubwürdiger Informationen zu treffen.[364] In der Praxis wird jedoch bemängelt, dass das „*Labeling*" an seine

358 F. Hofmann/Raue/Raue DSA Art. 14 Rn. 86 f. mwN.

359 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (176 f.).

360 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (177).

361 EuGH Urt. v. 8.7.2010 – C-343/09, EU:C:2010:419, Rn 45 = BeckRS 2010, 90872 – Afton Chemical; Urt. v. 23.10.2012 – verb. Rs. C-581/10 u. C-629/10, ECLI:EU:C:2012:657, Rn. 71 = BeckRS 2012, 82188 – Nelson u.a.; Urt. v. 15.2.2016 – C-601/15, ECLI:EU:C:2016:84, Rn. 54 = BeckRS 2016, 80404 – PPU.

362 Ungern-Sternberg Content Regulation/G'Sell S. 85 (99).

363 Möller/Hameleers/Ferreau Desinformation und Misinformation/Ferreau S. 44 (52 ff.); Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (177). Zur Schwierigkeit der Abgrenzung von „*Fake News*" bzw. Desinformation s. Grabenwarter/Holoubek/Leitl-Staudinger Kommunikationsplattformen/Gärner S. 89 (90 ff.).

364 Auch „*marketplace of ideas*" genannt; vgl. Goldman MTLR 2021, 1 (55 f.).

Grenzen stößt und sich sogar kontraproduktiv auswirken kann, insbesondere wenn Angaben die Nutzer in die Irre führen.[365] Deutlich eingriffsintensiver ist hingegen die Reduktion der Sichtbarkeit, da diese zu einer objektiven Beeinträchtigung der Meinungsfreiheit des betroffenen Nutzers und der Informationsfreiheit Dritter führt.[366] Der schwerwiegendste Eingriff in Bezug auf einen einzelnen Beitrag stellt die Löschung desselben dar, weil in diesem Fall die Meinungsäußerung bezogen auf diesen Beitrag zur Gänze unterdrückt wird und von Dritten nicht mehr rezipiert werden kann.[367] Die Löschung ist bspw. bei einem Beitrag denkbar, dessen Inhalt diskriminierend, rassistisch oder beleidigend ist.[368]

Greift die Maßnahme des Plattformanbieters nicht nur in den einzelnen Beitrag ein, sondern sperrt das Konto des Nutzers temporär oder sogar unbefristet, stellt dies einen besonders schweren Eingriff dar, denn hierdurch wird die Meinungs- und Informationsfreiheit vorübergehend bzw. dauerhaft zur Gänze eingeschränkt.[369] Diese Form der Sanktion darf daher nur im Falle wiederholter oder besonders schwerwiegender Verstöße gegen die Nutzungsbedingungen bzw. AGB als *ultima ratio* eingesetzt werden.[370]

Problematisch kann dabei auch der vermehrte Einsatz von Systemen sein, die Künstliche Intelligenz (KI) zur automatisierten Moderation nutzen,[371] weil die eingesetzten Filtersysteme den Kontext einer Äußerung nicht erfassen und dadurch die Gefahr des „*Overblocking*"[372] entsteht.[373] Solche falsch-positiven Ergebnisse führen schließlich dazu, dass auch zulässige Inhalte entfernt werden[374] und damit die Kommunikationsfreiheit

365 Marwick Geo L. Tech. Rev. 2018, 474 (475 ff.).
366 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (177).
367 Goldman MTLR 2021, 1 (23 ff.); Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (177).
368 Skobel Regulierung S. 365 f.
369 Pille Meinungsmacht S. 314 ff.
370 Friehe NJW 2020, 1697 (1700); Holznagel CR 2018, 369 (376).
371 Zimmer KI Regulierung/Kühling S. 89 (94 ff.).
372 Das Phänomen des „*Overblocking*" beschreibt eine Content-Moderation der Plattformanbieter, bei welcher bes. viel oder bereits bei bloßem Verdacht auf rechtswidrige Inhalte blockiert wird; s. Denga EuR 2021, 569 (583).
373 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (178).
374 SWD(2020) 348 final, Rn. 80; Keller GRUR-Int 2020, 616 (622). Der Einsatz von KI kann weiters durch Voreingenommenheit des verwendeten Algorithmus zu ungerechten oder diskriminierenden Ergebnissen führen (sog. „*Algorithmische Diskriminierung*"), s. hierzu Klamert Jahrbuch/Rauchegger/Jaud S. 69 (73).

der Nutzer zu Unrecht beschränkt wird.[375] Aus Sicht der Plattformanbieter stellt der Einsatz KI-basierter Systeme eine zeit- und kostensparsame Methode zur Überwachung und Durchsetzung der Einhaltung der AGB dar, jedoch darf die hieraus entstehende Fehlerquote zu Lasten der Nutzer die Vorteile nicht überwiegen.[376] Daher sieht Art. 20 Abs. 6 DSA vor, dass „*Entscheidungen unter der Aufsicht angemessen qualifizierten Personals und nicht allein mit automatisierten Mitteln getroffen werden*" dürfen.[377]

