Editorial – Grußwort des Forschungsprojektleiters von «BayWiDI» Prof. Dr. Dirk Heckmann

Sehr geehrte Leserinnen und Leser,

von wegen Sommerpause: Der BGH hat Anfang September zu drei medienwirksamen Verfahren über die Kennzeichnungspflicht von Influencer-Posts auf Social Media entschieden. Im Fokus der Verfahren standen insbesondere sogenannte „Tap Tags“, die beim Anklicken abgebildeter Produkte auf Instagram-Beiträgen angezeigt werden. Die Tap Tags verweisen auf Marken oder Anbieter von Schuhen, Kleidung, Kosmetik oder anderen Produkten und führen beim Anklicken auf das Instagram-Profil des jeweiligen Unternehmens.

Für drei Konstellationen traf der BGH nun eine eindeutige Klarstellung: Fließt für den konkreten Post eine Gegenleistung – also beispielsweise ein Entgelt –, so ist der Beitrag als Werbung zu kennzeichnen. Fehlt es an einer Gegenleistung, ist die Kennzeichnung nur dann nötig, wenn der Gesamteindruck übertrieben werblich ist. Allein die Tatsache, dass Produkte abgebildet und mit Tap Tags versehen werden, genügt hierfür noch nicht. Die Verlinkung auf die Hersteller- bzw. Anbieterseite hingegen begründet nach Ansicht des BGH regelmäßig einen „werblichen Überschuss“. Wirbt ein Influencer oder eine Influencerin für eigene Produkte oder Dienstleistungen, handelt er oder sie also zugunsten des eigenen Unternehmens, so ergebe sich der kommerzielle Zweck unmittelbar aus den Umständen selbst.

Diese mit Spannung erwarteten Urteile dürften zumindest in den meisten Fällen für mehr Klarheit im Instagram-Universum sorgen. Inwieweit beispielsweise eine Verlinkung eines Unternehmens, die dessen Aufmerksamkeit erst erregen soll und künftige Werbe-Kooperationen bezweckt, von den „Influencer I-III“-Fallgestaltungen erfasst werden kann, lässt sich daraus indes nicht ableiten.

Es wird sicherlich nicht das letzte Mal sein, dass sich der Bundesgerichtshof mit Fragestellungen rund um Influencer-Werbung befassen darf.

Interessante Entwicklungen gab es allerdings nicht nur in diesem Bereich. Auch in Bezug auf den Datenschutz lassen sich Neuigkeiten vermelden. Daher ist diese Ausgabe des BayWiDI-Magazins ganz dem Thema Datenschutz gewidmet:

Zunächst ist Julia Schwegler mit einem Überblick über die Entwicklungen im Datenschutzrecht seit Beginn der Corona-Pandemie im März 2020 vertreten.

Anschließend stellt Priska Katharina Büttel das neue chinesische Datenschutzgesetz, das Personal Information Protection Law (PIPL), sowie dessen abzusehende Auswirkungen (unter anderem) auf deutsche Unternehmen vor – und wirft einen genaueren Blick auf die Bezeichnung „chinesische DSGVO“.

Ich wünsche Ihnen eine unterhaltsame Lektüre

Ihr Prof. Dr. Dirk Heckmann
Leiter des Forschungsprojekts «BayWiDI»

Inhalt

- Entwicklungen im Datenschutzrecht im „zweiten Corona-Jahr“ 2021 / 2
- Datenschutz „Made in China“ – Das PIPL und die Auswirkungen auf deutsche Unternehmen / 6
- Leiter des Forschungsprojekts und AutorInnen / 11
- Impressum / 12

Entwicklungen im Datenschutzrecht im „zweiten Corona-Jahr“ 2021

Das vergangene Jahr war in jeder Hinsicht von der Corona-Pandemie und ihren Auswirkungen geprägt. Dies zeigte sich auch im Bereich des Datenschutzrechts, wobei sich hier auch viele Themen unabhängig von der Pandemie weiterentwickeln konnten.

Homeoffice, Remote Work und Arbeitszeiterfassung

Im Zusammenhang mit der Coronakrise wurde im Bereich des Arbeitsrechts einmal mehr deutlich, welch eine große Rolle eine digitalisierte Arbeitswelt spielen kann. Dennoch bringt die Leistungserbringung von zuhause aus unter anderem auch datenschutzrechtliche Schwierigkeiten mit sich. Neben dem erhöhten Schwierigkeitsgrad bei der Geheimhaltung von betriebsbezogenen Daten gegenüber Dritten – wie anderen Haushaltsmitgliedern – bedeutet eine Stelle im Homeoffice oft auch, dass der Arbeitgeber seine Mitarbeiterinnen und Mitarbeiter für die Arbeitszeitnachweiserbringung noch intensiver überwachen muss (oder zumindest: möchte).

Diskutiert wird hier, ob bei der Arbeitszeiterfassung über § 16 Abs. 2 ArbZG hinausgehend die europarechtlichen Vorgaben umgesetzt werden können. Einerseits wird der Gesetzgeber dabei zwingend zum Handeln aufgerufen, andererseits wird das europäische Recht ohnehin bereits als de facto in Kraft angesehen. Allein zur Klarstellung dieser Diskussion ist eine vertragliche Anpassung der Arbeitszeitregelung daher von Vorteil.[1]

Eine weitere Entwicklung stellt das neue Telekommunikation-Telemedien-Datenschutz-Gesetz, kurz TTDG, dar, das ab dem 01.12.2021 gelten wird.[2]

Damit sollen die bisherigen Datenschutzbestimmungen des Telekommunikationsgesetzes (TKG) sowie des Telemediengesetzes (TMG) an die DSGVO angepasst sowie die e-Privacy-Richtlinie RL 2002/58/EG endlich umgesetzt werden.

Die Gesetzesänderung soll darüber hinaus die Rechtsunsicherheit beseitigen, die durch das bisherige Nebeneinanderbestehen von TMG, TKG und DSGVO vorlag. Die Bestimmungen von TMG und TKG wurden dementsprechend in nun einem Gesetz zusammengefasst.[3]

Datenschutzaufsicht: Nicht nur federführende Behörde zuständig

Eine im Juni 2021 verkündete Entscheidung des EuGH[4] hat das Potenzial, die Arbeit der Datenschutzaufsichtsbehörden auf ein neues Niveau zu heben: Im Rahmen eines Rechtsstreits zwischen der belgischen Datenschutzbehörde (als Nachfolgerin des Präsidenten des belgischen Ausschusses für den Schutz des Privatlebens) und Facebook entschied das Gericht unter anderem, dass nationale Datenschutzaufsichtsbehörden auch dann gegen DSGVO-Verstöße vorgehen dürfen, wenn sie selbst nicht die federführende Behörde sind.[5] Voraussetzung dafür ist, dass die DSGVO der Behörde die Zuständigkeit für die betreffende Entscheidung, dass die Verarbeitung datenschutzrechtswidrig ist, verleiht und diese Befugnis unter Beachtung der in der DSGVO vorgesehenen Verfahren der Zusammenarbeit und Kohärenz ausgeübt wird.

