Aufsatz

Der europäische Datenschutz und seine deutschen Wurzeln?

Fabio Stark

Open Peer Review

Dieser Beitrag wurde lektoriert von: Hendrik Eppelmann und Isabel Lihotzky

Fabio Stark wurde 1996 in Starnberg geboren und studiert seit 2017 Rechtswissenschaften an der LMU München mit Schwerpunkt auf Wettbewerbsrecht und Geistigem Eigentum.

Es gibt hier wenig zu verhandeln. Maximilian Schrems blieb auch kurz nach seinem erneuten Sieg vor dem EuGH so kompromisslos wie gelassen. Zweimal ging er buchstäblich durch alle Instanzen und zweimal bekam er Recht. *„Es gibt europäische Grundrechte, der europäische Gerichtshof hat das heute wiederholt*."[1] In genau diesen hatte sich der österreichische Jurist und Datenschutz-Aktivist verletzt gefühlt: Die massenhafte Übermittlung seiner persönlichen Daten durch *Facebook* zur weiteren Verarbeitung in die USA verstoße gegen Unionsrecht. Dort nämlich reiche das Niveau des Grundrechtsschutzes in Bezug auf personenbezogene Daten nicht an den hohen europäischen Standard heran. Ausgerechnet am wichtigsten Standort des internationalen Datenverkehrs entfalte dieser also auch für Unionsbürger schlicht keine Geltung.

1 Zitat aus einem Interview mit WELT vom 16.07.2020, hier abrufbar (Stand: 04.11.2021).

Dabei ist die EU schon seit 1995 dazu verpflichtet, auch für die Sicherheit von in Drittstaaten vermittelte Daten ihrer Bürger Sorge zu tragen.[2] Dem wollte die Europäische Kommission mit ihrer ***Safe-Harbour***-Regelung nachgekommen sein: einem 2000 mit den USA ausgehandelten Beschluss über den Transfer personenbezogener Daten aus der EU in die Vereinigten Staaten. Allerdings sei dies in nur unzureichender Weise gelungen, findet ***Schrems***.

Seine Schlussfolgerung: ***Safe Harbour*** sei unwirksam, ***Facebook*** dürfe daher gar keine persönlichen Daten von EU-Bürgern in die USA verschicken. Nach einem dreijährigen, mühsamen Rechtsstreit mit der irischen Datenschutzbehörde ***DPC*** zieht der Datenschützer schließlich vor den irischen High Court, welcher seinerseits den EuGH anruft. Und tatsächlich: Mit seinem Urteil ***Schrems I*** vom 06. Oktober 2015 erklärte der Gerichtshof das Transferabkommen für ungültig. Die Personendaten von Unionsbürgern würden in den Vereinigten Staaten nicht den gleichen Grundrechtsschutz genießen wie innerhalb der EU.[3]

Schrems und einige Mitstreiter aus ganz Europa hatten bereits ein erneutes Gerichtsverfahren in Gang gesetzt, um endgültig die Rechtswidrigkeit des ***Facebook***-Datentransfers auf Grundlage des ergangenen Richterspruchs feststellen zu lassen, da lässt die Europäische Kommission 2016 eilig ihr zweites Abkommen mit den USA vom Stapel: das ***EU-US Privacy Shield***.

Wie erwartet wird auch diesbezüglich der EuGH konsultiert. Und der stellt am 16. Juli 2020 in seiner Entscheidung ***Schrems II*** fest: Auch ***Privacy Shield*** verstößt – aus den gleichen Gründen wie die Vorgängerregelung – gegen europäisches Datenschutzrecht und ist folglich gleichermaßen unwirksam.[4] Die beiden Urteile sind so rigoros wie verhängnisvoll, drängen sie doch die Frage auf: Wie kann der notwendige personenbezogene Datenverkehr zwischen den beiden bedeutenden Wirtschaftsräumen rechtskonform ausgestaltet werden?

„Die Orwellsche Vision des allwissenden Staates, der die intimsten Winkel menschlicher Lebenssphäre ausforscht, wird in unserem Land nicht Wirklichkeit werden.“

– Hessens Ministerpräsident Albert Osswald (1970)

Um dieses Kernproblem lösen zu können, müssen jedoch noch einige Verständnisfragen geklärt werden: Welche dogmatischen und praktischen Unterschiede können zwischen den beiden Rechtsregimen festgestellt werden? Wie kann ein wirksames Datentransferabkommen ausgestaltet werden?

Der Kampf des ***Maximilian Schrems*** gegen ***Facebook*** gibt Gelegenheit, die Grundlagen des deutschen und europäischen Datenschutzrechts gerade in Abgrenzung zu den USA aufzuzeigen, und in seiner Historie und Struktur zu beleuchten. Es soll nachfolgend eine Skizzierung der Systematik und Wertungen des deutsch-europäischen Datenschutzrechts in seiner Entwicklung bis heute erfolgen.

A. Entwicklung und Struktur des deutschen und europäischen Datenschutzes

Im Folgenden wird primär auf die Rechtssystematik der europäischen Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) eingegangen.

2 S. Art. 25 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, heute: Art. 44 ff. DSGVO.
3 Vgl. Pressemitteilung Nr.117/15 zum Urteil in der Rechtssache C-362/14 vom 06.10.2015, („*Schrems* I“) hier abrufbar (Stand: 29.12.2021).
4 Vgl. Pressemitteilung Nr. 91/20 zum Urteil in der Rechtssache C-311/18 vom 16.07.2020, („*Schrems* II“): hier abrufbar (Stand 29.12.2021).

