AXEL SPIES

USA: Datenschutzbestimmungen für europäische Unternehmen

Eine Checkliste

US-Datenschutz
CCPA
Compliance
EU-US Data Privacy Framework

■ Europäische Unternehmen sind immer wieder überrascht über die große Anzahl und die Komplexität der Datenschutzbestimmungen in den USA. Das gilt auch und gerade für neu im US-Markt agierende europäische Unternehmen. Manche glauben, sich durch eine Geschäftsverlagerung in die USA aus bürokratischen Zwängen des Datenschutzes in Europa befreit zu haben. Sie merken schnell: Der Compliance-Aufwand ist erheblich.

■ European companies are always surprised by the large number and complexity of data protection regulations in the US. This is also and especially true for European companies new to the US market. Some believe they have freed themselves from the bureaucratic constraints of data protection in Europe by relocating their business to the US. They quickly realise that the compliance effort is considerable.

Lesedauer: 12 Minuten

In vielen Fällen stellen Unternehmen mit Geschäftsbeziehungen in die USA beim Datenschutz auf den Bundesstaat Kalifornien als Best Practice ab. Das kann sich aber als teurer Trugschluss herausstellen, wenn die Unternehmen in anderen US-Bundesstaaten Geschäfte betreiben, wo die Regeln dann doch anders sind als in Kalifornien. Dies macht die Compliance in den USA kompliziert, zumal in naher Zukunft kein Bundesgesetz zum Datenschutz zu erwarten ist.[1] Wer sich mit der Sache beschäftigt, merkt schnell: Die benutzten Rechtsbegriffe sind in den USA nicht einheitlich definiert, die Schwellenwerte für die Anwendung der Gesetze sind unterschiedlich. Da die US-Gesetze keine Bestellung eines internen oder externen Datenschutzbeauftragten zwingend vorsehen, müssen die europäischen Unternehmen zusätzlich klären, wer für die datenschutzrechtliche Compliance in den USA verantwortlich ist (zB ein Chief Privacy Officer) und wann was umgesetzt werden muss. Kurzum: Mit der DS-GVO im Gepäck kommen die Unternehmen in den USA häufig nicht weiter.

Nicht nur die neuen Datenschutzgesetze fordern Aufmerksamkeit; auch diverse rechtliche Vorgaben und Leitlinien der einschlägigen Behörden müssen beachtet werden. An erster Stelle ist die Federal Trade Commission (FTC) als die de facto „Bundesdatenschutzbehörde" für den Verbraucherschutz zu nennen, dann die Federal Communications Commission (FCC) für den TK-Sektor. Andere Behörden mit Datenschutzkompetenzen sind: Office of the Comptroller of the Currency (OCC), Department of Health and Human Services (HHS), Securities and Exchange Commission (SEC) und das Consumer Financial Protection Bureau (CFPB). Als einziger Bundesstaat verfügt bis dato Kalifornien über eine unabhängige Datenschutzbehörde, die California Privacy Protection Agency (CPPA).[2] Der Schwerpunkt der Tätigkeit der Behörden liegt in jedem Fall auf dem Verbraucherschutz, mit der Möglichkeit der Durchsetzung von Bußgeldern direkt durch die Behörde oder durch die Strafverfolgungsbehörden (Attorney General).

Wenn sich das US-Unternehmen als Datenimporteur zur Einhaltung des EU-US Data Privacy Framework (DPF) verpflichtet hat, müssen außerdem die DPF-Prinzipien intern umgesetzt werden.[3] Vorsorge muss je nach Art der verarbeiteten Daten gegen die Gefahr von Sammelklagen bei Verstößen gegen die US-Vorschriften getroffen werden, vor allem, wenn es unversehens zu einem Bruch der Datensicherheit kommt. Ein Bruch der Datensicherheit kann jede Menge andere Compliance-Probleme zu Tage fördern. Dem müssen die internen Regeln Rechnung tragen. Hilfreich ist eine Abarbeitung der nachfolgenden Checkliste, die man je nach Geschäftssektor noch erweitern könnte:

Aktionsfeld	Kommentare
Welche bundesstaatlichen Gesetze sind für die Datenverarbeitung einschlägig?	■ Zahlreiche bundesstaatliche Gesetze (alte und neue) gelten bereits jetzt für EU-Unternehmen oder werden in Kürze anwendbar. Sie beruhen auf der Verarbeitung von Daten von Einzelpersonen im jeweiligen Staat und der Anwendung von Schwellenwerten. Bisher gibt es reformierte Datenschutzgesetze in folgenden Bundesstaaten: Kalifornien, Colorado, Connecticut, Utah, Virginia, Iowa, Indiana, Montana, Tennessee, Texas, Oregon, Florida und seit neuestem Delaware.[4] ■ Die Gesetze gelten auch für außerhalb des Bundesstaats ansässige Unternehmen[5] – egal ob sie als Dienstleister/Datenverarbeiter oder Verantwortlicher die Daten verarbeiten. Eine Webseite, über die personenbezogene Daten von Kalifornern gesammelt werden, kann zB für die Anwendung der kalifornischen Vorschriften völlig ausreichen.

