Typoskript im Sinne des § 38 Abs. 4 UrhG. Das Original ist abgedruckt im Verwaltungsarchiv 2019, S. 235-279.

# UNDURCHSICHTIGE DATENTRANSFERS – GLÄSERNE STUDIERENDE?

Datenschutzrechtliche Schranken der Datenübermittlung in die USA am Beispiel von Massive Open Online Courses (MOOCs)

Von Univ.-Prof. Dr. *Mario Martini und* Forschungsreferent *Jonas Botta*, Speyer*

## I. Das Phänomen „Massive Open Online Course“

*Massive Open Online Courses* (MOOCs) machen es möglich: Die weltweit besten Bildungsangebote sind im digitalen Zeitalter nur noch wenige Klicks entfernt. Dank ihrer Hilfe kann im Grunde jeder Interessierte seinen Wissenshorizont bequem erweitern – ganz gleich, ob er unterwegs ist oder auf dem heimischen Sofa sitzt. In den vergangenen Jahren haben MOOCs eine rasante Entwicklung durchlaufen. Die interaktiven Online-Kurse haben das herkömmliche Vorlesungsformat in das digitale Zeitalter überführt. Die Studierenden erwartet eine neue Lernatmosphäre: verdichtete Lernvideos statt Bücher, Online-Multiple-Choice-Tests statt Klausurbögen und Online-Foren statt Seminarräume.

Mit etwas Verzögerung sind inzwischen auch deutsche Hochschulen auf den fahrenden Zug des E-Learnings aufgesprungen. Sie kooperieren dabei vornehmlich mit (zumeist kommerziellen) Plattformbetreibern aus den USA. Diese stellen die digitale Infrastruktur zur Verfügung und übernehmen die gesamte Abwicklung der Online-Kurse.

Die Kehrseite der Medaille machen sich nicht alle Hochschulen bewusst: Wer Einblick in die virtuellen Hörsäle nehmen kann, der erfährt nicht nur, mit welchem Ergebnis oder innerhalb welcher Zeitspanne ein Nutzer seinen Kurs abgeschlossen hat. Dank moderner

* *Mario Martini* ist Lehrstuhlinhaber an der Deutschen Universität für Verwaltungswissenschaften Speyer und Leiter des Programmbereichs „Digitalisierung“ am Deutschen Forschungsinstitut für öffentliche Verwaltung (FÖV), Fellow am Center for Advanced Internet Studies in Bochum sowie Mitglied der Datenethikkommission. *Jonas Botta* ist Forschungsreferent am FÖV; mit der Thematik der MOOCs setzt er sich auch im Rahmen seines laufenden Promotionsvorhabens zum Datenschutz in der digitalen Hochschulbildung an der DUV Speyer auseinander. Die Autoren danken besonders den beiden Forschungsreferenten *Michael Kolain* und *Quirin Weinzierl, LL.M. (Yale)* für die sehr gelungene Mitwirkung. Soweit nicht anders vermerkt, haben die Autoren Internetquellen zuletzt am 27.6.2019 aufgerufen.

Analyseverfahren vermag der „Herr über die Daten“ mitunter auch Rückschlüsse auf sensible Charaktereigenschaften der Studierenden zu ziehen – etwa auf ihre Intelligenz, Zuverlässigkeit oder Belastbarkeit. Das Ergebnis kann eine panoptische Durchleuchtung der Studierenden sein, wie sie in Zeiten von Kreidetafeln und papierenen Zeugnissen noch undenkbar gewesen wäre.

Die grundlegenden Unterschiede in den Datenschutzregimen auf beiden Seiten des Atlantiks geben dieser Sorge reichlich Nahrung: Während der Unionsgesetzgeber seit Langem einen ganzheitlichen Ansatz im Datenschutzrecht verfolgt, zeichnet sich der US-amerikanische Rechtsrahmen zum einen durch sektorale Regelungen aus. Zum anderen lässt er Ausländern nicht den gleichen Schutz wie US-Bürgern angedeihen.[1] Je nach Einsatzszenario können MOOCs daher entweder dem Humboldt’schen Ideal „gleicher Bildung für alle“ frönen oder aber in einer Orwell‘schen Dystopie panoptisch durchleuchteter Studierender enden – Grund genug, um dem Phänomen „MOOC“ aus datenschutzrechtlicher Sicht nachzuspüren,[2] insbesondere zu fragen, inwieweit das transatlantische Datenschutzabkommen, der sog. *EU-US Privacy Shield,* die Risiken der digitalen Bildungsanwendungen überwinden kann.

## 1. MOOCs als Wegbereiter örtlich entgrenzter Bildung

Dass das Angebot von MOOCs in den Augen mancher nicht unbedingt ein Gütesiegel des Privatheitsschutzes ist,[3] mussten die Ludwig-Maximilians-Universität und die Technische Universität München im Jahre 2017 erfahren. Exzellenztitel hin oder her – der datenschutzpolitisch aktive Verein Digitalcourage e. V. verlieh den beiden Universitäten eine Auszeichnung eigener Art: den *Big Brother Award*[4] in der Kategorie Bildung.[5] Hintergrund der unrühmlichen Ehrung ist die Kooperation beider Universitäten mit dem US-amerikanischen Unternehmen *Coursera*. Dieses bietet eine kommerzielle Plattform für MOOCs an.

Aller persönlichkeitsrechtlicher Kritik zum Trotz haben sich MOOCs als innovatives E-Learning-Format einen festen Platz in der Bildungslandschaft erobert. Seit dem ersten Hype

---

[1] Hinzu tritt der – spätestens seit den Snowden-Enthüllungen bekannte – umfassende Datenzugriff US-amerikanischer Sicherheitsbehörden auf Daten Dritter. Dazu im Einzelnen unten III. 3. a) bb) (1).

[2] Zum Phänomen „MOOC“ aus einer bildungswissenschaftlichen Perspektive weiterführend *Bershadskyy/Bremer/Gaus*, Bildungsfreiheit als Geschäftsmodell: MOOCs fordern die Hochschulen heraus, in: Bremer/Krömker (Hrsg.), E-Learning zwischen Vision und Alltag, 2013, S. 33 ff.; *Jungermann/Wannemacher*, Innovationen in der Hochschulbildung: Massive Open Online Courses an den deutschen Hochschulen, 2015, S. 1 ff.; *Porter*, To MOOC or not to MOOC, 2015, S. 3 ff.; *Schulmeister*, Der Beginn und das Ende von OPEN, in: ders. (Hrsg.), MOOCs – Massive Open Online Courses. Offene Bildung oder Geschäftsmodell?, 2013, S. 17 ff.

[3] Datenschutzrechtliche Bedenken äußerten schon *Albrecht/Revermann*, Digitale Medien in der Bildung, TAB-Arbeitsbericht Nr. 171 (BT-Drucks. 18/9606), 2016, S. 41; *Hochschulrektorenkonferenz*, Potenziale und Probleme von MOOCs: Eine Einordnung im Kontext der digitalen Lehre, 2014, S. 28 f.; *Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation*, Arbeitspapier zum Thema E-Learning-Plattformen, S. 1 f.

[4] Dabei handelt es sich um einen Negativpreis für staatliche Einrichtungen, Unternehmen oder Privatpersonen, welche die Privatheit von Menschen in besonderem Maße beeinträchtigten – insbesondere indem sie personenbezogene Daten in großem Umfang an Dritte übermitteln.

[5] S. https://bigbrotherawards.de/2017/bildung-lmu-tu-muenchen.

um diese Technologie im Jahre 2011 erfreuen sie sich anhaltender Beliebtheit:[6] Sie stehen grundsätzlich ohne jegliche Teilnehmerbegrenzung (*Massive*) und unentgeltlich (*Open*) jedem, der über einen Internetzugang verfügt (*Online*), zur Verfügung. Üblicherweise binden sie mehrere, zumeist nur wenige Minuten lange Video- und Audiosequenzen, ein – ferner begleitendes Lehrmaterial, ein Forum für den Austausch zwischen den Nutzern, aber auch mit dem Kursverantwortlichen sowie regelmäßige Wissensabfragen und einen Abschlusstest. Die Leistungsbewertung erfolgt i. d. R. durch eine Software oder sog. *Peer Reviews*, d. h. andere Nutzer bewerten ihre „digitalen Kommilitonen".

Der offene Nutzerkreis in Verbindung mit dem Renommee beteiligter US-amerikanischer Eliteuniversitäten wie *Harvard*, *Stanford* oder dem *Massachusetts Institute of Technology (MIT)* legte den Grundstein für die hochfliegenden Erwartungen in ihr Potenzial, die Digitalisierung der Hochschullandschaft zu bereichern. Von dieser Hoffnung getragen, schossen zahlreiche (zumeist kommerzielle) MOOC-Anbieter wie Pilze aus dem Boden – insbesondere die Marktführer aus den USA: *Coursera*, *Udacity* und *edX*.[7] Sie stellen ihren universitären Kooperationspartnern Plattformen für deren Online-Kurse zur Verfügung. Bei Bedarf unterstützen sie diese auch bereits dabei, das digitale Bildungsangebot zu produzieren.[8] Viele Hochschulen erhoffen sich von dieser Symbiose nicht nur, ihre Präsenzlehre in attraktiver Form zu ergänzen (bzw. zu entlasten), sondern auch nie geahnte Studierendenzahlen aus aller Welt anzuziehen. Denn wer mit MOOCs auf der Bildungslandkarte präsent ist, hat Aussicht auf ein besseres internationales Profil und eine globale Sichtbarkeit.[9]

MOOCs ist ein emanzipatorisches Potenzial eigen. Beispielhaft hierfür steht die deutsche Initiative *Kiron Open Higher Education*. Sie hat ein Studienprogramm für Flüchtlinge entwickelt, welches auf MOOCs setzt.[10] Nach einem qualifizierten Online-Studium erkennen die Hochschulen, die mit *Kiron* kooperieren, die Studienleistungen als Äquivalent zum ersten Studienjahr an. Die *Kiron*-Studierenden können im Anschluss ihren Bachelor-Abschluss im Präsenzstudium erlangen.

Bei vielen Anbietern hat sich das Format der MOOCs von der ausschließlich kostenfreien digitalen Hochschulbildung unterdessen weiterentwickelt: Oftmals sind sie zu Bildungsplattformen mit entgeltpflichtigen Angeboten avanciert.[11] Die Anbieter werben nicht mehr nur mit Kurszertifikaten und vollständigen Studiengängen um ihre Nutzer. Sie

---

[6] Auslöser für diesen Hype war der MOOC „Einführung in die Künstliche Intelligenz" der Informatiker *Peter Norvig* und *Sebastian Thrun*. Er konnte rund 160.000 Teilnehmer und 20.000 Absolventen vorweisen. Vgl. *Jungermann/Wannemacher* (Fußn. 2), S. 4.

[7] Deutsche Anbieter sind etwa *iversity* oder *openHPI* des Hasso-Plattner-Instituts der Universität Potsdam.

[8] Vgl. *Hochschulrektorenkonferenz* (Fußn. 3), S. 22.

[9] *Porter* (Fußn. 2), S. 100.

[10] S. https://kiron.ngo/our-kiron-model/the-academic-model/.

[11] Als „Open" lassen sich die Kurse dann nur noch im Hinblick darauf bezeichnen, dass sie grundsätzlich jedermann offenstehen. Das impliziert aber nicht mehr notwendig, dass sie kostenfrei sind.

adressieren sie auch mit (im Vergleich zur herkömmlichen Hochschullehre) niederschwelligen Gebühren.[12] Der Wandel im Geschäftsmodell der Anbieter reagiert auch auf die hohen Abbrecherquoten und Erkenntnisse über die biografischen Hintergründe der Nutzer. Denn die Mehrheit der Nutzer verfügt bereits über einen ersten Hochschulabschluss oder steht sogar schon mit beiden Beinen fest im Berufsleben.[13] Daher fokussieren die Anbieter verstärkt die berufliche Weiterbildung und kooperieren immer häufiger mit privaten Unternehmen – vornehmlich aus der IT- und Telekommunikationsbranche. Teilweise integrieren Unternehmen MOOCs auch in ihre innerbetrieblichen Weiterbildungsprogramme oder entwickeln zusammen mit den Anbietern und Hochschulen neue Kursangebote. Gleichzeitig treten heutige MOOC-Anbieter nicht mehr nur als Plattformbetreiber für digitale Bildung auf, sondern auch als Arbeitsvermittler.

## 2. Bandbreite der erfassten MOOC-Nutzerdaten

Obgleich die anfängliche Euphorie um die MOOC-Technologie inzwischen etwas abgeklungen ist, steigen die Nutzerzahlen seit Jahren konstant an:[14] Die marktführenden Anbieter können weltweit zusammen auf über 100 Millionen Nutzer verweisen.[15] Auch die Datenbecken der Online-Kurse füllen sich unablässig. MOOCs spülen viele Informationen über die Teilnehmer der Bildungsangebote an. Bereits das Datenvolumen der ersten Kurse belief sich auf rund 20 Gigabyte bzw. mehrere Millionen Papierseiten.[16] Das generiert aussagekräftige Informationen über den Einzelnen, die noch vor wenigen Jahren kaum im selben Maße quantifizierbar gewesen wären.[17]

In den Datenstrom der MOOC-Anbieter fließen nicht nur die Informationen ein, die sie bereits bei der Anmeldung erheben – etwa der Name und die E-Mail-Adresse des Nutzers. Hinzu gesellen sich Angaben wie der höchste Bildungsabschluss oder der aktuelle Arbeitsplatz. Der Einzelne gibt sie regelmäßig gern preis, um den *Career Service* des Anbieters nutzen zu können. Vor allem aber erheben die Anbieter (u. a. durch *Tracking-Tools* wie *Google Analytics* oder den Einsatz sog. *Cookies*) vielfältige Daten über den gesamten Nutzungszeitraum des Online-Kursprogrammes hinweg. Sie erfahren dadurch nicht nur die exakten Anmeldezeiten, die besuchten Kurse oder die Inhalte von Forenbeiträgen. Sie wissen auch, wie häufig der

---

[12] So beziffern sich die Studienkosten für den Analytik-Master im Präsenzstudium am *Georgia Institute of Technology* auf mindestens 36.000 US-Dollar. Denselben Abschluss können Studierende online für unter 10.000 US-Dollar erwerben. S. *Brown*, Georgia Tech's Online Master of Science in Analytics Costs Under $10,000, engineering.com vom 12.1.2017.

[13] *Bischof/von Stuckrad*, Die digitale (R)evolution?, 2013, S. 51; *Schulmeister* (Fußn. 2), S. 26 f.

[14] Der Trend, vollständige MOOC-Studiengänge anzubieten, beflügelt jedoch die Erwartungen in einen neuen Hype der Bildungstechnologie. S. *Shah*, The Second Wave of MOOC Hype Is Here, and It's Online Degrees, EdSurge.com vom 21.5.2018.

[15] S. https://www.class-central.com/report/mooc-stats-2018/.

[16] *Ho/Reich et al.*, HarvardX and MITx: The First Year of Open Online Courses, 2014, S. 5.

[17] Zum Umfang dieser Datensammlungen vgl. eine Studie zum ersten MOOC des Anbieters *edX.* Für die Studie wertete ein Forscherteam alle 230 Millionen Interaktionen der über 150.000 Nutzer aus: *Breslow/Pritchard et al.*, Research & Practice in Assessment 2013, 13 (14 f.).

Angemeldete Kursmaterialien nutzt, welche Wissensstärken und -schwächen er aufweist oder mit welchem Ergebnis er ein Modul abgeschlossen hat.[18] Verknüpft der Nutzer sein MOOC-Profil mit seinem Account eines sozialen Netzwerks, etwa *Facebook*, kann der jeweilige Anbieter zusätzlich auf die dort vorhandenen Nutzerdaten zugreifen.

Jeden einzelnen Kursteilnehmer identifizieren zu können, liegt aus zahlreichen Gründen im legitimen Interesse des Anbieters (in Teilen auch des Nutzers): Er muss Daten bspw. dem Nutzer zuordnen können, um Abschlusszertifikate auszustellen. Die berufsbezogenen Daten benötigt er, um dem Nutzer ggf. einen Arbeitsplatz vermitteln zu können. Aber auch um das personalisierte Lernangebot stetig zu verbessern (d. h. zu individualisieren), besteht ein ökonomischer Anreiz, den Datenstaubsauger in so viele Ecken der Persönlichkeit ihrer Nutzer wie möglich vordringen zu lassen. So lassen sich Daten, die im Rahmen eines MOOCs anfallen, im Ergebnis überwiegend dem konkreten Nutzer zuordnen: Sie weisen einen Personenbezug auf.[19]

Um die verfügbaren Daten auszuwerten, setzen die Anbieter verschiedene Methoden algorithmischer Analyse ein. Bspw. verwendete der Anbieter *Coursera* über lange Zeit sog. *Keylogging*[20], um seine Nutzer authentifizieren zu können.[21] Wachsender Beliebtheit erfreut sich auch Gesichtserkennungssoftware: Sie ermöglicht es nicht nur, Personen zu identifizieren. Sie befähigt den Anbieter auch dazu, auf eine abnehmende Lernmotivation der Nutzer in Echtzeit zu reagieren.[22]

## II. Gefährdungsszenarien für die Privatheitsentfaltung

Kraft ihrer umfangreichen Datensammlungen bergen digitale Bildungsanwendungen nicht nur die Chance, mit ein wenigen Klicks niedrigschwellig hochwertiges Wissen im virtuellen Seminarraum zu erschließen. Sie reihen sich auch in das Phänomen einer ubiquitären Datenverarbeitung ein, die sich (jedenfalls zum Teil) als Gegenleistung der Nutzer für ein kostenloses oder -günstiges Angebot, im Extremfall aber als Spion, entpuppt. Im schlimmsten Fall sind die Studierenden dann nicht mehr die Kunden, sondern das Produkt.[23]

---

[18] *Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation* (Fußn. 3), S. 1; *O'Reilly/Veeramachaneni*, Research & Practice in Assessment 2014, 29 (29).
[19] Vgl. Art. 4 Nr. 1 DS-GVO.
[20] Dabei handelt es sich um ein technisches Verfahren, das einzelne Personen allein anhand ihres individuellen Tastaturtippmodus erkennt. Aus der individuellen Benutzung der Tasten lassen sich zugleich auch Erkenntnisse über die Tageslaune, die Müdigkeit oder andere persönlichkeitsrechtlich relevante Informationen sammeln.
[21] *Becker*, Ein Weltmarkt für Internet-Bildung, Telepolis vom 19.1.2014; *Michel*, Digitales Prüfen und Bewerten im Hochschulbereich, 2015, S. 23 f.
[22] Ein bekanntes Bsp. ist der Einsatz der Software *Nestor* an der *Paris School of Business* (*Toor*, This French school is using facial recognition to find out when students aren't paying attention, The Verge vom 26.5.2017). Weiterführend *Robal/Zhao et al.*, Webcam-based Attention Tracking in Online Learning: A Feasibility Study, in: Berkovsky (Hrsg.), Proceedings of the 23nd International Conference on Intelligent User Interfaces, March 7-11, 2018, S. 189.
[23] Vgl. https://bigbrotherawards.de/2017/bildung-lmu-tu-muenchen.

## 1. Datenweitergabe an Dritte

Besonders brisant sind MOOC-Angebote dann, wenn ihr Geschäftsmodell darauf zielt, die gesammelten Daten auch an Dritte (ggf. gegen Entgelt) weiterzugeben. In der Praxis geschieht dies keineswegs selten.[24]

Bei den Dritten handelt es sich in erster Linie um (potenzielle) Arbeitgeber der Nutzer sowie Hochschulen, die mit den Anbietern kooperieren. Während Letztere die Nutzerdaten hauptsächlich zu Forschungszwecken anonymisiert[25] auswerten,[26] wecken die Nutzerdaten bei den Personalabteilungen großer Konzerne im Zweifel andere Begehrlichkeiten: Sie möchten diese nutzen, um die besten Bewerber aus dem Datenpool herauszufischen.[27] Unter den Bedingungen eines teilweise verwaisten Arbeitsmarktes ist dies für viele geradezu unwiderstehlich attraktiv. Die Nutzerdaten eines MOOCs umfangreich analysieren zu können, ist jedenfalls längst keine Meisterleistung technischen Fortschritts mehr. Vielmehr ist es eine Frage des Wollens – und Dürfens, können moderne Analyse-Algorithmen doch unübersehbar große Datenhalden in Echtzeit auswerten. Dabei fördern sie mitunter Zusammenhänge und persönliche Eigenschaften zutage, die selbst dem Betroffenen gänzlich neu sind – oder eben auch Scheinkorrelationen, die Fehlschlüsse induzieren (Stichwort: Big Data)[28].[29] Nicht nur die konkret belegten Kurse und die Leistungsübersichten liefern Arbeitgebern wertvolle Informationen. Auch Daten über das individuelle Nutzungsverhalten der Kursteilnehmer sind für sie von Interesse, lässt dies doch tief in deren Persönlichkeit blicken: Wie viel Zeit benötigte ein Nutzer, um ein Modul zu absolvieren? Hat er oft neue Online-Kurse begonnen, ohne sie abzuschließen? Überdurchschnittliche Bearbeitungszeiten können etwa auf eine wenig stringente Arbeitsmotivation schließen lassen. Längere Unterbrechungen einzelner Kursbestandteile indizieren womöglich Erkrankungen oder eine Schwangerschaft, die ein Bewerber im Vorstellungsgespräch nicht mitgeteilt hat.[30] Interagiert ein Nutzer in den MOOC-Foren nur selten mit anderen Teilnehmern, könnte ein Personalverantwortlicher daraus folgern, dass der jeweilige Nutzer sich nicht gut in (digitale) Teams einfügt.