I. Eine kurze Geschichte des deutschen und europäischen Datenschutzes

1. Wie ein hessischer Einfall zum Grundrecht wurde: Die Anfänge des deutschen Datenschutzes

„Die Orwellsche Vision des allwissenden Staates, der die intimsten Winkel menschlicher Lebenssphäre ausforscht, wird in unserem Land nicht Wirklichkeit werden."[5] Nicht Bundeskanzler ***Willy Brandt*** kommentierte mit diesem eindringlichen Versprechen 1970 die Verabschiedung des weltweit ersten Datenschutzgesetzes (HDSG), sondern Hessens Ministerpräsident ***Albert Osswald***. Sein Landtag hatte mit diesem Gesetz auf einige drohende Risiken des *„**Großen Hessenplans**"* – eines umfassenden Infrastrukturprojekts der Vorgängerregierung – reagiert. In diesem war aus Gründen der Effizienzsteigerung unter anderem der Ausbau der Verwaltungsautomatisierung vorgesehen. So sollten etwa in öffentlichen Kliniken und Schulen Patienten- und Schülerdaten nicht mehr zersplittert in Aktenordnern abgeheftet, sondern zentral und elektronisch abgespeichert werden können. Im selben Zeitraum hatte auch die Datenverwaltung deutscher Sozialversicherungen einen gewaltigen Automatisierungsschub erfahren.[6]

Nicht zur Freude aller: *„**Die sanfte Revolution der Elektronengehirne hat in der Bundesrepublik längst begonnen.*** […] ***In diesem Stadium des Aufbruchs*** […] ***müssen Gefahren auf die Wand unserer Zukunft projiziert werden, Tendenzen zur Totalisierung des Staates auf Umwegen,*** […] ***und zur Entblößung und Degradierung der menschlichen Person***",[7] schrieb ***FAZ***-Redakteur ***Hanno Kühnert*** in einem Artikel vom 10. Juni 1969 und setzte damit der Legende nach die Datenschutzgesetzgebung erstmalig in Gang.[8]

Erst sieben Jahre später verabschiedete der Deutsche Bundestag das erste bundesrechtliche Datenschutzgesetz (BDSG-1977).[9] Materiell-rechtlich folgten beide Regelungen ähnlichen Prinzipien. Allerdings unterwarf das HDSG[10] noch ausschließlich Behörden und sonstige öffentliche Stellen den Datenschutzvorschriften, § 1 HDSG. Das BDSG-1977 adressierte auch *„**Nicht-Öffentliche**"*. Für diese galten jedoch mildere Bestimmungen. Geschützt wurden in beiden Regimen Daten mit Bezug zu natürlichen Personen vor bestimmten Verarbeitungsformen: namentlich dem Speichern, Übermitteln, Verändern und Löschen, § 1 I BDSG-1977. Diese unterstanden bundesrechtlich erstmalig einem allgemeinen Verbot mit Erlaubnisvorbehalt, welches sich aus der Einwilligung des Betroffenen, aus Gesetz oder auch einer Vertragsbeziehung ergeben konnte, §§ 3, 23 BDSG-1977. Als Betroffenenrechte waren Auskunfts- und Berichtigungsansprüche, und mit dem BDSG auch Informationspflichten vorgesehen, § 4 HDSG-1970, § 26 I BDSG-1977. Technische und organisatorische Maßnahmen sollten eine effektive Datensicherheit gewährleisten, § 2 HDSG-1970. Und schließlich war eine neuartige, auch von der Politik weisungsunabhängige Instanz – der Datenschutzbeauftragte – berufen, über die Einhaltung der Vorschriften zu wachen und die Aufsichtsbehörde über mögliche Verstöße in Kenntnis zu setzen.[11] Stoßrichtung der ersten deutschen Regelungen war also der Schutz vor klar definierten, überwiegend hoheitlichen Eingriffen. Sie wiesen die Wesenszüge von Abwehrrechten auf, wenngleich es dafür seinerzeit noch keine anerkannte grundrechtliche Verankerung gab.[12] Diese folgte erst 1983 mit dem Volkszählungsurteil des Bundesverfassungsgerichts (BVerfG).[13] Anlässlich eines Volkszählungsgesetzes, über dessen Grundrechtskonformität das BVerfG befinden sollte, konstituierte es das ***Recht auf informationelle Selbstbestimmung (RiS)***: Also das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Informationen zu entscheiden. Als Ausfluss des Allgemeinen Persönlichkeitsrechts (APR) gem. Art. 2 I i.V.m. 1 I GG gebiete es, dass bereits „auf Stufe der Persönlichkeitsgefährdung" der Grundrechtsschutz greife.[14] Personenbezogene

5 Zit. *Osswald*, hier abrufbar (Stand: 29.12.2021).
6 Vgl. Das älteste Datenschutzgesetz der Welt, hier abrufbar (Stand: 29.12.2021).
7 Zit. *Kühnert*, hier abrufbar (Stand: 29.12.2021).
8 *Rüpke/v. Lewinski/Eckhardt*, Datenschutzrecht. Grundlagen und europarechtliche Neugestaltung, 1. Aufl., 2018, 21, Rn. 59 ff.
9 Gesetzestext BDSG-1977 hier abrufbar (Stand: 29.12.2021).
10 Gesetzestext HDSG-1970 hier abrufbar (Stand: 29.12.2021).
11 *Stoiber*, Geschichte des Datenschutzes, hier abrufbar (Stand: 29.12.2021).
12 *Roßnagel*, Hessisches Datenschutz- und InformationsfreiheitsG, 1. Aufl. 2021, HESDSIG vor § 1, Rn. 2, 3.
13 BVerfGE 65, 1 - 71.
14 Später in BVerfGE 120, 274 (311 f.).

Informationen, verstanden als „Abbild sozialer Realität“,[15] also auch der persönlichkeitsrechtlichen Entfaltung, müssten ebenso in den Schutzbereich des APR fallen wie die Entfaltung selbst.[16] Demgegenüber stünde das Interesse der Allgemeinheit an personenbezogenen Informationen. Schließlich entfalten letztere gerade erst durch ihre Gemeinschaftsgebundenheit ihren Sinn: An der Auskunft über die Bonität des Schuldners hat dieser selbst meist weniger Interesse als der Geschäftsverkehr.[17] Um also diese häufig ebenfalls grundrechtlich geschützten Interessen mit dem RiS in Ausgleich zu bringen, bestätigte das BVerfG schlicht die vorangegangene Gesetzgebung aus Wiesbaden und Bonn, und erklärte insbesondere:

- den Gesetzesvorbehalt
- die Zweckbindung und Verhältnismäßigkeit der Verarbeitung
- das Transparenzgebot sowie
- flankierende Organisations- und Verfahrensregeln

zu verfassungsrechtlichen Vorgaben.[18] Dies hatte für die Gesetzgebung die Folge einer nicht mehr enden wollenden Normenflut.[19]

2. *Zwischen (Grund-)Freiheit und (Datenverkehrs-)Sicherheit:* die europäischen Entwicklungen bis zur DSGVO

Auch auf europäischer Ebene setzte in den 1970ern eine datenschutzrechtliche Debatte ein. Das Parlament war dabei schon seit 1975 bemüht, die Kommission zu einer entsprechenden Initiative zu bewegen.