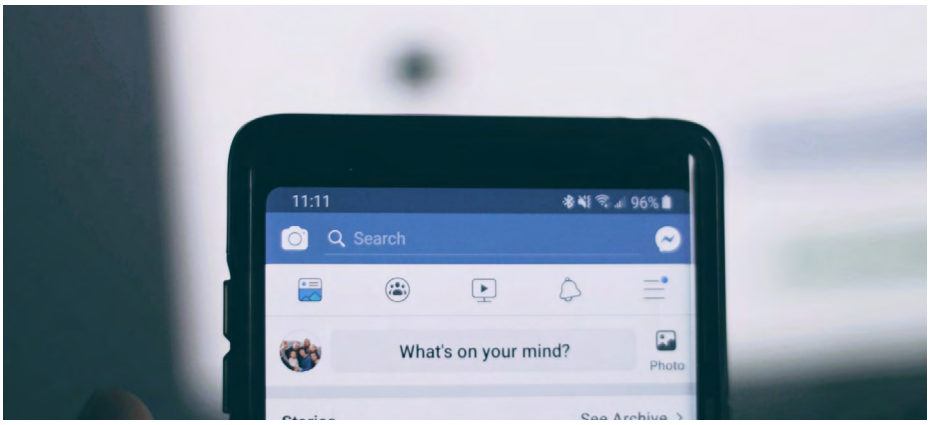
Der EuGH folgte damit dem EuGH-Generalanwalt Michal Bobak, der sich für eine Befugnis der „anderen betroffenen nationalen Datenschutzbehörden […], in Situationen, in denen es ihnen die Datenschutz-Grundverordnung spezifisch gestatte, derartige Verfahren in ihren jeweiligen Mitgliedstaaten einzuleiten“, aussprach.[6] Sofern die Ausübung der Befugnis in den räumlichen Anwendungsbereich der DSGVO fällt, ist eine (Haupt-) Niederlassung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in jenem Mitgliedstaat ausdrücklich nicht vorauszusetzen. Es genügt, wenn der Verantwortliche über eine Niederlassung im Gebiet der Union verfügt. Die Zuständigkeit einer anderen als der federführenden Behörde kann sich dabei aus Art. 65 Abs. 2, Art. 66 DSGVO ergeben

und umfasst – entgegen der Ansicht von Facebook – auch die Befugnis, Gerichtsverfahren einzuleiten.

Schrems II – EuGH kippt EU-US-Privacy Shield

Ein weiteres wichtiges Urteil in Bezug auf internationale Datentransfers aus dem Jahr 2020, das sich auch 2021 auswirkte, war die Schrems-II-Entscheidung vom 16.07.2020.[7] Dessen Ausgangspunkt war eine Beschwerde des österreichischen Datenschutzaktivisten Maximilian Schrems, in welcher er die Datenübermittlung der Facebook Ireland Ltd an die Facebook Inc. in den USA beklagte. Seine preisgegebenen Nutzerdaten waren nach den bisher geltenden Bestimmungen zu transatlantischen Datentransfers und in den USA geltenden Sicherheitsgesetzen auch für Behörden weitreichend zugänglich.[8] Im Laufe des Prozesses änderte Schrems seine Beschwerde und klagte nunmehr gegen die von Facebook verwendeten Standarddatenschutzklauseln und das US Privacy Shield.[9] In der Folge legte der Irish High Court dem EuGH die Frage vor, ob das Privacy Shield, Nachfolger des Safe-Harbour-Abkommens, wirksam sei.[10] Dieser stellte zunächst klar, dass das EU-Datenschutzrecht bei der gesamten Datenübermittlung in ein Drittland einschließlich dortiger Verarbeitungsprozesse als Bewertungsmaßstab zu berücksichtigen ist, selbst wenn die übermittelten Daten dort für Zwecke der nationalen

Sicherheit verwendet werden. Ein angemessenes Datenschutzniveau ist durchgehend zu gewährleisten und muss dem Schutzniveau der EU-DSGVO sowie der Grundrechtecharta entsprechen.[11] Die Sicherheitsgesetze der USA räumen den zuständigen Behörden weitreichende Befugnisse für den Zugriff auf personenbezogene Daten ein, während die europäischen Bürger, die davon betroffen sind, keine diesbezüglichen gerichtlichen Kontrollen durchsetzen können. Dies stelle Eingriffe in die Achtung auf Privatsphäre, den Schutz personenbezogener Daten und den effektiven gerichtlichen Rechtsschutz und damit in die Art. 7, 8 und 47 der EU-Grundrechtecharta dar. Die Regeln des Privacy Shields gewährten so den US-Sicherheitsgesetzen den Vorrang gegenüber den Rechten der Betroffenen.[12] Davon ausgehend entschied der EuGH, dass das Privacy Shield kein angemessenes Schutzniveau biete und demensprechend keine geeignete Grundlage für die Datentransfers in die USA darstelle.[13]



Überarbeitungsbedürftige Standardvertragsklauseln

Demgegenüber bewertete der EuGH die Standarddatenschutzklauseln als gültig. Begründet wurde dies damit, dass sie wirksame Schutzmechanismen enthalten, die sicherstellen, dass das erforderliche Schutzniveau eingehalten wird. Der Datenempfänger versichert dadurch, keinen Gesetzen des Drittlandes zu unterliegen, die dem Einhalten seiner Pflichten aus den Standarddatenschutzklauseln entgegenstehen.

Als Einschränkung stellte das Gericht jedoch fest, dass Unternehmen beim Einsatz solcher Klauseln umfangreiche Pflichten haben. Bei jeder Datenübermittlung sei eine Einzelfallprüfung vorzunehmen, ob das geforderte Schutzniveau im Drittland tatsächlich eingehalten wurde. Gibt es im Drittland nationale Sicherheitsgesetze, die es dem Empfänger unmöglich machen, seine Pflichten aus den Klauseln zu erfüllen, weil er entgegen der dortigen Garantien Daten offenlegen muss, ist das Schutzniveau nicht

eingehalten worden. Die Datenübermittlung ist in diesem Fall zu unterlassen oder abzubrechen. Dieselbe Prüfpflicht gilt im Übrigen auch für Datenschutzbehörden.