Um die Risiken, die von den algorithmischen Systemen ausgehen,[378] besser einschätzen zu können, sind VLOP und VLOSE iSd Art. 33 DSA zunächst verpflichtet, jährlich die systemischen Risiken gem. Art. 34 Abs. 1 DSA zu evaluieren.[379] Insbesondere sind dabei die systemischen Risiken in Bezug auf „*etwaige tatsächliche oder vorhersehbare nachteilige Auswirkungen auf die Ausübung der Grundrechte*" zu bewerten.[380] Anhand der ermittelten besonderen systemischen Risiken haben VLOP und VLOSE angemessene, verhältnismäßige und wirksame Risikominderungsmaßnahmen, bspw. die Anpassung der Moderationsverfahren und der algorithmischen Systeme, zu treffen.[381]

Angesichts der Einschränkung dieser Regelung auf VLOP und VLOSE ergibt sich eine Regelungslücke für jene Plattformen, die die Schwelle zur sehr großen Plattform mit durchschnittlich 45 Mio. aktiven Nutzern pro Monat nicht überschreiten.[382] Da es diesen oftmals an entsprechenden Ressourcen zum Einsatz menschlicher Arbeitskraft fehlt und Uploadfilter nur unter der Voraussetzung verwendet werden dürfen, dass sie hinreichend

375 Denga EuR 2021, 569 (583) mwN; Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (178).

376 Finck AI S. 6; Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (178).

377 Art. 20 Abs. 6 DSA; vgl. hierzu auch *Finck*, die bemängelt, dass die KI zwar „*good at spotting nudity or sexual activity*" sei, aber im ersten Quartal des Geschäftsjahrs 2018 nur 38 % der insges. 2,5 Mio. gelöschten Beiträge erkannt habe, s. Finck AI S. 6 mit Verweis auf Meta, Facebook Publishes Enforcement Numbers for the First Time, abrufbar unter https://newsroom.fb.com/news/2018/05/enforcement-numbers/ (Stand 15.12.2023).

378 Ukrow Vorschläge S. 34 ff.

379 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (178).

380 Art. 34 Abs. 1 UAbs. 2 lit. b DSA.

381 Art. 35 Abs. 1 lit. c und d DSA; Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (178).

382 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (179).

zwischen zulässigen und unzulässigen Inhalten unterscheiden können,[383] erscheint ein grundrechtliches Korrektiv iSd Art. 14 Abs. 4 DSA notwendig.[384]

VI. Zwischenfazit

Die Grundrechtsbindung der Diensteanbieter folgt – wie oben dargestellt – nicht unmittelbar aus der Bestimmung des Art. 14 Abs. 4 DSA, sondern aus der Horizontalwirkung der einschlägigen Grundrechte.[385] Art. 14 Abs. 4 DSA stellt dabei eine sekundärrechtliche Normierung der in der herrschenden Lehre bereits anerkannten mittelbaren Drittwirkung von Grundrechten dar.[386] Dies hat zur Folge, dass etwaige Sanktionen gegen Nutzer eines sachlichen Grundes bedürfen und mit den grundrechtlichen Belangen der Diensteanbieter abzuwägen sind.[387] Im Rahmen dieser Abwägung ist auch der Grundsatz der Verhältnismäßigkeit zu berücksichtigen, der von den Diensteanbietern fordert, das gelindeste Mittel zur Durchsetzung der Nutzungsbedingungen anzuwenden, das geeignet und erforderlich ist, den gewünschten Zweck zu erreichen.[388] Die auf prozeduralen und materiellen Voraussetzungen beruhende Entscheidung darf dabei nur als *ultima ratio* die Sperre des Nutzerkontos zur Folge haben.[389]

E. Conclusio und Ausblick

Meinungsbildung und Meinungsvielfalt sind in einem Zeitalter, in welchem Online-Medien die klassischen Medien wie Presse und Rundfunk überholt haben, geprägt durch Gatekeeper von Informationen.[390] Dabei hängt der

383 EuGH Urt. v. 26.4.2022 – C-401/19, ECLI:EU:C:2022:297, Rn. 86 f. = BeckEuRS 2022, 754093 – Polen/Parlament und Rat; 24.11.2011 – C-70/10, ECLI:EU:C:2011:771, Rn. 52 = BeckRS 2011, 81685 – Scarlet Extended.
384 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (179).
385 Wischmeyer, Rechtsgutachten, 2023, S. 31 (Stand 12.2.2024).
386 Kraul HdB digitale Dienste/Maamar Sorgfaltspflichten Rn. 46 f.
387 Wischmeyer, Rechtsgutachten, 2023, S. 31 f. (Stand 12.2.2024).
388 EuGH Urt. v. 16.7.2020 – C-311/18, ECLI:EU:C:2020:559, Rn. 174 ff. = BeckEuRS 2020, 642528 – Facebook Ireland und Schrems; Urt. v. 26.4.2022 – C-401/19, ECLI:EU:C:2022:297, Rn. 67 = BeckEuRS 2022, 754093 – Polen/Parlament und Rat.
389 Friehe NJW 2020, 1697 (1700); Holznagel CR 2018, 369 (376).
390 Engelmann Gatekeeping S. 11 ff.; Paal/Hennemann ZRP 2017, 76 (79).