Abb. 1: Die Grundprinzipien des Datenschutzrechts.

Angesichts der wachsenden und gleichzeitig sehr unterschiedlichen Regelungsdichte auf mitgliedstaatlicher Ebene schien ein einheitlicher Persönlichkeitsschutz

15 BVerfGE 65, 1 - 71 (149).
16 *Rüpke/v. Lewinski/Eckhardt*, Datenschutzrecht. Grundlagen und europarechtliche Neugestaltung, 1. Aufl. 2018, 46, Rn.15.
17 BVerfGE 65, 1 - 71 (148).
18 BVerfGE 65, 1 - 71, 2. Leitsatz; *Kühling/Klar/Sackmann*, Datenschutzrecht. 5. Aufl. 2021, 38, Rn. 69.
19 *Roßnagel*, MMR 2003, 693 (694).

mehr als geboten.[20] Die Kommission erkannte insoweit ebenfalls die Gefahren für die Barrierefreiheit des Binnenmarkts, fühlte sich aber ihrer Rolle als Garantin der Grundfreiheiten verpflichtet und strebte daher zunächst einen möglichst ungehemmten Datenverkehr an.[21] Vielleicht aufgrund dieses Widerspruchs präsentierte sie erst 1990 dem Parlament ein entsprechendes Maßnahmenpaket, welches 1992 noch einmal modifiziert wurde.[22] Eine Einigung konnte drei Jahre später erzielt werden, sodass ab 1995 mit der Datenschutzrichtlinie 95/46/EG (DSRL) endlich ein unionsrechtlicher Standard galt. Das Ergebnis fiel dabei sehr persönlichkeitsrechtlich aus. Der Anwendungsbereich war denkbar weit gefasst: Die bloße Bestimmbarkeit einer Person sollte genügen, um einen Personenbezug bejahen zu können, Art. 2 lit. a DSRL.[23] Unter Verarbeitung wurde jedwede Form des vollständig, teilweise oder auch überhaupt nicht automatisierten Umgangs mit Daten verstanden, sofern zumindest eine Speicherung in Dateisystemen erfolgt, Art. 2 lit. c DSRL. Und Adressat war als „verantwortliche Stelle" schließlich jeder, der über Zweck und Mittel der Verarbeitung entschied, gleich ob Behörde, Unternehmen oder natürliche Person, Art. 2 lit d DSRL. Somit ging die Schutzwirkung der Richtlinie weiter als die der älteren deutschen Regelungen.[24]

Materiell-rechtlich erinnerten die Grundsätze allerdings sehr an die deutschen Vorgänger. Auch die DSRL postulierte ein allgemeines Verbot jeder Verarbeitung personenbezogener Daten mit Erlaubnisvorbehalt, wobei sich auch hierfür nur die Einwilligung des Betroffenen oder eine gesetzliche Befugnis anboten. Der allgemeine Zweckbindungs- und Verhältnismäßigkeitsgrundsatz nach Art. 6 I UAbs. 1 lit. b DSRL band die legale Verarbeitung an eindeutige und rechtmäßige Zwecke. Im Unterschied zum deutschen Recht galt dies jedoch auch für nicht-öffentliche Stellen.[25]

Auch das Transparenzgebot und die daraus abgeleiteten Betroffenenrechte in Art. 10 ff. DSLR wurden übernommen. Und schließlich war ein Datenschutzbeauftragter vorgesehen, Art. 18 I DSRL. Neu war insoweit nur das Konzept der sogenannten ‚Art. 29-Gruppe', einer ständigen Versammlung aus Vertretern nationaler Aufsichtsbehörden, welche die Kommission in ihrer datenschutzrechtlichen Aktivität beraten und die einheitliche Anwendung der Richtlinie gewährleisten sollte, Art. 28, 29 DSRL. Hinsichtlich der Grundrechtebasis für den Erlass sekundären Datenschutzrechts war die Ausgangslage eigentlich wegweisender als in der Bundesrepublik: Bis 2009 galten nach Art. 6 II EUV a.F. neben den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten die Europäische Menschenrechtskonvention von 1950 (EMRK). Letztere kannte in Art. 8 EMRK das Grundrecht auf ***Achtung der Privatsphäre und der Korrespondenz***. Und das wiederum erstreckte seinen Schutzraum nicht nur auf den Inhalt vertraulicher Kommunikationen, sondern auch auf deren Umstände.[26] Kurz: Nicht nur der Inhalt einer E-Mail oder eines Telefonats, sondern auch Zeit, Lokalisierung und Dauer fielen unter die Norm. Das deutsche Recht hingegen erkannte die Konvention ausschließlich als einfaches Bundesrecht an, weshalb es sich mit der Herleitung eines gefestigten Datenschutzgrundrechts erheblich schwerer tat.[27] Mit der Aufwertung der europäischen Grundrechtecharta (GRC) zur Primärrechtsquelle im Zuge der Lissabon-Reform 2009 trat anstelle des Art. 8 EMRK der materiellrechtlich identische Art. 7 GRC und zusätzlich Art. 8 GRC, das erste ausdrückliche Grundrecht auf Datenschutz.

Der EuGH wendet beide Vorschriften – ohne eine nähere Ausführung zu ihrem Verhältnis – parallel an.[28] In ihrer dogmatischen Ausgestaltung blieb die Rechtsprechung zwar jahrelang äußerst vage, entnahm ihre zögerliche Klarstellung aber regelmäßig dem bereits bestehenden Sekundärrecht.[29] So wurden die Vorgaben des Verhältnismäßigkeits-, Zweckbindungs- und Transparenzgebots übernommen.[30] Auch ein Gesetzesvorbehalt wurde postuliert, der jedoch bei erheblichen Grundrechts-