Die bestehenden Standardvertragsklauseln boten in dieser Hinsicht keine ausreichende Sicherheit für die personenbezogenen Daten von Betroffenen. Unter Berücksichtigung der Schrems II-Rechtsprechung wurden deshalb im Juni 2021 neue Standardvertragsklauseln beschlossen, welche den neuen Anforderungen Rechnung tragen.[14]

Noch immer zu viele DSGVO-widrige Cookie-Banner im Netz

In Bezug auf Cookie-Banner war die von Schrems mitgegründete Datenschutzorganisation *noyb* ebenfalls fleißig. Mit mehr als 500 Beschwerden wegen rechtswidriger Cookie-Banner starteten die Datenschutzaktivisten im Mai 2021 die „größte Beschwerdewelle seit dem Inkrafttreten der DSGVO vor drei Jahren“.[15] Kritisiert werden insbesondere die „Klick-Labyrinthe“, die Nutzerinnen und Nutzern eine – weder als informiert noch als tatsächlich freiwillig anzusehende – Einwilligungen abnötigen. Mithilfe eines Systems werden automatisch verschiedene Arten von Verstößen aufdeckt, eine entsprechende DSGVO-Beschwerde generiert und an das jeweilige Unternehmen verschickt. Reagiert dieses nicht, leitet noyb die Beschwerde an die zuständige Behörde weiter, die ein hohes Bußgeld verhängen kann. Im Fokus sind dabei nicht nur „Dark Patterns“ und komplizierte Einwilligungsformulare, sondern auch jene Banner, die lediglich über den Einsatz von Cookies informieren und ein bloßes Weiternutzen der Website als Einwilligung auslegen wollen.

Gerade letzteres ist aus Sicht des LG Köln unzulässig, weil die Anforderungen des § 15 Abs. 3 TMG nicht erfüllt werden – eine ausdrückliche Einwilligung in zielgerichtete Werbung erfordere mehr als nur die konkludente weitere Nutzung der Seite.[16] Das Erfordernis einer ausdrücklichen Einwilligung hatte auch der EuGH in seiner vielbeachteten Planet49-Entscheidung Ende 2019 klargestellt.[17]

Auch hinsichtlich der besonders von Online-Zeitungen gern genutzten „Cookie-Paywalls“, die für das Aufrufen von Beiträgen entweder eine umfassende Werbeeinwilligung oder ein kostenpflichtiges „PUR“-Abonnement verlangen, reichte *noyb* eine Reihe von Beschwerden ein.

Die Datenschützer monieren, dass bei diesem Vorgehen nicht nur ein klares Ungleichgewicht missbräuchlich ausgenutzt werde, auch stelle die so eingeholte Erklärung einen Verstoß gegen das Koppelungsverbot dar, weil die Datenverarbeitung zur Erbringung der Leistung nicht erforderlich sei.[18]

Schrems III steht noch aus

Im Juli 2021 lieferte der gegen Facebook geführte Prozess durch Schrems eine weitere Frage für den EuGH, die der Oberste Gerichtshof in Österreich dem EuGH auf Grundlage des Prozesses stellt: Es soll geklärt werden, auf welcher rechtlichen Grundlage soziale Netzwerke generell die persönlichen Daten ihrer Nutzer verarbeiten dürfen. Facebook nutzt die Daten der Nutzer neben dem Betreiben des sozialen Netzwerkes auch für personalisierte Werbung, was das rechtliche Verhältnis zwischen dem Unternehmen und den Nutzern in Frage stellt. Seit der DSGVO-Reform existiert keine direkte Einwilligung der Nutzer in die Dateneingriffe des Unternehmens mehr, was Facebook damit rechtfertigt, dass zwischen den Parteien ein Vertrag bestehe und so keine Einwilligung bezüglich der Daten erforderlich sei. Nach der DSGVO müssen Nutzer ihre Einwilligung jedoch jederzeit widerrufen können, was Nutzenden erlauben würde, ihre Zustimmung zur Datennutzung für Werbung rückwirkend zurückzunehmen. Die datenschutzrechtliche Einwilligung ist ein immer wiederkehrendes Diskussionsthema: Der EuGH ist grundsätzlich der Ansicht, dass der für die Datenverarbeitung Verantwortliche nachzuweisen hat,

dass eine „aktive“ Einwilligung der Betroffenen hierzu vorliegt.[19] Im Fall einer Niederlage Facebooks vor dem EuGH würden so nicht nur zahlreiche Daten gelöscht werden müssen, sondern das Unternehmen hätte auch Schadensersatzzahlungen an Millionen von Nutzerinnen und Nutzern zu leisten.[20]

Eine zusätzliche Frage im Rahmen des Prozesses ist unter anderem im Rahmen von Werbe-Targeting, ob Facebook zu Werbezwecken die Nutzerdaten nach sensiblen Bereichen wie politischer Überzeugung, sexueller Orientierung etc. gezielt filtern darf. Schrems kann für sich bereits einen Erfolg verbuchen: Ihm wurden 500 Euro Schadensersatz gegen Facebook zugesprochen, da das Unternehmen ihm keinen Zugang zu von ihm gespeicherten Daten gewährt hat.[21] Der Oberste Gerichtshof in Österreich soll hierbei von einer unnötig komplizierten „Ostereiersuche“ gesprochen haben. Das Teilurteil stieß auf ein enormes Medienecho, da sich dadurch für eine Vielzahl anderer Nutzerinnen und Nutzer die Möglichkeit eröffnet, Schadensersatz (beispielsweise wegen einer nicht ordnungsgemäßen Datenschutzauskunft) zu fordern.

Ausblick

Die DSGVO feierte im Mai 2021 ihren dritten Geburtstag[22] – mit wegweisenden Entscheidungen und Bußgeldrekorden, aber auch mit allerlei Kritik und Rufen nach Reformen.