Die Problematik verschärft sich, wenn die massenhafte Datenaggregation mittels MOOC den Nutzern einer digitalen Bildungsanwendung verborgen bleibt. Studierende wähnen sich dann

---

[24] *Becker* (Fußn. 21); *Boie/Grassegger*, Der gläserne Student, Süddeutsche Zeitung Online vom 2.12.2015.
[25] (Ehemals) personenbezogene Daten sind erfolgreich anonymisiert, wenn sie dauerhaft keiner konkreten Person mehr zuordenbar sind. Vgl. für technische Anonymisierungslösungen *Martini/Botta*, NZA 2018, 625 (630).
[26] Personenbezogene Daten verarbeiten die Hochschulen jedoch, wenn sie in den MOOCs erbrachte Leistungen als eigene Studienleistungen anerkennen.
[27] *Thiel*, Entmündigung als Bildungsziel, FAZ online vom 14.7.2016.
[28] Big Data steht als Trendbegriff für die Möglichkeit, immer größere Datenmengen mit Hilfe komplexer Analyse-Algorithmen und schneller Rechner auszuwerten. S. dazu ausführlich *Martini*, DVBl 2014, 1481 (1482).
[29] Big-Data-Analysen sind im Grundsatz nichts weiter als Ausdruck statistischer Methoden und algorithmischer Vergleichsgruppenbildung, die darauf programmiert sind, aus vorhandenen Datenmassen Schlüsse zu ziehen. Fehlschlüsse oder Ergebnisse, die an Spekulation grenzen, sind darin eingeschlossen. Zu den Gefahren einer Diskriminierung durch Algorithmen weiterführend *Martini*, JZ 2017, 1017 (1018 f.).
[30] Auf Fragen nach der Schwangerschaft braucht eine Bewerberin nach deutschem Recht nicht zu antworten.

der vermeintlichen Privatheit der eigenen vier Wände oder der Anonymität eines belebten Cafés sicher. In Wahrheit finden sie sich womöglich in einem panoptischen Hörsaal wieder. Es entsteht eine digital ausgeleuchtete Lernumgebung, die keinen Schritt unbeobachtet lässt.

### 2. Datentransfers in die USA

Die Nutzerdaten – etwa der Münchner Studierenden – speichern und verarbeiten US-amerikanische MOOC-Plattformen typischerweise jenseits des Atlantiks – also außerhalb der physischen Einflusssphäre der Europäischen Union.[31] Die Datenverarbeitung in den USA und insbesondere auch die Datenweitergabe an dort ansässige Private oder Behörden kann im Extremfall weitreichende Folgen für den Einzelnen nach sich ziehen. Zugespitzt formuliert, rufen die Risiken die Frage auf den Plan: Muss derjenige, der mithilfe eines MOOC die arabische Sprache erlernen will, womöglich bald damit rechnen, auf Schwierigkeiten bei der Einreise in die USA zu stoßen?[32]

US-amerikanische Behörden haben private Unternehmen in der Vergangenheit immer wieder dazu gedrängt, Nutzerdaten selbst dann herauszugeben, wenn sie diese auf europäischen Servern speichern. Paradigmatisch steht dafür der Konflikt zwischen *Microsoft* und der US-Regierung darüber, ob das IT-Unternehmen Daten eines *Outlook*-Nutzers von einem irischen Server an US-Sicherheitsbehörden übermitteln muss.[33] Der *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act)[34] erleichtert den US-amerikanischen Behörden unterdessen sogar, an Daten zu gelangen, die auf europäischen Servern gespeichert sind.[35] Zudem planen die Europäische Kommission und die US-Regierung ein Abkommen über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle Zusammenarbeit in Strafsachen.[36]

## III. Grenzüberschreitender Datenverkehr als Herausforderung für den Privatheitsschutz

Den grenzüberschreitenden Datenverkehr setzen die Art. 44 ff. DS-GVO einem strengen Rechtsregime aus.[37] Sie errichten gleichsam einen unionalen Deich gegen privatheitsgefährdende Sturmwellen in Zeiten transnationaler Datenströme. Sensible Informationstanker dürfen nicht mehr ohne Weiteres unsichere Häfen ansteuern.

---

[31] S. die Ausführungen unter *International Privacy Practices* bzw. *International Users* in den Datenschutzerklärungen von *Coursera* und *Udacity*: https://www.coursera.org/about/privacy; https://www.udacity.com/legal/privacy.

[32] Diese Sorge formulierte zumindest die Datenschutzbeauftragte des Landes Schleswig-Holstein *Marit Hansen*; nachzulesen bei *Baars/Grassegger*, Massig Daten von Studenten, tagesschau.de vom 7.12.2015.

[33] *Gausling*, MMR 2018, 578 (579); *Pauly/Dieckhoff*, CCZ 2017, 270 (270 ff.).

[34] 18 U.S.C. § 2523.

[35] *Determann/Nebel*, CR 2018, 408 (409 f.); *Spies*, ZD-Aktuell 2018, 04291.

[36] S. den Beschluss des Rats der Europäischen Union vom 21.5.2019, Ratsdokument 9114/19, https://data.consilium.europa.eu/doc/document/ST-9114-2019-INIT/de/pdf.

[37] Zuvor waren diese Schutzmechanismen in den §§ 4b und 4c BDSG a. F. geregelt. Sie setzten Art. 25 und 26 der Richtlinie 95/46/EG (DS-RL) in nationales Recht um.

## 1. Anwendbarkeit der Art. 44 ff. DS-GVO auf transatlantische Datentransfers

### a) Räumlicher Anwendungsbereich: Marktortprinzip (Art. 3 Abs. 2 lit. a DS-GVO)

Warum die DS-GVO auf MOOC-Anbieter überhaupt anwendbar sein sollte, erschließt sich nicht auf den ersten Blick. Denn *Coursera* & Co. haben ihren Sitz oftmals in den USA. Das *Marktortprinzip* des Art. 3 Abs. 2 lit. a DS-GVO erweitert jedoch nunmehr den normativen Radius des unionsrechtlichen Datenschutzes: An die Regelungen der DS-GVO sind nicht nur diejenigen Verarbeitenden gebunden, die ihren *Sitz* in der Union haben. Ihrem Regelungsanspruch unterliegt vielmehr jeder, der erkennbar beabsichtigt, Unionsbürgern *Dienstleistungen anzubieten* – seien diese kostenlos oder nicht (EG 23 Satz 2 DS-GVO).[38] Auf den Ort der Niederlassung kommt es also nicht (mehr) an.

Ob der Verantwortliche seine Dienstleistung tatsächlich i. S. d. Art. 3 Abs. 2 lit. a DS-GVO in der EU anbieten möchte, bestimmt sich danach, wie das Angebot inhaltlich ausgestaltet ist, z. B. welche Sprache zum Einsatz kommt oder welche Währung gilt (EG 23 Satz 3 DS-GVO).

Zahlreiche außereuropäische Anbieter sprechen mit ihren digitalen Bildungsangeboten, insbesondere durch Kooperationen mit deutschen Hochschulen, explizit auch hiesige Studierende an.

### b) Grenzüberschreitende Datenübermittlung

Auch wenn die DS-GVO mit Hilfe des Marktortprinzips die transatlantische Verarbeitung der Nutzerdaten als datenschutzrechtlicher Ordnungsrahmen steuert: Die Art. 44 ff. DS-GVO unterwerfen Datenverkehr ihrem Regime nur, wenn die Verantwortlichen Daten grenzüberschreitend[39] „übermitteln“. Je nachdem wie man den interpretationsoffenen Begriff der Datenübermittlung versteht, fällt die Verarbeitung durch MOOC-Anbieter darunter oder nicht.

Um ein Datum im natürlichen Wortsinne „übermitteln“ zu können, bedarf es jedenfalls einer (zweiten) Person, die sich vom Übermittelnden unterscheidet. Der Begriff insinuiert, dass er sich auf Szenarien beschränkt, in denen ein Verantwortlicher Daten *an Dritte außerhalb der EU* überträgt. Ein US-amerikanischer Kursanbieter, der die Daten europäischer Nutzer *direkt*

---

[38] Dies hatte die *Artikel-29-Datenschutzgruppe*, Stellungnahme 01/2012 zu den Reformvorschlägen im Bereich des Datenschutzes, WP 191, 2012, S. 10 ausdrücklich gefordert.

[39] Grenzüberschreitender Datenverkehr ist in zwei Varianten denkbar: Innerhalb und außerhalb des datenschutzrechtlichen Binnenraums der Union. *Innerhalb* der EU gewährleistet die DS-GVO ein einheitliches Datenschutzniveau. Gesonderte Regelungen für einen grenzüberschreitenden Datenverkehr sind deshalb nicht erforderlich. Wenn bspw. ein zypriotisches Unternehmen personenbezogene Daten deutscher Nutzer in einem französischen Rechenzentrum verarbeitet, geben mithin die allgemeinen Bestimmungen der DS-GVO den Rechtsrahmen vor. Anders verhält es sich mit einer Datenübermittlung an sog. *Drittländer*. Fließen Daten – wie im Fall der Münchner Universitäten – an die USA, unterstellt die DS-GVO nicht von vornherein, dass dort ein gleichwertiges Schutzniveau herrscht. Sie knüpft eine rechtskonforme Übermittlung vielmehr an die spezifischen Zulässigkeitsvoraussetzungen der Art. 44 ff. DS-GVO.

erhebt und ausschließlich selbst verarbeitet, könnte dann das Regelungsregime der Art. 44 ff. DS-GVO ignorieren.

In diese Richtung deutet prima facie auch die Begriffsbestimmung des Art. 4 Nr. 2 DS-GVO: Er benennt die „Offenlegung durch Übermittlung" explizit als einen Unterfall der Datenverarbeitung. „Offenlegen" setzt semantisch einen Empfänger, also einen Dritten, voraus.

In Art. 44 selbst spricht die DS-GVO dann zwar wieder nur von „übermitteln", gerade nicht auch von „offenlegen". Das heißt aber noch nicht zwingend, dass die DS-GVO in Art. 44 (anders als in Art. 4 Nr. 2) ein „Übermitteln" ohne „offenlegen" genügen lässt. Denn auch an anderer Stelle verwendet sie Begriffe aus Art. 4 DS-GVO, ohne ihnen eine neue Bedeutung zuzuschreiben.[40]

Immerhin unterscheidet die englische Sprachversion klar zwischen „transmission" (Art. 4 Nr. 2 DS-GVO) und „transfer" bzw. „transfert(s)" (Art. 44 ff. DS-GVO). Sie insinuiert damit, dass sie einen anderen Übermittlungsbegriff als Art. 4 Nr. 2 DS-GVO verwendet. Auch der EuGH hat aus den Vorgängerregelungen der Art. 44 ff. DS-GVO (namentlich Art. 25 und 26 Datenschutz-Richtlinie 95/46/EG [DS-RL]) einen *eigenständigen* Übermittlungsbegriff herausgelesen – statt auf die (mit Art. 4 Nr. 2 DS-GVO vergleichbare) Definition des Art. 2 lit. b DS-RL zu rekurrieren.[41]

„Übermitteln" in Art. 44 DS-GVO nicht auf eine Dreieckskonstellation zu beschränken, entspricht auch der Zielrichtung des V. Kapitels: Es soll generell verhindern, dass sich in Drittstaaten das unionale Datenschutzniveau untergraben lässt (Art. 44 Satz 2, EG 101 Satz 3 DS-GVO). Für die Gefahrenlage, der die Art. 44 ff. DS-GVO entgegentreten sollen, macht es aber keinen Unterschied, ob der exterritoriale Verantwortliche die Daten an Dritte außerhalb der EU überträgt oder sie dort selbst verarbeitet. Konsequenterweise sprechen die Art. 44 ff. DS-GVO auch nicht von der Übermittlung an *eine Person*, sondern *„an ein Drittland"*. Entscheidend ist also, dass Daten die EU verlassen, nicht hingegen, in welchem Kontext dies geschieht oder dass die Daten einen Dritten erreichen. Der Begriff der Datenübermittlung in den Art. 44 ff. DS-GVO bedarf daher im Ergebnis einer weiten Lesart: Er umfasst jede grenzüberschreitende Datenverarbeitung, bei der personenbezogene Daten das Unionsgebiet verlassen.[42]

---

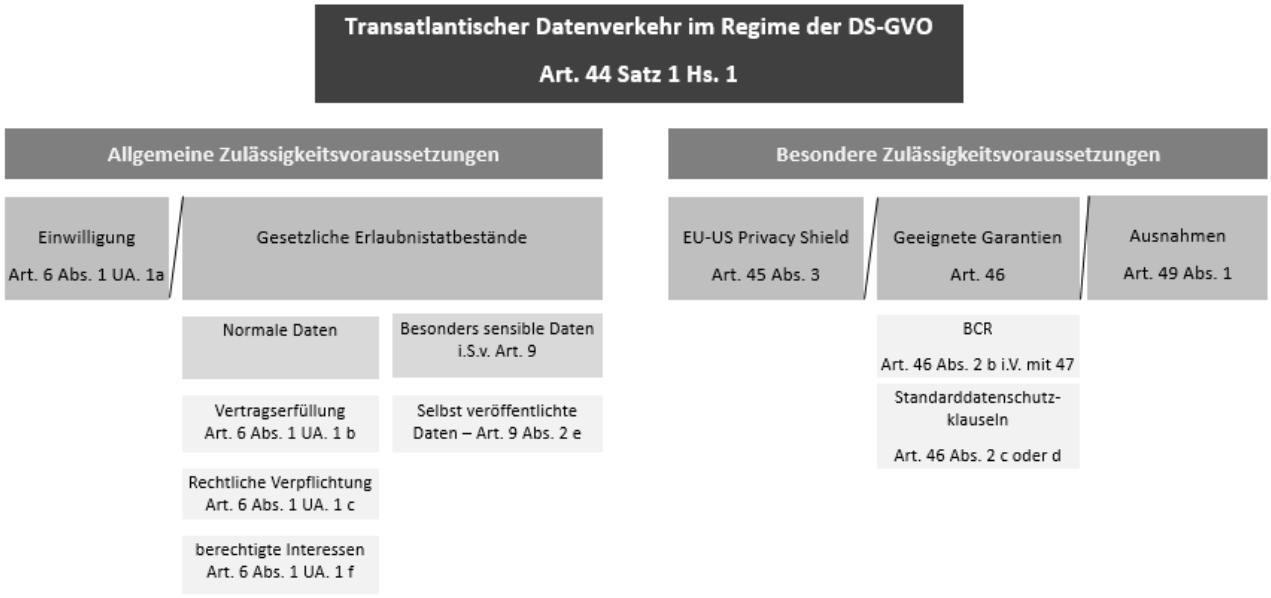
[40] Bspw. den Begriff der Pseudonymisierung in Art. 25 Abs. 1 DS-GVO oder den des Unternehmens in Art. 83 Abs. 4 DS-GVO.

[41] EuGH, Urteil vom 6.11.2003, ECLI:EU:C:2003:596, Rdnr. 56 f. – Lindqvist.

[42] Vgl. ebenso *Schantz/Wolff*, Das neue Datenschutzrecht, 2017, Rdnr. 757; *Zerdick*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2. Aufl., 2018, Art. 44 Rdnr. 7; a. A. *Pauly*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 44 DSGVO Rdnr. 4, welcher die Datenübermittlung nur als Offenlegung versteht.

### c) Normatives Prüfprogramm der Art. 44 ff. DS-GVO

Wenn ein MOOC-Anbieter die personenbezogenen Daten seiner Kursteilnehmer in ein Drittland übermitteln möchte, muss er die *besonderen „Bedingungen"*[43] der Art. 45 ff. DS-GVO einhalten (Art. 44 Satz 1 Hs. 1 DS-GVO; III. 3.): Diese müssen ein angemessenes Datenschutzniveau im Drittland sicherstellen (Art. 44 Satz 2 DS-GVO), um den Kontrollverlust des Unionsgesetzgebers bei außereuropäischen Datentransfers zu kompensieren – aber nicht nur dies: Nach dem ausdrücklichen Willen des Unionsgesetzgebers muss der Anbieter zusätzlich die *allgemeinen datenschutzrechtlichen Verarbeitungsvoraussetzungen* erfüllen, die das Fundament einer jeden Datenverarbeitung bilden (namentlich „auch die sonstigen Bestimmungen dieser Verordnung ein[…]halten"; Art. 44 Satz 1 Hs. 1 DS-GVO; III. 2.). Liegt etwa schon kein Erlaubnistatbestand i. S. d. Art. 6 Abs. 1 UAbs. 1 DS-GVO vor, ist die Verarbeitung unabhängig vom Datenschutzniveau im Drittland unzulässig. Die Art. 44 ff. DS-GVO gleichen mithin keine Defizite bei den allgemeinen Datenschutzanforderungen aus. Vielmehr sollen sie zusätzlich verbürgen, dass die Wertungen der DS-GVO ihre Schutzwirkung für natürliche Personen auch in Drittländern realiter wirkungsvoll entfalten (vgl. Art. 44 Satz 2 DS-GVO; EG 101 Satz 3 DS-GVO). Darin manifestiert sich das ausgeprägte Misstrauen des Unionsgesetzgebers gegenüber dem Datenschutzniveau in Drittländern. Er weiß dieses nur besänftigt, wenn der Verarbeitende die materiellen Verarbeitungsvoraussetzungen der DS-GVO einhält und die Gleichwertigkeit der Datenverarbeitung auf der Grundlage der Art. 44 ff. DS-GVO gesichert ist.




[43] Hervorbebung d. Verf.

## 2. Allgemeine datenschutzrechtliche Zulässigkeitsvoraussetzungen

Kraft des zweistufigen Anforderungsprogramms des Art. 44 DS-GVO sind Datenübermittlungen der MOOC-Anbieter aus der Union heraus nur zulässig, wenn die Anbieter ihr Handeln entweder auf eine Einwilligung (a) oder eine gesetzliche Verarbeitungserlaubnis (b) gründen können (Art. 6 Abs. 1 DS-GVO).

### a) Einwilligung (Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO)

Populäre US-amerikanische MOOC-Anbieter stützen ihre Datenverarbeitung – einschließlich der Datenweitergabe an Dritte in den USA – nach eigenen Angaben regelmäßig auf die Einwilligung ihrer Nutzer.[44] Auch in der dogmatischen Konzeption der DS-GVO ist die Einwilligung der Königsweg zur zulässigen Verarbeitung:[45] Sie gilt ihr als unmittelbarster Ausdruck der Autonomie des Einzelnen.

#### aa) Einwilligungserklärung (Art. 4 Nr. 11 DS-GVO)

Eine Einwilligung kann zwar auch durch eine konkludente Erklärung erfolgen (Art. 4 Nr. 11 DS-GVO). Es reicht jedoch weder zu schweigen noch einen Dienst faktisch zu nutzen.[46] Auch ein reines Opt-out genügt nicht – ebenso wenig, dass der Nutzer lediglich angibt, die Datenschutzerklärung gelesen zu haben.[47] Erforderlich ist vielmehr, dass er eine eindeutige bestätigende Handlung (Art. 4 Nr. 11; vgl. auch EG 32 Satz 3 DS-GVO) vornimmt,[48] also bspw. per Mausklick aktiv der Datenschutzerklärung des Anbieters zustimmt.

#### bb) Bestimmtheit und Informiertheit (Art. 4 Nr. 11, Art. 5 Abs. 1 lit. b, Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO)

Damit eine Einwilligung wirksam ist, muss der Nutzer sie in informierter Weise für einen bestimmten Verarbeitungszweck[49] erklären (Art. 4 Nr. 11, Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO). Dazu gehört auch die Aufklärung darüber, ob der Verarbeitende die Daten an Dritte weitergibt, sowie, dass er Daten in die USA überträgt.

---

[44] S. bspw. die Ausführungen unter *International Users* in der Datenschutzerklärung des Anbieters *Udacity*: https://www.udacity.com/legal/privacy.

[45] *Albrecht*, CR 2016, 88 (91). Dennoch steht die Einwilligung keineswegs als höherrangiger Erlaubnistatbestand über den gesetzlichen Verarbeitungsgrundlagen; s. hierzu auch Fußn. 87.

[46] Bis zur Geltung der DS-GVO sahen zahlreiche MOOC-Anbieter die Einwilligung bereits dann als erteilt an, wenn sich ein Nutzer rein faktisch dazu entschloss, ihre Website zu nutzen. S. die seinerzeitige Datenschutzerklärung des Anbieters *Coursera* (https://www.coursera.org/about/privacy) im Vergleich mit ihrem Stand vor Geltung der DS-GVO (https://www.diffchecker.com/NcyXrhIL).

[47] Vgl. KG Berlin, Urteil vom 21.3.2019, Az. 23 U 268/13 (*nicht rechtskräftig*).

[48] Vgl. *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, 2017, Teil 3 Rdnr. 39.

[49] Das impliziert, dass der Anbieter den konkreten Zweck der Datenverarbeitung – die grenzüberschreitende Übermittlung und Weitergabe der Nutzerdaten an Dritte in einem Drittstaat – klar benennt. Dies muss so präzise wie möglich zum Zeitpunkt der Einwilligung erfolgen, um die normativ gebotene Zweckbindung der Datenverarbeitung (Art. 5 Abs. 1 lit. b Hs. 1 DS-GVO) sicherzustellen.

Zahlreiche MOOC-Anbieter geben Nutzerdaten an Private („*Business Partners*“ und „*Service Providers*“) oder staatliche Stellen weiter, die ebenfalls in den USA sitzen. In ihren Datenschutzerklärungen weisen sie dies auch durchaus ausdrücklich aus.[50] Die bloße *Möglichkeit*, dass Daten an Dritte fließen, bleibt aus der Sicht des Nutzers aber (zu) unspezifisch. Schließlich weiß er nicht, in wessen Hände seine Daten letztlich strömen. Insbesondere bleibt er im Unklaren darüber, ob seine Informationen lediglich anonymisiert an eine Evaluationsagentur fließen oder etwa an die *National Security Agency* (NSA) und er deshalb mit staatlichen Maßnahmen in Berührung kommen kann. Wer sich in seinen Studien etwa besonders für die Geschichte des Nahen Ostens interessiert, eine Huldigung über *Julian Assange* eingereicht hat oder in einem Forumsbeitrag eine kritische Einschätzung zur Einwanderungspolitik der USA veröffentlicht, muss dann im schlimmsten Fall damit rechnen, vor oder bei der nächsten Einreise in die USA auf Schwierigkeiten zu stoßen.