Prozess der Meinungsbildung stark von der Auffindbarkeit meinungsbildender Inhalte sowie der Personalisierung von Angeboten ab, welche aufgrund der Plattformökonomie bislang größtenteils ungeregelt den Diensteanbietern oblag.[391]

Mit der Bestimmung des Art. 14 Abs. 4 DSA im Speziellen zeichnet sich eine bedeutsame Rechtsentwicklung ab, die zu einer erheblichen Verbesserung der Rechtspositionen der strukturell unterlegenen Netzwerknutzer führt.[392] Angesichts der potenziell weitreichenden Folgen für sowohl Diensteanbieter als auch Netzwerknutzer, ist die Formulierung aber vage ausgestaltet und lässt Raum für Diskussion.[393] Die vorangehenden Ausführungen haben verdeutlicht, dass sich die Horizontalwirkung aus den einschlägigen Unionsgrundrechten selbst ergibt.[394] Art. 14 Abs. 4 DSA kann dabei als einfachgesetzliche Normierung der mittelbaren Drittwirkung angesehen werden.[395] Die unmittelbare Drittwirkung von Grundrechten ist bisher nur in Einzelfällen, wie bspw. bei Art. 21 GRC und Art. 31 Abs. 2 GRC, ausdrücklich anerkannt. Ob eine Übertragbarkeit dieser Rechtsprechung auf andere Unionsgrundrechte möglich ist, ist noch nicht abschließend geklärt. Doch lässt sich aus der bisherigen Rechtsprechung des EuGH schließen, dass jedenfalls die Kriterien der unmittelbaren Geltung und des zwingend eigenständigen Charakters vorliegen müssen.[396]

In der Praxis haben für jene Diensteanbieter, die unter das Regulierungsregime des DSA fallen, die – teilweise ab 16.11.2022, jedenfalls ab 17.2.2024 – geltenden Verpflichtungen zur Folge, dass die bestehende Haftungsprivilegierung samt „*notice and take down-Verfahren*" erhalten bleibt, die Handhabung rechtswidriger Inhalte jedoch schneller, effizienter und unter Abwägung der Grundrechte zu erfolgen hat. In Fortführung der Rechtsprechung des EuGH in der Rs. *Glawischnig-Piesczek*[397] zur E-Commerce-RL sind Diensteanbieter verpflichtet, eine Maßnahme zu treffen, deren angestrebte Ziele nicht außer Verhältnis zu den verursachten Nachteilen

391 Paal/Hennemann ZRP 2017, 76 (79); Schulz/Dankert Informationsintermediäre S. 27 ff.
392 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (179).
393 Appelman/Quintais/Fahy, VerfBlog, 2021 (Stand 12.2.2024).
394 Wischmeyer, Rechtsgutachten, 2023, S. 31 (Stand 12.2.2024).
395 Kraul HdB digitale Dienste/Maamar Sorgfaltspflichten Rn. 46 f.
396 Frantziou CYELS 2020, 208 (217 f.); Prechal RDCE 2020, 407 (417 ff.); Kainer NZA 2018, 894 (898 f.); Wischmeyer, Rechtsgutachten, 2023, S. 19 (Stand 12.2.2024).
397 EuGH Urt. v. 3.10.2019 – C-18/18, ECLI:EU:C:2019:821 Rn. 53 = BeckRS 2019, 23113 – Glawischnig- Piesczek.

steht. Dies kann dazu führen, dass Plattformbetreiber verpflichtet sind, bei Kenntniserlangung über einen rechtswidrigen Inhalt wort- und sinngleiche Beiträge weltweit zu löschen.[398] Eine solche Entscheidung darf jedoch nur unter Abwägung der Grundrechte aller Betroffenen, einschließlich des Plattformbetreibers, erfolgen und muss einem internen, leicht zugänglichen Beschwerdemanagement unterliegen, das seine nicht automatisierte Entscheidung begründen muss. Erreicht der Verstoß keine solche Schwere, die eine Löschung rechtfertigen würde, kann es hingegen verhältnismäßig sein, den Nutzer zunächst zu warnen.[399] Ausschließlich *ultima ratio* darf der Diensteanbieter das Nutzerkonto sperren bzw. löschen.[400]

Literaturverzeichnis

Achleitner, Der Digital Services Act als risikobasierte Regulierung. Zu den Auswirkungen des risikobasierten Ansatzes des DAS auf Desinformation und Grundrechtsschutz, MR-Int 2022, 114.

Achleitner, Der künftige Digital Services Act der EU: Neue Pflichten und Verantwortlichkeiten für Anbieter digitaler Dienste. Regulierung von Online-Inhalten im Spannungsfeld zwischen Meinungsfreiheit und effizienter Rechtsdurchsetzung, ZTR 2021, 1.

Achleitner, Illegale Inhalte und Internetgiganten: Ein neues E-Commerce-Recht für die EU, ecolex 2021, 512.