20 Europäisches Parlament: Entschließung über den Schutz der Rechte des Einzelnen angesichts der fortschreitenden technischen Entwicklung auf dem Gebiet der automatischen Datenverarbeitung. In: ABl. C 60., 13. 03. 1975, S. 48, hier abrufbar (Stand: 03.12.2021); zu den unterschiedlichen Datenschutzgesetzen der EU-Mitgliedsstaaten von ihren Anfängen und heute s.: *Custers / Dechesne* et al, Computer Law & Security Report, 2018, Band 34, 234 ff., hier abrufbar (Stand 29.12.2021).
21 Europäische Kommission: Towards a Dynamic European Economy. Green Paper on the Development of the Common Market for Telecommunications Services and Equipment [COM(87) 290 final], 30.06.1987, 142 f., hier abrufbar (Stand: 03.12.2021).
22 *Wuermling,* Handelshemmnis Datenschutz, 1. Aufl. 2000, 17 ff.
23 Zur Bestimmbarkeit als Personenbezug siehe Stark, CTRL 1/22, 27 ff. (in dieser Ausgabe).
24 *Kühling/Klar/Sackmann*, Datenschutzrecht. 5. Aufl. 2021, 72, Rn. 132 f.
25 *Brühann/Zerdic*k, CR 1996, 429 (430).
26 *Grabenwarter/Pabel*, EMRK, 6. Aufl. 2016, § 22, Rn. 10.
27 *Kühling/Klar/Sackmann*, Datenschutzrecht. 5. Aufl. 2021, 12, Rn. 28 f.
28 EuGH, C-92/09 u. C-93/09, 2010 I-11063 (Rn. 47) (*"Schecke und Eifert"*).
29 *Jarass,* GRCh, 5. Aufl. 2019, Art. 8, Rn. 22.
30 EuGH, C-28/08 P (Rn. 53 f.) (*„Kommission und Bavarian Lager"*).

eingriffen dem EU-Parlament zustehen sollte.[31] Erneut war es also weder die breite Öffentlichkeit noch höchstrichterliche Rechtsprechung, die dem Datenschutzrecht seine Gestalt verlieh. Pionier blieb auch hier der Gesetzgeber.

II. *Der milchgläserne EU-Bürger:* Die rechtlichen Wertungen der DSGVO

Seit dem 25. Mai 2018 ist die 2016 verabschiedete DSGVO in Kraft. Durch sie soll ein in allen Mitgliedsstaaten unmittelbar geltendes einheitliches Datenschutzrecht etabliert werden. Materiell-rechtlich durchlief das europäische Datenschutzrecht dabei mehr eine Entwicklung als eine Revolution. In Anlehnung an die bereits geschilderten Ursprünge lassen sich ihre Prinzipien wie folgt darstellen:

1. Das Verhältnis der DSGVO zum BDSG

Erste wesentliche Neuerung der DSGVO ist ihr Anwendungsvorrang: Nicht mehr als Richtlinie sondern als Verordnung normiert, entfaltet sie gem. Art. 288 II AEUV unmittelbare Geltung. Widersprechende nationale Vorschriften sind von vornherein unanwendbar.[32] Damit hat Brüssel auf vorangegangene Harmonisierungsprobleme, insbesondere in Deutschland,[33] reagiert und die Vereinheitlichung mit Macht durchgesetzt. Dennoch behält das BDSG eine Funktion: Die DSGVO enthält zahlreiche Öffnungsklauseln, d.h. punktuell ergänzende oder erweiternde Regelungsspielräume für die Mitgliedstaaten.[34] Von diesen hat der deutsche Gesetzgeber eher zurückhaltenden Gebrauch gemacht, als er 2017 mit dem Datenschutzanpassungsgesetz das BDSG novellierte. So enthält bspw. § 26 BDSG i. V. m. Art. 88 I DSGVO einige besondere Vorschriften für Datenverarbeitung im Beschäftigungskontext. Auch in der Ausgestaltung der Betroffenenrechte konnte Deutschland dank Art. 23 I DSGVO mit den §§ 29 ff. BDSG einige spezielle Regelungen treffen.

Über die Öffnungsklauseln hinaus bleibt es aber beim Primat der DSGVO, wie § 1 V BDSG anerkennt.

2. Anwendungsbereich und Adressat der DSGVO

Die DSGVO umfasst nach Art. 2 I jede „***automatisierte Verarbeitung […] sowie […] nicht-automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen***."[35] Es wird also nicht mehr nur das Scannen einer Visitenkarte oder die elektronische Auswertung einer Online-Umfrage als typische automatisierte Verarbeitungsform erfasst. Auch manuelle Verarbeitungen sind betroffen, soweit eine systematisierte Zugriffsmöglichkeit, v.a. durch die strukturierte Anordnung personenbezogener Daten, geschaffen wird.[36] Werden Patientenangaben zunächst händisch niedergeschrieben, im Anschluss aber in ein analoges, nach bestimmten Kriterien sortiertes Karteisystem eingeordnet, greift die DSGVO gleichermaßen. Damit soll eine Umgehung der Vorschriften durch „technologieneutrale" Verarbeitungsformen vermieden werden.[37] Eng umfasste Ausnahmen hiervon bestehen nach Art. 2 II lit. c DSGVO insbesondere für rein persönliche oder familiäre Tätigkeiten. Adressat datenschutzrechtlicher Verpflichtungen sind „Verantwortliche". Nach Art. 4 Nr. 7 DSGVO ist dies „***jede natürliche oder juristische Person, Behörde […] oder andere Stelle, die […] über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet***." Die urdeutsche Differenzierung zwischen öffentlichen und nicht-öffentlichen Stellen fällt somit gänzlich weg. Es wird auch nicht auf die Organisationsform oder die Durchführung der Verarbeitung abgestellt. Einziger Bezugspunkt ist die Veranlassung und die Entscheidungsbefugnis. Entsprechend gelten auch die weisungsabhängigen „Auftragsverarbeiter" nach Art. 4 Nr. 8 und 28 f. DSGVO grundsätzlich als bloße Verrichtungsgehilfen der Verantwortlichen.[38] Auch der räumliche Anwendungsbereich ist bewusst umfassend gehalten. Nach Art. 3 II DSGVO genügt, dass der Verantwortliche das Verhalten von sich in der Union aufhaltenden Personen beobachten will (lit. b), oder die

31 EuGH, C-293/12 u. C-594/12 (Rn. 38 ff.) (*„Digital Rights Ireland Ltd* und *Minister for Communications, Marine and Natural Resources")*; *Kühling*, NVwZ 2014, 681.
32 *Kühling/Buchner,* DSGVO und BDSG, 3. Aufl. 2020, § 1, Rn. 14 ff.
33 *Kühling/Klar/Sackmann,* Datenschutzrecht. 5. Aufl. 2021, 77, Rn. 145.
34 *Simitis/Hornung/Spiecker,* Datenschutzrecht | DSGVO, 1. Aufl. 2019, Art. 6 III, Rn. 1-3.
35 Zum Personenbezug sowie der allg. Datenverarbeitung s. Stark, CTRL 1/22, 27 ff. (in dieser Ausgabe).
36 *Rüpke/v. Lewinski/Eckhardt,* Datenschutzrecht. Grundlagen und europarechtliche Neugestaltung, 1. Aufl. 2018, 122, Rn. 23 ff.
37 Erwägungsgrund 15 DSGVO.
38 *Rüpke/v. Lewinski/Eckhardt*: Datenschutzrecht. Grundlagen und europarechtliche Neugestaltung, 1. Aufl., 2018, 151, Rn. 6 ff.

verarbeiteten Daten einen Bezug zu einer Ware oder Dienstleistung aufweisen, die sich an EU-Bürger richtet (lit. a).