Nach Maßgabe des Art. 13 Abs. 1 lit. e DS-GVO kommt der Verantwortliche seiner Informationspflicht zwar im Grundsatz bereits dann hinreichend nach, wenn er lediglich Empfänger*kategorien* nennt. Diese Vorschrift adressiert jedoch nur *allgemeine gesetzliche* Informationspflichten, beschreibt aber nicht den erforderlichen Inhalt einer informierten *Einwilligung*. Diese hat so konkret wie möglich zu erfolgen (vgl. insbesondere EG 32 Satz 5, EG 33 S. 1 [e contrario], EG 42 Satz 2 und 4 DS-GVO).

Aus dem Geschäftsmodell des Anbieters ergeben sich – trotz aller Flexibilität, die sein Betrieb und Einwilligungsmanagement benötigen – zahlreiche für ihn absehbare Empfänger, bspw. die spezifischen Unternehmen und Hochschulen, die mit ihm kooperieren. Nennt er also trotz besseren Wissens nur abstrakte Empfängerkategorien (wie „Dienstleister“ oder „Geschäftspartner“), ist der Betroffene nicht ausreichend informiert und die Einwilligung damit nicht wirksam.

Soweit zum Einwilligungszeitpunkt noch nicht absehbar ist, wer die konkreten Empfänger der Nutzerdaten sind, reicht es aber aus, wenn sich der Anbieter darauf beschränkt, potenzielle Empfängergruppen zu nennen; die spätere Datenweitergabe muss sich dann jedoch tatsächlich auf Personen beschränken, die einer solchen Gruppe angehören.[51]

### cc) Einwilligungsfähigkeit minderjähriger Nutzer (Art. 8 Abs. 1 DS-GVO)

Seit einige Landesgesetzgeber die Schulzeit verkürzt haben, sind in Deutschland immer mehr Studienanfänger unter 18 Jahre alt. Ihrer besonderen Schutzbedürftigkeit trägt die DS-GVO

[50] S. etwa die Datenschutzerklärung des Anbieters *Udacity*: „With your consent, Udacity may share information that can be used to directly contact you with third party business partners, such as companies that may be offering products or services or other opportunities that may be of interest to you”; nachzulesen unter: https://www.udacity.com/legal/privacy.
[51] Vgl. *Bäcker*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 13 DSGVO Rdnr. 30; *Franck*, in: Gola (Hrsg.), DS-GVO, 2. Aufl., 2018, Art. 13 Rdnr. 17.

(anders als die DS-RL) ausdrücklich Rechnung: Sie etabliert eine konkrete Schutzvorschrift, die ihre Einwilligungsfähigkeit sichert (Art. 8 DS-GVO).[52]

Ob ein Minderjähriger dazu fähig ist, wirksam in eine Datenverarbeitung einzuwilligen, knüpft sie bei einem *direkten Angebot* eines *Dienstes der Informationsgesellschaft* daran, ob er sein sechzehntes Lebensjahr bereits vollendet hat – anderenfalls müssen seine Eltern eingewilligt oder zumindest der Einwilligung des Minderjährigen im Voraus zugestimmt haben (Art. 8 Abs. 1 Satz 1 und 2 DS-GVO).[53]

Ein MOOC ist zwar ein Dienst der Informationsgesellschaft.[54] Er adressiert sein Angebot in seiner bisherigen Bauart regelmäßig aber nicht *direkt* an Minderjährige. „Direkt" ist nämlich nicht i. S. v. „unmittelbar", sondern vielmehr von „*speziell*" bzw. „*gezielt*" zu verstehen.[55] MOOCs bisheriger Bauart zielen in erster Linie auf Volljährige, insbesondere Hochschulabsolventen oder Berufstätige – nicht minderjährige Studienanfänger. MOOC-Anbietern erwachsen aus Art. 8 Abs. 1 DS-GVO daher i. d. R. keine besonderen Pflichten, wenn Minderjährige sich online (fort)bilden. Die Kursanbieter schulden insofern grundsätzlich auch keine kindgerechte Information (vgl. EG 58 Satz 4 DS-GVO).[56] Etwas anderes gilt jedoch, wenn sie bspw. gezielt Schüler als Nutzer werben.[57]

---

[52] *Kühling/Martini*, EuZW 2016, 448 (451).

[53] Vgl. *Martini/Nink*, NVwZ-Extra 10/2017, 1 (6).

[54] Unter dem Begriff „Dienste der Informationsgesellschaft" versteht die DS-GVO „jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung" (Art. 4 Nr. 25 i.V. mit Art. 1 Abs. 1 lit. b Richtlinie [EU] 2015/1535). MOOCs sind zwar oftmals (noch) kostenfrei nutzbar. Der Begriff „Dienste der Informationsgesellschaft" umschließt jedoch auch Konstellationen, in denen der Nutzer für eine digitale Anwendung nicht selbst bezahlt, sondern der Anbieter sich durch Werbeanzeigen auf seiner Website finanziert (vgl. EuGH, Urteil vom 11.9.2014, ECLI:EU:C:2014:2209, Rdnr. 27 ff. – Papasavvas; Urteil vom 15.9.2016, ECLI:EU:C:2016:689, Rdnr. 41 f. – Mc Fadden). Diese Rechtsprechung lässt sich auf unentgeltliche Online-Kurse übertragen, bei denen der Anbieter wirtschaftlich davon profitiert, dass er die Nutzerdaten verwertet (vgl. *Schumacher*, K&R 2015, 771 [776]).

[55] Der MOOC-Anbieter müsste sein Bildungsangebot demnach *gezielt an Minderjährige richten*. Dafür kommt es auf den objektiven Empfängerhorizont an (*Funke*, Dogmatik und Voraussetzungen der datenschutzrechtlichen Einwilligung im Zivilrecht, 2017, S. 199 f.). Ob der Anbieter einseitig erklärt hat, dass Minderjährige den MOOC nicht nutzen dürfen, ist daher unerheblich. Anhaltspunkte können stattdessen sein, dass das Unternehmen sich einer kind- oder jugendgerechten Sprache oder Website-Gestaltung bedient (BGH, Urteil vom 18.9.2014, NJW 2015, 485 [488] mit Rdnr. 27). Ebenso *Funke* a.a.O., S. 211 f.; *Gola/Schulz*, ZD 2013, 475 (477 f.); *Joachim*, ZD 2017, 414 (416); *Schantz/Wolff* (Fußn. 42), Rdnr. 480 f.; vgl. auch *Artikel-29-Datenschutzgruppe*, Guidelines on Consent under Regulation 2016/679, WP 259, 2017, S. 24; a. A. *Buchner/Kühling*, in: dies. (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 8 DSGVO Rdnr. 18; *Heberlein*, Datenschutz im Social Web, 2017, S. 195 f.; wohl auch *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), DatenschutzR, 2019, Art. 8 Rdnr. 14 f.

[56] Vgl. *Martini/Nink* (Fußn. 53), S. 6.

[57] Ein Beispiel hierfür ist der Anbieter *openHPI*, der sich explizit mit seinen Online-Kursen wie „Spielend Programmieren lernen" oder „Wie designe ich meine eigene Homepage?" an Minderjährige richtet: https://open.hpi.de/courses?category=openHPI%20Junior.

### dd) Freiwilligkeit (Art. 7 Abs. 4 DS-GVO)

#### (1) Kopplungsverbot – Erforderlichkeit der Datenweitergabe für die Vertragserfüllung

Die DS-GVO gibt dem Anbieter mit dem Instrument der Einwilligung keine Carte blanche an die Hand. Er darf seinen Nutzern insbesondere keine Globaleinwilligung abringen, mit der diese gebündelt in disparate Verarbeitungsvorgänge zu den verschiedensten Zwecken einwilligen (EG 43 Satz 2 Hs. 1 DS-GVO, *horizontales Kopplungsverbot*).[58] Dem Nutzer muss vielmehr grundsätzlich die Möglichkeit offenstehen, in die Datenverarbeitung zu Zwecken der Online-Kursnutzung und der internationalen Datenweitergabe an Dritte gesondert einzuwilligen.

Der Anbieter darf seine Vertragserfüllung auch nicht von einer Einwilligung in die Verarbeitung von Daten abhängig machen, die zu diesem Zweck gar nicht erforderlich sind (*vertikales Kopplungsverbot*; Art. 7 Abs. 4 DS-GVO, EG 43 Satz 2 Hs. 2).[59] Das Kriterium der Erforderlichkeit meint dabei keine grundrechtliche Verhältnismäßigkeitsprüfung. Es gleicht vielmehr die Einwilligung mit dem vereinbarten Vertragsinhalt ab:[60] Der Verantwortliche darf seine eigene vertragliche Leistung grundsätzlich[61] nicht davon abhängig machen, dass der Betroffene ihm noch zusätzlich eine Einwilligung für eine Verarbeitung erteilt, die gar nicht erforderlich ist, um seinen Vertrag zu erfüllen. Im Falle von MOOCs kommt es dann darauf an, inwieweit eine Einwilligung in die grenzüberschreitende Datenübermittlung bzw. eine Datenweitergabe an Dritte in den USA notwendig ist, um den vertraglichen Pflichten im Verhältnis zwischen Anbieter und Nutzer[62] nachzukommen.

Bei *entgeltpflichtigen* Online-Kursen richtet sich der Vertrag vornehmlich auf zweierlei: Der Anbieter macht seine Kurse zugänglich und stellt am Ende ein Zertifikat aus, der Nutzer vergütet die Leistung vereinbarungsgemäß. Nutzerdaten grenzüberschreitend zu übermitteln, ist in diesem Fall Teil des vertraglichen Pflichtenhefts, wenn der Anbieter seinen Sitz in den USA hat und dort nötige Verarbeitungen etwa des Namens, der Kursdaten und der Leistungen

---

[58] *Krohm/Müller-Peltzer*, ZD 2017, 551 (552).

[59] Bei genauerem Hinsehen offenbart sich indes ein Widerspruch zwischen dem Norminhalt und den Erwägungsgründen: Während Art. 7 Abs. 4 DS-GVO den Erforderlichkeitszusammenhang nur »in größtmöglichem Umfang« berücksichtigen will, sieht EG 43 Satz 2 DS-GVO schon gar keine Freiwilligkeit (»gilt als nicht freiwillig erteilt«), wenn der Verantwortliche einen unzulässigen Konnex herstellt. Bei Widersprüchen geht der verfügende Teil der Verordnung vor: Erwägungsgründe haben keine normative Wirkung. Sie dienen lediglich als Auslegungshilfe (vgl. EuGH, Urteil vom 13.7.1989, ECLI:EU:C:1989:331, Rdnr. 31 – Casa Fleischhandel). Im Ergebnis formuliert Art. 7 Abs. 4 DS-GVO deshalb kein absolutes Kopplungsverbot.

[60] Das Kopplungsverbot des Art. 7 Abs. 4 DS-GVO greift also, wenn der Verantwortliche den Geltungsradius des gesetzlichen Erlaubnistatbestands der Vertragserfüllung (Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO) überschreitet. Dieser setzt voraus, dass die Datenverarbeitung erforderlich sein muss, um den Vertrag zwischen Verarbeitendem und Betroffenem zu erfüllen; s. hierzu III. 2. b) aa).

[61] Die DS-GVO schließt die Freiwilligkeit einer Einwilligung in dieser Situation zwar nicht kategorisch aus. Sie stellt sie jedoch auf einen besonders kritischen Prüfstand.

[62] Zwischen Anbieter und Nutzer eines MOOC besteht regelmäßig ein schuldrechtliches Vertragsverhältnis mit miet-, dienst- und werkvertragsrechtlichen Elementen. Vgl. KG Berlin, Urteil vom 31.5.2017, ZD 2017, 386 (387) mit Rdnr. 56; *Bräutigam*, MMR 2012, 635 (636).

vornimmt. Die Daten *an Dritte* weiterzugeben, gehört hingegen grundsätzlich nicht zu den Vertragspflichten des Anbieters.

Bei *kostenfreien* MOOCs „bezahlt" der Nutzer den Kurs auch dadurch, dass er dem Anbieter erlaubt, seine personenbezogenen Daten zu verarbeiten: Das Geschäftsmodell heißt dann „Bildung gegen Daten" (die unter Umständen auch an Dritte gehen). Die DS-GVO verschließt sich einer solchen Kommerzialisierung der eigenen Daten nicht absolut.[63] Daten als Teil dieses Geschäftsmodells Dritten weiterzureichen, mag dann von den Vertragsklauseln *gedeckt* sein. Sie ist aber auch in einem Bildung-gegen-Daten-Modell „nicht *erforderlich*[64]" im Sinne des Art. 7 Abs. 4 DS-GVO, um vertragliche Pflichten gegenüber dem Nutzer zu erfüllen (vgl. auch die Formulierung des Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO: „Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist"). Ein solches Vertragsverhältnis gestattet dem Kursanbieter mithin keine unbegrenzten Verwertungsrechte an den Nutzerdaten. In eine Datenweitergabe an US-amerikanische Dritte muss der Nutzer deswegen stets explizit und aufgrund klar erkennbaren Hinweises einwilligen, wenn sie freiwillig und damit zulässig sein soll. Der Verantwortliche darf dem Nutzer nicht verschleiern, dass er mit seinen Daten für die erbrachten Dienstleistungen „bezahlt".[65] Sonst erschleicht er sich in den Augen des Art. 7 Abs. 4 DS-GVO eine Einwilligung, die nur scheinbar von dem freien Willen des Nutzers getragen ist. Insoweit erweist sich Art. 7 Abs. 4 DS-GVO auch als Transparenzgebot für den Verantwortlichen.[66]

### (2) Ungleichgewicht zwischen MOOC-Nutzer und Verantwortlichem

Freiwillig ist eine Einwilligung ihrem Wesen nach nur, wenn der Erklärende *echte Wahlfreiheit* genießt (EG 42 Satz 5 DS-GVO). Daran fehlt es, wenn er sie in einer faktischen Zwangssituation – insbesondere einem Abhängigkeitsverhältnis – gegenüber dem Verantwortlichen abgibt (EG 43 Satz 1 DS-GVO).[67]

Zwisch*en dem verantwortlichen MOOC-Anbieter und den studentischen Nutzern* besteht kein greifbares Machtungleichgewicht.[68] Eine Zwangssituation kann sich allenfalls *zwischen der Hochschule und ihren Studierenden* manifestieren – etwa, wenn Letztere Online-Kurse als Teil

---

[63] A. A. *Golland*, MMR 2018, 130 (131 f.). Will der Verantwortliche sich für eine Datenweitergabe an Dritte eine Einwilligung einholen, verlangt der Unionsgesetzgeber ihm daher – entgegen teilweise vertretener Auffassung; s. *Ernst*, ZD 2017, 110 (112); *Golland,* a.a.O., S. 133 f.; *Krohm/Müller-Peltzer* (Fußn. 58), S. 553 – nicht zwingend ab, eine (kostenpflichtige) Alternative vorzuhalten, in der seine Daten nicht im selben Umfang an Dritte fließen. Dafür hat das Berücksichtigungsgebot des Art. 7 Abs. 4 zu wenig Bisskraft; vielmehr hätte es einer klareren Formulierung bedurft; ebenso *Schantz/Wolff* (Fußn. 42), Rdnr. 515 f.

[64] Hervorhebung d. Verf.

[65] *Buchner/Kühling*, in: dies. (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 7 DSGVO Rdnr. 51; *Schulz*, in: Gola (Hrsg.), DS-GVO, 2. Aufl., 2018, Art. 7 Rdnr. 30; a. A. *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), DatenschutzR, 2019, Art. 7 Rdnr. 63, der aus Art. 7 Abs. 4 DS-GVO kein Transparenzerfordernis herausliest.

[66] *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (91).

[67] EG 43 Satz 1 DS-GVO nennt exemplarisch das Verhältnis zwischen einem Betroffenen und einer Behörde.

[68] Vgl. *Krohm/Müller-Peltzer* (Fußn. 58), S. 555.

ihres Offline-Studiums auf einer Plattform belegen müssen, um ihren Hochschulabschluss erwerben zu können.

Diese (von der Hochschule ausgehende) Drucksituation muss sich womöglich der Anbieter als Teil einer gemeinsamen Verantwortung beider Stellen zurechnen lassen (Art. 4 Nr. 7, Art. 26 Abs. 1 Satz 1 DS-GVO). Dann ist auch eine Einwilligung, die der Nutzer dem MOOC-Anbieter erteilt hat, nicht freiwillig. Dafür müsste aber zum einen tatsächlich eine *gemeinsame* Verantwortlichkeit zwischen Hochschule und Anbieter bestehen (a). Zum anderen müsste sich daraus eine *Zurechnungsgrundlage* dafür ergeben, dass die Einwilligung auch gegenüber dem MOOC-Anbieter unfreiwillig ist (b).

### (a) Hochschule und MOOC-Anbieter als gemeinsam Verantwortliche

MOOC-Anbieter sind grundsätzlich nicht von Weisungen der Hochschulen abhängig, mit denen sie kooperieren. Sie bestimmen vielmehr selbst über die Zwecke und Mittel ihrer Nutzerdatenverarbeitung sowie deren wirtschaftlichen Ziele.[69] Sie fungieren daher nicht als bloße Auftragsverarbeiter ihrer universitären und privatwirtschaftlichen Kooperationspartner (Art. 4 Nr. 8 DS-GVO), sondern sind selbst Verantwortliche i. S. v. Art. 4 Nr. 7 DS-GVO.

Aus der Verantwortlichkeit jedes *einzelnen* Beteiligten erwächst jedoch noch keine *gemeinsame* Verantwortlichkeit. Gemeinsam verantwortlich sind Hochschule und MOOC-Anbieter erst, wenn sie die Zwecke und Mittel der Verarbeitung *zusammen festlegen* (Art. 26 Abs. 1 Satz 1 DS-GVO). Dafür muss jeder Beteiligte eine substanzielle Entscheidungsbefugnis über das „Warum“ (das Ziel) und „Wie“ (die Art und Weise, dieses Ziel zu erreichen) der Datenverarbeitung innehaben.[70] Die Hochschule muss dem Anbieter gleichsam potenziell in das Steuerrad greifen können, um einen Kurswechsel zu bewirken.

#### (aa) Aufgrund von Vertragsgestaltung

Wie die beiden denkbaren Sphären gegeneinander abzuschichten sind, bestimmt sich nach den faktischen Einflussmöglichkeiten der Beteiligten – nicht allein auf der Grundlage formeller Absprachen (etwa in bestehenden Kooperationsverträgen, die bspw. auch eine Seite gänzlich von der Verantwortung ausnehmen könnten).[71]

Das Vertragsverhältnis zwischen Hochschule und Anbieter ist jedoch ein wichtiger Anhaltspunkt für die Möglichkeit, steuernd auf die Zwecke und Mittel der Verarbeitung einwirken zu können.

---

[69] Vgl. zum Begriff *Artikel-29-Datenschutzgruppe*, Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, 2010, S. 25.
[70] *Artikel-29-Datenschutzgruppe* (Fußn. 69), S. 13; *Martini/Weinzierl*, NVwZ 2017, 1251 (1254); *Monreal*, ZD 2014, 611 (612).
[71] *Artikel-29-Datenschutzgruppe* (Fußn. 69), S. 8 f.

Die Hochschule kann sich i. R. d. Vertragsautonomie Kontrollmöglichkeiten sichern.[72] Insbesondere wenn sie Leistungspunkte nach dem *European Credit Transfer and Accumulation System* (ECTS)[73] dafür vergeben will, dass ein Student einen MOOC belegt hat, muss sie eine hinreichende Qualität des Bildungsangebots gewährleisten können. Dass die Hochschule in solchen Fällen Vorgaben für die Struktur und Durchführung des Online-Kurses trifft und geben muss, streitet dafür, sie als Mitverantwortliche einzustufen.

Im Fall der Münchener Universitäten erschöpft sich die Kooperation jedoch weitestgehend darin, die mit eigenen Ressourcen produzierten Kurse kostenfrei über die Plattform des Anbieters bereitzustellen. Als offizielle Prüfungsleistungen erkennen die Hochschulen die MOOC-Bewertungen bislang nicht an.[74] Auch außerhalb des Freistaats sind deutsche Hochschulen bei der Vergabe von ECTS-Punkten für absolvierte MOOCs zurückhaltend.[75]

### (bb) Gemeinsame Verantwortung aufgrund bloßer Mitursächlichkeit? Das EuGH-Urteil zu *Facebook-Fanpages*

Hat die Hochschule den Kooperationsvertrag nicht individuell – bspw. durch Qualitätsanforderungen oder Evaluierungsmechanismen – mit Einwirkungsmöglichkeiten ausgestaltet, erlangt sie grundsätzlich keine Kontrolle darüber, wie der Anbieter die Nutzerdaten verarbeitet. Sie setzt zwar den *Anlass* dafür, dass die MOOC-Anbieter die personenbezogenen Daten ihrer Studierenden verarbeiten, indem sie Online-Kurse anbietet oder sogar als Studienleistungen anerkennt. Sie gibt aber im Übrigen alle weiterführenden Möglichkeiten aus der Hand, um auf den Verbleib der Daten Einfluss zu nehmen. Die MOOC-Plattform steht dann grundsätzlich allein in der Verantwortung des Anbieters. Sie formt keine gemeinsam mit der Hochschule gesteuerte Infrastruktur.[76]

Die streng klingenden normativen Anforderungen an eine Mitverantwortlichkeit interpretiert der EuGH jedoch (zumindest im Hinblick auf das Verhältnis zwischen dem Betreiber einer *Facebook-Fanpage* und dem sozialen Netzwerk) großzügig:[77] Wer eine Fanpage erstellt hat,

---

[72] Insofern unterscheidet sich die Stellung der Hochschule etwa vom Betreiber einer *Facebook-Fanpage*. Dieser kann die Nutzungsbedingungen des sozialen Netzwerks nur entweder akzeptieren oder auf eine *Fanpage* gänzlich verzichten, s. *Martini/Fritzsche*, NVwZ-Extra 21/2015, 1 (4 f.).

[73] Weiterführend Bergmann (Hrsg.), Handlexikon der Europäischen Union, 5. Aufl., 2015, ECTS/European Credit Transfer System.

[74] *Rampelt/Niedermeier et al.*, Digital Anerkannt: Möglichkeiten und Verfahren zur Anerkennung und Anrechnung von in MOOCs erworbenen Kompetenzen, Arbeitspapier Nr. 34 des Hochschulforums Digitalisierung, 2018, S. 18 f.