Das Urteil des EuGH vom Juni 2021 dürfte es Tech-Unternehmen künftig schwerer machen, sich mit einer Hauptniederlassung in Irland der dortigen Aufsichtsbehörde DPC – die für ihre schleppende und vergleichsweise wenig nachdrückliche Vorgehensweise berüchtigt ist[23] – zu unterwerfen, und so in Datenschutzfragen *forum shopping*, d.h. ein systematisches Ausnutzen von Zuständigkeitsregeln, zu betreiben. Die Cookie-Banner-Beschwerdeaktion von *noyb* zeigte erste Erfolge: 42 Prozent der Verstöße wurden nach dem „ersten Durchlauf“ behoben, doch insgesamt 82 Prozent aller Unternehmen handeln weiter DSGVO-widrig.[24] Die Datenschutzorganisation reichte konsequenterweise 422 Datenschutzbeschwerden bei den Aufsichtsbehörden ein. Wie sich der Schrems III-Prozess für Facebook weiterentwickeln wird, bleibt vorerst abzuwarten. Es dürfte in jedem Fall eine weitere aufsehenerregende Entscheidung im ewigen Rechtsstreit zwischen Europas wohl bekanntestem Datenschützer und Zuckerbergs Social-Network-Imperium werden.

Insgesamt gab es viele spannende Entwicklungen im Bereich des Datenschutzrechts. Nicht immer war die Pandemie ein ausschlaggebender Faktor, doch vor dem Hintergrund der zunehmenden Online-Aktivitäten – sei es im Homeoffice oder privat – vermochte sie doch zumindest mittelbar zu deren Relevanz beizutragen.

Julia Schwegler

Literaturnachweise

1 *Gola/Klug*, NJW 2021, 680, 682 f.

2 *Gola/Klug*, NJW 2021, 680, 682.

3 Vgl. *Schmale*, Jahresrückblick 2020 und Ausblick 2021. Informationen zum Datenschutz. Brandi Newsletter, Januar 2021.

4 EuGH, Urt. v. 15.06.2021 – C-654/19 – ECLI:EU:C:2021:483.

5 Vgl. *Gerichtshof der Europäischen Union*, Pressemitteilung Nr. 103/21, 15.06.2021, dort auch zum Folgenden.

6 Vgl. *Gerichtshof der Europäischen Union*, Pressemitteilung Nr. 1/21, 13.01.2021.

7 EuGH, Urt. v. 16.07.2020 – C-311/18 – ECLI:EU:C:2020:559 – NJW 2020, 2613.

8 EuGH, Urt. v. 16.07.2020 – C-311/18 – NJW 2020, 2613, 2614.

9 EuGH, Urt. v. 16.07.2020 – C-311/18 – NJW 2020, 2613, 2614.

10 Vgl. *Wybitul/Halim*, Das Schrems II-Urteil des EuGH: Was müssen Unternehmen bei internationalen Datentransfers ändern?, Latham&Watkins Client Alert Commentary, 24.07.2021.

11 EuGH, Urt. v. 16.07.2020 – C-311/18 – NJW 2020, 2613, 2615.

12 EuGH, Urt. v. 16.07.2020 – C-311/18 – NJW 2020, 2613, 2617, 2618.

13 EuGH, Urt. v. 16.07.2020, C – 311/18.

14 Vgl. hierzu *Europäische Kommission*, Pressemitteilung vom 04.06.2021.

15 Vgl. *noyb*, noyb setzt dem Cookie-Banner-Wahnsinn ein Ende, noyb.eu, 31.05.2021, dort auch zum Folgenden.

16 LG Köln, Beschl. v. 13.04.2021 – 31 O 36/21.

17 EuGH, Urt. v. 01.10.2019 – C-673/17 – ECLI:EU:C:2019:801.

18 Vgl. *noyb*, News-Seiten: Leser:innen sollen eigene Daten zum Wucherpreis „zurückkaufen“, noyb.eu, 13.08.2021.

19 EuGH, Urt. v. 11.11.2020 – C-61/19 – ECLI:EU:C:2020:901.

20 Vgl. *Fanta*, Neue Klage von Schrems. Schadensersatz für Millionen von Facebook-Nutzer:innen?, Netzpolitik.org, 20.07.2021.

21 Vgl. *Fanta*, Neue Klage von Schrems. Schadensersatz für Millionen von Facebook-Nutzer:innen?, Netzpolitik.org, 20.07.2021.

22 Vgl. dazu *Büttel*, Ist die DSGVO „gescheitert“?, For..Net Blog, 27.05.2021.

23 Vgl. das Interview mit dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit in Rheinland-Pfalz Prof. Dr. Dieter Kugelmann bei *Dachwitz*, Datenschutzwüste Irland – „So langsam müssen die mal in die Pötte kommen“, Netzpolitik.org, 22.05.2021.

24 Vgl. *noyb*, noyb reicht 422 formelle DSGVO-Beschwerden gegen Cookie-Banner-Wahnsinn ein, noyb.eu, 10.08.2021, dort auch zum Folgenden.

Sämtliche Links wurden zuletzt am 10.09.2021 abgerufen.

Datenschutz „Made in China“

Das PIPL und die Auswirkungen auf deutsche Unternehmen

Zum 1. November 2021 tritt das neue chinesische *Personal Information Protection Law* (PIPL) in Kraft. In den Medien ist die Rede von einer „chinesischen DSGVO“. Doch ist das PIPL mit dem europäischen Datenschutzregelwerk überhaupt wirklich vergleichbar – und worauf müssen sich Unternehmen, die in China tätig sind, einstellen?

Ein regulatorischer Flickenteppich

Das chinesische Recht befasst sich nicht erst seit dem PIPL mit dem Thema Datenschutz. So enthält etwa das *Chinese Security Law* (CSL) entsprechende Vorschriften.[1] Doch erstmals verfolgt China mit dem PIPL einen derart umfassenden Ansatz. Bislang waren einschlägige Vorschriften über eine Vielzahl von Regelungswerken – unter anderem diverse nicht verbindliche Standards – verstreut, was zur schweren Handhabbarkeit des chinesischen Datenschutzrechts beitrug.[2]

Das Gesetz ist stark an die DSGVO angelehnt, doch es bleiben einige wichtige Unterschiede zwischen den beiden Regelungswerken bestehen. Der wichtigste Unterschied ist wohl, dass in China, anders als in Europa, kein verfassungsrechtlich verbrieftes Recht auf Datenschutz existiert: Auf primärrechtlicher Ebene garantieret Art. 8 Abs. 1 GrCh (ebenso wie Art. 16 Abs. 1 AEUV) ausdrücklich ein Recht auf den Schutz der eigenen personenbezogenen Daten, die grundrechtliche Dimension des Datenschutzes ist dabei jedenfalls als Facette des Privatlebens im Sinne des Art. 8 EMRK bereits seit langem anerkannt.[3] Das PIPL gewährleistet zwar „auf der Grundlage der Verfassung“ den Datenschutz, doch ein entsprechendes Recht lässt sich der chinesischen Verfassung nicht entnehmen.[4] Auch das deutsche Grundgesetz enthält zwar kein originäres Datenschutzgrundrecht, doch dessen wesentliche Inhalte sind mit dem Grundrecht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sowie durch die Zielsetzung weiterer auf die Privatsphäre abzielender Grundrechte wie die der Kommunikationsfreiheiten des Art. 10 GG oder der Unverletzlichkeit der Wohnung nach Art. 13 GG anerkannt und werden in der Gesetzgebung und Rechtsprechung grundsätzlich gewürdigt.[5] Dennoch ist allein schon aufgrund der insgesamt hohen Gewichtung öffentlicher Interessen in China im Gegensatz zu Deutschland und Europa ein mit der DSGVO vergleichbares Schutzniveau nicht zu erwarten.[6]