Adelberg, Hassrede in sozialen Netzwerken. Reichweite und Grenzen der Pflichten und Rechte der Netzwerkbetreiber, K&R 2022, 19.

Ammann/Bottega/Bukovac/Lehner/Meier/Piskóty/Rausch/Rehmann/Schneider/Weder/Wilhelm Verantwortung und Recht/Karg, 1. Aufl. 2022, Marktmacht S. 67.

Appelman/Quintais/Fahy, Using Terms and Conditions to apply Fundamental Rights to Content Moderation, VerfBlog 1.9.2021, abrufbar unter https://verfassungsblog.de/power-dsa-dma-06/ (Stand 12.2.2024).

Badó/Belling, Rechtsentwicklungen aus europäischer Perspektive im 21. Jahrhundert/Belling/Herold/Kneis, 1. Aufl. 2014, Wirkung S. 53.

Bajlicz/Bohnert/Ganglbauer/Gärner/Petermair/Ponader/Tilzer/Werderitsch, Recht im Umbruch – Umbruch im Recht. Tagung ÖffR XI/Achleitner, 1. Aufl. 2022, Revision S. 3.

398 Eine solche Verpflichtung folgte jüngst auch in der dt. Rechtsprechung; s. OLG Frankfurt a.M. Urt. v. 25.1.2024, Az. 16 U 65/22.

399 Wischmeyer/Meißner NJW 2023, 2673 (2678).

400 Schrör/Keiner/Müller/Schumacher Entscheidungsträger/Röhling/Weil S. 151 (177).

Bayer/Holznagel/Korpisaari/Woods, Perspectives on Platform Regulation. Concepts and Models of Social Media Governance Across the Globe/ Koivukari/Korpisaari, 1. Aufl. 2021 S. 473.

Berberich/Seip, Der Entwurf des Digital Services Act, GRUR-Prax 2021, 4.

Bering, Grundrechtsbindung sozialer Netzwerke. Wie soziale Netzwerke die Grundrechte ihrer Nutzer*innen schützen müssen, 1. Aufl. 2022.

Bohlen, Der zivilrechtliche Auskunftsanspruch bei der Bekämpfung von Hass im Internet, NJW 2020, 1999.

Brauneck, Das Verantwortungsbewusstsein der Plattformbetreiber im Digital Services Act, NVwZ 2024, 377.

Breton, Capitol Hill — the 9/11 moment of social media, 2021, abrufbar unter https://www.politico.eu/article/thierry-breton-social-media-capitol-hill-riot/ (Stand 12.2.2024).

Calliess/Ruffert, EUV/AEUV/Kingreen, 6. Aufl. 2022, GRC Art. 51.

Calliess/Ruffert, EUV/AEUV/Rossi, 6. Aufl. 2022, GRC Art. 21.

Casolari/Gatti, The Application of EU Law Beyond Its Borders/Lonardo, 1. Aufl. 2022, S. 9.

Colombi Ciacchi, The Direct Horizontal Effect of EU Fundamental Rights. ECJ 17 April 2018, Case C-414/16, *Vera Egenberger v Evangelisches Werk für Diakonie und Entwicklung e.V.* and ECJ 11 September 2018, Case C-68/17, *IR v JQ*, EuConst 2019, 294.

Demschik, Provider in der Pflicht – ein Überblick über die allgemeinen Sorgfaltspflichten nach dem Digital Services Act, ecolex 2023, 183.

Denga, Plattformregulierung durch europäische Werte: Zur Bindung von Meinungsplattformen an EU-Grundrechte, EuR 2021, 569.

Di Fabio, Grundrechtsgeltung in digitalen Systemen. Selbstbestimmung und Wettbewerb im Netz, 1. Aufl. 2016.

Eifert/Gostomzyk, Netzwerkrecht/Ladeur, 1. Aufl. 2018, Netzwerkrecht S. 169.

Eifert/Metzger/Schweitzer/Wagner, Taming the giants: The DMA/DSA package, CMLR 2021, 987.

Engelmann, Gatekeeping, 1. Aufl. 2016.

Engert, Digitale Plattformen, AcP 218 (2018), 304.

EPRS, Liability of online platforms, 1. Aufl. 2021.

Europäische Kommission, Code of conduct on countering illegal hate speech online, 2016, abrufbar unter https://commission.europa.eu/document/download/551c44da-baae-4692-9e7d-52d20c04e0e2_en?prefLang=de (Stand 19.2.2024).

Europäische Kommission, Das Digital Services Act Paket, 2022, abrufbar unter https://digital-strategy.ec.europa.eu/de/policies/digital-services-act-package (Stand 12.2.2024).

Europäische Kommission, DSA: Sehr große Online-Plattformen und Suchmaschinen, 2023, abrufbar unter https://digital-strategy.ec.europa.eu/de/policies/dsa-vlops (Stand 12.2.2024).

Europäische Kommission, Kommission benennt zweite sehr große Online-Plattformen im Rahmen des Gesetzes über digitale Dienste, 2023, abrufbar unter https://digital-strategy.ec.europa.eu/de/news/commission-designates-second-set-very-large-online-platforms-under-digital-services-act (Stand 12.2.2024).