Es wird deutlich: Ziel der DSGVO ist der möglichst umfassende Schutz personenbezogener Informationen. Um dies zu gewährleisten, werden grundsätzlich alle Formen der Datenverwertung, gleich von welchem Dritten sie ausgehen und auf welche Weise sie erfolgen, ins Auge gefasst.

3. Die Grundprinzipien des Datenschutzrechts

a) Das Souveränitätsprinzip: Wann dürfen meine Daten verarbeitet werden?

Der protektive Ansatz der DSGVO wird auch durch die Fortführung des bereits etablierten Verbotsgrundsatzes untermauert. Wie aus Art. 5 I lit. a i.V.m. 6 I Hs. 1 DSGVO hervorgeht, bleibt jede Verarbeitung persönlicher Daten weiterhin verboten, soweit kein expliziter gesetzlicher Erlaubnistatbestand greift.[39] Diese gehen abschließend aus Art. 6 I 1 lit. a-f DSGVO hervor (vgl. Abb. 2). Zur Durchsetzung der Datenhoheit des Betroffenen sieht Art. 17 DSGVO ein Recht auf Löschung vor, soweit die Verarbeitung unzulässig ist.[40] Noch enger gefasste Ausnahmen definiert Art. 9 II DSGVO für besonders sensible oder freiheitsrelevante Daten, wie genetische und biometrische Informationen, solche zur sexuellen oder politischen Orientierung sowie jene, aus denen die ethnische Herkunft einer Person hervorgeht, Art. 9 I DSGVO. Auch wenn der Verbotsgrundsatz vor allem durch den weit gefassten und daher praktisch hochrelevanten Art. 6 I lit. f DSGVO gelockert wird:[41]

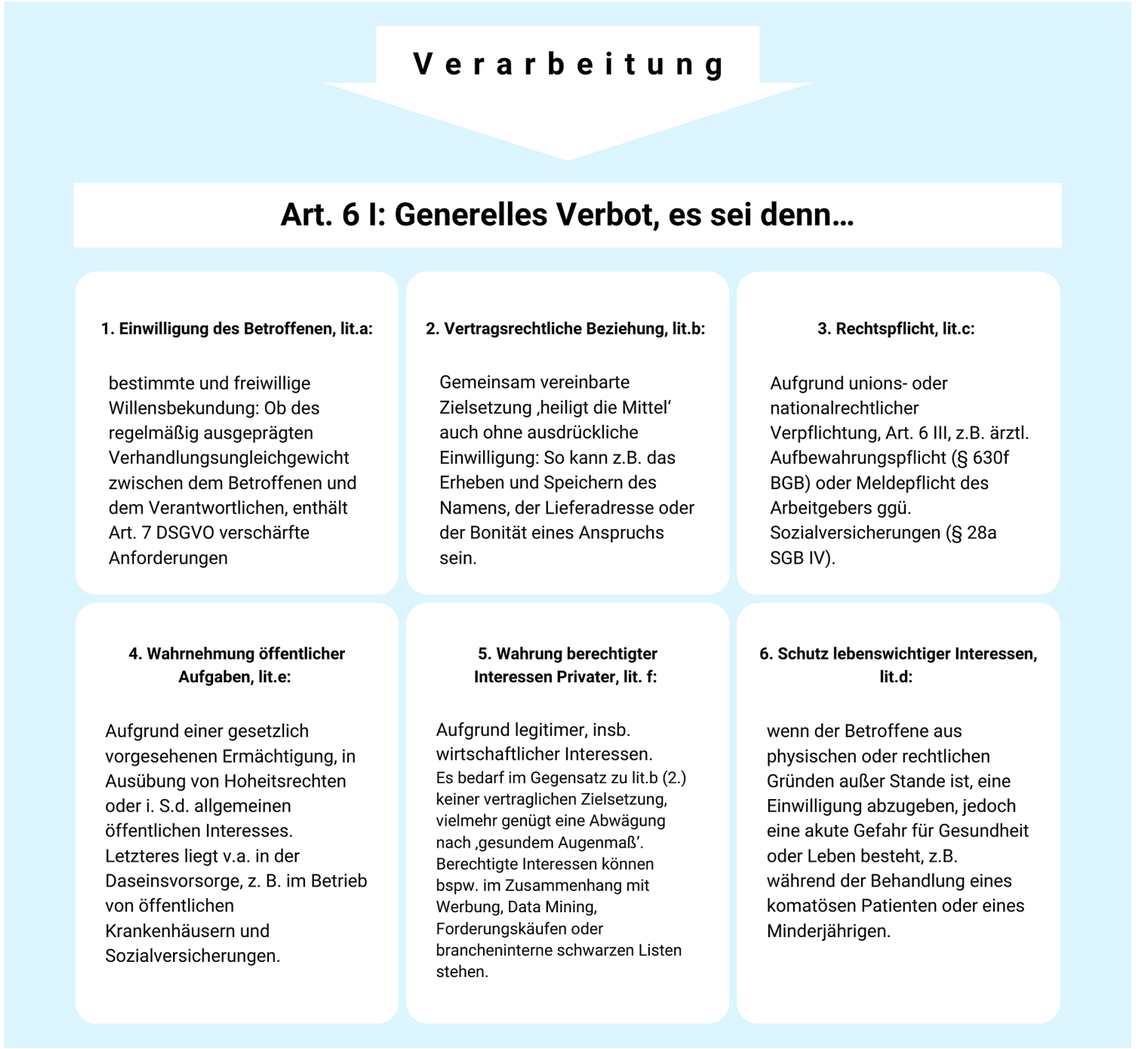

Abb. 2: Erlaubnistatbestände nach Art. 6 I DSGVO.