1 Spies MMR-Aktuell 2023, 458941 mwN.

2 https://cppa.ca.gov mit den einschlägigen Regeln hier: https://cppa.ca.gov/regulations/.

3 Näher zum DPF Spies/ Schmitz ZD 2023, 517.

4 Zu diesen Gesetzen gibt es vom Autor derzeit folgende deutsche Übersichten in den Zeitschriften ZD und MMR (Reihe wird fortgesetzt): ZD-Aktuell 2020, 04407; ZD-Aktuell 2020, 04414; ZD-Aktuell 2020, 07398; ZD-Aktuell 2021, 05047; ZD-Aktuell 2021, 05130; ZD-Aktuell 2021, 05257; ZD-Aktuell 2022, 01093; ZD-Aktuell 2022, 01177; ZD-Aktuell 2020, 01191; ZD-Aktuell 2020, 01392, ZD-Aktuell 2020, 01396; ZD-Aktuell 2023, 01010; ZD-Aktuell 2023, 01050; ZD-Aktuell 2020, 01124; ZD-Aktuell 2020, 01184; ZD-Aktuell 2023, 01298; ZD-Aktuell 2023, 01326; ZD-Aktuell 2023, 01360 sowie MMR-Aktuell 2020, 426334; MMR 2022, 839 und die Übersicht in MMR 2023, 69.

5 California Code, Civil Code – CIV § 1798.140 (d) "Business" means:
(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California.

Aktionsfeld	Kommentare
	■ Ein „common branding“[6] oder „joint venture“[7] kann zur Anwendung dieser Gesetze ausreichend sein, ausgenommen sind „not for profit“-Unternehmungen (zumindest in Kalifornien).[8]
Sind Sondergesetze für den Datenschutz auf Bundesebene oder Bundesstaatsebene anwendbar?	Übersicht: ■ Health Insurance Portability and Accountability Act (HIPAA) – Gesundheitsdaten ■ Gramm-Leach-Bliley Act (GLBA) – Finanzdaten ■ Children's Online Privacy Protection Act (COPPA) – Daten, die Kinder betreffen ■ Fair Credit Reporting Act (FCRA) – Kreditakte usw. ■ Telephone Consumer Protection Act (TCPA) – TK-Daten ■ Sektorspezifische KI-Gesetze (zB für Arbeitnehmerdaten)[9]
Gibt es in den Bundesstaaten Registrierungspflichten (vornehmlich für Datenhändler)?	■ Manche US-Bundesstaaten schreiben die Registrierung von Data Brokers (Datenhändlern) vor, wobei der Begriff weit definiert ist. Die Gesetze verlangen im Allgemeinen keine spezifische Beschreibung der einschlägigen Datenverarbeitungstätigkeiten. ■ In Kalifornien ist es dem Datenhändler freigestellt, im Rahmen seiner Registrierung Informationen über seine Datenerhebungspraktiken anzugeben. ■ Vermont hingegen – um ein Beispiel zu nennen – ist anspruchsvoller und verlangt von den Datenhändlern, dass sie jede Menge Informationen offenlegen: - die Opt-out-Möglichkeit der Verbraucher, - ob der Datenhändler ein Verfahren zur Zertifizierung des Käufers durchlaufen hat, sowie - die Anzahl und das Ausmaß von Sicherheitsverletzungen des Datenhändlers im vergangenen Jahr.
Sind die Konzepte von Art. 5 DS-GVO (Datenminimierung, Zweckbindung, Begrenzung der Datenspeicherung) „rechtmäßig“, „notwendig und verhältnismäßig“ intern vollständig umgesetzt?	■ Diese bekannten Konzepte wurden in die neuen Gesetze vieler US-Bundesstaaten (kalifornischer CPRA, Virginia CDPA, Colorado Privacy Act, Utah Consumer Privacy Act, Connecticut Privacy Act) aufgenommen und die Durchsetzung durch die Maßgaben der FTC verstärkt. ■ In vielen Fällen kann das europäische Unternehmen hier auf die Vorarbeiten zur DS-GVO zurückgreifen, aber die Umsetzung sollte an den einschlägigen bundesstaatlichen Gesetzen geprüft werden. ■ In Kalifornien wird derzeit ein „Delete Data Act“ diskutiert. Die Datenschutzbehörde CPPA soll bis Januar 2026 eine Möglichkeit schaffen, dass Verbraucher mit einem standardisierten Formular die Löschung all ihrer Daten verlangen können.[10]
Sind die externen (und ggf. internen) Datenschutzhinweise an die einschlägigen Bundesstaaten angepasst worden?	■ Auch bei den Vorgaben für die Datenschutzhinweise für Verbraucher gibt es einige Unterschiede zu Art. 13 und 14 DS-GVO – wiederum je nach Bundesstaat.[11] ■ Neben den bundestaatlichen Datenschutzgesetzen für Verbraucher gelten die einschlägigen FTC-Richtlinien, die kurz zusammengefasst Folgendes vorsehen: - klare, kurze und standardisierte Datenschutzhinweise, - angemessener Zugang zu den von ihnen gespeicherten Verbraucherdaten, der in einem angemessenen Verhältnis zur Sensibilität der Daten und der Art ihrer Verwendung steht, - Aufklärung der Verbraucher über die Datenschutzpraktiken der Unternehmen (Datenzugang, Datenberichtigung, Opt-out usw.). ■ Vereinzelt schützen US-Bundesstaaten (vornehmlich wiederum Kalifornien) mit ihren Datenschutzgesetzen auch Arbeitnehmer- und B2B-Daten. Dann könnten zusätzlich überarbeitete interne Datenschutzhinweise erforderlich werden. ■ Die unterschiedlichen Regeln können es erforderlich machen, verschiedene Schutzebenen in der Datenschutzerklärung vorzusehen (etwa: „Rules for residents in Vermont …“ usw.), wenn die Schwellenwerte in den Bundesstaaten überschritten werden.
Sind die Vorschriften über den „Sale“ oder das Teilen von personenbezogenen Daten einschlägig? Muss ein Opt-out gewährt werden? Funktioniert das Opt-out reibungslos und zügig?	■ Der Begriff „Sale“ ist in den einschlägigen US-Datenschutzgesetzen extrem weit definiert.[12] Praktisch jede Form von „Gegenleistung“ (consideration) des Datenempfängers ist von der Definition abgedeckt. ■ Die Vorschriften erfordern eine intensive Prüfung, ob und wann ein Verkauf/eine Weitergabe von personenbezogenen Daten vorliegt (sowohl offline als auch bei der Weitergabe durch Tracker/Cookies). Eventuell muss ein (funktionierendes) Opt-out gewährt werden (möglicherweise gibt es Fristen zu beachten).