Europäische Kommission, Kommission leitet förmliches Verfahren gegen TikTok im Rahmen des Gesetzes über digitale Dienst ein, 2024, abrufbar unter https://ec.europa.eu/commission/presscorner/detail/de/IP_24_926 (Stand 12.2.2024).

Europäische Kommission, Impact assessment of the Digital Services Act, 2020, abrufbar unter https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-services-act (Stand 12.2.2024).

F. Hofmann/Raue, Digital Services Act: DSA. Gesetz über digitale Dienste/Raue, 1. Aufl. 2023, Art. 14.

F. Hofmann/Raue, Digital Services Act: DSA. Gesetz über digitale Dienste/Raue, 1. Aufl. 2023, Art. 54.

F. Hofmann/Raue, Digital Services Act: DSA. Gesetz über digitale Dienste/F. Hofmann/Raue, 1. Aufl. 2023, Einleitung.

Facebook, Facebook-Gemeinschaftsstandards, 2015, abrufbar unter https://transparency.fb.com/de-de/policies/community-standards (Stand 12.2.2024).

Finck, Artificial Intelligence and Online Hate Speech, 1. Aufl. 2019.

Frantziou, The Horizontal Effect of the Charter: Towards an Understanding of Horizontality as a Structural Constitutional Principle, CYELS 2020, 208.

Friehe, Löschen und Sperren in sozialen Netzwerken, NJW 2020, 1697.

Frosio/Geiger, Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime, Eur. Law J. 2023, 31.

Gerdemann/Spindler, Das Gesetz über digitale Dienste (Digital Services Act) (Teil 1), GRUR 2023, 3.

Gerdemann/Spindler, Das Gesetz über digitale Dienste (Digital Services Act) (Teil 2), GRUR 2023, 115.

Gielen/Uphues, Digital Markets Act und Digital Services Act. Regulierung von Markt- und Meinungsmacht durch die Europäische Union, EuZW 2021, 627.

Giere, Grundrechtliche Einordnung sozialer Netzwerke vor dem Hintergrund des Netzwerkdurchsetzungsgesetzes (NetzDG), 1. Aufl. 2021.

Goldman, Content Moderation Remedies, MTLR 2021, 1.

Grabenwarter/Holoubek/Leitl-Staudinger, Regulierung von Kommunikationsplattformen/Oswald, 1. Aufl. 2022, Hate Speech S. 67.

Grabenwarter/Holoubek/Leitl-Staudinger, Regulierung von Kommunikationsplattformen. Aktuelle Fragen der Umsetzung/Gärner, Fake News, 1. Aufl. 2022, S. 89.

Grabenwarter/Holoubek/Leitl-Staudinger, Regulierung von Kommunikationsplattformen. Aktuelle Fragen der Umsetzung/Holoubek, Plattformregulierung, 1. Aufl. 2022, S. 29.

Grabenwarter/Holoubek/Leitl-Staudinger, Regulierung von Kommunikationsplattformen. Aktuelle Fragen der Umsetzung/Kettemann/Rachinger/Sekwenz, Deplatforming, 1. Aufl. 2022, S. 55.

Haratsch/Koenig/Pechstein, Europarecht, 12. Aufl. 2020.

Heckmann, Persönlichkeitsschutz im Internet. Anonymität der IT-Nutzung und permanente Datenverknüpfung als Herausforderungen für Ehrschutz und Profilschutz, NJW 2012, 2631.

Helberger/Pierson/Poell, Governing online platforms: From contested to cooperative responsibility, TIS 2018, 1.

Heldt, Intensivere Drittwirkung. Die mittelbare Drittwirkung der Meinungsfreiheit in Öffentlichkeiten der digitalen Gesellschaft. Eine verfassungsrechtliche, rechtsvergleichende und interdisziplinäre Analyse, 1. Aufl. 2023.

Hellgardt, Wer hat Angst vot der unmittelbaren Drittwirkung? Die Konsequenzen der Stadionverbot-Entscheidung des BVerfG für die deutsche Grundrechtsdogmatik, JZ 2018, 901.

Hermstrüwer/Lüdemann, Der Schutz der Meinungsbildung im digitalen Zeitalter/Lüdemann, 1. Aufl. 2021, Informationsintermediäre S. 1.

V. Hofmann/Dinar/Kettemann/Böke/Gradulewski/Hinrichs, Governance by Geschäft: Recht und Macht der App Stores, 2021, abrufbar unter https://leibniz-hbi.de/de/blog/recht-und-macht-der-app-stores (Stand 12.2.2024).

Holoubek/Lienbacher, GRC-Kommentar/Köchle, 2. Aufl. 2019, Art. 21.

Holznagel, Overblocking durch User Generated Content (UGC) – Plattformen: Ansprüche Der Nutzer Auf Wiederherstellung Oder Schadensersatz? Eine Untersuchung zur zivilrechtlichen Einordnung des Vertrags über die Nutzung von UGC-Plattformen sowie der AGB-rechtlichen Zulässigkeit von „Lösch- und Sperrklauseln", CR 2018, 369.