[75] Eine Ausnahme besteht allerdings bei englischsprachigen Online-Kursen, die das Sprachenzentrum der Technischen Universität München als Fremdsprachenstudium anerkennt. S. https://www.sprachenzentrum.tum.de/fileadmin/w00buo/www/Ueber_uns/Issue_01-2014_23.pdf.

[76] *Veil*, in: Gierschmann/Schlender/Stenzel et al. (Hrsg.), DSGVO, 2018, Art. 26 Rdnr. 42 ff.

[77] EuGH, Urteil vom 5.6.2018, ECLI:EU:C:2018:388, Rdnr. 35 ff. – Wirtschaftsakademie SH. Eine ähnlich weite Auslegung ist auch im Verfahren zum Facebook-Like-Button zu erwarten. S. die Schlussanträge v. GA, Rs. C‑40/17 (Fashion ID), ECLI:EU:C:2018:1039, Rdnr. 66 ff.

ermögliche es dem sozialen Netzwerk, Daten zu verarbeiten.[78] Mittels individueller Filtereinstellung könne er auch darauf einwirken, welche personenbezogenen Daten i. R. d. Besucherstatistik einer Verarbeitung unterliegen.[79] Das genügt dem EuGH für eine Mitverantwortlichkeit.

Auch in dieser weiten Lesart reicht allein der Umstand, ein Angebot auf einer MOOC-Plattform vorzuhalten, indes nicht aus, um eine Mitverantwortlichkeit zu begründen.[80] Die Hochschule muss dafür – zumindest tatsächlich – auf die Datenverarbeitung in einer Weise Einfluss nehmen, die über die bloße Mitursächlichkeit hinausgeht.[81] Hat sie in ihr Bildungsangebot nur die Option integriert, MOOCs freiwillig zu belegen, trägt sie zwar faktisch dazu bei, dass ihre Studierenden an einem spezifischen Kurs teilnehmen. Sie nimmt dadurch aber keinen Einfluss darauf, ob und wie der Anbieter die Nutzerdaten auswertet. Sie ist daher für die Datenverarbeitung des Anbieters nicht mitverantwortlich.

Zu einem anderen Ergebnis gelangt man nur unter zwei Prämissen: Soweit die Hochschule ihre Studierenden dazu verpflichtet, Online-Kurse auf der Plattform des Anbieters zu absolvieren, und sie Nutzerdaten aus den Kursen erlangt, mutiert sie zum Mitverantwortlichen.[82] Denn dann ermöglicht sie es dem Anbieter nicht nur, die Daten zu verarbeiten. Sie regelt vielmehr auch, wessen Daten er konkret verarbeiten soll und profitiert von der Datenverarbeitung unmittelbar. Selbiges gilt, wenn die Studierenden das digitale Hochschullehrangebot zwar nicht nutzen müssen, aber personelle und/oder räumliche Kapazitäten an der jeweiligen Universität sie in die virtuellen Seminarräume drängen, da sie Pflichtveranstaltungen (zumindest de facto) nur online besuchen können. Die Hochschule nimmt dann tatsächlich auf die Verarbeitung Einfluss und ist für sie nicht nur mitursächlich.

### (b) Mitverantwortlichkeit als Zurechnungsgrundlage für die Unfreiwilligkeit der Einwilligung

Soweit eine deutsche Hochschule und ein MOOC-Anbieter gemeinsam Verantwortliche sind, zieht das die Frage nach sich, ob sie sich auch solche Umstände wechselseitig zurechnen lassen müssen, die eine Einwilligung unfreiwillig machen können.

---

[78] Weiterführend *Botta*, EuGH-Urteil zu Facebook-Fanpages: Mitgefangen, mitgehangen?, JuWissBlog Nr. 65/2018 vom 26.6.2018.
[79] EuGH, Urteil vom 5.6.2018, ECLI:EU:C:2018:388, Rdnr. 35 ff. – Wirtschaftsakademie SH. Ob der Fanpage-Betreiber lediglich anonymisierte Daten erhält, erachtet der EuGH nicht für entscheidend. Nicht jeder Mitverantwortliche müsse Zugang zu den personenbezogenen Daten haben. EuGH, aaO, Rdnr. 38.
[80] EuGH, Urteil vom 5.6.2018, ECLI:EU:C:2018:388, Rdnr. 35 – Wirtschaftsakademie SH.
[81] In diesem Sinne bereits *Martini/Fritzsche* (Fußn. 72), S. 5; *Veil* (Fußn. 76), Art. 26 Rdnr. 36.
[82] Ob *die Hochschulen* auch personenbezogene Daten ihrer Studierenden an die MOOC-Anbieter weitergeben können, bestimmt sich vorrangig nach den Sonderregelungen für die Übermittlung von Daten an nicht-öffentliche Stellen, welche das jeweilige Landesdatenschutz- bzw. Hochschulgesetz als Parallelvorschrift zu § 25 Abs. 2 BDSG vorhält (vgl. *Aßhoff*, in: Wolff/Brink [Hrsg.], BeckOK DatenschutzR, 27. Ed., Stand: 1.2.2019, § 25 Rdnr. 10).

EG 43 Satz 1 DS-GVO wertet ein klares Ungleichgewicht »zwischen der betroffenen Person und dem Verantwortlichen« immerhin als Ausschlussgrund für die Freiwilligkeit. Die gemeinsam Verantwortlichen erwähnt er indes nicht.[83] Diese auch zu erfassen, entspricht jedoch der Rationalität des Instruments der gemeinsamen Verantwortlichkeit: Art. 26 DS-GVO will in Zeiten, in denen sich die Verarbeitungsprozesse auf immer mehr Akteure verteilen, Rechtsunsicherheiten vermeiden, die sich mit unklaren Zurechnungssituationen verknüpfen.[84] Der Betroffene soll nicht als Leidtragender verworrener Zuständigkeiten und komplexer Gestaltungsprozesse an der Front zwischen den Mitverantwortlichen zerrieben werden. Besonders deutlich manifestiert sich dies auf der Rechtsfolgenebene: Die Mitverantwortlichen haften quasi-gesamtschuldnerisch (Art. 26 Abs. 3, Art. 82 Abs. 4 DS-GVO).

Aus der Mitverantwortlichkeit erwächst daher auch eine Zurechnungsgrundlage, die über gemeinsame Transparenzpflichten hinausgeht. Anderenfalls ginge für Verarbeitende davon ein Anreiz aus, Kooperationen einzugehen, in denen eine Seite Zwang auf den Betroffenen ausübt und die andere Seite dessen Daten verarbeitet; im Ergebnis müsste keiner der beiden Konsequenzen fürchten.[85] Geht eine Zwangswirkung also nur von einem der gemeinsam Verantwortlichen aus, ist sie im Ergebnis auch dem anderen Mitverantwortlichen zuzurechnen.

#### ee) Zwischenfazit

Erteilt der Nutzer dem MOOC-Anbieter die Einwilligung, seine personenbezogenen Daten in den USA zu verarbeiten, kann diese rechtmäßig sein. Möchte der Anbieter die Nutzerdaten jedoch an Dritte weitergeben, muss er darauf klar und erkennbar hinweisen. Anderenfalls ist die Einwilligung nicht freiwillig (und verstößt insbesondere gegen das Kopplungsverbot i. S. d. Art. 7 Abs. 4 DS-GVO).

Üben die Hochschulen auf ihre Studierenden faktisch Druck aus, MOOCs zu belegen, und erlangen sie dadurch selbst Nutzerdaten, begründet dies eine Mitverantwortlichkeit zwischen ihnen und den kommerziellen Plattformbetreibern (Art. 4 Nr. 7, Art. 26 Abs. 1 Satz 1 DS-GVO). Die gemeinsame Verantwortlichkeit schafft eine gegenseitige Zurechnungsgrundlage für das arbeitsteilige Zusammenwirken der Beteiligten. Die faktische Zwangswirkung, welche die

---

[83] Das heißt aber nicht, dass der Verordnungsgeber die gemeinsam Verantwortlichen an dieser Stelle nicht auch mitgedacht hat. Auch in Art. 4 Nr. 10 (Abgrenzung von Dritten) spricht die DS-GVO bspw. nur von „dem Verantwortlichen", meint aber immer auch den gemeinsam Verantwortlichen (*Martini*, in: Paal/Pauly [Hrsg.], DS-GVO, 2017, Art. 26 Rdnr. 3a). Die gemeinsame Verantwortung zeichnet sich gerade dadurch aus, dass sich die Personen das Verhalten jeweils zurechnen lassen müssen.

[84] *Martini* (Fußn. 83), Art. 26 Rdnr. 1.

[85] Den Begriff und die Konsequenzen der Verantwortlichkeit möglichst weit auszulegen, trägt nach Einschätzung des EuGH nicht zuletzt dazu bei, ein möglichst hohes Datenschutzniveau in der Union zu verwirklichen. Vgl. EuGH, Urteil vom 13.5.2014, ECLI:EU:C:2014:317, Rdnr. 34 – Google Spain und Google; Urteil vom 5.6.2018, ECLI:EU:C:2018:388, Rdnr. 28 – Wirtschaftsakademie SH.

Hochschulen auslösen, kann eine Einwilligung des studentischen Nutzers gegenüber dem MOOC-Anbieter unfreiwillig werden lassen (vgl. EG 43 Satz 1 DS-GVO).

Zusätzlich zu ihren Wirksamkeitsrisiken hat die Einwilligung aus der Perspektive des Anbieters vor allem einen großen Pferdefuß: Der Nutzer kann sie jederzeit *pro futuro* widerrufen.[86] Die Verarbeitungsgrundlage entfällt dann ex nunc (Art. 7 Abs. 3 Satz 1 und 2 DS-GVO).

### b) Gesetzliche Erlaubnistatbestände

Selbst wenn eine Einwilligung einen rechtssicheren Transfer der MOOC-Nutzerdaten an Dritte in den USA nicht trägt, ist dieser deshalb nicht zwangsläufig unzulässig: Die transatlantische Datenübermittlung kann sich im Grundsatz (unabhängig von einer Einwilligung[87]) auch auf einen gesetzlichen Erlaubnistatbestand stützen (insbesondere Art. 6 Abs. 1 UAbs. 1 lit. b, c und f DS-GVO).

#### aa) Erfüllung eines Vertrages (Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO)

Kraft Gesetzes gestattet die Union Verantwortlichen, personenbezogene Daten zu verarbeiten, soweit dies erforderlich ist, um seine Vertragspflichten zu erfüllen oder vorvertragliche Maßnahmen durchzuführen (Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO). MOOC-Anbieter dürfen daher ohne Weiteres alle Daten verarbeiten, die sie benötigen, um ihre vertragliche Leistungspflicht zu erfüllen, also dem Nutzer Bildungsinhalte zur Verfügung zu stellen, z. B. Anmeldeinformationen oder Leistungsbewertungen.[88] Das deckt grundsätzlich auch grenzüberschreitende Verarbeitungsvorgänge, wenn der Verantwortliche selbst in einem

---

[86] Darauf muss ihn der Anbieter hinweisen (Art. 7 Abs. 3 Satz 3, Art. 13 Abs. 2 lit. c bzw. Art. 14 Abs. 2 lit. d DS-GVO). Die Rechtslage hat sich insoweit grundlegend geändert: Im Regime des § 28 Abs. 3a Satz 1 BDSG a. F. setzte ein Widerruf in einem Vertragsverhältnis eine Interessenabwägung voraus. Vgl. BAG, Urteil vom 11.12.2014, BAGE 150, 195 (204 f., Rdnr. 38 ff.). Ebenso *Schantz/Wolff* (Fußn. 42), Rdnr. 532. An der alten Rechtslage entgegen dem eindeutigen Wortlaut und Normzweck des Art. 7 Abs. 3 DS-GVO festhaltend: *Buchner/Kühling* (Fußn. 65), Art. 7 DSGVO Rdnr. 38 f.; *Schulz* (Fußn. 65), Art. 7 Rdnr. 57.

[87] Legt man die Normensystematik zugrunde, besteht diese Erlaubnis auch dann, wenn eine erteilte Einwilligung, z. B. infolge Widerrufs, unwirksam ist – sogar dann, wenn der Anbieter dem Nutzer treuwidrig vortäuscht, dass er den Schutz seiner personenbezogenen Daten durch Einwilligung effektiv ausüben kann, während die Datenverarbeitung tatsächlich allein auf einem gesetzlichen Tatbestand fußt. Auch das Gebot einer Verarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. a Var. 2 DS-GVO) versperrt dem Anbieter nicht, sich zugleich auf Art. 6 Abs. 1 UAbs. 1 b DS-GVO zu berufen (a. A. *Buchner/Petri*, in: Kühling/Buchner [Hrsg.], DS-GVO/BDSG, 2. Aufl., 2018, Art. 6 Rdnr. 23; *Datenschutzkonferenz*, Einwilligung nach der DS-GVO, Kurzpapier Nr. 20, https://www.tlfdi.de/mam/tlfdi/themen/kurzpapier_20.pdf., S. 3). Denn alle Erlaubnistatbestände stehen gleichrangig nebeneinander. Ist eine Einwilligung unwirksam, „infiziert" das daher die anderen Erlaubnistatbestände nicht; vgl. ebenso *Veil*, NJW 2018, 3337 (3341 f.); wohl auch *Schantz/Wolff* (Fußn. 42), Rdnr. 543. Eine ähnliche Wertung trifft der Gesetzgeber auch an anderer Stelle: in dem Kopplungsverbot des Art. 7 Abs. 4 DS-GVO. Dort verankert der Unionsgesetzgeber die Wertentscheidung, dass der Verantwortliche den Betroffenen nicht eine Einwilligung unter Berufung darauf abringen kann, diese sei erforderlich, um den Vertrag zu erfüllen (Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO), obwohl das gar nicht der Fall ist. Dass eine *Einwilligung* in diesem Fall nicht besteht, bleibt nach dem Willen des Gesetzgebers auf die *gesetzliche Verarbeitungserlaubnis* aber ohne Einfluss.

[88] S. hierzu bereits III. 2. a) dd) (1).

Drittstaat sitzt. Daten an Dritte (in den USA) weiterzugeben, ist jedoch regelmäßig nicht erforderlich, um die eigene Leistungspflicht zu erfüllen – jedenfalls, soweit das nicht eine zusätzliche Dienstleistung (z. B. die Arbeitsvermittlung) voraussetzt, zu der der Vertrag den Anbieter verpflichtet.[89]

### bb) Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO)

Auch soweit das Vertragsverhältnis eine Datenverarbeitung nicht trägt, kann der Anbieter eine grenzüberschreitende Weitergabe der Nutzerdaten in die USA auf eine gesetzliche Verarbeitungserlaubnis stützen, soweit er damit eine rechtliche Verpflichtung erfüllt (Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO). [90] Die Pflicht, die Daten grenzüberschreitend weiterzuverarbeiten, kann und muss sich dabei aus dem Unionsrecht oder dem Recht der Mitgliedstaaten ergeben (Art. 6 Abs. 1 UAbs. 1 lit. c i.V. mit Art. 6 Abs. 3 DS-GVO) – eine allein nach US-amerikanischem Recht bestehende Pflicht reicht nicht aus.

Eine rechtliche Pflicht i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. c besteht bspw., soweit das nationale oder unionale Recht vorschreibt, dass Verantwortliche einem US-amerikanischen Rechtshilfeersuchen i.R.e. sog. e-Discovery-Verfahrens zu entsprechen haben.[91] Diesem Anwendungsfall kommt bei MOOCs jedoch allenfalls randständige Bedeutung zu: Zum einen kommt Deutschland solchen Anfragen nicht nach.[92] Zum anderen besteht für ein solches Ersuchen auch kein Bedarf, wenn es sich – wie i.d.R. – um US-amerikanische Plattformbetreiber handelt. Denn deren Server befinden sich nicht in der Union, sondern in den USA. Insoweit ebnet auch Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO dem MOOC-Anbieter keinen Weg, Nutzerdaten datenschutzkonform an US-amerikanische Dritte weiterzuleiten.

### cc) Wahrung berechtigter Interessen an einer grenzüberschreitenden Datenweitergabe an Dritte (Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO)

Greift keine Einwilligung oder ein sonstiger Erlaubnistatbestand, erweist sich als zentrale Verarbeitungsgrundlage für die grenzüberschreitende Geschäftspraxis der MOOC-Anbieter das Recht, berechtigte Interessen zu wahren (Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO).

---

[89] Zur Frage, inwieweit Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO „Daten gegen Leistungen"-Geschäfte legitimiert, s. *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), DatenschutzR, 2019, Art. 6 Abs. 1 Rdnr. 33 ff.; vgl. auch *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3747).

[90] Diese Verarbeitungsgrundlage grenzt sich von dem Erlaubnistatbestand der Vertragserfüllung (Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO) dadurch ab, dass sie nicht aus einem schuldrechtlichen Rechtsverhältnis, sondern aus einer *öffentlich-rechtlich gesetzten Vorschrift* resultiert. S. *Albrecht/Jotzo* (Fußn. 48), Teil 3 Rdnr. 45; *Buchner/Petri* (Fußn. 87), Art. 6 Rdnr. 77; *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 6 Rdnr. 16.

[91] Weiterführend *Deutlmoser/Filip*, in: Hoeren/Sieber/Holznagel (Hrsg.), Stand: 46. Erg.-Lfg., 2018, Teil 16.6 E-Discovery, Rdnr. 2 ff.

[92] Vgl. § 14 Abs. 1 Gesetz zur Ausführung des Haager Übereinkommens über die Beweisaufnahme im Ausland vom 18.3.1970.

Möchte der Anbieter Nutzerdaten an Private in den USA – etwa an seine Dienstleister und Geschäftspartner – weitergeben, genießt dies grundsätzlich den Schutz seiner unternehmerischen Freiheit (Art. 16 GRCh)[93].[94] Hat er die Nutzerdaten rechtmäßig erhoben, wird er insoweit für sich ein *berechtigtes Interesse* reklamieren.[95] Anders als Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO ist der Erlaubnistatbestand „berechtigte Interessen" jedoch nicht vertragsakzessorisch. Es kommt also nicht darauf an, ob der Nutzer dem Anbieter in dem Vertrag Rechte eingeräumt hat, Daten zu verarbeiten – auch nicht darauf, ob der Vertrag wirksam ist oder nicht.

Berechtigte Interessen legitimieren nicht als solche bereits eine Verarbeitung. Sie muss für diese Ziele vielmehr auch *erforderlich* sein. Daran fehlt es insbesondere dann, wenn der Anbieter Nutzerdaten an Dritte weitergibt, obwohl es bereits ausreichend wäre, sie anonymisiert weiterzuleiten.[96]

Auf Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO kann sich der Anbieter auch nur dann stützen, wenn die Interessen oder Rechte des Betroffenen, [97] insbesondere sein Recht auf Schutz personenbezogener Daten (Art. 8 GRCh bzw. Art. 16 Abs. 1 AEUV), nicht überwiegen. Lässt sich nicht eindeutig feststellen, ob die Interessen des Nutzers die Interessen des Anbieters überwiegen, sondern stehen sich beide gleichrangig gegenüber (sog. Non-liquet-Situation), gesteht der Unionsgesetzgeber den Interessen des Verantwortlichen den Vorrang zu.[98] Das ergibt sich aus dem klaren Wortlaut des Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO. Der Erlaubnistatbestand knüpft nämlich explizit an eine Negativ-Voraussetzung („sofern nicht")

---

[93] Berufsfreiheit (Art. 15 GRCh) und unternehmerische Freiheit überschneiden sich zwar weitestgehend. Die wirtschaftliche Tätigkeit des Anbieters als privatrechtliches Unternehmen unterfällt jedoch dem Schutzbereich des Art. 16 GRCh, da er Selbstständiger ist. S. *Jarass*, Charta der Grundrechte der Europäischen Union, 3. Aufl., 2016, Art. 15 Rdnr. 9; *Ruffert*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 5. Aufl., 2016, Art. 15 GRCh Rdnr. 7 f. Infolge des Anwendungsvorrangs des Unionsrechts bemessen sich grundrechtliche Erwägungen im Geltungsbereich der DS-GVO nach den Vorschriften der GRCh und nicht nach denen des deutschen Grundgesetzes. S. bspw. *Albrecht/Jotzo* (Fußn. 48), Teil 1 Rdnr. 25.

[94] Auch wenn der Anbieter infolge öffentlich-rechtlich gesetzter Vorgaben (etwa an US-amerikanische Strafverfolgungsbehörden auf der Grundlage des *Stored Communications Act* [18 U.S.C. § 2703.]) verpflichtet ist, Daten weiterzugeben, hat er ein berechtigtes Interesse daran, sich insoweit rechtstreu zu verhalten. Vgl. *Metz/Spittka*, ZD 2017, 361 (364).

[95] Zu berücksichtigen sind nicht nur die Interessen des Verarbeitenden, sondern auch Dritter. Die Dritten müssen dabei nicht zwingend die Empfänger der Daten sein – dies hatte noch Art. 7 lit. f DS-RL verlangt. Vgl. dazu *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP 217, 2014, S. 32; *Robrahn/Bremert*, ZD 2018, 291 (292).

[96] Vgl. BAG, Beschluss vom 3.6.2003, BAGE 106, 188 (199 f.).

[97] Einen erhöhten Schutz erfahren die Betroffenen-Interessen, wenn der Nutzer noch ein „Kind", d. h. noch nicht einsichtsfähig, ist (Art. 6 Abs. 1 UAbs. 1 lit. f a. E. DS-GVO; vgl. auch *Martini/Kienle*, JZ 2019, 235 [239] mit Fußn. 60 sowie III. 2. a) cc)). Aus der Minderjährigkeit selbst resultiert zwar noch kein absolutes Verarbeitungsverbot; sie lässt die Betroffeneninteressen aber typischerweise überwiegen. Vgl. EuGH, Urteil vom 4.5.2017, ECLI:EU:C:2017:336, Rdnr. 33 – Rīgas.