Es ist erkennbar, dass der Einzelne die möglichst uneingeschränkte Entscheidungsmacht über den Umgang mit seinen Daten haben soll. Dieses Prinzip ist historischer Ausfluss des deutschen Rechts auf informationelle Selbstbestimmung und wird in der Literatur regelmäßig mit dem Stichwort „***Datensouveränität***" umschrieben.[42]

39 *Sydow*, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 7 DSGVO, Rn. 8 f.
40 *Kühling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2021, 275, Rn. 652 ff.
41 *Rüpke/v. Lewinski/Eckhardt*, Datenschutzrecht. Grundlagen und europarechtliche Neugestaltung, 1. Aufl. 2018, 166, Rn. 12 (Relevanz); *Paal/Pauly*, DS-GVO BDSG, 3. Aufl. 2021, Art. 6, Rn. 26-31.
42 So *Krüger*, ZRP 2016, 190; *Beise*, RDi 2021, 597.

b) Das Rechtmäßigkeitsprinzip: Wie dürfen meine Daten verarbeitet werden?

Über die bloße Erlaubnis hinaus stellt Art. 5 I DSGVO einige besondere Anforderungen an die Durchführung der Datenverarbeitung. Allgemein wird auf Rechtmäßigkeit und Treu und Glauben abgestellt. Konkret folgt daraus zunächst, dass jede Verarbeitung grundsätzlich einer strikten Zweckbindung unterliegt, Art. 5 lit. b DSGVO. Das bedeutet: Bereits vor der Erhebung muss ein eindeutiges und legitimes Ziel der Verarbeitung im Rahmen der Art. 6 I, 9 II DSGVO festgelegt werden. Unter anderem sollte dies schon nach dem BDSG a.F. bewirken, dass mehrere Verantwortliche für sie relevante Daten nicht untereinander austauschen dürfen, sondern stets beim Betroffenen selbst einholen müssen.[43] Würden beispielsweise Adressdaten einer Person zwischen verschiedenen Online-Händlern ausgetauscht werden, ohne dass der Betroffene darüber informiert wäre, würde er zusehends die Übersicht darüber verlieren, wer über seine Daten verfügt. Und damit auch die Kontrolle. Erneut kommt also das Souveränitäts- und Transparenzprinzip zum Tragen. Vor allem fungiert die Zweckbindung aber als Grundlage des zweiten wesentlichen Rechtmäßigkeitsgrundsatzes: der Erforderlichkeit der Verarbeitung. Neben seiner allgemeinen Verankerung in Art. 5 I lit. b und c DSGVO kommt dies terminologisch in den Erlaubnisklauseln des Art. 6 I und 9 II DSGVO zum Ausdruck. Auch die Erforderlichkeit wurde bereits im BDSG-1977 gefordert, wobei man darunter seinerzeit eine regelrecht kausale Notwendigkeit der Verarbeitung verlangte.[44] Der EuGH spricht heute noch vom „absolut Notwendigen“,[45] wohingegen nach dem BDSG n.F. „der Zweckbestimmung dienen“ gemeint ist, vgl. § 28 I 1 Nr. 1 BDSG. Jedenfalls muss eine hinreichende Geeignetheit sowie eine angemessene Zweck-Mittel-Relation zwischen dem verfolgten Ziel und der Verarbeitung vorliegen.[46] Damit wird letztlich aus grundrechtlicher Tradition heraus eine reguläre Verhältnismäßigkeitsprüfung verlangt. Dies ergibt sich auch aus weiteren DSGVO-Kriterien: Dem Datenminimierungsgrundsatz nach Art. 5 I lit. c DSGVO zufolge dürfen quantitativ keine über die verfolgten Ziele

Informationsrecht, Art. 13 f.:	**Auskunftsrecht, Art. 15**
Betroffener muss auch ohne sein Verlangen innerhalb eines angemessenen Zeitraums über bestimmte Umstände der Verarbeitung seiner Daten unterrichtet werden (Metainformationen). Dazu zählen u.a.: • Zweck und Rechtsgrundlage der Verarbeitung • Dauer der Speicherung • bestehende Betroffenenrechte • Name und Kontakt des Verantwortlichen Einschränkungen können sich aus Zweck- und Geheimnisschutz, Aufgaben öffentlicher Stellen, Wahrung zivilrechtlicher Ansprüche, Gefahrenabwehr oder der Unverhältnismäßigkeit des Aufwands ergeben, *Art. 13 I, II 14 I, II DSGVO, §§ 32 I, 33 I BDSG*	Auf Verlangen des Betroffenen ist ihm Auskunft über das Bestehen der Verarbeitung, die verarbeiteten Daten selbst und zusätzlich einige Metadaten gem. *Art. 13, 14* zu erteilen. Im Unterschied zum Informationsrecht, welches den Rahmen der Verarbeitung zum Gegenstand hat, erfasst das Auskunftsrecht also vor allem die verarbeiteten Daten und gewonnen Informationen selbst. So kann ich in Erfahrung bringen, zu welchem Zweck ein Unternehmen meine Suchanfragen speichert und mit wem diese geteilt werden.

Abb. 3: Informations- und Auskunftsrecht

„hinausschießenden” Daten erhoben werden. Art. 5 I lit. e DSGVO verlangt eine angemessene zeitliche Begrenzung der Speicherung personenbezogener Daten. Und mit der Pseudonymisierung des Art. 4 Nr. 5 DSGVO wird auch ein konkretes Mittel vorgegeben, das eine besonders persönlichkeitsschützende Verarbeitung ermöglicht: Bei ihrer Anwendung kann erst durch den Zugriff auf weitere, gesondert aufbewahrte und geschützte Daten Personenbezug hergestellt werden.[47]

c) Das Transparenzprinzip: Was habe ich über die Verarbeitung zu wissen?