Weiterhin fällt auf, dass das PIPL – anders als die DSGVO – nicht (vollumfänglich) für öffentliche Stellen gilt Vgl. Art. 33 PIPL). Die Regelungen zielen vielmehr auf die Regulierung großer Internetkonzerne ab, die Unmengen von Daten über ihre Nutzer sammeln und gewinnbringend für ihre eigenen Zwecke nutzen. Die Novelle ist somit vorwiegend gegen den „Datenkapitalismus“ von Unternehmen gerichtet.[7] Art. 34 PIPL besagt, dass öffentliche Stellen bei der Erfüllung ihrer Aufgaben ebenfalls grundsätzlich den Grundsatz der Notwendigkeit zu beachten haben. Die Informationspflichten des Art. 17 PIPL werden durch verschiedene Ausnahmen aufgeweicht, womit dem starken Fokus der chinesischen Regierung und Gesetzgebung auf nationale Sicherheit und Stabilität Rechnung getragen wird.[8]

China und Datenschutz – Öl und Wasser?

Darüber hinaus sind die durch das PIPL statuierten Prinzipien stets vor dem Hintergrund der gängigen Überwachungspraxis zu sehen, da dem Datenschutz bei einer Abwägung mit den diversen Interessen des Staates ein regelmäßig geringes

Gewicht zugemessen wird. Als Beispiel hierfür genügt ein Blick auf das 2020 eingeführte Sozialpunktesystem SCS, bei dem das Verhalten von Privatpersonen wie auch von Unternehmen, die in der Volksrepublik tätig sind, digital erfasst und nach einem Punktesystem bewertet wird.[9]

In den *Social Credit Score* fließen beispielsweise verspätete Mietzahlungen sowie Verstöße gegen Verkehrsregeln oder Mülltrennungsvorschriften negativ ein, positiv hingegen werden etwa ehrenamtliche Tätigkeiten bewertet.[10] Für die Erfassung relevanter Verhaltensweisen werden unter anderem weitreichende Gesichtserkennungssysteme im öffentlichen Raum genutzt.[11] Dabei muss je nach Stand

des Punktekontos mit Sanktionen wegen der Verletzung von Vorschriften oder politisch unliebsamen Ansichten gerechnet werden. Der Score beeinflusst z.B. die Zuteilung eines Kindergarten- oder Studienplatzes, die Chancen auf einen bestimmten Arbeitsplatz, auf eine Wohnung oder einen Kredit, da auch Arbeitgeber, Vermieter oder Banken den über die Data-Websites allgemein zugänglichen Stand des Punktekontos einsehen können. Doch auch abseits des Sozialpunktesystems werden eine Vielzahl von Kontrollsystemen genutzt, die zu einem widersprüchlichen Kontrast zwischen Datenschutz und Unterdrückung durch (bzw. als Folge von) Überwachung beitragen.[12]

Das PIPL im Überblick: Was müssen Unternehmen künftig beachten?

Das PIPL besteht aus insgesamt acht Kapiteln. Das 1. Kapitel enthält, ähnlich einem „Allgemeinen Teil“ grundsätzliche Bestimmungen. Kapitel 2 befasst sich mit den Vorschriften für die Verarbeitung personenbezogener Daten. In Kapitel 3 ist die grenzüberschreitende Bereitstellung personenbezogener Daten geregelt. Das 4. Kapitel statuiert individuelle Rechte im Zusammenhang mit der Datenverarbeitung. Kapitel 5 regelt Pflichten von Datenverarbeitern, Kapitel 6 betrifft die Aufsichtsbehörden. In den Kapiteln 7 und 8 finden sich schließlich Bestimmungen zur Haftung sowie Übergangs- und Schlussbestimmungen.

Begriffe und Anwendungsbereich

Mit dem zentralen Begriff „Personal Information“ lehnt sich das PIPL stark an die DSGVO an. Art. 4 PIPL stellt klar, dass damit „jedwede Informationen in Bezug auf identifizierte oder identifizierbare natürliche Personen, die elektronisch oder anderweitig aufgezeichnet wird, ausgenommen anonymisierte Informationen“ gemeint sind.[13] Diese Definition erfasst auch Informationen, die zwar selbst keine Identifizierung ermöglichen, aber ggf. im Zusammenwirken mit weiteren Informationen hierfür ausreichend sind und geht damit über die dem CSL und dem Zivilgesetzbuch der Volksrepublik China zugrunde liegende Verständnis des Begriffs hinaus.[14] Die Bezeichnung „Personal Information Handler“ findet hingegen keine direkte Entsprechung in der DSGVO, die Rolle ist jedoch vergleichbar mit der des „Verantwortlichen“ i.S.d. Art. 4 Nr. 7 DSGVO.[15] Besonders „sensible Daten“ sind in Art. 28 PIPL definiert. Ihre Verarbeitung ist nur in engen Schranken und unter Beachtung weiterer Vorgaben zulässig.

Ein maßgeblicher Punkt ist in Art. 3 PIPL geregelt: Der Geltungsbereich umfasst neben der Verarbeitung personenbezogener Daten natürlicher Personen im Staatsgebiet der Volksrepublik auch Verarbeitungsvorgänge *außerhalb* Chinas, wenn sie sich auf Daten natürlicher Personen beziehen, die sich innerhalb der chinesischen Grenzen befinden, sofern der Zweck der Verarbeitung die Bereitstellung von Produkten oder Dienstleistungen in China ist, das Verhalten solcher natürlicher Personen analysiert oder bewertet werden sollen oder wenn die Anwendbarkeit durch Gesetz oder Verwaltungsvorschrift angeordnet wird. Insbesondere die Frage, ob mit einer Verarbeitung die Bereitstellung von Diensten bezweckt wird, dürfte in der Praxis entscheidend sein. Genauere Ausführungen, wie die Zweckbestimmung auszulegen ist, bietet das PIPL nicht. Vor dem Hintergrund, dass im Kontext anderer Regelwerke bereits die Verwendung der chinesischen Sprache oder das

Akzeptieren von Yuan als Zahlungsmittel als ausreichend erachtet wird, ist von einer sehr weiten Auslegung auszugehen.[16]

Art. 72 PIPL schränkt den Anwendungsbereich ähnlich eines Haushaltsprivilegs für natürliche Personen, die personenbezogene Daten in persönlichen oder Familienangelegenheiten verarbeiten, sowie für staatliche Verarbeitungen im Zusammenhang mit Statistiken und Archivierungsmanagement ein.