[98] So bereits *Martini/Botta* (Fußn. 25), S. 631 mit Fußn. 58.

an: Der Verantwortliche darf nur dann nicht verarbeiten, wenn die Interessen des Betroffenen das größere Gewicht haben.[99]

Die Durchschlagskraft der Nutzerinteressen bestimmt sich insbesondere nach ihren *berechtigten* Erwartungen (vgl. EG 47 Satz 1 Hs. 2, Satz 3 und 4 DS-GVO). Bei US-amerikanischen Anbietern muss ein Nutzer zwar im Grundsatz regelmäßig damit rechnen, dass diese die anfallenden Daten auch auf der anderen Seite des Atlantiks verarbeiten und potenziell an dort ansässige Dritte weitergeben. Die faktische Wahrscheinlichkeit, dass ein Verarbeiter ein bestimmtes Verarbeitungsverhalten an den Tag legt, macht seine Interessen zum einen aber noch nicht legitim. Da die Anbieter ihr Weitergabeverhalten im Regelfall nicht kommunizieren, kann der Nutzer zum anderen i. d. R. nicht ausreichend vorhersehen, welche konkreten Dritten seine Daten künftig in den Händen halten werden. Sind seine Daten erst einmal an Dritte in den USA übermittelt, birgt das zudem die Gefahr, dass sie anschließend auch an andere Stellen gelangen.[100] Der Anbieter kann und muss daher jedenfalls ausreichende Schutzmaßnahmen ergreifen, um die Betroffenenrechte zu wahren.[101]

Im Regelfall überwiegen die Interessen des Nutzers, keiner Weitergabe seiner Daten an Dritte ausgesetzt zu sein, das gegenläufige Interesse des Anbieters. Zu schwer wiegt der Eingriff in seine Privatheitsentfaltung, wenn die ihn betreffenden Informationen ohne sein Zutun in die Zugriffsmacht Dritter gelangen. So sehr der Anbieter ein ökonomisches Interesse daran haben darf, Nutzerdaten an Dritte weiterzugeben, so wenig gewährt die Rechtsordnung dieser Datenpreisgabe den Vorrang vor den berechtigten Schutzinteressen des Betroffenen, wenn der Nutzer ihr nicht ausdrücklich seinen Segen erteilt hat.

#### dd) Zwischenfazit

Ein MOOC-Anbieter kann eine grenzüberschreitende Verarbeitung der personenbezogenen Nutzerdaten *als solche* grundsätzlich auf berechtigte Interessen (Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO) stützen. Das Verwertungsinteresse des Anbieters legitimiert regelmäßig hingegen nicht, die Daten *an Dritte* weiterzugeben – ebenso wenig das vertragliche Erfüllungsinteresse des MOOC-Anbieters (Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO). Es rechtfertigt eine Datenweitergabe an Dritte nur, wenn sie (bspw. zu Zwecken der Arbeitsvermittlung) zum

---

[99] Anders war die Rechtslage noch unter dem Regime des § 29 Abs. 11 Nr. 1 BDSG a. F.: Danach war eine Datenverarbeitung bereits dann unzulässig, wenn ihr ein schutzwürdiges Interesse des Betroffenen entgegenstand.

[100] Eine Ursache dafür ist die in den USA geltende *Third Party Doctrine*: Einmal freiwillig preisgegebene Daten darf der Verarbeitende ohne erneute Einwilligung Dritten weitergeben, vgl. Smith v. Maryland, 442 U.S. 735, 743 (1979) sowie III. 3. a) bb).

[101] *Artikel-29-Datenschutzgruppe* (Fußn. 95), S. 53 ff. Wesentliche Maßnahmen zum Schutz gegen den unberechtigten Zugriff Dritter sind die Pseudonymisierung und Verschlüsselung der Nutzerdaten. Dem Ideal des Selbstdatenschutzes kommen Anwendungen am nächsten, die den Nutzer in Gestalt eines Datenupdates über eine Datenweitergabe informieren, und ihm ermöglichen, die eigenen digitalen Fußspuren soweit wie möglich nachzuvollziehen und zu verwischen. Daneben erwächst aus Art. 35 Abs. 1 Satz 1 DS-GVO für den Anbieter i. d. R. die Pflicht, eine Datenschutz-Folgenabschätzung vorzunehmen: Die grenzüberschreitende Datenverarbeitung birgt regelmäßig ein hohes Risiko für die Betroffenenrechte.

vertraglichen Pflichtenheft des Anbieters gehört. Dass der Vertrag dem Anbieter das Recht *einräumt*, die Daten an Dritte weiterzugeben, reicht insoweit nicht. Auch eine US-amerikanische Pflicht, Nutzerdaten herauszugeben, löst keine rechtliche Verpflichtung i. S. d. Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO aus, die einen Datentransfer an andere Stellen rechtfertigen könnte.

Dritten Daten zu übermitteln, kann sich der Anbieter grundsätzlich aber im Wege einer ausdrücklichen Einwilligung gestatten lassen. Diese ist auch als Teil eines Daten-gegen-Bildung-Modells zulässig. Gegen das Kopplungsverbot des Art. 7 Abs. 4 DS-GVO verstößt die Zustimmung jedoch nur so lange nicht, wie der Anbieter klar und erkennbar darauf hinweist, dass er Daten an Dritte weitergibt.

### c) Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DS-GVO)

Elektronische Lernangebote verarbeiten mitunter sensible personenbezogene Daten – insbesondere das Geschlecht, die ethnische Herkunft, biometrische Daten [102] sowie Gesundheitsdaten. Für solche sog. besonderen Datenkategorien dekretiert der unionale Verordnungsgeber ein gesteigertes Schutzniveau: Art. 9 Abs. 1 DS-GVO unterwirft ihre Verarbeitung einem strikten Verarbeitungsverbot, das nur wenige, eng gesteckte Ausnahmen kennt.

#### aa) Normatives Zulässigkeitsprogramm

Die DS-GVO gestattet dem MOOC-Anbieter, solche besonderen personenbezogenen Daten zu verarbeiten, die der Nutzer selbst der Öffentlichkeit zugänglich gemacht hat (Art. 9 Abs. 2 lit. e DS-GVO). Gleiches gilt in den seltenen Fällen, in denen der Anbieter eigene Rechtsansprüche geltend macht (Art. 9 Abs. 2 lit. f DS-GVO). Im Übrigen verbleibt als Rechtfertigungstatbestand i. d. R. alleine eine ausdrückliche Einwilligung[103] des Nutzers (Art. 9 Abs. 2 lit. a Hs. 1 DS-GVO).

#### bb) Abgrenzung zwischen besonderen personenbezogenen und sonstigen Daten

Unter Big-Data-Bedingungen lässt sich durch Datenverknüpfung vielfach – wenn auch nicht unmittelbar, so doch immerhin *mittelbar* – leicht eine sensible Eigenschaft i. S. d. Art. 9 Abs. 1 DS-GVO destillieren, etwa wenn der MOOC-Anbieter aus dem Namen des Nutzers dessen ethnische Herkunft herauslesen kann.[104] Kennt er zudem seinen Wohnort, kann er bisweilen sogar dessen religiöse Überzeugung (mit hoher Wahrscheinlichkeit) ermitteln.[105] Im Lichte des technischen Fortschritts ist daher eine vorausschauende Erkenntnis des BVerfG aus dem

[102] Verlangt der Anbieter, dass ein Nutzer sein Personalausweisdokument vorlegt oder identifiziert er den Nutzer mittels Webcam, verarbeitet er biometrische Daten (Art. 4 Nr. 14 bzw. Art. 9 Abs. 1 DS-GVO).
[103] Vgl. III. 2. a).
[104] *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 9 Rdnr. 8.
[105] *Frenzel* (Fußn. 104), Art. 9 Rdnr. 13.

Jahre 1983 heute zur Gewissheit gereift: „Unter den Bedingungen der automatischen Datenverarbeitung [gibt es] kein »belangloses« Datum mehr“.[106]

Wenn nahezu jedes Datum ein besonderes personenbezogenes Datum markieren kann, dann drohen die Grenzen der Erlaubnistatbestände des Art. 6 Abs. 1 UAbs. 1 und des Art. 9 DS-GVO im Ergebnis weitgehend zu verschwimmen. Soll das gestufte System der beiden Zulassungsregime seinen Sinn nicht verlieren, ist es daher geboten, Art. 9 Abs. 1 DS-GVO (jedenfalls mit Blick auf Var. 1, die es ausreichen lässt, dass die kritischen Merkmale, wie z. B. die religiöse Überzeugung, aus der Verarbeitung „hervorgehen“) [107] teleologisch zu reduzieren:[108] Es genügt nicht, dass sich aus Daten überhaupt Rückschlüsse auf Merkmale i. S. d. Art. 9 ziehen lassen. Entscheidend ist vielmehr der objektivierte Verarbeitungskontext. [109] Es kommt also darauf an, ob der Verantwortliche die personenbezogenen Nutzerdaten für einen objektiven Dritten erkennbar zu dem Zwecke verarbeitet oder erkennbar verarbeiten wird, Erkenntnisse über die Eigenschaften im Sinne des Art. 9 Abs. 1 DS-GVO zu erlangen.

Ist das nicht der Fall – kann der Verantwortliche insbesondere (z. B. durch Protokolldaten, die technisch beschränkende Gestaltung der Verarbeitungsalgorithmen etc.) plausibel dartun, dass er keine besonderen personenbezogenen Daten verarbeitet hat –, bemisst sich die Zulässigkeit der Verarbeitung allein nach Art. 6 Abs. 1 UAbs. 1 DS-GVO. Verbleiben Zweifel darüber, ob besonders sensible oder nicht-sensible Daten vorliegen, ist im Lichte des unionsrechtlich gewollten gestuften Kategorienschutzes jedoch der strengere Maßstab des Art. 9 DS-GVO anzulegen.[110]

### 3. Spezifische Zulässigkeitsvoraussetzungen der Art. 44 ff. DS-GVO

Wer Daten in das außereuropäische Ausland[111] transferieren möchte, der muss zusätzlich zu allgemeinen Anforderungen an Datenverarbeitungen auch die besonderen Bedingungen des

---

[106] BVerfG, Urteil vom 15.12.1983, BVerfGE 65, 1 (45).

[107] In der Konstellation der Var. 2 muss sich die sensible Eigenschaft, bspw. das Gesundheitsdatum, demgegenüber *unmittelbar* aus der verarbeiteten Information ergeben. Das folgt aus einem Umkehrschluss zur Var. 1 sowie den konkretisierenden Begriffsbestimmungen für die sensiblen Datenkategorien (Art. 4 Nr. 13-15 DS-GVO [„Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit diese natürlichen Person liefern“; „Daten, die sich auf die körperliche oder geistige Gesundheit natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen“]).

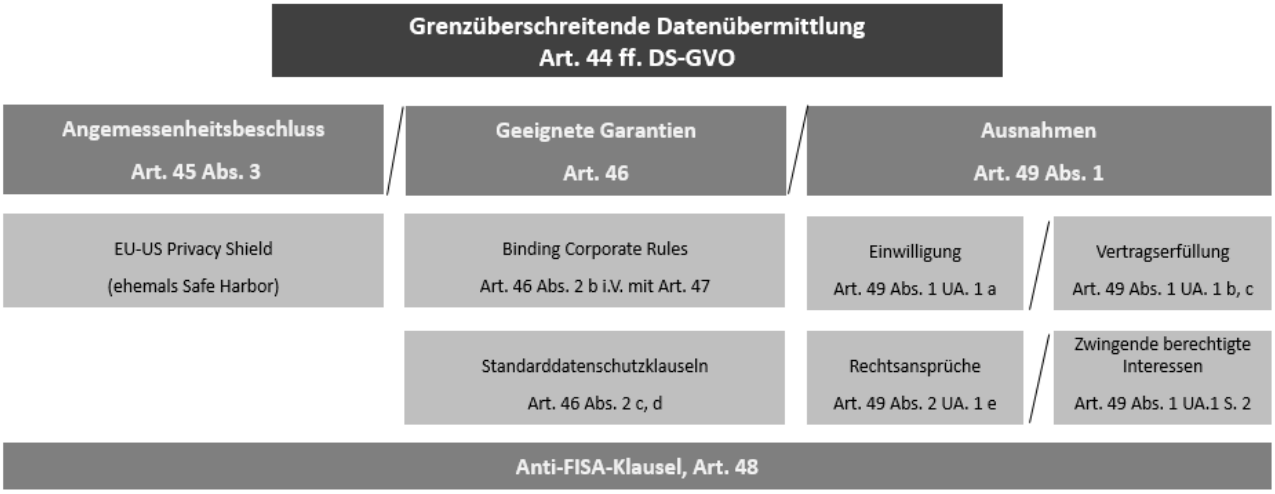
[108] Vgl. zur Abgrenzungsproblematik auch *Frenzel* (Fußn. 104), Art. 9 Rdnr. 8 f.; *Schiff*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2. Aufl., 2018, Art. 9 Rdnr. 13; *Weichert*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 9 DSGVO Rdnr. 22 f.

[109] Vgl. *Artikel-29-Datenschutzgruppe*, Letter to Mr Timmers, Annex – Health data in apps and devices, 2015, S. 4 f.

[110] *Martini/Kienle* (Fußn. 97), S. 239; *Schiff* (Fußn. 108), Art. 9 Rdnr. 13; a. A. *Schulz*, in: Gola (Hrsg.), DS-GVO, 2. Aufl., 2018, Art. 9 Rdnr. 13.

[111] Die Formulierung „Übermittlung *an ein Drittland“* in Art. 44 Satz 1 DS-GVO ist missverständlich: Die Art. 44 ff. DS-GVO finden auf alle Datenübermittlungen *in Drittstaaten* Anwendung – also auch an Private. Nichts anderes gilt, wenn Akteure personenbezogene Daten innerhalb eines Drittstaats weitergeben (Art. 44 Satz 1 Hs. 2 DS-GVO; sog. *onward transfers*).

Kapitels V der DS-GVO erfüllen. Diese sollen den Umstand kompensieren, dass bei Verarbeitungen im Ausland unionale Kontrollinstrumentarien vor Ort fehlen.[112] Entweder muss daher ein Angemessenheitsbeschluss der Europäischen Kommission die Vereinbarkeit mit den Prinzipien des Unionsrechts feststellen (Art. 45 DS-GVO; a) oder geeignete äquivalente Garantien (Art. 46 DS-GVO; b) verbürgen ein hinreichendes Schutzniveau. Anderenfalls können dem MOOC-Anbieter lediglich die Ausnahmetatbestände des Art. 49 DS-GVO (c) zu Hilfe eilen.[113]




### a) Angemessenheitsbeschluss: EU-US Privacy Shield (Art. 25 DS-RL bzw. Art. 45 DS-GVO)

Ob bestimmte Regionen, spezifische Sektoren oder auch ein gesamter Drittstaat ein angemessenes Datenschutzniveau wahren (Art. 45 Abs. 1 Satz 1 DS-GVO), bedingt eine komplexe Wertungsentscheidung. Der Unionsgesetzgeber legt diese in die Hände der Europäischen Kommission.

Gelangt sie zu dem Schluss, dass im Drittstaat ein angemessenes Schutzniveau herrscht, kann sie einen Angemessenheitsbeschluss in Gestalt eines Durchführungsrechtsakts treffen (Art. 45 Abs. 3 DS-GVO). [114] Die Datenübermittlung ist dann als datenschutzkonform anzusehen. Der Verantwortliche muss keine weiteren Genehmigungen einholen (Art. 45 Abs. 1 Satz 2 DS-GVO).

Dass die DS-GVO das Datenschutzniveau der USA als angemessen betrachtet, versteht sich keineswegs von selbst. Denn die Vorstellungen der EU und der USA von Privatheit divergieren.

---

[112] Sie führen die Art. 25, 26 DS-RL im neuen Verordnungsregime fort.
[113] Von besonderer Bedeutung für die Vorgaben der Art. 44 ff. DS-GVO ist zudem das Urteil des EuGH vom 6.10.2015 in der Rechtssache „Schrems“ (ECLI:EU:C:2015:650).
[114] Eine Übersicht über die bestehenden Angemessenheitsbeschlüsse findet sich bspw. bei *Hladjk*, in: Eßer/Kramer/von Lewinski (Hrsg.), DSGVO/BDSG, 6. Aufl., 2018, Art. 45 DSGVO Rdnr. 22.

15 Jahre lang galt für die Datenübermittlung *in die USA* das sog. *Safe-Harbor-Abkommen*[115]. Dessen Kernelement war ein sektoraler Angemessenheitsbeschluss der Kommission auf der Grundlage des Art. 25 Abs. 6 DS-RL. Der EuGH hat das Abkommen im Jahr 2015 jedoch für unwirksam erklärt.[116] Seinen Nachfolger, den sog. *EU-US Privacy Shield* (PS), hat die Europäische Kommission am 12.7.2016 beschlossen und damit die transatlantische Datenübermittlung gegen wirtschaftliche Verwerfungen gesichert.[117]

#### aa) Regelungsgehalt

Der Schutzmechanismus des Privacy Shield basiert auf dem Prinzip der Selbstzertifizierung: Sein Dreh- und Angelpunkt ist die freiwillige Erklärung der beteiligten US-amerikanischen Unternehmen, die Datenschutzgrundsätze des Abkommens (EG 20 ff. PS bzw. PS-Anhang II) zu achten (EG 14 ff. PS). Die Schutzwirkung des Privacy Shield sichert die Angemessenheit des Schutzniveaus mithin erst dann ab, wenn sich Unternehmen hierzu gegenüber dem *Department of Commerce* (US-Handelsministerium) bekennen.[118] Auf diese Weise können sich (nur) diejenigen Unternehmen selbst zertifizieren, welche der Aufsicht der *Federal Trade Commission* (FTC) oder des *Department of Transport* (US-Verkehrsministerium) unterliegen.[119] Auch der weltweit führende MOOC-Anbieter *Coursera* hat hiervon Gebrauch gemacht.[120]

Die Kontrollmechanismen, die dieses Regime auslöst, sind jedoch intransparent. Die Furcht vor einem Umsetzungsdefizit jenseits des Atlantiks ist groß. Das Zertifizierungsverfahren sieht sich daher erheblicher Kritik ausgesetzt. Seit Geltung der DS-GVO und dem Skandal um *Facebook* und *Cambridge Analytica* ist die Skepsis noch gewachsen.[121] Auch deshalb steht der Privacy Shield gegenwärtig auf dem Prüfstand.[122]

#### bb) Rechtmäßigkeit

In der Vergangenheit verlangte das unionale Datenschutzrecht für einen Angemessenheitsbeschluss nicht, dass das Datenschutzniveau im Drittstaat bzw. jeweiligen Sektor *äquivalent* ist. Es reichte vielmehr aus, dass dort die *wesentlichen Grundsätze* des

---

[115] Dabei handelte es sich um eine informelle Absprache zwischen der EU-Kommission und der US-Regierung.
[116] EuGH, Urteil vom 6.10.2015, ECLI:EU:C:2015:650, Rdnr. 98 – Schrems.
[117] Europäische Kommission, Durchführungsbeschluss (EU) 2016/1250 v. 12.7.2016, ABl. L 207/1.
[118] Da der Privacy Shield unmittelbar nur auf die zertifizierten US-Unternehmen Anwendung findet, legitimiert er keine Datenverarbeitung durch US-amerikanische Behörden, obgleich er hierzu Regelungen enthält (EG 67 ff. PS).
[119] *Schantz/Wolff* (Fußn. 42), Rdnr. 767.
[120] Die gesamte Liste aller (aktuell wie ehemals) zertifizierten Unternehmen findet sich unter: https://www.privacyshield.gov/list.
[121] *Botta*, Zieht Brüssel die Reißleine? – Die ungewisse Zukunft des EU-US Privacy Shields, JuWissBlog Nr. 74/2018 vom 17.8.2018.
[122] Vorabentscheidungsersuchen des High Court (Irland) v. 9.5.2018, Rs. C-311/18, ABl. 2018 C 249/17.

Datenschutzes gelten.[123] Das drittstaatliche Datenschutzniveau durfte vom unionalen also auch nach unten abweichen; der Europäischen Kommission verblieben dadurch geostrategische Spielräume für „Datenschutz-Deals".[124]

Der EuGH hat die Daumenschrauben im Jahr 2015 (noch auf der Grundlage der DS-RL) jedoch angezogen: Das Drittland bedürfe zwar *keines identischen* Datenschutzniveaus. Es müsse im Licht der GRCh aber einen *gleichwertigen Schutz der Freiheiten und Grundrechte* verbürgen.[125] Mit Erlass der DS-GVO hat der Unionsgesetzgeber diese erhöhten Anforderungen in die Vorschrift des Art. 45 Abs. 2 transferiert. Sie formulieren einen umfassenden Prüfungskatalog: Die Europäische Kommission hat insbesondere zu berücksichtigen, inwieweit der Drittstaat die Menschenrechte achtet sowie die Rechtsstaatlichkeit und die Grundfreiheiten wahrt. Von besonderer Bedeutung ist auch, ob eine unabhängige Datenschutzbehörde besteht. Die Drittstaaten dürfen in der Folge nur noch die Mittel wählen, mit denen sie ein dem unionalen Datenschutzregime entsprechendes Schutzniveau erreichen.[126] Die Messlatte der „Angemessenheit" hat sich mithin zu derjenigen der „Gleichwertigkeit" verschoben (vgl. insbesondere EG 104 Satz 3 DS-GVO: „dem innerhalb der Union gewährleisteten Schutzniveau der Sache nach gleichwertig" sowie Art. 44 Satz 2: „gewährleistete Schutzniveau […] nicht untergraben wird").[127] Defizite im drittstaatlichen Schutzniveau sind vor diesem Hintergrund nicht mehr hinnehmbar.