Horvath/Lebesmuehlbacher/Lehne/Lütte/Murer, Ungleichheit im aktuellen Diskurs. Tagung ÖffRe III/Scholz, Drittwirkung, 1. Aufl. 2013, 17.

Hoven/Forschungsgruppe g/d/p, Hass im Netz. Ergebnisse einer Studie von Prof. Elisa Hoven, Universität Leipzig und der Forschungsgruppe g/d/p, 2022, abrufbar unter https://www.uni-leipzig.de/fileadmin/prins_import/dokumente/dok_20220829123452_ae0b27c451.pdf (Stand 12.2.2024).

Janisch, EuGH: Grundsätzliche Möglichkeit zur Verpflichtung von Facebook zur weltweiten aktiven Suche und Entfernung von Kommentaren, die mit für rechtswidrig erklärten wort- und sinngleich sind, jusIT 2019, 225.

Jarass, Charta der Grundrechte der Europäischen Union. Unter Einbeziehung der sonstigen Grundrechtsregelungen des Primärrechts und der EMRK, 4. Aufl. 2021.

Kahl/Horn, Auslegung von Äußerungen in sozialen Netzwerken und Betreiberpflichten, NJW 2023, 639.

Kahl/Horn, Sperrungen in sozialen Netzwerken: Verfahrensrechtliche Vorgaben des BGH. Zugleich Kommentar zu BGH, Urteile vom 29. 7. 2021 – III ZR 179/20, KuR 2021, 723 ff. (in diesem Heft) und III ZR 192/20, KuRL2021–723–3, K&R 2021, 703.

Kahl/Raschauer/Storr, Grundsatzfragen der europäischen Grundrechtecharta/Stangl, 1. Aufl. 2013, Anwendungsbereich S. 1.

Kainer, Rückkehr der unmittelbar-horizontalen Grundrechtswirkung aus Luxemburg?, NZA 2018, 894.

Kastor/Püschel, Faktenchecker vor dem Hintergrund des Digital Services Act. Eine rechtliche Einordnung, K&R 2023, 20.

Keller, Facebook Filters, Fundamental Rights, and the CJEU's Glawischnig-Piesczek Ruling, GRUR-Int 2020, 616.

Kettemann/Kraml/Rachinger/Rauchegger/Tiedecke, Weltweite Löschpflichten für rechtswidrige Inhalte auf digitalen Plattformen vor dem österreichischen OGH. Der mühsame Weg zur Entfernung von Äußerungsrechtsverstößen in Social Media, CR 2021, 154.

Kettemann/Schulz/Fertmann, Anspruch und Wirklichkeit der Plattformregulierung. Kommissionsentwürfe der Rechtsakte zu digitalen Diensten und Märkten, ZRP 2021, 138.

Klamert, Jahrbuch 22 Europarecht/Rauchegger/Jaud, 1. Aufl. 2022, Grundrechte S. 69.

Knebel, Die Drittwirkung der Grundrechte und -freiheiten gegenüber Privaten, 1. Aufl. 2018.

Kohl, Platform regulation of hate speech – a transatlantic speech compromise? J. Media Law 2022, 25.

Korpisaari, From Delfi to Sanchez – when can an online communication platform be responsible for third-party comments? An analysis of the practice of the ECtHR and some reflections on the Digital Services Act, J. Media Law 2022, 352.

Kraul, HdB Das neue Recht der digitalen Dienste/Bartels, 1. Aufl. 2023, Durchsetzung.

Kraul, HdB Das neue Recht der digitalen Dienste/Kraul, 1. Aufl. 2023, Einführung.

Kraul, HdB Das neue Recht der digitalen Dienste/Maamar, 1. Aufl. 2023, Sorgfaltspflichten.

Kraul, HdB Das neue Recht der digitalen Dienste/Nathanail, 1. Aufl. 2023, Ziele.

Kulick, Horizontalwirkung im Vergleich. Ein Plädoyer für die Geltung der Grundrechte zwischen Privaten, 1. Aufl. 2020.

Kumarasamy, Digital Services Act – Der richtige Weg zur Regulierung von Online Diensten?, 2022, abrufbar unter https://infopoint-europa.de/de/articles/digital-services-act-der-richtige-weg-zur-regulierung-von-online-diensten (Stand 12.2.2024).

Ladeur, Ausschluss von Teilnehmern an Diskussionsforen im Internet – Absicherung von Kommunikationsfreiheit durch „netzwerk gerechtes" *(sic!)* Privatrecht, MMR 2001, 787.

Langvardt, Regulating Online Content Moderation, Geo. L. Tech. Rev. 2018, 1353.

Legner, Der Digital Services Act – Ein neuer Grundstein der Digitalregulierung, ZUM 2024, 99.

Leuschner, Sicherheit als Grundsatz, 1. Aufl. 2018.

Limbach, Das Rechtsverständnis in der Vertragslehre, JuS 1985, 10.