Art. 44 ff. PIPL räumen betroffenen Personen das Recht ein, über die Verarbeitung der sie betreffenden personenbezogenen Daten informiert zu werden und in Bezug auf diese eine Entscheidungs- bzw. Beschränkungsmöglichkeit zu haben. Art. 45 PIPL enthält ein Recht auf Auskunft und Kopie; Art. 46 PIPL eines auf Berichtigung unrichtiger oder unvollständiger Daten und Art. 47 PIPL eines auf Löschung. Gemäß Art. 49 PIPL, der anders als die DSGVO eine ausdrückliche Regelung zur Erbfolge enthält[17], steht den Angehörigen im Falle des Versterbens des Anspruchsinhabers zu, die Rechte im Einklang mit ihren eigenen berechtigten Interessen geltend zu machen, soweit der Verstorbene keine entgegenstehenden Wünsche getroffen hat. Für eine

unkomplizierte Geltendmachung der Betroffenenrechte haben Verantwortliche organisatorische Verfahren einzurichten (Art. 50 PIPL).

Voraussetzungen der Datenverarbeitung

Art. 13 PIPL legt die allgemeinen Voraussetzungen für eine Datenverarbeitung fest. Nötig ist dafür entweder beispielsweise eine Einwilligung der betroffenen Person (Nr. 1), die Erforderlichkeit zur Vertragserfüllung, zur Erfüllung anderer Pflichten (genannt wird beispielsweise das Personalmanagement) (Nr. 2) oder die Erforderlichkeit zur Gefahrenabwehr (Nr. 4). Die Anforderungen an die Einwilligung werden in Art. 14 PIPL näher konkretisiert, wobei die Nähe zu denjenigen der DSGVO deutlich erkennbar ist.

Vor Beginn des Verarbeitungsvorgangs sollen betroffene Personen wahrheitsgemäß, zutreffend und vollständig insbesondere über den Namen des Verantwortlichen und eine Kontaktmöglichkeit, Zweck und Art der Verarbeitung, Kategorien der zu verarbeitenden Daten sowie über die Modalitäten für die Ausübung der Rechte aus dem PIPL informiert werden (Art. 17 PIPL). Die Informationspflicht kann unter bestimmten Umständen entfallen (Art. 18 PIPL). Bei der Weitergabe von Daten, die im Zusammenhang mit M&A-Aktivitäten anfallen, sind die betroffenen Personen gemäß Art. 22 PIPL über die Identität und Kontaktmöglichkeiten der Empfänger der Informationen zu informieren, welche dann ebenfalls an die Verpflichtungen der Verantwortlichen unterliegen. Die Weitergabe ist streng zweckgebunden; ändert sich der Verarbeitungszweck, muss eine neue Einwilligung eingeholt werden.[18]

Der Datentransfer ins Ausland ist an strenge Voraussetzungen geknüpft (Art. 38 ff. PIPL). Es muss eine informierte (voraussichtlich individuell zweckgebundene) Einwilligung der betroffenen Person eingeholt, eine Folgenabschätzung durchgeführt und Dokumentationspflichten beachtet sowie eine der vier besonderen Anforderungen erfüllt werden: das Bestehen einer Sicherheitsüberprüfung, eine spezielle Zertifizierung, der Abschluss eines Standardvertrags mit der betroffenen Person, der wohl mit den EU-Standardvertragsklauseln vergleichbar sein wird, oder das Erfüllen sonstiger bestimmter gesetzlicher bzw. regulatorischer Anforderungen.[19] Ausländische Justiz- und Strafverfolgungsbehörden darf ohne Zustimmung der zuständigen chinesischen Behörde kein Zugriff auf in China gespeicherte Daten eingeräumt werden (Art. 41 PIPL). In diesem Zusammenhang ist insbesondere auch an Remote-Zugriffsmöglichkeiten aus dem Ausland zu denken. Bestimmte Daten – etwa solche, die bei Betreibern Kritischer Infrastrukturen anfallen oder sobald ein Verantwortlicher bestimmte Grenzwerte hinsichtlich der Datenverarbeitung überschreitet – dürfen grundsätzlich vorbehaltlich strenger zusätzlicher Voraussetzungen nicht im Ausland gespeichert werden (Art. 40 PIPL).

Repräsentanzen, Haftung, Dokumentations- und Meldepflichten

Gemäß Art. 53 PIPL müssen ausländische Verantwortliche eine Repräsentanz in China einrichten, die für Datenschutzbelange verantwortlich zeichnet und deren (Kontakt-)Daten den zuständigen Behörden übermitteln.

Das chinesische System der Aufsichtsbehörden weist nur wenig Ähnlichkeit mit demjenigen der DSGVO auf. Verschiedene Abteilungen wie die *Cyberspace Administration of China* (CAC) und das Ministerium für öffentliche Sicherheit sind mit bestimmten

Befugnissen ausgestattet.[20] Federführend war zumindest bislang das *Chinese National Information Security Standardization Technical Committee* (TC260), das von der *Standardization Administration of the People's Republic of China* (SAC) und der CAC überwacht wird.[21] Art. 60 ff. PIPL bieten hier nur eine rudimentäre Klarstellung: Ein besonderer Status kommt dem *State Cybersecurity and Informatization Department* zu, das für Planung und Koordination zuständig ist (Art. 60 PIPL).[22] Andere Behörden wie etwa das CAC oder das Ministerium für öffentliche Sicherheit sind jedoch in ihren jeweiligen Sachbereichen ebenfalls zum Teil mit solchen Aufgaben betraut.