Wesentliche Voraussetzung für die effektive Ausübung der Datensouveränität ist die Kenntnis über den Umstand und Umfang der Verarbeitung, und zwar sowohl im Vorfeld als auch während der Verarbeitung. Daher sieht die DSGVO Transparenz als eigenen Grundsatz vor, Art. 5 I lit. a DSGVO. Allgemein gilt, dass Verarbeitungsinformationen für den Betroffenen leicht zugänglich und verständlich sein müssen.[48]

43 *Rüpke/v. Lewinski/Eckhardt*, Datenschutzrecht. Grundlagen und europarechtliche Neugestaltung, 1. Aufl. 2018, S. 177, Rn. 38.
44 *Auernhammer*, Bundesdatenschutzgesetz. Kommentar, 1. Aufl. 1977, § 9 Rn. 4.
45 EuGH, C-311/18 (Rn. 176) („*Facebook Ireland* und *Schrems*“).
46 *Rüpke/v. Lewinski/Eckhardt*, Datenschutzrecht. Grundlagen und europarechtliche Neugestaltung, 1. Aufl. 2018, 170, Rn. 22.
47 *Kühling/Buchner*, DS-GVO und BDSG, 3. Aufl. 2020, Art. 4, Abs. 5, Rn. 5 ff.
48 Erwägungsgrund 39, DSGVO.

d) Das Datenqualitäts- und Datensicherheitsprinzip

Als letzte beiden Prinzipien der DSGVO sei auf den Richtigkeitsgrundsatz des Art. 5 I lit. d DSGVO, und auf das Integritäts- und Vertraulichkeitsgebot des Art. 5 I lit. f DSGVO verwiesen.

Ersterem zufolge müssen verarbeitete Daten sachlich richtig und auf dem neuesten Stand sein. So hat ein ehemaliger Angeklagter nach dem Freispruch ein berechtigtes Interesse daran, in Datensystemen nicht mehr als potenzieller Straftäter geführt zu werden.

Zur Durchsetzung sieht Art. 16 DSGVO einen Anspruch auf Berichtigung vor, welcher sich jedoch nur auf unrichtige Tatsachen und nicht auf Werturteile bezieht.[49] Auch eine Vervollständigung kann eingefordert werden.

Des Weiteren besteht grundsätzlich ein Anspruch auf Einschränkung der Verarbeitung, soweit die Unrichtigkeit der Daten festgestellt werden kann, Art. 18 I lit. a DSGVO. Und schließlich muss die Integrität und Vertraulichkeit personenbezogener Daten durch entsprechende technische und organisatorische Maßnahmen (TOMs) sichergestellt werden. Ziel ist vor allem die Verhinderung von unbefugtem Zugriff oder der unberechtigten Veränderung oder Zerstörung der Daten.[50]

Die Anforderungen an die Maßnahmen sind in Art. 32 DSGVO sowie 28 III 2 lit. b und 29 DSGVO aufgelistet, und umfassen die Pseudonymisierung und Verschlüsselung von Daten, die Fähigkeit zur raschen Wiederherstellung bei unerwünschten technischen Zwischenfällen sowie die regelmäßige Überprüfung der TOMs hinsichtlich ihrer Wirksamkeit.

Damit hat die zuvor vom Datenschutz eigens losgelöste Datensicherheit zumindest teilweise Einzug ins Datenschutzrecht gehalten.

49 *Paal/Pauly*, DS-GVO und BDSG, 3. Aufl. 2021, Art. 16, Rn. 15.
50 *Kühling/Klar/Sackmann*, Datenschutzrecht. 5. Aufl. 2021, 169, Rn. 363.

4. Kontrolle und Durchsetzung der DSGVO

Hinsichtlich der Frage wie sich die hohen Anforderungen des unionsrechtlichen Datenschutzes effektiv durchsetzen lassen, bediente sich der europäische Gesetzgeber erneut am Ideenreichtum des deutschen Rechts.

So findet sich der Datenschutzbeauftragte (DSB) in die DSGVO wieder. Als weisungsunabhängiges und verschwiegenheitspflichtiges Instrument dient er der Selbstkontrolle des Verantwortlichen.[51] Nach Art. 37 I DSGVO sind öffentliche Stellen und private Unternehmen, deren Kerntätigkeit in der Datenverarbeitung liegt, zur Bestellung eines DSB verpflichtet. Die Kernaufgaben liegen in der begleitenden Beratung des Verantwortlichen, der Überprüfung der Verarbeitungsvorgänge sowie der Sensibilisierung von Mitarbeitern. Wenngleich Art. 39 I lit. b DSGVO von der „Überwachung der Einhaltung“ des Datenschutzrechts spricht, so hat er doch keine eigenen Weisungs- oder Durchsetzungsbefugnisse. Diese verbleiben vielmehr beim Verantwortlichen selbst.[52]

Daneben bleiben die staatlichen Aufsichtsbehörden in allen EU-Mitgliedstaaten bestehen, Art. 51 ff. DSGVO. Um sowohl Kohärenz in der Anwendung als auch die Unabhängigkeit der Behörden zu stärken, kooperieren diese in einem eigenen Verbundsystem: dem EU-Datenschutzausschuss nach Art. 68, 73 ff. DSGVO, einem Nachfolger der ‚Art. 29-Gruppe’.[53] Sowohl die EU als auch die Bundesrepublik beschäftigen eigene Datenschutzbeauftragte, Art. 16 II 2 AEUV,[54] §§ 8 ff. BDSG.[55]

Ironischerweise wurde gerade Deutschland schon 2010 vom EuGH für die mangelhafte politische Unabhängigkeit seiner öffentlichen Datenschutzbeauftragten kritisiert.[56] Bis heute hat sich daran nicht viel geändert.[57]

51 *Paal/Pauly*, DS-GVO und BDSG, 3. Aufl. 2021, Art. 37, Rn. 3.
52 *Ehmann/Selmayr/Heberlein*, DSGVO, 2. Aufl. 2018, Art. 37, Rn.1.
53 *Kühling/Klar/Sackmann*, Datenschutzrecht. 5. Aufl. 2021, 294, Rn. 719.
54 vgl. Selbstbeschreibung des European Data Protection Board, hier abrufbar (Stand: 29.12.2021).
55 *Heinzelmann*: Datenschutzaufsicht: *Deutscher Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)*, aus Haufe Compliance Office Online, hier abrufbar (Stand: 29.12.2021).
56 EuGH, C-518/07 (Rn. 56) (*„Kommission und Deutschland“*).
57 *Schulzki-Haddouti*, Gutachten: Auswahlverfahren für Datenschützer verstößt gegen DSGVO, hier abrufbar (Stand: 29.12.2021).