Marwick, Why Do People Share Fake News? A Sociotechnical Model of Media Effects, Geo. L. Tech. Rev. 2018, 474.

Mast/Kettemann/Dreyer/Schulz, DSA/DMA/Mast/Kettemann/Schulz. 1. Aufl. 2024 (i.E.), Art. 14 DSA.

Mendelsohn, Die „normative Macht" der Plattformen – Gegenstand der zukünftigen Digitalregulierung? Erfassung und mögliche Grenzen der regulierenden und verhaltenssteuernden Macht von Unternehmen im Digitalen, MMR 2021, 857.

Metzger, Dienst gegen Daten: Ein synallagmatischer Vertrag, AcP 216 (2016), 817.

Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union/Schwerdtfeger, 5. Aufl. 2019, Art. 51.

Michl, Unionsgrundrechte aus der Hand des Gesetzgebers, 1. Aufl. 2018.

Möller/Hameleers/Ferreau, Typen von Desinformation und Misinformation/Ferreau, 1. Aufl. 2020, Desinformation S. 44.

Müller, Künftige Plattformregulierung und effektive Durchsetzung in Deutschland. Notwendigkeit und Umsetzung des Digital Services Act, MMR 2022, 1007.

Neumann/Nipperdey/Scheuner, Die Grundrechte: HdB der Theorie und Praxis der Grundrechte II/Ipsen, 1. Aufl. 1954, Grundrechte S. 111.

Paal/Hennemann, Meinungsvielfalt im Internet, ZRP 2017, 76.

Palzer, Persönlichkeitsschutz im Internet, AfP 48 (2017), 199.

Peifer, Verpflichtung zur Löschung wort-/sinngleicher Äußerungen ist keine durch Art. 15 E-Commerce-Richtlinie verbotene allgemeine Überwachung, GRUR-Prax 2019, 534.

Pille, Meinungsmacht sozialer Netzwerke, 1. Aufl. 2016.

Podszun, Empfiehlt sich eine stärkere Regulierung von Online-Plattformen und anderen Digitalunternehmen?, NJW-Beil. 2022, 56.

Prechal, Horizontal direct effect of the Charter of Fundamental Rights of the EU, RDCE 2020, 407.

Quintais/Appelman/Fathaigh, Using Terms and Conditions to apply Fundamental Rights to Content Moderation, GLJ 2023, 881.

Raue, Meinungsfreiheit in sozialen Netzwerken, JZ 2018, 961.

Ristic/Frybert, Das neue Mandatsverfahren nach dem Hass-im-Netz-Bekämpfungs-Gesetz, JAP 2020/2021, 239.

Rohrßen, Digitale Distribution in der EU – Digital Single Market: Neue Regeln im E-Commerce ab 2022, ZVertriebsR 2021, 71.

Rössel, Digital Services Act. Innovation und Verbesserungsbedarf des ersten Verordnungsentwurfs, AfP 54 (2021), 93.

Schäufele/Krück, Der Digital Services Act – Revolution für Vermittlungsdienste, GRUR-Prax 2023, 120.

Schiek, Von der mittelbaren Drittwirkung zur unmittelbaren Grundrechtsbindung Privater? – Inhaltsentfernung und Sperren in sozialen Netzwerken, StudZR-WissOn 2021, 61.

Schneiders, Hate Speech auf Online-Plattformen, UFITA 85 (2021), 269.

Schoditsch, Grundrechte und Privatrecht, 1. Aufl. 2019.

Schröder, Der risikobasierte Ansatz in der DS-GVO. Risiko oder Chance für den Datenschutz?, ZD 2019, 503.

Schroeder/Reider, A Step Forward in Fighting Online Antisemitism, 2023, abrufbar unter https://verfassungsblog.de/a-step-forward-in-fighting-online-antisemitism/ (Stand 12.2.2024).

Schrör/Keiner/Müller/Schumacher, Entscheidungsträger im Internet. Private Entscheidungsstrukturen und Plattformregulierung/Röhling/Weil, 1. Aufl. 2022, Grenzen privater Normsetzung: Zur Drittwirkung der Unionsgrundrechte bei Community Standards am Beispiel von Hate Speech S. 151.

Schulz/Dankert, Die Macht der Informationsintermediäre. Erscheinungsformen, Strukturen und Regulierungsoptionen, 1. Aufl. 2016.

Schwartmann, Vor Trump schützen und die Meinungsfreiheit wahren: Regeln für soziale Netzwerke, 2021, abrufbar unter https://web.de/magazine/politik/wahlen/us-wahl/social-media-dilemma-trump-schuetzen-meinungsfreiheit-wahren-35417460 (Stand 12.2.2024).

Schweitzer, Digitale Plattformen als private Gesetzgeber: Ein Perspektivwechsel für die europäische „Plattform-Regulierung", ZEuP 2019, 1.

Sesing-Wagenpfeil, Suchmaschinen im Digital Services Act, CR 2023, 113.

Skobel, Regulierung nutzergenerierter Inhalte auf sozialen Netzwerken, 1. Aufl. 2021.