Gemäß Art 56 PIPL sind Datenschutzverletzungen unverzüglich an die zuständige Behörde zu melden. Hinsichtlich einer Notifizierung der betroffenen Person(en) besteht keine grundsätzliche Pflicht, sie kann jedoch durch die Aufsichtsbehörde angeordnet werden.[23]

Bei der Verletzung von PIPL-Vorschriften können Bußgelder in Höhe von bis zu 50 Millionen Yuan (ca. 6,5 Millionen Euro) oder fünf Prozent des Jahresumsatzes verhängt werden (Art. 66 Abs. 2 PIPL). Zudem können unrechtmäßige Einnahmen konfisziert werden. Auch Unterlassungsverfügungen im Zusammenhang mit einschlägigen Geschäftstätigkeiten sind denkbar. Ausländischen Organisationen oder Individuen, die datenschutzrechtswidrig handeln oder mit ihrem Verhalten die nationale Sicherheit und/oder öffentliche Interessen gefährden, können auf eine „Schwarze Liste“ gesetzt werden (Art. 42 PIPL). Damit können unter anderem eine offizielle Warnung, Auflagen und Beschränkungen sowie die Untersagung der Bereitstellung von Daten an diese Personen verbunden sein. Gemäß Art. 67 PIPL wirken sich Verstöße auch auf den Social Credit Score aus.

Art. 69 PIPL sieht eine Schadensersatzpflicht des Verantwortlichen vor. Neu im Vergleich zu bisherigen Regelungen ist die Beweislastverteilung:[24] So liegt die Beweislast für eine Exkulpation gemäß Art. 69 PIPL beim Verantwortlichen. Auch sind nach Art. 71 PIPL strafrechtliche Sanktionen möglich. Sollte ein ausländischer Staat oder eine Region – damit dürfte insbesondere die Europäische Union gemeint sein – „diskriminierende Verbote oder Beschränkungen erlassen oder ähnliche Schritte gegen die Volksrepublik China im Bereich des Datenschutzes“ einleiten, drohen diesem bzw. dieser gemäß Art. 43 PIPL Vergeltungsmaßnahmen.[25]

Parallelen zur europäischen Plattformregulierung sind bei den besonders strengen Pflichten für Plattformbetreiber bzw. soziale Netzwerke erkennbar, die unter anderem die Einrichtung eines unabhängigen Aufsichtskommitees und die regelmäßige Veröffentlichung von *„Social Responsibility Reports“* vorsehen (Art. 58 PIPL). [26]

Fazit

Unternehmen, die in China geschäftlich tätig sind oder werden wollen, müssen sich auf eine Vielzahl neuer Pflichten einstellen. Generell dürften gerade für europäische bzw. in der EU tätige Unternehmen einige Punkte, vor allem bezüglich der strengen Anforderungen der DSGVO, „bekanntes Fahrwasser“ darstellen. Die DSGVO-Grundsätze können jedoch keinesfalls unmittelbar übertragen werden. Bei einigen Aspekten wie der Einordnung als der Bereitstellung von Produkten oder Dienstleistungen in China dienend bleibt zudem eine nähere Konkretisierung durch chinesische Behörden bzw. Gerichte abzuwarten.[27]

Allgemein ist allerdings anzuraten, im Zweifel von einer Anwendbarkeit des PIPL auszugehen und entsprechende Maßnahmen zu ergreifen, um auf der sicheren Seite zu sein – insbesondere vor dem Hintergrund der generell eingeschränkten Rechtsschutzmöglichkeiten in der

Volksrepublik und der umfangreichen behördlichen Befugnisse, die Unternehmen zur Offenlegung von Informationen, u.U. sogar von Geschäftsgeheimnissen zwingen können.[28] Inwieweit das chinesische Datenschutzrecht tatsächlich primär dem Datenschutz dienen wird oder ob es zuvorderst ein Instrument zur Beschränkung der unternehmerischen Handlungsspielräume[29], insbesondere mit Blick auf ausländische Firmen, darstellt, wird sich zeigen.

Zumindest wird jedoch angesichts der – doch in vielen Aspekten durchaus erkennbaren – Orientierung an der DSGVO die Exportfähigkeit der europäischen Datenschutzsystematik und -standards deutlich:[30] Nachgeahmt wird nur, was gut ist.[31]

Priska Katharina Büttel

Literaturnachweise

1 Zum CSL siehe *Kipker*, DSRITB 2019, 877.

2 Vgl. ausführlich *Geller*, GRUR Int. 2020, 1191, insbesondere 1192 ff.

3 Vgl. *Heckmann/Scheurer*, in: Heckmann/Paschke, jurisPK-Internetrecht, 7.Aufl., Kap. 9 Rn. 14 (m.w.N.).

4 Vgl. die vorläufige inoffizielle englische Übersetzung des PIPL bei *Creemers/Webster*, Translation: Personal Information Protection Law of the People's Republic of China (Effective Nov. 1, 2021), DigiChina Cyber Policy Center, Stanford University, 20.08.2021 sowie die Übersetzung der chinesischen Verfassung durch den Nationalen Volkskongress, *National People's Congress of the People's Republic of China*, Constitution of the People's Republic of China (Full text after amendment on March 14, 2004), 06.09.2021; *Geller*, GRUR Int. 2020, 1191, 1192.

5 Vgl. *Heckmann/Scheurer*, in: Heckmann/Paschke, jurisPK-Internetrecht, 7.Aufl., Kap. 9 Rn. 26 ff. (m.w.N.)

6 Vgl. auch *Lejeune*, PinG 3/2021, 109, 114.

7 Vgl. *o.V.*, China will gewerblichen Datenschutz verbessern und lehnt sich insoweit an DSGVO an, Haufe Online, 25.08.2021.

8 Vgl. *Geller*, GRUR Int. 2020, 1191, 1202.

9 Vgl. *Freyeisen*, Chinas Sozialpunkte-System: Schikane von Wirtschaft und Bürgern?, Tagesschau.de, 04.08.2021; *Bellmann*, Sehnsucht nach dem Überwachungsstaat, SZ.de, 11.09.2019.

10 Vgl. *Martinek*, jM 2020, 41, 41 f., dort auch zum Folgenden.

11 Das bleibt auch weiterhin erlaubt, siehe Art. 27 PIPL; Vgl. *Johannes*, ZD-Aktuell 2021, 05219.

12 Vgl. *Hao*, Chinas Datenschutz-Paradoxon, Heise Online, 02.11.2020.

13 Siehe die englische Übersetzung von *Creemers/Webster*, Translation: Personal Information Protection Law of the People's Republic of China (Effective Nov. 1, 2021), DigiChina Cyber Policy Center, Stanford University, 20.08.2021; Dt. Übers. d. Verf.

14 Vgl. *Lejeune*, PinG 3/2021, 109, 111; *Dai/Deng*, Dentons Guide to China's Personal Information Protection Law (PIPL), S. 6.

15 Vgl. *Johannes*, ZD-Aktuell 2021, 05219; Dai/Deng, Dentons Guide to China's Personal Information Protection Law (PIPL), S. 6.