6 California Code, Civil Code – CIV § 1798.140 (d) (2) "Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business and with whom the business shares consumers' personal information. 'Control' or 'controlled' means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. 'Common branding' means a shared name, service mark, or trademark that the average consumer would understand that two or more entities are commonly owned."

7 California Code, Civil Code – CIV § 1798.140 (d) (3) A joint venture or partnership composed of businesses in which each business has at least a 40 percent interest. For purposes of this title, the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business.

8 In den Draft Regulations der CPPA heißt es klarstellend: "Nonbusiness" means a person or entity that does not meet the definition of a "business" as defined in Civil Code section 1798.140, subdivision (d). For example, non-profits and government entities are Nonbusinesses because "business" is defined, among other things, to include only entities "organized or operated for the profit or financial benefit of its shareholders or other owners.", abrufbar unter: https://cppa.ca.gov/meetings/materials/20230203_item4_text.pdf.

9 Nach dem neuen New York City AI Audit Law ist zB ein expliziter Bias Audit bei Einstellungen und Beförderungen erforderlich, vgl. https://news.bloomberglaw.com/daily-labor-report/new-york-citys-ai-hiring-bias-law-creates-hurdles-for-companies.

10 Vgl. https://www.heise.de/news/Gesetzentwurf-Delete-Act-soll-Datenloeschung-in-Kalifornien-vereinfachen-9307339.html.

11 S. die spezifischen Vorgaben in § 7011 (e) (1) der CPPA-Regeln für Kalifornien: "A comprehensive description of the business's online and offline information practices, which includes the following: (A) Identification of the categories of personal information the business has collected about consumers in the preceding 12 months. … (B) Identification of the categories of sources from which the personal information is collected. (C) Identification of the specific business or commercial purpose for collecting personal information from consumers …" Häufig bietet sich eine Tabellenform an.