Specht-Riemenschneider/F. Hofmann, Verantwortung von Online-Plattformen. Ein Plädoyer für funktionszentrierte Verkehrspflichten. Gutachten im Auftrag des vzbv., 2021, abrufbar unter https://www.vzbv.de/sites/default/files/downloads/2021/02/04/specht_hofmann_gutachten_plattformverantwortlichkeitdocx.pdf (Stand 12.2.2024).

Statistik Austria, Österreichischer Zahlenspiegel, 2023, abrufbar unter https://www.statistik.at/fileadmin/shared/IV/Zsp_12_23_barrierefrei.pdf (Stand 12.2.2024).

Steinebach/Bader/Rinsdorf/Krämer/Roßnagel, Desinformation aufdecken und bekämpfen/Bader, 1. Aufl. 2020, Einleitung S. 15.

Steinrötter, RHdB Europäische Plattformregulierung/Achleitner Durchsetzung: Befugnisse von und Zusammenarbeit mit Behörden.

Stern/Sachs, Europäische Grundrechte-Charta: GRC/Krämer, 1. Aufl. 2016, Art. 52 GRC.

Stern/Sachs, Europäische Grundrechte-Charta: GRC/von Coelln, 1. Aufl. 206, Art. 11 GRC.

Stöggl, Der Staat als Adressat des Unionsrechts, ZÖR 2019, 465.

Streinz, EUV/AEUV/Streinz, 3. Aufl. 2018, Art. 21 GRC.

Struth, Hassrede und Freiheit der Meinungsäußerung. Der Schutzbereich der Meinungsäußerungsfreiheit in Fällen demokratiefeindlicher Äußerungen nach der Europäischen Menschenrechtskonvention, dem Grundgesetz und der Charta der Grundrechte der Europäischen Union, 1. Aufl. 2019.

Thiele, OGH: Vorabentscheidungsersuchen zum Schutz der Persönlichkeitsrechte in Sozialen Netzwerken, jusIT 2018, 8.

Tommasi, The Liability of Internet Service Providers in the Proposed Digital Services Act, ERPL 2021, 925.

Turillazzi/Taddeo/Floridi/Casolari, The digital services act: an analysis of its ethical, legal, and social implications, Law Innov Technol 2023, 83.

Ukrow, Die Vorschläge der EU-Kommission für einen Digital Services Act und einen Digital Markets Act Darstellung von und erste Überlegungen zu zentralen Bausteinen für eine digitale Grundordnung der EU, 1. Aufl. 2021.

Ungern-Sternberg, Content Regulation in the European Union/G'Sell, 1. Aufl. 2023, DSA S. 85.

Ungern-Sternberg, Content Regulation in the European Union/Janal, 1. Aufl. 2023, Impacts S. 119.

Ungern-Sternberg, Content Regulation in the European Union/Wendel, 1. Aufl. 2023, Legislative Responsibility S. 59.

Unseld, Zur Bedeutung der Horizontalwirkung von EU-Grundrechten, 1. Aufl. 2018.

Vereinigung der Deutschen Staatsrechtslehrer Veröffentlichungen LXXIV/Pöschl, 1. Aufl. 2015, Sicherung S. 405.

Wagner/Eidenmüller, In der Falle der Algorithmen? Abschöpfen von Konsumentenrente, Ausnutzen von Verhaltensanomalien und Manipulation von Präferenzen: Die Regulierung der dunklen Seite personalisierter Transaktionen, ZfPW 2019, 220.

Weidlinger, Digital Services Act: Haftung sehr großer Online-Plattformen für Inhalte Dritter, ecolex 2023, 186.

Wielsch, Funktion und Verantwortung. Zur Haftung im Netzwerk, RW 2019, 84.

Windhager, OLG Wien: Haftung von Facebook für die Persönlichkeitsrechte beeinträchtigende Postings nach Löschungsaufforderung, ZIIR 2017, 349.

Wischmeyer, Grundrechtliche Bindung privater Plattformbetreiber unter dem EU Digital Services Act. Rechtsgutachten im Auftrag der Gesellschaft für Freiheitsrechte e.V., https://freiheitsrechte.org/uploads/publications/Digital/Grundrechte-im-Digitalen/Gutachten-Wischmeyer-Gesellschaft-fuer-Freiheitsrechte-2023-Grundrechtsbindung-unter-dem-Digital-Services-Act.pdf (Stand 12.2.2024).

Wischmeyer/Meißner, Horizontalwirkung der Unionsgrundrechte – Folgen für den Digital Services Act, NJW 2023, 2673.

Witzeneder, Das EuGH-Urteil "Glawischnig-Piesczek vs. Facebook Ireland Limited". Zur Ausweitung der Überwachungsverpflichtungen von Internet-Service-Providern, 1. Aufl. 2020.

Zankl, RHdB der Digitalisierung/Kresbach, Judikatur – die drei wichtigsten Leading Cases, 1. Aufl. 2021 Rn 22.1.

Zimmer, Regulierung für Algorithmen und Künstliche Intelligenz. Tagung Bonn V/Kühling, Verantwortung der Medienintermediäre, 1. Aufl. 2021, S. 89.