#### (1) *Digital Privacy Divide*: Datenschutz in der EU und den USA

##### (a) Privatheit im US-amerikanischen Verfassungsrecht

Die *United States Bill of Rights* (also die ersten zehn Zusatzartikel zur US-Bundesverfassung) aus dem Jahr 1791 verankert – dem historischen Kontext geschuldet – nicht explizit ein Grundrecht auf Privatheit.[128] Auch der *Supreme Court of the United States* hat ein solches

[123] *Schantz/Wolff* (Fußn. 42), Rdnr. 756; *Schlender*, in: Gierschmann/Schlender/Stenzel et al. (Hrsg.), DSGVO, 2018, Art. 45 Rdnr. 21.
[124] Vgl. *Schröder*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 45 DSGVO Rdnr. 11.
[125] EuGH, Urteil vom 6.10.2015, ECLI:EU:C:2015:650, Rdnr. 72 f. – Schrems.
[126] *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), DatenschutzR, 2019, Art. 45 Rdnr. 6.
[127] Ebenso *Schantz* (Fußn. 126), Art. 45 Rdnr. 6; *Schröder* (Fußn. 124), Art. 45 DSGVO Rdnr. 13; *Towfigh/Ulrich*, in: Sydow (Hrsg.), DS-GVO, 2. Aufl., 2018, Art. 45 Rdnr. 10; *Zerdick*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2. Aufl., 2018, Art. 45 Rdnr. 6 f.
[128] Das US-amerikanische Verständnis von *Privacy* haben stattdessen die Rechtsanwälte *Samuel D. Warren* und *Louis D. Brandeis* in ihrer Abhandlung „The Right to Privacy" (Harvard Law Review 4, 193 ff.) aus dem Jahre 1890 geprägt. Sie formulierten – erstmalig unter Rückgriff auf das „right to be let alone" – einen für das *Common Law* innovativen Ansatz des Privatheitsschutzes. Im Vordergrund stand das Bemühen, ein deliktsrechtliches Abwehrrecht gegenüber der aufkommenden „Yellow Press" zu begründen. Der Aufsatz hat auch weit über den nordamerikanischen Kontinent hinaus Wirkung in der Rechtswissenschaft entfaltet; s. bspw. BGH, Urteil vom 19.12.1995, BGHZ 131, 332 (337) oder den Rückgriff auf den Topos „right to be let alone" in BVerfG, Urteil vom 5.6.1973, BVerfGE 35, 202 (233).

Recht bis heute nicht entwickelt[129].[130] Das oberste US-Gericht hat insbesondere nie ein verfassungsrechtliches „Right to Information Privacy" anerkannt.[131]

Grundrechtlichen Schutz erfährt der Betroffene eines staatlichen Eingriffs in seine Privatheit in den USA stattdessen vor allem aus dem *4. Zusatzartikel zur Bundesverfassung*. Dafür muss er vernünftigerweise erwarten dürfen („reasonable expectations"), dass seine Privatheit in der spezifischen Situation gewährleistet ist (was insbesondere in seiner eigenen Wohnung der Fall ist).[132]

Die sog. „Third Party Doctrine" schränkt die Reichweite des 4. Zusatzartikels jedoch erheblich ein: Wer freiwillig seine Daten an Dritte preisgibt, ist nicht dagegen geschützt, dass diese den Datensatz an Behörden weiterleiten.[133] Verpflichten bspw. US-amerikanische Strafverfolgungsbehörden einen MOOC-Anbieter, Daten herauszugeben, können sich die betroffenen Nutzer mithin nicht auf den 4. Zusatzartikel berufen: Sie dürfen nach seiner Wertung vernünftigerweise nicht mehr erwarten, dass ihre Privatheit weiterhin gewahrt ist, wenn sie zuvor in die Verarbeitung eingewilligt haben.

Da das US-amerikanische Verfassungsrecht zudem keine mittelbare Drittwirkung des 4. Zusatzartikels kennt, erwächst aus ihm auch kein Schutz gegenüber Privaten.[134] Ausländer ohne Wohnsitz in den USA genießen überdies grundsätzlich gar keinen Schutz aus dem 4. Zusatzartikel.[135] Die „reasonable expectation" eines Unionsbürgers auf Privatheit ist aus Sicht des US-amerikanischen Verfassungsrechts also nicht geschützt.

### (b) Einfachgesetzliches Datenschutzregime in den USA

Nicht nur im Verfassungsrecht verbürgen die USA keinen mit dem Unionsrecht vergleichbaren Privatheitsschutz. Sie kennen auch keine einheitliche Datenschutzgesetzgebung.[136] Vielmehr bestehen unterschiedliche Regelwerke für einzelne Sachgebiete und Bundesstaaten.[137] Bspw. begründet der *Privacy Act of 1974* individuelle

---

[129] Die kalifornische Verfassung kennt hingegen seit einer Volksabstimmung im Jahr 1972 – ebenso wie andere einzelstaatliche Verfassungen – ein explizites Grundrecht auf Privatheit (Art. 1 § 1). Weiterführend dazu *Kelso*, Pepperdine Law Review 19 (1992), 327 (328 ff.).
[130] *Klar/Kühling*, AöR 141 (2016), 165 (177).
[131] Whalen v. Roe, 429 U.S. 589, 599 f. (1977); Nixon v. General Services Administration, 433 U.S. 425, 457 (1977); NASA v. Nelson, 131 S.Ct. 746, 751 (2011).
[132] Wegweisend hierfür war die Entscheidung Katz v. United States, 389 U.S. 347, 366 (1967).
[133] Couch v. United States, 409 U.S. 322, 335 (1973); United States v. Miller, 425 U.S. 435, 442 (1976); Smith v. Maryland, 442 U.S. 735, 744 f. (1979). Eine Trendwende könnte jedoch aus dem Urteil des *Supreme Court* in der Rechtssache "Carpenter v. United States" folgen. Dazu *Weinzierl*, Der Fall Carpenter – Seismische Veränderungen im U.S. Datenschutzrecht?, JuWissBlog Nr. 69/2018 vom 11.7.2018.
[134] *Klar/Kühling* (Fußn. 130), S. 180.
[135] United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990).
[136] Sog. *omnibus legislation* (s. *Schwartz*, Harvard Law Review 126 [2013], 1966 [1973 f.]. Die US-amerikanischen Rechtswissenschaft stuft eine solche als Hindernis für Innovation ein und lehnt sie daher ab. S. *Schwartz*, The Yale Law Journal 118 (2009), 902 (928).
[137] Eine Vorreiterfunktion nimmt dabei der kalifornische Gesetzgeber ein. Am 28.6.2018 hat der *California Consumer Privacy Act* (CCPA) ein der DS-GVO zumindest vergleichbares Gesetz geschaffen. Es gewährleistet die

Zugangsrechte für personenbezogene Daten, die US-Bundesbehörden gespeichert haben.[138] Der Anspruch steht indes nur US-Staatsbürgern oder Ausländern mit dortiger Aufenthaltsgenehmigung zu.[139]

Einen Vorzug bergen die bereichsspezifischen Regelungen der USA jedoch – vor allem im Verhältnis zu den weitestgehend allgemein gehaltenen und technologieneutralen Vorgaben der DS-GVO: Sie verheißen grundsätzlich hohe Rechtssicherheit und ausdifferenziertere Schutzmechanismen für den Einzelnen.[140]

Der Regelungsansatz der beiden Regime ist aber geradezu antagonistisch: Während unter Geltung der DS-GVO die Verarbeitung personenbezogener Daten jeweils einer spezifischen Erlaubnis bedarf, gilt in den USA das exakte Gegenteil: Grundsätzlich ist jeder Verarbeitungsvorgang zulässig.[141] Beschränkungen erwachsen – neben den punktuellen gesetzlichen Regelungen – aus der Selbstregulierung.

Jenseits des Atlantiks hat sich auch keine Aufsichtsstruktur etabliert, die den Datenschutz-Aufsichtsbehörden in der EU entspricht.[142] Allein die *Federal Trade Commission* nimmt auf Bundesebene eine im Ansatz vergleichbare Position ein. Sie sanktioniert u. a. Unternehmen, die ihre eigenen Datenschutzvorschriften (*Privacy Policies*) missachten und somit gegen geltendes Wettbewerbsrecht (*Federal Trade Commission Act*) verstoßen.[143] Grundsätzlich müssen Betroffene ihre Rechte jedoch selbst durchsetzen.[144] Sie können sich in den USA nicht darauf verlassen, dass der Staat sich schützend vor ihre Privatsphäre stellt. Diese Entwicklung des US-amerikanischen Datenschutzrechts ist sowohl das Produkt des hohen Stellenwerts der *Freedom of Speech* (Meinungsfreiheit)[145] des 1. Zusatzartikels zur US-Bundesverfassung als auch der geteilten Gesetzgebungskompetenz zwischen der Bundesebene und den Einzelstaaten.[146]

### (c) Der *Family Educational Rights and Privacy Act*

Für den speziellen Bereich der Bildung gilt in den USA der *Family Educational Rights and Privacy Act* (FERPA)[147] aus dem Jahr 1974. Das Bundesgesetz verleiht (in- wie ausländischen) Studierenden ein Auskunftsrecht gegenüber ihrer Hochschule über ihre Daten (*Student*

---

informationelle Selbstbestimmung der Betroffenen indes durch Opt-out-Regelungen und einen nur eingeschränkten Rechtsschutz. S. weiterführend *Determann*, ZD 2018, 443 (443 ff.); *Lejeune*, CR 2018, 569 (569 ff.).

[138] 5 U.S.C. § 552a (d).

[139] 5 U.S.C. § 552a (a) (2).

[140] *Determann*, NVwZ 2016, 561 (563).

[141] *Schwartz* (Fußn. 136), S. 1978.

[142] *Determann* (Fußn. 140), S. 565; *Lejeune*, CR 2013, 755 (755).

[143] *Börding*, CR 2016, 431 (436).

[144] *Determann* (Fußn. 140), S. 565; *Klar/Kühling* (Fußn. 130), S. 181.

[145] Datenschutzgesetze sind stets daran zu messen, ob sie potenziell die Meinungsfreiheit verletzen. S. *Klar/Kühling* (Fußn. 130), S. 178.

[146] *Lejeune* (Fußn. 142), S. 755.

[147] 20 U.S.C. § 1232g, 34 C.F.R. 99.

*Records*). [148] Eine Datenweitergabe an Dritte unterwirft es grundsätzlich einem Einwilligungserfordernis.[149]

Dass der FERPA überhaupt auf MOOC-Anbieter bzw. Nutzer Anwendung findet, versteht sich dabei nicht von selbst.[150] Denn ein Anbieter ist an dessen Vorschriften grundsätzlich nur dann gebunden, wenn er Bundesmittel erhält.[151] In der Regel kommen MOOCs jedoch ohne staatliche Subventionen aus. Ein Kooperationsverhältnis zwischen einer US-amerikanischen Hochschule, die der Bund fördert, und einem Anbieter kann Letzteren dazu verpflichten, die gesetzlichen Bestimmungen des Bundesgesetzes einzuhalten.[152] Sofern ein europäischer Nutzer aber einen Online-Kurs bei einem MOOC-Anbieter belegt, der nicht unter diese Voraussetzungen fällt, steht er auch nicht unter dem Schutz des FERPA.

Selbst wenn der FERPA im Einzelfall einschlägig sein sollte, ist sein Schutzniveau begrenzt. Da er der Haushaltsgesetzgebung entstammt, besteht seine einzige Sanktion darin, die Fördermittel durch das *Department of Education* zu kürzen.[153] Von dem unionsrechtlichen Datenschutzregime unterscheidet er sich zudem darin, dass er dem Betroffenen keine wirksamen Rechtsmittel an die Hand gibt, um gegen einen MOOC-Anbieter vorzugehen, der ihn in seinen Rechten aus dem FERPA verletzt. Denn das Bundesgesetz gewährt generell keine individuellen Rechtspositionen.[154]

### (d) Zwischenfazit

Ein Vergleich des unionalen mit dem US-amerikanischen Datenschutzkonzept und der unterschiedlichen Ansätze, Persönlichkeitsrechte durch rechtliche Maßnahmen zu sichern, fördert einen „Digital Privacy Divide“[155] zu Tage: Das amerikanische Recht gewährt Nutzern eines US-amerikanischen MOOCs keinen mit der DS-GVO gleichwertigen Betroffenenschutz. Nur wenn der Privacy Shield dieses Ungleichgewicht tatsächlich austarieren kann, gewährleistet er im Ergebnis auch ein angemessenes Datenschutzniveau für Datentransfers in die USA.[156]

---

[148] 34 C.F.R. §§ 99.7, 10 (2014).
[149] 20 U.S.C. § 1232g (b) (1).
[150] *Young*, Harvard Journal of Law & Technology 28 (2015), 549 (570 ff.).
[151] *Young* (Fußn. 150), S. 572 f.
[152] *Young* (Fußn. 150), S. 573 f.
[153] *Polonetsky/Tene*, Vanderbilt Journal of Entertainment & Technology Law 17 (2015), 927 (960); *Young* (Fußn. 150), S. 589 f.
[154] Gonzaga University v. Doe, 536 U.S. 273, 290 (2002).
[155] *Reidenberg*, Houston Law Review 38 (2001), 717 (718).
[156] Gewiss grenzt es zum Teil an eine Hybris der alten Welt, das (aus europäischer Sicht) „richtige“ Maß an Datenschutz jedem anderen Staat der Welt überstülpen zu wollen. An der Tatsache, dass das Datenschutzrecht der Union kraft gesetzlichen Befehls maßgeblich dafür ist, die Angemessenheit nach Art. 25 DS-RL bzw. Art. 45 DS-GVO zu bestimmen, ändert die Sorge vor einem „europäischen Privacy-Imperialismus“ *de lege lata* dennoch nichts.

### (2) Privatheitsschutz gegenüber privaten Akteuren

#### (a) System der Selbstzertifizierung des Privacy Shield

Die USA haben sich in ihrem Selbstzertifizierungssystem des Privacy Shield gegen die höhere Bindungswirkung entschieden, die von einem staatlich festgelegten Schutzstandard (mitsamt staatlicher Sanktionierung) ausginge. Ob das so erreichte Datenschutzniveau demjenigen der DS-GVO äquivalent ist, hängt letztlich davon ab, ob es in seinem Rahmen hinreichend zuverlässig möglich ist, die beteiligten Unternehmen zu überwachen und zu kontrollieren.[157]

Beim Privacy Shield erfolgt die Kontrolle durch das *Department of Commerce* (DOC) bzw. die *Federal Trade Commission* (FTC) oder das *Department of Transport* (PS-Anhang IV bzw. V). Der Blick auf die bisherige Praxis legt jedoch offen, dass es faktisch in erster Linie den betroffenen Unternehmen selbst obliegt, ob sie die Datenschutzgrundsätze umsetzen.[158] Das kommt nicht von ungefähr: Es entspricht dem in den USA traditionell verankerten Prinzip der Selbstregulierung. Die US-Behörden konzentrieren sich weniger auf die unmittelbare staatliche Aufsicht laufender Geschäftsprozesse. Ihr Fokus liegt vielmehr auf dem jährlichen (Re-)Zertifizierungsprozess und seinen formellen Anforderungen.[159]

Das Selbstzertifizierungssystem haben die USA inzwischen jedoch einigen Neuerungen unterzogen. Während das DOC bislang ausschließlich reaktiv tätig wurde, führte es unterdessen rund 100 Stichprobenkontrollen auf Unternehmenswebsites durch. Es überprüfte bspw., ob die Datenschutzerklärungen öffentlich einsehbar oder die Ansprechpartner für Beschwerden und Auskunftsersuchen ordnungsgemäß benannt sind.[160] Außerdem hat sich die Aufsicht verstärkt des Missstands irreführender Angaben über die Teilnahme am Privacy Shield angenommen. So möchte sie erreichen, dass die Betroffenen besser nachvollziehen können, ob ein Unternehmen aktuell zertifiziert ist oder nicht.[161] Das DOC hat auch die offizielle Liste der zertifizierten Unternehmen (EG 31 ff. PS) reformiert: Sie listet Unternehmen nunmehr erst dann, wenn der erstmalige Zertifizierungsprozess auch abgeschlossen ist.[162]

So begrüßenswert diese Maßnahmen auch sind: Entscheidend für das Datenschutzniveau ist, dass die zertifizierten Unternehmen die Datenschutzgrundsätze des Privacy Shield tatsächlich einhalten.[163] Die FTC kontrolliert zwar nun *ex officio* die Datenschutzpraxis der Unternehmen: Sie holt von ihnen mittels Verwaltungsanordnung Informationen ein. Tiefergehende Nachweise über die Wirkung dieses Vorgehens ist die Behörde der EU-Kommission aber

---

[157] EuGH, Urteil vom 6.10.2015, ECLI:EU:C:2015:650, Rdnr. 81 – Schrems.
[158] *Artikel-29-Datenschutzgruppe*, EU – U.S. Privacy Shield – First annual Joint Review, WP 255, 2017, S. 10.
[159] *Dienste der Europäischen Kommission*, Second annual review of the functioning of the EU-U.S. Privacy Shield, SWD(2018) 497 final, 2018 S. 4 ff.
[160] *Dienste der Europäischen Kommission* (Fußn. 159), S. 8 f.
[161] *Dienste der Europäischen Kommission* (Fußn. 159), S. 10 ff.
[162] *Dienste der Europäischen Kommission* (Fußn. 159), S. 6.
[163] *European Data Protection Board*, EU-U.S. Privacy Shield – Second Annual Joint Review, 2019, S. 5.

schuldig geblieben.[164] Wie engmaschig die Kontrolle realiter ist, ist daher unklar. Um Äquivalenzanforderungen zu genügen, müssten US-Behörden auch umfangreiche (unangekündigte) inhaltliche Routinekontrollen durchführen können. So wäre eine effektive Überwachung gewährleistet. Angesichts der Vielzahl der zertifizierten Unternehmen (immerhin 3850 an der Zahl) geht davon anderenfalls der negative Anreiz aus, mit den Vorgaben des Privacy Shield mehr als flexibel und kreativ umzugehen – Umgehungsstrategien wären Tür und Tor geöffnet. Im Zweifel mutiert die Zertifizierung dann zu einem Feigenblatt, hinter dem sich ein (nach wie vor) laxer Umgang mit personenbezogenen Daten versteckt.[165]

### (b) Rechtsschutz gegen zertifizierte Unternehmen

Ein „angemessenes" Datenschutzniveau impliziert nicht notwendig eigenständige Rechtsschutzmöglichkeiten Betroffener. Im Grundsatz kann es ausreichen, dass die Aufsichtsbehörde die Kontrolle vermittelt. Die DS-GVO geht jedoch einen Schritt weiter: Sie verbürgt Betroffenen nicht nur das Recht, sich an eine Aufsichtsbehörde zu wenden. Sie gewährleistet ihnen auch umfassenden gerichtlichen Rechtsschutz gegen den Verantwortlichen (Art. 79 ff. DS-GVO). Gleichwertig ist das Datenschutzniveau des Privacy Shield daher nur dann, wenn er Unionsbürgern hinreichende Rechtsschutzmöglichkeiten für die vorgesehenen zahlreichen Rechte zugesteht oder das Defizit anderweit ausgleicht.

Der Privacy Shield verpflichtet zertifizierte Unternehmen, jedem Unionsbürger kostenlose und direkte Anfragen zu gestatten (EG 43 PS).[166] Darüber hinaus kann er eine unabhängige Beschwerdestelle (zumeist Streitschlichtungsstellen in den USA, sog. *Alternative Dispute Resolution Bodies*) in Anspruch nehmen (EG 45 PS). Die dafür notwendigen Kontaktdaten muss das jeweilige Unternehmen in seinem Listeneintrag beim *Department of Commerce* (DOC) angeben. Zudem kann sich der Betroffene an die eigene nationale Datenschutz-Aufsichtsbehörde wenden (EG 48 PS). Kraft deren Vermittlung kann der Betroffene seine Beschwerde auch beim DOC einreichen (EG 52 PS). Im äußersten Fall kann er das sog. Privacy-Shield-Panel anrufen (EG 56 ff. PS). Als Schiedsgericht ist es die oberste Instanz im Rechtsschutzsystem des transatlantischen Datentransfers. Bleibt auch dieser Weg ohne Erfolg, kann der Betroffene die zuständigen US-Gerichte anrufen (EG 59 PS).

---

[164] *Dienste der Europäischen Kommission* (Fußn. 159), S. 13.

[165] Allen Bedenken zum Trotz muss ein Selbstzertifizierungssystem nicht zwingend in ein niedrigeres Schutzniveau münden. Das Risiko, öffentlich als Datenschutzsünder angeprangert zu werden, sowie potenzielle Betroffenenentschädigungen (III. 11. e. PS-Anhang II) können Unternehmen nachhaltig davon abhalten, sich datenschutzwidrig zu verhalten. Der Zertifizierungsprozess geht (ähnlich wie eine Datenschutz-Folgenabschätzung i. S. d. Art. 35 DS-GVO) mit einer Vorabkontrolle einher. Diese zwingt die Unternehmen dazu, sich von Anfang mit den bestehenden Datenschutzvorgaben auseinanderzusetzen, wenn sie ihre Verarbeitung auf den Privacy Shield stützen wollen. Ein Modell der Zertifizierung kann die relevanten Geschäftsprozesse in praxi unter Umständen besser auf Datenschutzbedürfnisse einschwören als eine zwar denkbare, aber realiter nur selten zupackende „harte Hand", mit der Aufsichtsbehörden durchgreifen.

[166] Die Bearbeitungszeit hierfür beträgt maximal 45 Tage (EG 44 PS).

Allen differenzierten Rechtsschutzmöglichkeiten zum Trotz: Den Maßstäben und Möglichkeiten des DS-GVO-Standards genügt der Rechtsschutz unter dem Privacy Shield nicht. Die kärgliche Informationspolitik der zertifizierten Unternehmen erschwert es dem Betroffenen oftmals, seine Rechte umfassend geltend zu machen.[167] Und selbst wenn er im Grundsatz dazu bereit sein sollte, auf prozessualem Wege gegen den Verarbeitenden zu Felde zu ziehen, muss er regelmäßig erst die abschreckend hohen Anwaltskosten in den USA auf sich nehmen, um seine Anliegen durchzusetzen.[168] Um einen effektiven Rechtsschutz für Unionsbürger zu sichern, müsste die nationale Datenschutz-Aufsichtsbehörde den Betroffenen im Panel *vertreten*, nicht nur *beraten* dürfen.[169] Zumindest sollte der Fonds, den das DOC eingerichtet hat, um die Schiedsverfahren zu finanzieren (vgl. EG 57 PS), die Anwaltskosten Betroffener decken.