16 Vgl. *Dai/Deng*, Dentons Guide to China's Personal Information Protection Law (PIPL), S. 6.

17 Vgl. *Johannes*, ZD-Aktuell 2021, 05219.

18 Vgl. auch *Lejeune*, PinG 3/2021, 109, 111.

19 Vgl. *Dai/Deng*, Dentons Guide to China's Personal Information Protection Law (PIPL), S. 6, dort auch zum Folgenden.

20 Vgl. *Dai/Deng*, Dentons Guide to China's Personal Information Protection Law (PIPL), S. 23, dort auch zum Folgenden.

21 Vgl. *Wagner*, ZD 2021, 140, 141.

22 Vgl. *Johannes*, ZD-Aktuell 2021, 05219.

23 Vgl. *Dai/Deng*, Dentons Guide to China's Personal Information Protection Law (PIPL), S. 20.

24 Vgl. *Geller*, GRUR Int. 2020, 1191, 1200.

25 Siehe die englische Übersetzung von *Creemers/Webster* (Fn. 4); Dt. Übers. d. Verf.

26 Vgl. *Kipker*, Das neue chinesische Datenschutzgesetz PIPL ist da!, Beck Blog, 22.08.2021.

27 Vgl. auch *Johannes*, ZD-Aktuell 2021, 05219; *Lejeune*, PinG 3/2021, 109, 114; *Geller*, GRUR Int. 2020, 1191, 1194.

28 Vgl. *Lejeune*, PinG 3/2021, 109, 114; *Geller*, GRUR Int. 2020, 1191, 1192 f.

29 Vgl. *Lejeune*, PinG 3/2021, 109, 114; *Wagner*, ZD 2021, 140, 144.

30 Vgl. *Kipker*, ZD 2021, 397, 398.

31 *Richter*, ZD 2021, 233, 234.

Sämtliche Links wurden zuletzt am 10.09.2021 abgerufen.

Leiter des Forschungsprojekts und AutorInnen

Prof. Dr. Dirk Heckmann

Dirk Heckmann (Jahrgang 1960) ist seit Oktober 2019 Inhaber des Lehrstuhls für Recht und Sicherheit der Digitalisierung an der Technischen Universität München, wo er sowohl der TUM School of Governance als auch der Fakultät für Informatik angehört. Zuvor hatte der in Freiburg i. Br. habilitierte Staatsrechtler von 1996 bis 2019 den Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht an der Universität Passau inne, wo er als Affiliate Professor nach wie vor die Forschungsstelle für IT-Recht und Netzpolitik (For..Net) und das Forschungsprojekt BayWiDI leitet.

Seine Lehr- und Forschungsschwerpunkte liegen im Schnittfeld von IT und Recht mit besonderem Fokus auf Datenschutzrecht, IT-Sicherheitsrecht, Legal Tech, E-Government, E-Health und Künstliche Intelligenz. Aus seiner Feder stammen der juris Praxiskommentar Internetrecht (6. Aufl. 2019) sowie weitere rund 200 Publikationen zu Recht und Digitalisierung.

2003 wurde Heckmann zum nebenamtlichen Verfassungsrichter am Bayerischen Verfassungsgerichtshof gewählt, 2007 in den Expertenkreis des Nationalen IT-Gipfels der Bundesregierung berufen. Er ist seit 2018 Direktor am Bayerischen Forschungsinstitut für Digitale Transformation (bidt). Von 2014 bis 2020 war er Vorsitzender der Deutschen Gesellschaft für Recht und Informatik.

2015 wurde er in die Hauptjury des deutschen Computerspielpreises, 2016 in die Ethikkommission des Bundesverkehrsministeriums zum automatisierten und vernetzten Fahren und 2018 in die Datenethikkommission der Bundesregierung berufen.

Julia Schwegler

Julia Schwegler studiert seit September 2017 Rechtswissenschaft an der Universität Passau und unterstützt seit Juni 2019 als studentische Hilfskraft die Forschungsstelle für IT-Recht und Netzpolitik. Ihren Schwerpunkt schloss sie im Bereich Arbeitsrecht mit dem Thema „Anspruch auf Homeoffice“ für ihre Seminararbeit ab.

Priska Katharina Büttel

Priska Katharina Büttel betreut seit Oktober 2019 als geschäftsführende Wissenschaftliche Mitarbeiterin der Forschungsstelle For..Net unter anderem das Projekt BayWiDI an der Universität Passau. Im Rahmen ihrer Promotion beschäftigt sie sich gegenwärtig mit Rechtsfragen im Zusammenhang mit dem Einsatz von Künstlicher Intelligenz zu medzinischen Zwecken.

Impressum

Fotos Seite 1 und Seite 11: Universität Passau. Foto Seite 3 (oben rechts): Gerichtshof der Europäischen Union.

Sämtliche weiteren Abbildungen sind gemeinfrei-ähnlich freigegeben via Unsplash.com.

Impressum

Universität Passau
Innstraße 41
94032 Passau

Telefon: 0851/509-0
Telefax: 0851/509-1005

E-Mail: praesident@uni-passau.de
Internet: www.uni-passau.de

USt.-Id-Nr.: DE 811193057

Organisation

Gemäß Art. 11 Abs. 1 BayHSchG ist die Universität Passau als Hochschule des Freistaates Bayern eine Körperschaft des öffentlichen Rechts und zugleich staatliche Einrichtung. Aufsichtsbehörde ist das Bayerische Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst in München (Anschrift: Salvatorstraße 2, 80333 München).

Vertretung

Die Universität Passau wird vom Vorsitzenden des Leitungsgremiums, Präsident Prof. Dr. Ulrich Bartosch, gesetzlich vertreten. Verantwortlicher im Sinne des § 5 TMG (Telemediengesetz) ist der Präsident. Für namentlich oder mit einem gesonderten Impressum gekennzeichnete Beiträge liegt die Verantwortung bei den jeweiligen Autorinnen und Autoren.

Herausgeber

Prof. Dr. Dirk Heckmann

Leiter der Forschungsstelle für IT-Recht und Netzpolitik (For..Net)

Redaktion und Produktion

Priska Katharina Büttel

Layout und Satz

Priska Katharina Büttel

Die nächste Ausgabe erscheint Mitte Dezember 2021. Sie finden das Magazin und die Möglichkeit, sich für den kostenlosen Versand per E-Mail an- und abzumelden, unter www.baywidi.de.

Hinweise, Anregungen, Lob und Kritik sind herzlich willkommen. Schreiben Sie uns unter baywidi@uni-passau.de.