Besonders drastisch erscheinen die nochmals verschärften Sanktionen, die das aktuelle Datenschutzrecht für Verstöße vorsieht. Kannte das BDSG a.F. noch Bußgelder von maximal 50.000 DM (§ 42 II BDSG a.F.) und Freiheitsstrafen bis zu zwei Jahren, ordnet Art. 83 V DSGVO bis zu 20.000.000 € bzw. 4 % des Jahresumsatzes an Strafgeldern an, abhängig von der Schwere des Verstoßes und der Größe des Unternehmens.

Bis zu drei Jahre Haft drohen, sobald vorsätzlich nicht öffentliche personenbezogene Daten ohne Berechtigung in ein Drittland übermittelt werden oder gewerbsmäßiger Handel damit betrieben wird, § 42 I BDSG n.F.

C. Zwischen Bürokratie und Bürgerrecht: Ein Fazit

Das europäische Datenschutzrecht ist weder reine Technologie-Regulierung noch European Business Law. Als erkennbar „mutiertes Grundrecht" bemüht es sich um den möglichst effektiven und umfassenden Schutz personenbezogener Daten aller Unionsbürger. Und zwar gegenüber jedermann, nicht nur gegenüber staatlichen Stellen.

In seiner Evolution ist es dabei zusehends rigoroser geworden: Sein sachlicher und räumlicher Anwendungsbereich wurde sukzessive ausgeweitet. Der Adressatenkreis kennt derweil kaum Differenzierungen mehr und die vorgesehenen Strafen drohen – zumindest in der Theorie[58] – zu Bankrott und Existenzverlust zu führen.

Doch wie steht es um die praktischen Effekte? In einer Evaluation aus dem Jahr 2020 bewertete die Europäische Kommission die Wirkung der DSGVO als ***„zeitgemäß"*** und insgesamt gelungen: So sei seit ihrem Erlass das Bewusstsein für den Datenschutz in der Öffentlichkeit deutlich gestiegen.[59]

Von einem ***„gesamteuropäische(n) Entwurf und Leuchtturmprojekt zum Schutz von Rechten und Freiheiten im digitalen Zeitalter"*** sprach gar der Hamburgische Beauftragte für Datenschutz ***Johannes Caspar***.[60]

Und in der Tat, die DSGVO hat, zumindest innerhalb der EU, zu einem bislang beispiellosen Informationsschutzstandard beigetragen. Doch dieser hat seinen Preis. Vor allem kleinere Unternehmen und Vereine ächzen unter den bürokratischen Vorgaben aus Brüssel.

Die hohe Komplexität und Vieldeutigkeit der Anforderungen sowie der drastisch gestiegene Dokumentationsaufwand stellen eine erhebliche Mehrbelastung für sie dar.[61] So werden Therapieabläufe in Arztpraxen durch Einwilligungserfordernisse und Informationspflichten spürbar verzögert.[62]

Volkswirtschaftlich führt dies auch zu wettbewerblichen Nachteilen, etwa gegenüber US-amerikanischen oder asiatischen Marktteilnehmern. Und das, wo Einschränkungen des freien Datenverkehrs ohnehin schon verminderte Innovationskraft und Wertschöpfung bedeuten.[63]

Bedauerlicherweise können die Vorgaben dabei sogar kontraproduktive Wirkung entfalten: Die weit gefassten Transparenzpflichten etwa drohen zu einem regelrechten ***„Information-Overload"*** zu führen, einer Informationsflut, welche die Aufklärung des Betroffenen mehr behindert als fördert und sogar ein Einfallstor für Missbrauch darstellen kann.[64] ***Schrems*** selbst berichtet, von ***Facebook*** auf Anfrage hin mehr als 1.200 Seiten Meta-Informationen über die Verarbeitung seiner Daten erhalten zu haben: Nach seinen Angaben sind das mehr Dokumente, als die Stasi einst über ***Helmut Kohl*** führte.[65]

58 Zu den in Deutschland verhängten Bußgeldsummen *Wirminghaus*, Ein Jahr DSGVO: die Kritik bleibt, hier abrufbar (Stand 29.12.2021).
59 Kommissionsbericht v. 24.06.2020, hier abrufbar (Stand: 29.12.2021).
60 Zit. *Caspar*, hier abrufbar (Stand: 14.12.2021).
61 Hier abrufbar (Stand 14.12.2021).
62 *Kretschmer*, Drei Jahre DSGVO: „Zeitintensiver, mühsamer, teurer", hier abrufbar (Stand: 29.12.2021).
63 *Voss*, Wir müssen die DSGVO dringend ändern, hier abrufbar (Stand: 29.12.2021).
64 *Steinrötter/Rahimi/Tran*, EWS 2019, 301.
65 Hier abrufbar: (Stand 29.12.2021).

Im Ergebnis präsentiert sich der unionsrechtliche und somit auch deutsche Datenschutz als „Superbürgerrecht", dem sich andere allgemeine Interessen wie Forschung, Sicherheit, Gesundheit, Wertschöpfung und Innovation regelmäßig beugen müssen.

So nachvollziehbar der Wunsch nach einem schlagkräftigen Persönlichkeitsrecht auch ist, muss man sich doch gerade in Zeiten des internationalen Datenverkehrs die Frage stellen, wie zielführend ein derart universeller Ansatz erscheint. Insbesondere dann, wenn, wie der EuGH feststellen konnte, europäische Daten anderswo nahezu schutzlos verarbeitet werden können. Insoweit wird eine Lösung des internationalen Datentransfer-Problems gewiss nicht im ausschließlichen Verantwortungsbereich von Drittstaaten wie den USA liegen.

Weiterführender Hinweis:

Talking Legal Tech – Folge 28:

Regulierung & Innovation – Wie lässt sich beides vereinbaren, Martin Ebers?

Zurück zum dynamischen Inhaltsverzeichnis?

Zum dynamischen Inhaltsverzeichnis

1/22

2. Jahrgang, 1. Ausgabe
www.legaltechcologne.de/ctrl

CTRL

Cologne Technology & Law Review

Hier geht es zur ganzen Ausgabe

Dort findest Du in 19 Beiträgen alles von Datenschutz bei Connected Cars über Krypto-Auktionen bis hin zum Artificial Intelligence Act und Legal Tech.

LEGAL TECH LAB COLOGNE