### (3) Privatheitsschutz gegenüber staatlichen Akteuren

#### (a) Unbegrenzte Datenerfassung durch US-Sicherheitsbehörden

Die Union und die USA unterscheiden sich nicht nur in der Praxis *unternehmerischer* Datenverarbeitung. Auch der Umfang *staatlichen Zugriffs* auf private Daten bewegt sich in grundlegend anderen Dimensionen. US-Sicherheitsbehörden verarbeiten personenbezogene Daten aus Online-Angeboten ohne klar erkennbare Grenzen.[170]

##### (aa) Der *Foreign Intelligence Surveillance Act*

Die weitreichenden Befugnisse der US-amerikanischen Sicherheitsbehörden stützen sich vornehmlich auf § 702 des *Foreign Intelligence Surveillance Act* (FISA)[171]. Auf ihm basieren die Überwachungsprogramme PRISM and UPSTREAM. FISA gestattet es den Nachrichtendiensten, (vornehmlich) Menschen ohne US-Staatsbürgerschaft außerhalb den USA auszuspähen.[172] Auch Unionsbürger gehören zur Zielgruppe der Nachrichtendienste.

Die US-Regierung diagnostiziert selbst gleichwohl keine unbegrenzte Massenüberwachung: Die Sicherheitsbehörden beschränkten sich darauf, durch konkrete *Selectors* (Suchkriterien)

---

[167] Vgl. *Artikel-29-Datenschutzgruppe* (Fußn. 158), S. 8 f.
[168] *Molnár-Gábor/Kaffenberger*, ZD 2018, 162 (163).
[169] Vgl. *Weichert*, ZD 2016, 209 (211).
[170] EuGH, Urteil vom 6.10.2015, ECLI:EU:C:2015:650, Rdnr. 93 f. – Schrems. Zum Gesamtbild gehört jedoch auch, dass (rechtswidrige) nachrichtendienstliche Tätigkeiten keineswegs ein ausschließlich US-amerikanisches Phänomen sind. Im Zuge der Enthüllungen *Snowdens* trat bspw. auch der Datenaustausch des britischen *Government Communications Headquarters* mit zahlreichen Nachrichtendiensten weltweit zu Tage (*King*, Snowden spyware revelations: we need to unmask the five-eyed monster, The Guardian online vom 26.11.2013). Erst im Juni 2018 wurde bekannt, dass der BND zwischen 1999 und 2006 Privatpersonen und Unternehmen in Österreich ausgespäht haben soll (*Riedl*, Ausgespäht: Warum hat der deutsche Nachrichtendienst in Österreich spioniert?, Zeit Online vom 22.6.2018).
[171] 50 U.S.C. ch. 36.
[172] Vgl. 50 U.S.C. § 1881a (a), (b).

bestimmte *Targets* (Zielpersonen) auszuwählen.[173] Im Jahre 2018 befanden sich aber immerhin über 164.000 solcher *Targets* unter Überwachung.[174]

(bb) Das Ende der Ungleichbehandlung? Die *Presidential Policy Directive 28*

Die *Presidential Policy Directive 28* (PPD-28),[175] die noch auf die Präsidentschaft *Barack Obamas* zurückgeht, hat unterdessen den Schutz ausländischer Bürger verbessert: Sie verfolgt das Ziel, die rechtliche Ungleichbehandlung von US-Staatsbürgern und Ausländern zu beenden (§ 4). Aus der Direktive erwachsen indes ausdrücklich weder Individualrechte (§ 6 [d] PPD-28) noch hat sie als präsidiale Direktive Gesetzeskraft.

Auch der massenhaften Datenerhebung durch US-Sicherheitsbehörden hat sie keineswegs einen unverrückbaren Riegel vorgeschoben: Die Direktive beschränkt die Massenüberwachung zwar auf sechs Zwecke der nationalen Sicherheit (§ 2 PPD-28). Ihre Fußnote 5 formuliert jedoch eine wichtige Rückausnahme: Die Beschränkungen der Massenüberwachung erfassen *temporär* gespeicherte Daten nicht. Was „temporär" in diesem Zusammenhang bedeutet, lässt der Text offen. US-Nachrichtendienste können daher im Grundsatz weiterhin in großem Umfang Daten europäischer Bürger ausspähen.[176]

Die Europäische Kommission erkennt in den Defiziten der Direktive (wenig überzeugend) keinen wesentlichen Malus. Die Schutzerweiterungen der PPD-28 reichen ihr als Argument dafür, dass das US-amerikanische Datenschutzniveau nunmehr gleichwertig sei.[177] Sie verknüpfte damit zwar zugleich die Erwartung, dass die notwendige Verlängerung des § 702 FISA dem Rechtsschutz der PPD-28 auch tatsächlich Gesetzeskraft verleiht.[178] Diese Hoffnung hat der US-amerikanische Gesetzgeber aber enttäuscht: Am 19.1.2018 verlängerte er § 702 FISA ohne eine solche Ergänzung bis 2023.[179] Nichtsdestotrotz hat die Kommission ihre Beurteilung des Datenschutzniveaus in den USA in ihrem zweiten Prüfbericht[180] nicht revidiert.[181]

---

[173] *Artikel-29-Datenschutzgruppe* (Fußn. 158), S. 15.
[174] *Office of the Director of National Intelligence*, Statistical Transparency Report Regarding Use of National Security Authorities – Calendar Year 2018 -, 2019 S. 13.
[175] S. https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.
[176] *Goitein*, The Privacy and Civil Liberties Oversight Board's Disappointing Report on PPD-28 Implementation, https://www.justsecurity.org/61199/privacy-civil-liberties-oversight-boards-disappointing-report-ppd-28-implementation/..
[177] *Europäische Kommission*, Erster Bericht zur jährlichen Überprüfung der Funktionsweise des EU-US-Datenschutzschilds, COM(2017) 611 final, 2017, S. 4.
[178] *Europäische Kommission* (Fußn. 177), S. 7.
[179] *Spies*, ZD-Aktuell 2018, 05932.
[180] *Europäische Kommission*, Zweiter Bericht zur jährlichen Überprüfung der Funktionsweise des EU-US-Datenschutzschilds, COM(2018) 860 final, 2018, S. 6.
[181] Immerhin habe der US-amerikanische Gesetzgeber das Schutzniveau für Unionsbürger auch nicht abgesenkt und die Befugnisse der Nachrichtendienste nicht ausgeweitet (*Dienste der Europäischen Kommission* (Fußn. 159), S. 26). Kritisch hierzu *Botta*, Augen zu und durch? Der neue Kommissionsbericht zum EU-US Privacy Shield, JuWissBlog Nr. 16/2019 vom 12.2.2019.

### (b) Unabhängige Aufsichtsbehörden

Der Unsicherheit über das tatsächliche Ausmaß, in dem US-amerikanische Behörden Daten europäischer Bürger erheben, könnten die USA vergleichsweise einfach begegnen: durch eine Aufsichtsbehörde für die Kontrolle der nachrichtendienstlichen Tätigkeiten. Eine solche fehlt aber bislang.

Die USA kennen zwar seit 2004 das *Privacy and Civil Liberties Oversight Board* (PCLOB). Seine Funktion als unabhängiges Beratungsgremium ist es, darauf zu achten, dass die Regierung im Kampf gegen den Terrorismus nicht den Schutz der Privatsphäre missachtet. Ihm fehlte aber über lange Zeit die ausreichende politische Rückendeckung. Bis Oktober 2018 war das fünfköpfige Gremium, das für einen Beschluss zumindest dreier Mitglieder bedarf, handlungsunfähig.[182]

Auch in diesem Bereich hat es unterdessen aber Nachbesserungen gegeben – vornehmlich durch die Besetzung vakanter Dienstposten. So kann das PCLOB mittlerweile seinen Aufgaben nachkommen.[183] Auch den Bericht des PCLOB zum PPD-28 hat die US-Regierung veröffentlicht – wenn auch nicht aus eigenem Antrieb, sondern auf Druck einer Informationsfreiheitsanfrage des Journalisten *Charlie Savage.*[184] Antworten auf wesentliche Fragen, wie nach der Auslegung der Ausnahmeregelung für lediglich *temporär* gespeicherte Daten (Fußnote 5 PPD-28[185]), lässt der Bericht indes vermissen.[186]

Als Aufsichtskorrelat (und zugleich als Kompensation dafür, dass aus dem PPD-28 keine subjektiven Rechte des Einzelnen erwachsen[187]) sieht der Privacy Shield ergänzend eine Ombudsperson vor. An sie können sich Unionsbürger – vermittelt über die mitgliedstaatlichen Datenschutz-Aufsichtsbehörden – in konkreten Einzelfällen wenden (PS-Anhang III). Im Juni 2019 hat die US-Regierung die Ombudsstelle erstmals ordnungsgemäß besetzt.[188] Zuletzt hatte die Europäische Kommission der US-Regierung hierfür eine Frist bis zum 28.2.2019 gesetzt.[189] Ob die nun ordnungsgemäß ernannte Ombudsperson eine reale Auswirkung auf den Datenschutz europäischer Bürger hat, ist aber unklar. Eine mit Art. 47 GRCh vergleichbare Schutzwirkung greift nur dann, wenn ihr auch hinreichende Befugnisse zukommen.

---

[182] *Kahn*, Trump Nominates Two New Members to the Privacy and Civil Liberties Oversight Board, Lawfare vom 13.3.2018.
[183] *Dienste der Europäischen Kommission* (Fußn. 159), S. 32.
[184] S. https://www.documentcloud.org/documents/5003660-PCLOB-PPD28-Report.html.
[185] Vgl. dazu bereits oben III. 3. a) bb) (3) (a).
[186] *Goitein*, The Privacy and Civil Liberties Oversight Board's Disappointing Report on PPD-28 Implementation, https://www.justsecurity.org/61199/privacy-civil-liberties-oversight-boards-disappointing-report-ppd-28-implementation/..
[187] *European Data Protection Board* (Fußn. 163), S. 19; *Börding* (Fußn. 143), S. 435.
[188] S. https://www.state.gov/privacy-shield-ombudsperson/.
[189] *Europäische Kommission* (Fußn. 180), S. 6.

Der Ombudsstelle steht zwar gegenüber den Nachrichtendiensten ein Informationsrecht zu. Einem europäischen MOOC-Nutzer wird sie bei der Suche nach Informationen darüber, ob die NSA tatsächlich seine Daten ausgespäht hat, aber wenig helfen. Denn die Ombudsperson bestätigt lediglich, „dass [der] Beschwerde ordnungsgemäß nachgegangen wurde und dass die einschlägigen amerikanischen Rechtsvorschriften […] befolgt wurden bzw. bei Nichteinhaltung der Grundsätze der Verstoß abgestellt wurde" (EG 121 Satz 2 PS). Darüber hinaus ist die Ombudsstelle dem US-Außenministerium (*Department of State*) zugeordnet. Dieses hat ein ureigenes Interesse an Nachrichtenaufklärung im Ausland. Dadurch steht ihre Unabhängigkeit zumindest auf tönernen Füßen.[190] Eine ausdrückliche Weisungsfreiheit der Ombudsperson, wie sie die europäischen Datenschutz-Aufsichtsbehörden innehaben (Art. 52 Abs. 1 DS-GVO), kennt der Privacy Shield zudem nicht. Schwer wiegt auch der Umstand, dass dem Einzelnen keine Rechtsmittel zustehen, wenn die Ombudsstelle keine oder nur eine unbefriedigende Auskunft erteilt.[191] Effektiven Rechtsschutz gewährleistet die Ombudsperson deshalb bislang nicht.[192]

### (4) Zwischenfazit

In seiner derzeitigen Konstruktionsform sichert der Privacy Shield – trotz der Reformen im Nachgang zum ersten jährlichen Prüfbericht der Europäischen Kommission – kein Datenschutzniveau, das dem Regelungsregime der DS-GVO auf Augenhöhe begegnen kann. Es mangelt bislang nicht nur an einer ausreichenden Transparenz, insbesondere über die tatsächlich erfolgte Datenverarbeitung durch US-Behörden. Es fehlen auch ausreichende Rechtsschutzinstrumente für Unionsbürger, die ihre Privatsphäre verteidigen möchten. Der Betroffenenschutz im transatlantischen Datenverkehr hat Schlagseite.

Nicht zuletzt der Schutz des FERPA erweist sich (soweit er im Ausnahmefall überhaupt greift) als mangelhaft. Denn er gesteht weder Individualrechte zu noch etabliert er zureichende Sanktionsmittel. Europäische MOOC-Nutzer können bei US-amerikanischen Anbietern deshalb keinen äquivalenten Schutz ihrer personenbezogenen Daten erwarten. Stattdessen müssen sie befürchten, dass ihre personenbezogenen Daten – einmal über den virtuellen Atlantik verschifft – zu gehandelter Ware auf fremden Märkten mutieren. Ihre informationelle Autonomie können sie so nicht in einer Weise wahrnehmen, wie es ihnen die Rechtsordnung der EU verheißt.

---

[190] Vgl. *European Data Protection Board* (Fußn. 163), S. 19; *Börding* (Fußn. 143), S. 439.
[191] *European Data Protection Board* (Fußn. 163), S. 19; *Weichert* (Fußn. 169), S. 216.
[192] *European Data Protection Board* (Fußn. 163), S. 20. Diesen verlangt der EuGH aber (Urteil vom 6.10.2015, ECLI:EU:C:2015:650, Rdnr. 95 – Schrems).

### cc) Wirkung des Angemessenheitsbeschlusses

Die Defizite des Privacy Shield machen ihn rechtswidrig. Sie tangieren aber nicht seine Wirksamkeit. Solange die Kommission ihn nicht selbst aufhebt[193] oder er für nichtig erklärt wird, sind die Mitgliedstaaten und deren Datenschutz-Aufsichtsbehörden daher an ihn gebunden (Art. 291 AEUV, Art. 45 Abs. 3 DS-GVO). Bis dahin darf ein MOOC-Anbieter, der beim US-Handelsministerium zertifiziert ist, die Daten der Nutzer daher – trotz aller Zweifel – weiterhin in die USA transferieren.

Die Bindungswirkung des Durchführungsbeschlusses schließt Kontrollmöglichkeiten der Aufsichtsbehörden über konkrete Verarbeitungsprozesse aber nicht aus: Sie dürfen und müssen seine Rechtmäßigkeit bei der Datenübermittlung von MOOC-Anbietern prüfen.[194] In Deutschland trägt bspw. § 21 BDSG dies dem Bundesbeauftragten für Datenschutz und Informationsfreiheit auf. Hält er den Privacy Shield für rechtswidrig, darf er ihn zwar nicht verwerfen, kann und muss aber einen Antrag auf gerichtliche Entscheidung beim BVerwG stellen (§ 21 Abs. 1 und 3 BDSG).

Die endgültige Entscheidung darüber, ob der Privacy Shield tatsächlich unwirksam ist, trifft dann nicht das BVerwG.[195] Sie bleibt dem Verwerfungsmonopol des EuGH vorbehalten.[196] Solange gilt die Rechtmäßigkeitsvermutung des Privacy Shield (Art. 45 Abs. 1 Satz 1 [„wenn die Kommission beschlossen hat, dass …"]).[197]

Für Übermittlungen im Anwendungsbereich der Richtlinie (EU) 2016/680 „Polizei und Justiz" (sog. JI-RL) gilt etwas anderes: Trotz Angemessenheitsbeschlusses auf der Grundlage des Art. 36 Abs. 3 JI-RL muss in diesen Fällen eine Datenübermittlung „unterbleiben, wenn im Einzelfall ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrender Umgang mit den Daten beim Empfänger nicht hinreichend gesichert ist oder sonst überwiegende schutzwürdige Interessen einer betroffenen Person entgegenstehen" (§ 78 Abs. 2 Satz 1 BDSG).[198] Was der deutsche Gesetzgeber zum Schutz der Strafverfolgung verhindern kann, bleibt ihm zum Schutz der Betroffenen transatlantischer Datenströme nach geltendem Recht also verwehrt.

### dd) Ausblick

Am Horizont des transatlantischen Datenverkehrs ziehen graue Wolken auf. Seine Zulässigkeit steht gänzlich in Frage. Auf dem Spiel stehen einerseits die Rendite der

---

[193] Die Europäische Kommission kann ihn mit Ex-nunc-Wirkung widerrufen, ändern oder zumindest aussetzen (Art. 45 Abs. 5 bis 7 DS-GVO).
[194] Vgl. EuGH, Urteil vom 6.10.2015, ECLI:EU:C:2015:650, Rdnr. 53 ff. (insbes. Rdnr. 57) – Schrems.
[195] Bis zur Entscheidung des EuGH setzt das BVerwG die Entscheidung aus (§ 21 Abs. 5 BDSG).
[196] Vgl. EuGH, Urteil vom 6.10.2015, ECLI:EU:C:2015:650, Rdnr. 61 – Schrems.
[197] Vgl. EuGH, Urteil vom 6.10.2015, ECLI:EU:C:2015:650, Rdnr. 51 – Schrems.
[198] *Molnár-Gábor/Kaffenberger* (Fußn. 168), S. 167 erwägen jedoch i.R.e. systematischen Auslegung, diese Vorschrift auch auf einen Angemessenheitsbeschluss nach Art. 45 DS-GVO anzuwenden.

Goldgruben des Digitalmarkts, andererseits die Privatsphäre der Unionsbürger. Zwar hat das Gericht der Europäischen Union die Nichtigkeitsklage der Datenschutzorganisation *Digital Rights Ireland* (DIR) gegen den Beschluss der Kommission[199] bereits Ende 2017 als unzulässig abgewiesen: Die Datenschutzorganisation sei weder im eigenen noch im Namen seiner Mitglieder klagebefugt.[200] Eine materielle Prüfung des Privacy Shield hat das Gericht indes nicht vorgenommen.[201]

Anderes steht in der Rechtssache „Schrems II" zu vermuten.[202] Denn der EuGH muss aufgrund einer Vorlage des irischen *High Court* auf der Grundlage des Art. 267 AEUV prüfen, ob der Standardvertragsklausel-Beschluss[203] der Kommission sowie der Privacy Shield rechtmäßig sind. Einer gerichtlichen Überprüfung hält der Privacy Shield nach bisherigen Erkenntnissen mutmaßlich nicht stand.[204]

### b) Geeignete Garantien (Art. 46 DS-GVO)

Der Privacy Shield ist nicht der einzige Weg, um einen Datentransfer in die USA zu legitimieren. Auch andere Instrumente können – wenn auch mit Abstrichen im Privilegierungsniveau – einen Ausgleich für das fehlende Datenschutzniveau im jeweiligen Drittstaat gewährleisten. [205] US-amerikanische MOOC-Anbieter könnten den grenzüberschreitenden Datentransfer insbesondere auf geeignete Garantien i. S. d. Art. 46 DS-GVO[206] stützen.[207] Die Unternehmen können so gleichsam eine alternative Route wählen, um die Daten sicher über den Atlantik zu verschiffen.

---

[199] EuG, Beschluss vom 22.11.2017, ECLI:EU:T:2017:838, Rdnr. 7 ff. – Digital Rights Ireland/Kommission.
[200] EuG, Beschluss vom 22.11.2017, ECLI:EU:T:2017:838, Rdnr. 24 ff. – Digital Rights Ireland/Kommission.
[201] EuG, Beschluss vom 22.11.2017, ECLI:EU:T:2017:838, Rdnr. 44. – Digital Rights Ireland/Kommission.
[202] Vorabentscheidungsersuchen des High Court (Irland) v. 9.5.2018, Rs. C-311/18, ABl. 2018 C 249/17. Außerdem liegt dem EuGH auch eine Klage der französischen Nichtregierungsorganisation »La Quadrature du Net« gegen den Privacy Shield zur Entscheidung vor (Rs. T-738/16).
[203] Dazu sogleich unten III. 3. b) bb).
[204] *Weichert* (Fußn. 169), S. 217; *Molnár-Gábor/Kaffenberger*, ZD 2017, 18 (23 f.); zurückhaltender äußern sich *von Lewinski*, EuR 2016, 405 (418 f.) und *Schreiber/Kohm*, ZD 2016, 255 (257 ff.).
[205] *Hladjk*, in: Eßer/Kramer/von Lewinski (Hrsg.), DSGVO/BDSG, 6. Aufl., 2018, Art. 46 DSGVO Rdnr. 3.
[206] Neben BCR und Standarddatenschutzklauseln kommen auch genehmigte Verhaltensregeln (*Codes of Conduct*; Art. 46 Abs. 2 lit. e i.V. mit Art. 40 DS-GVO) als Instrumente in Betracht, um einen transatlantischen Datenverkehr zu legitimieren. Bislang haben diese in der Praxis gleichwohl keine entscheidende Bedeutung erlangt (*Wybitul/Ströbel/Rueß*, ZD 2017, 503 [506]).
[207] Schon als der EuGH den Safe-Harbor-Beschluss für rechtswidrig erklärt hatte, mussten Unternehmen für den transatlantischen Datenverkehr verstärkt auf verbindliche interne Datenschutzvorschriften und Standarddatenschutzklauseln ausweichen (vgl. auch EG 108 Satz 1 DS-GVO).

### aa) Binding Corporate Rules (Art. 46 Abs. 2 lit. b i.V. mit Art. 47 DS-GVO)

Mit verbindlichen internen Datenschutzvorschriften (sog. *Binding Corporate Rules*; BCR)[208] kann eine Unternehmensgruppe oder eine Gruppe von Unternehmen (bspw. ein *Joint Venture*) ein eigenes Datenschutzregime etablieren.[209]

Auch genehmigte[210] BCR gestatten Verarbeitenden jedoch nur, personenbezogene Daten *innerhalb* dieser Gruppe zu übermitteln[211] – nicht aber an Dritte.[212] Sie entfalten keine externe Wirkung und legitimieren daher nicht, dass der Anbieter einer MOOC-Plattform die Nutzerdaten an US-amerikanische Sicherheitsbehörden oder Gerichte weitergibt.[213]

### bb) Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c DS-GVO)

Der Anbieter kann seine transatlantische Übermittlung personenbezogener Nutzerdaten an Dritte anstelle von Binding Corporate Rules auch auf Standarddatenschutzklauseln gründen. Hierfür müssen er und die Empfänger der Nutzerdaten die Klauseln in ihre Vertragsbeziehungen integrieren und einhalten. Die Vertragsparteien müssen insbesondere den Zweckbindungsgrundsatz achten und den Betroffenen Auskunftsrechte gewährleisten.

Standarddatenschutzklauseln zu erlassen, legt die DS-DVO in die Hände der Europäischen Kommission (Art. 46 Abs. 2 lit. c DS-GVO). Die drei Klauselwerke, die sie bereits vor Geltung der DS-GVO beschlossen hat,[214] tragen einen internationalen Datentransfer weiterhin als

---

[208] Die BCR müssen so ausgestaltet sein, dass sie alle beteiligten Unternehmen und deren Beschäftigte binden (Art. 47 Abs. 1 lit. a DS-GVO). Sie müssen den Betroffenen ferner durchsetzbare Rechte, wie Beschwerden und Rechtsbehelfe, vermitteln (Art. 47 Abs. 1 lit. b DS-GVO). Dafür müssen die BCR drittbegünstigend ausgestaltet sein. S. *Artikel-29-Datenschutzgruppe*, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules (updated), WP 256, 2017, S. 6 f.

[209] *Schantz/Wolff* (Fußn. 42), Rdnr. 780.

[210] Die zuständige Datenschutz-Aufsichtsbehörde (Art. 56 Abs. 1 DS-GVO) genehmigt die BCR grundsätzlich im Kohärenzverfahren nach Art. 63 i.V. mit Art. 64 Abs. 1 Satz 2 lit. f DS-GVO (Art. 47 Abs. 1 DS-GVO). Das Genehmigungsverfahren der Aufsichtsbehörden gilt jedoch als langwierig und kosten- bzw. arbeitsintensiv; *Geppert*, ZD 2018, 62 (65); *Wybitul/Ströbel/Rueß* (Fußn. 206), S. 506. Eine kurzfristige Lösungsoption bieten BCR daher nicht, falls der Privacy Shield wegfallen sollte. Sollten MOOC-Anbieter, die Daten in den USA verarbeiten, erwägen, BCR als Rechtsgrundlage zu nutzen, sollten sie also nicht zu viel Zeit verstreichen lassen, bis sie deren Genehmigung bei den zuständigen Behören beantragen. Bislang kann sich noch kein Anbieter auf BCR berufen. S. die Liste der derzeit abgeschlossenen Genehmigungsverfahren: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=613841.

[211] Mangels Hierarchieverhältnisses bilden der Anbieter und seine Kooperationspartner aber *keine Unternehmensgruppe* i. S. d. Art. 4 Nr. 19 DS-GVO. Allenfalls wenn ein Unternehmen einen Anbieter (zumindest faktisch) kontrolliert (vgl. *Schröder*, in: Kühling/Buchner [Hrsg.], DS-GVO/BDSG, 2. Aufl., 2018, Art. 4 Nr. 19 DSGVO Rdnr. 1), bestünde eine Unternehmensgruppe. Bspw. hat das (inzwischen zu *Microsoft* gehörende) Karrierenetzwerk *LinkedIn* den MOOC-Anbieter *Lynda.com* (jetzt *LinkedIn Learning*) übernommen (*Etherington*, LinkedIn To Buy Online Education Site Lynda.com For $1.5 Billion, TechCrunch vom 9.4.2015).

[212] *Pauly*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 47 DSGVO Rdnr. 5; *Schröder*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 47 DSGVO Rdnr. 15.

[213] Vgl. *Metz/Spittka* (Fußn. 94), S. 365.

[214] Europäische Kommission, Entscheidung 2001/497/EG v. 4.7.2001, ABl. L 181/19; Entscheidung 2004/915/EG v. 27.12.2004, ABl. L 385/74; Beschluss 2010/87/EU v. 5.2.2010, ABl. L 39/5.

zulässige Rechtsgrundlagen (Art. 46 Abs. 5 Satz 2 DS-GVO).[215] Standarddatenschutzklauseln verhindern gleichwohl nicht, dass die Datenschutz-Aufsichtsbehörden (bis hin zum Verbot der Datenübermittlung) eingreifen können, wenn ein drittstaatlicher Datenzugriff oder eine Missachtung der Klauseln droht bzw. bereits vorliegt.[216] Muss ein Anbieter umfassend Daten an US-Sicherheitsbehörden oder Gerichte herausgeben, kann das deshalb für die Frage relevant sein, ob er grenzüberschreitend Daten auf Grundlage der Klauseln übermitteln darf. Hinzu kommt, dass die Standarddatenschutzklauseln den Verarbeitenden dazu verpflichten, keinen ihm bekannten nationalen Gesetzen zu unterliegen, die es ihm unmöglich machen, die Klauseln zu befolgen.[217]

Die Klauselwerke können daher nur bedingt einen Rettungsanker für den transatlantischen Datenverkehr bereitstellen. Insbesondere wenn Herausgabepflichten an drittstaatliche Stellen bestehen, gewähren Standarddatenschutzklauseln i. d. R. keinen rechtlichen Halt.

### c) Ausnahmeregelungen (Art. 49 Abs. 1 DS-GVO)

Sollte der Privacy Shield tatsächlich gleichsam im Meer der unionsrechtlichen Anforderungen untergehen und sollten keine geeigneten Garantien i. S. d. Art. 46 DS-GVO bestehen, verbleibt dem Kursanbieter für seine transatlantische Datenübermittlung nur noch ein rettendes Ufer: die Ausnahmetatbestände aus Art. 49 Abs. 1 DS-GVO.

Neben einer ausdrücklichen Einwilligung (Art. 49 Abs. 1 UAbs. 1 lit. a DS-GVO) des Nutzers in die risikobehaftete grenzüberschreitende Datenverarbeitung, kann sich der Anbieter darauf berufen, diese sei erforderlich, um das Vertragsverhältnis zwischen ihm und dem Nutzer zu erfüllen (Art. 49 Abs. 1 UAbs. 1 lit. b bzw. c DS-GVO). Auch hier kommt es nicht darauf an, was der Vertrag dem Anbieter gestattet, sondern wozu ihn der Vertrag *verpflichtet*, um sein Leistungsversprechen einhalten zu können (s. dazu III. 2. b) aa)).

Ein Vertrag zwischen dem MOOC-Anbieter und seinen Geschäftspartnern kann die Datenübermittlung zwar ebenso legitimieren (Art. 49 Abs. 1 UAbs. 1 lit. c DS-GVO) – allerdings nur, wenn die Vertragspflicht auch tatsächlich »im Interesse« des MOOC-Nutzers besteht. Wirtschaftliche Interessen der Nutznießer eines Daten-gegen-Bildung-Modells genügen insoweit nicht.

Auch wenn der Kursanbieter Rechtsansprüche geltend machen, ausüben oder verteidigen möchte (Art. 49 Abs. 1 UAbs. 1 lit. e DS-GDVO), kann dies im Einzelfall gegenüber dem Betroffenenschutz Vorrang genießen. Darauf kann sich der Anbieter insbesondere dann berufen, wenn er die personenbezogenen Nutzerdaten i.R.e. Pre-Trial-Discovery-Verfahrens

---

[215] Die datenverarbeitenden Unternehmen können die Klauselwerke um eigene Regelungen ergänzen, soweit diese nicht inhaltlich mit denen der Kommission kollidieren (EG 109 Satz 1 DS-GVO).
[216] Vgl. Europäische Kommission, Durchführungsbeschluss (EU) 2016/2297 v. 16.12.2016, ABl. L 344/100, welcher eine Konsequenz aus dem EuGH-Urteil in der Rechtssache „Schrems“ war.
[217] Klausel 5 lit. a der E. 2001/497/EC; Klausel Abs. 2 lit. c der E. 2004/915/EG; Klausel 5 lit. b des B. 2010/87/EU.

an Dritte herausgibt.[218] Die Beschränkung auf Rechtsansprüche „vor Gericht“, wie sie noch Art. 26 Abs. 1 lit. d DS-RL (bzw. § 4c Abs. 1 Satz 1 Nr. 4 2. Alt. BDSG a. F.) vorsah, hat die DS-GVO entfallen lassen.

Da diese »Ausnahmen für bestimmte Fälle« nicht das Schutzniveau der DS-GVO unterlaufen dürfen (Art. 44 Satz 2 DS-GVO), sind sie gleichwohl äußerst restriktiv anzuwenden.[219] Sie verbürgen insbesondere nicht bereits als solche ein angemessenes Datenschutzniveau, weil sie im Gegensatz zu Art. 45 und 46 strukturelle Kontrolldefizite nur sehr bedingt ausgleichen. Sie können mithin nie die gesamte Datenfracht eines Kursanbieters ohne die Zustimmung des Nutzers legitimieren.[220]

### d) „Anti-FISA-Klausel“ (Art. 48 DS-GVO)

Soweit der Kursanbieter die Nutzerdaten an US-amerikanische Behörden oder Gerichte übermittelt, setzt die Vorschrift des Art. 48 DS-GVO zusätzliche normative Leitplanken.[221] Sie erklärt Urteile oder Verwaltungsentscheidungen eines Drittstaates, welche die Herausgabe personenbezogener Daten anordnen, nur dann für anerkenn- bzw. vollstreckbar, wenn dem Herausgabeersuchen eine internationale Übereinkunft (bspw. ein Rechtshilfeabkommen) zugrunde liegt oder ein anderer Tatbestand des Kapitels V der DS-GVO greift.[222]

Diese Regelung konnte das Europäische Parlament – mit dem politischen Rückenwind aus den *Snowden*-Enthüllungen in den Segeln – in den Trilog-Verhandlungen in den sicheren „normativen Hafen“ der DS-GVO bringen (daher auch „Lex Snowden“ oder „Anti-FISA-Klausel“ als Replik auf das US-amerikanische Gesetzeswerk zur Auslandsaufklärung).[223]

Obgleich die Formulierung „unbeschadet anderer Gründe für die Übermittlung“ durchaus einen Charakter als Befugnisnorm vermuten lässt: Art. 48 DS-GVO etabliert keinen selbständigen Erlaubnistatbestand. Denn im Unterschied zu Art. 45, 46 und 49 DS-GVO regelt die „Anti-FISA-Klausel“ nicht direkt, ob eine grenzüberschreitende Datenübermittlung zulässig ist. Dafür benötigt der MOOC-Anbieter vielmehr den Rechtsakt der zuständigen Stellen der Union bzw. des Mitgliedstaats, die außereuropäische Urteile bzw. Verwaltungsentscheidungen auf Grundlage eines internationalen Übereinkommens

---

[218] Vgl. *Pauly*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 49 DSGVO Rdnr. 21.
[219] Dies gilt insbesondere für den Ausnahmetatbestand der *zwingenden berechtigten Interessen* (Art. 49 Abs. 1 UAbs. 2 DS-GVO). Er greift nur als letztmögliche Rechtsgrundlage für den internationalen Datentransfer des MOOC-Anbieters.
[220] Vgl. *Artikel-29-Datenschutzgruppe*, Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, WP 114, 2005, S. 8 f.
[221] Art. 48 DS-GVO findet auch auf US-amerikanische Anbieter Anwendung, die Nutzerdaten europäischer Bürger verarbeiten und diese an lokale staatliche Stellen herausgeben sollen. Die Vorschrift bei extraterritorialen Sachverhalten nicht anzuwenden, verstieße gegen die Regelungssystematik der Art. 44 ff. DS-GVO. Ebenso *Schlender*, in: Gierschmann/Schlender/Stenzel et al. (Hrsg.), DSGVO, 2018, Art. 48 Rdnr. 4; a. A. *Schröder*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 48 DSGVO Rdnr. 14.
[222] Nicht erfasst sind Herausgabeersuchen Privater; s. *Pauly*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 48 DSGVO Rdnr. 6; *Schröder* (Fußn. 221), Art. 48 DSGVO Rdnr. 13.
[223] *Pauly* (Fußn. 222), Art. 48 DSGVO Rdnr. 2; *Piltz*, K&R 2016, 777 (779); *Schantz/Wolff* (Fußn. 42), Rdnr. 801.

anerkennen. Auch ein Umkehrschluss aus der Einzelfallregelung des Art. 49 Abs. 1 UAbs. 2 DS-GVO widerstreitet der Natur eines eigenständigen Erlaubnistatbestandes. Als Zulassungsgrundlagen nennt sie Art. 45 und 46, nicht aber Art. 48 DS-GVO.

Im Ergebnis ist Art. 48 DS-GVO überwiegend deklaratorisch. Er verdeutlicht in erster Linie, dass außereuropäische Rechtsvorschriften und Hoheitsakte, die auf deren Grundlage ergangen sind, nicht das Datenschutzniveau der DS-GVO untergraben dürfen.[224] Ob der MOOC-Anbieter datenschutzkonform handelt, wenn er einer ausländischen Herausgabepflicht nachkommt, bemisst sich deshalb weniger nach Art. 48 DS-GVO als allgemeinem Rechtsgrundsatz als an Art. 49 Abs. 1 UAbs. 1 lit. e DS-GVO, der sich in einem solchen Fall regelmäßig als die entscheidende Rechtsgrundlage erweist.[225]

## IV. Fazit

Die Vision, Bildung via MOOC örtlich und zeitlich entgrenzt in die Welt zu tragen, inspiriert die Hochschullehre. Sie hat diese zwar bislang nicht in einer Weise revolutioniert, wie Experten dies zum Höhepunkt ihres Hypes vorausgesagt haben. Dennoch haben sich Online-Kurse zu einer festen Instanz digitaler Bildung gemausert und erfreuen sich großer Beliebtheit. Ihr Erfolgsgeheimnis ist einfach: Sie eröffnen dem Einzelnen die Chance, selbstbestimmt und niederschwellig in neue Wissenswelten einzutauchen. Mit nur einem Klick kann sich grundsätzlich jeder als Harvard- oder Stanford-Studierender fühlen – doch oftmals nur zum Preis, seine Hoheit über die Daten in den Untiefen internationaler Datenströme aufs Spiel zu setzen. Denn wer die digitalen Pforten der virtuellen Bildungsstätten durchquert, offenbart und hinterlässt Informationen über sich, wie sie kein physischer Seminarraum zutage fördern könnte – im Gegenteil: Die Anbieter digitaler Bildungsanwendungen behandeln ihre Nutzer oftmals wie gläserne Studierende.

Sofern die Anbieter Nutzerdaten in den USA verarbeiten, knüpft die DS-GVO daran jedoch besondere datenschutzrechtliche Kontrollmechanismen. Übermittlungen in Drittstaaten sind einerseits an den allgemeinen Zulässigkeitsvoraussetzungen (vornehmlich Art. 9 Abs. 2 und Art. 6 Abs. 1 DS-GVO) zu messen. Diese decken die – häufig praktizierte – Weitergabe der Nutzerdaten an Dritte grundsätzlich nur auf der Grundlage einer Einwilligungserklärung, welche die Drittempfänger dem Nutzer hinreichend klar ausweist. Auch die besonderen Bestimmungen der Art. 44 ff. DS-GVO ziehen dem transatlantischen Datenverkehr enge Grenzen: Als Ausdruck der Vorsicht gegenüber dem Datenschutzniveau von Drittstaatenregimen und des Schutzes der Unionsbürger vor Verletzungen ihrer Privatheitsentfaltung knüpfen die Sicherungsmechanismen der Art. 45 ff. DS-GVO die Datenübermittlung an gleichwertige Datenschutzstandards.

---

[224] *Metz/Spittka* (Fußn. 94), S. 365); *Schantz/Wolff* (Fußn. 42), Rdnr. 802.
[225] *Pauly* (Fußn. 218), Art. 49 DSGVO Rdnr. 22; *Zerdick*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2. Aufl., 2018, Art. 49 Rdnr. 15.

Weder die US-amerikanische Bundesverfassung noch einfachgesetzliche Individualrechte aus dem *Family Educational Rights and Privacy Act* nehmen europäische MOOC-Nutzer bisher unter ihre Schutzgarantie. Den transatlantischen *Digital Privacy Divide* vermag auch der *EU-US Privacy Shield* in seiner derzeitigen Fassung nicht zu überbrücken. Dafür bedürfte es strengerer *Überwachungsmechanismen* für alle Unternehmen, die sich selbst beim US-Handelsministerium zertifiziert haben, um zu überprüfen, ob sie seine Datenschutzgrundsätze tatsächlich einhalten. Denkbar wären bspw. routinemäßige und verdachtsunabhängige Kontrollen.

Auch die individuellen *Rechtsschutzmöglichkeiten* unter dem Privacy Shield verbürgen kein gleichwertiges Datenschutzniveau: Sie sind zwar facettenreich, aber überwiegend außergerichtlich bei Schiedsstellen und zudem äußerst komplex. Um die Betroffenenrechte zu stärken, sollten die Datenschutz-Aufsichtsbehörden den Beschwerdeführer nicht nur unterstützen können, sondern ihn auch im Privacy-Shield-Panel vertreten dürfen. Nicht zuletzt die umfangreichen Aufklärungstätigkeiten der US-Nachrichtendienste gefährden die Privatheit der Nutzer: NSA & Co. greifen in großem Umfang auf die Datenreserven US-amerikanischer Unternehmen zu. Doch die (nun ordnungsgemäß bestellte) Ombudsperson erweist sich nicht als ausreichender Garant einer Aufsicht über die Sicherheitsbehörden. Zudem müsste der US-amerikanische Gesetzgeber die subjektiven Rechte betroffener Ausländer substanziell stärken. Doch statt wirksame Verbesserungen zu verheißen, beschwört der CLOUD Act neue Datenschutzsorgen herauf. Er öffnet mit den Exekutivabkommen eine Hintertür für den Zugriff weiterer Nationalstaaten (ohne gleichwertiges Schutzniveau) auf die Daten europäischer Bürger.

Nach dem derzeitigen Umsetzungsstand des Privacy Shield hätte die Europäische Kommission – gemessen an der reinen Lehre der DS-GVO – in ihrem zweiten Prüfbericht nicht zu dem Ergebnis kommen dürfen, dass das Abkommen ein angemessenes Schutzniveau für Datentransfers in die USA gewährt. Doch auch unabhängig davon, wie man den Kommissionsbericht beurteilt: Die Zukunft des Privacy Shield ist mit Blick auf das bevorstehende EuGH-Urteil in der Rechtssache „Schrems II“ ungewiss.[226] Bis dahin bietet das Abkommen den US-amerikanischen MOOC-Anbietern zwar – vorläufig – wie ein Leuchtturm die Orientierung für eine rechtssichere, grenzüberschreitende Datenverarbeitung. Wer seinen Zustand analysiert, erkennt jedoch: Seine Schutzfunktion für die studentischen Nutzer europäischer Hochschulen gegen die Untiefen des transatlantischen Datenstroms erfüllt es nicht. Auch *Binding Corporate Rules* (interne verbindliche Datenschutzvorschriften) oder Standarddatenschutzklauseln versagen gegenüber dem weiterhin umfassenden Datenzugriff hoheitlicher Stellen in den USA.[227]

[226] Dazu III. 3. a) dd).
[227] Dazu III. 3. b).

Integrieren deutsche Hochschulen die Online-Kurse US-amerikanischer Bildungsunternehmen in ihr Lehrangebot oder erstellen sie in Zusammenarbeit mit einem kommerziellen Plattformbetreiber eigene MOOCs, kann aus dieser Kooperation ausnahmsweise auch eine gemeinsame Verantwortlichkeit der Hochschulen mit dem jeweiligen Anbieter erwachsen (Art. 4 Nr. 7, Art. 26 Abs. 1 Satz 1 DS-GVO). [228] Die Zwangssituationen, welche die Hochschule bspw. durch eine Pflicht, die Online-Kurse zu belegen, gegenüber ihren Studierenden erzeugt, muss sich der MOOC-Anbieter sub specie der Freiwilligkeit der Einwilligung zurechnen lassen.[229]

Selbst soweit deutsche und europäische Hochschulen für die Datenverarbeitung der Anbieter nicht mitverantwortlich sind, ist ihnen mehr Sensibilität gegenüber den Risiken der MOOC-Nutzung für die Privatheit ihrer Studierenden anzuraten. Denn wer über die personenbezogenen Nutzerdaten herrscht, verfügt über die Möglichkeit, tiefgehende Einblicke in die Persönlichkeit der Studierenden zu gewinnen. Empfehlenswert ist es daher, die personenbezogenen Daten europäischer Nutzer ausschließlich in der Union zu speichern. Doch selbst dann wäre ein Zugriff US-amerikanischer Behörden nicht ausgeschlossen, wenn der Anbieter Herausgabepflichten nach US-amerikanischem Recht Folge leisten muss. Daher kann es im Ergebnis für deutsche Hochschulen vorzugswürdig sein, mit einem Anbieter zu kooperieren, der nicht der US-amerikanischen, sondern ausschließlich der europäischen Hoheitsgewalt unterliegt. Die kommerziellen Plattformbetreiber müssten ihr Geschäftsmodell für MOOCs dann unter Umständen grundlegend modifizieren.

Bei der Transformation ihrer Lehre in das digitale Zeitalter sollten die deutschen Hochschulen ihren Kompass im Ergebnis also auf einen Mittelweg zwischen Digitalisierungsnaivität und Datenschutzhysterie ausrichten, auf dem Innovation und Persönlichkeitsschutz Hand in Hand gehen. Dann könnten ihre Studierenden online lernen, ohne den Verlust ihrer informationellen Selbstbestimmung fürchten zu müssen – ganz getreu dem Motto *Wilhelm von Humboldts* „Bilde dich selbst, und dann wirke auf andere durch das, was du bist!“

---

[228] S. III. 2. a) dd) (2) (a).

[229] Zudem kann ein studentischer Nutzer gegenüber seiner mitverantwortlichen Universität mitunter sogar Schadensersatzansprüche geltend machen, die aus den Datenschutzverletzungen des US-amerikanischen Unternehmens erwachsen (Art. 82 Abs. 4 DS-GVO). Die Hochschulen müssen jedoch i. d. R. keine Bußgeldanordnungen der zuständigen Datenschutzbehörden fürchten. Denn die deutschen Landesgesetzgeber haben auf Grundlage der Öffnungsklausel des Art. 83 Abs. 7 DS-GVO entschieden, dass die Aufsichtsbehörden gegen öffentliche Stellen keine Bußgelder verhängen dürfen (s. bspw. § 22 Abs. 3 MVLDSG). Dazu *Martini/Wagner/Wenzel*, VerwArch 108 (2018), 163 (177).