Aktionsfeld	Kommentare
	■ Weitere Opt-out-Rechte für Verbraucher gibt es auch in folgenden Gesetzen (Auswahl): - CAN-SPAM Act für kommerzielle (Werbe-)E-Mails, - TCPA für Werbeanrufe/Texte an Mobiltelefone, - kalifornischer Shine the Light Act für personenbezogene Daten für Direktmarketingzwecke, - CPRA, Virginia CDPA, Colorado Privacy Act, Utah Consumer Privacy Act, Connecticut Privacy Act für zielgerichtete Online-Werbung.
Werden Online-Tracker benutzt?	■ Die größte Gefahr sind in diesem Sektor Sammelklagen, neben einer möglichen Durchsetzung der Regeln durch die Regulierungsbehörden – insbesondere die FTC mit ihren neuesten Verfahren wegen „third-party tracking pixels" und der Weitergabe von Gesundheitsdaten (GoodRx, BetterHelp, Easy Healthcare).[13] ■ Video-Tracking ist zB durch ein Sondergesetz (VPPA) abgedeckt.[14]
Werden biometrische Daten verarbeitet?	■ Ein leider häufig übersehenes Problem! Derzeit haben nur Illinois, Texas und Washington spezifische Gesetze zum Schutz biometrischer Daten erlassen. Mindestens acht weitere Staaten haben neue biometrische Gesetze in Erwägung gezogen. ■ Es ist wahrscheinlich, dass US-Bundesstaaten ohne biometrische Gesetze das Gesetz von Illinois als Vorbild nehmen werden. In einigen Fällen haben lokale Gebietskörperschaften wie New York City die Erhebung und Verwendung biometrischer Daten geregelt. ■ Die FTC sanktioniert selbst falsche oder irreführende Angaben und unzuverlässige KI bei biometrischen Daten. ■ Die Durchsetzung des BIPA in Illinois hat schon zu gerichtlich zugesprochenem Schadensersatz in 9-stelliger Höhe geführt. ■ Lokale Vorschiften existieren: Ein texanisches Gesetz über die Erfassung oder Verwendung biometrischer Identifikatoren (CUBI)[15] schreibt die Vernichtung biometrischer Identifikatoren innerhalb eines angemessenen Zeitraums vor, jedoch spätestens nach einem Jahr, nachdem der Zweck der Erfassung der biometrischen Identifikatoren beendet wurde.
Werden Gesundheitsdaten verarbeitet? Ist ein Opt-in statt eines Opt-out erforderlich?	■ Hier ist besondere Vorsicht geboten! Neben dem schon genannten HIPAA gibt es zahlreiche bundesstaatliche Vorschriften, FTC-Regeln und anhängige Sammelklagen zum Schutz von Gesundheitsdaten, zB nach dem „My Health My Data"-Gesetz (MHMDA) des Bundesstaats Washington.[16] ■ Die Definition von sensiblen Informationen in den US-Datenschutzgesetzen ist häufig weiter gefasst als die Definition der besonderen Datenkategorien in Art. 9 DS-GVO.
Werden personenbezogene Daten von Kindern verarbeitet?	■ Sonderregeln gibt es zB im Children's Online Privacy Protection Act (COPPA), welche die Daten von Kindern bis zu 12 Jahren besonders schützen. Die Schwelle liegt niedriger als in Art. 8 Abs. 1 DS-GVO. ■ Bundesstaatliche Gesetz können davon abweichende Schwellenwerte für bestimmte Aktivitäten beinhalten.
Muss eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden? Und wenn ja, wie?	■ Verglichen mit der DS-GVO gibt es in den USA zahlreiche in den Gesetzen vorgesehene Fälle, in denen eine DSFA erforderlich ist. Ein Beispiel unter vielen ist die Verarbeitung von Gesundheitsdaten. ■ Falls schon eine DSFA nach der DS-GVO existiert, muss deren Inhalt aktualisiert und auf die bundesstaatlichen Erfordernisse angepasst werden.
Ist der Bruch der Datensicherheit intern (hinreichend konkret) geregelt? Weiß jeder, was zu tun ist?	■ In diesem auch für ausländische Unternehmen wichtigen Sektor gibt es trotz lauter Klagen der Industrie immer noch kein vereinheitlichendes Bundesgesetz, abgesehen von einigen Sonderbestimmungen auf Bundesebene. ■ Die FCC-Bestimmungen zu Customer Proprietary Network Information (CPNI) zB verlangen von allen erfassten TK-Anbietern, dass sie angemessene Maßnahmen ergreifen, um Versuche eines unbefugten Zugriffs auf diese begrenzte Kategorie von Informationen aufzudecken, und sich dagegen schützen. Die CPNI-Regeln schreiben auch vor, dass CPNI-Sicherheitsverletzungen gemeldet werden müssen und wie diese Meldung zu geschehen hat. ■ Die Securities and Exchange Commission (SEC) hat für börsennotierte Unternehmen eigene Regeln. ■ Auf Bundesstaatsebene ist die Situation in den USA ausgesprochen unübersichtlich: Alle 50 US-Bundesstaaten, der District of Columbia, Guam, Puerto Rico und die US-Jungferninseln verfügen über eigene Gesetze zur Meldung von Verletzungen der Datensicherheit. ■ Cybersecurity-Versicherer (cyber insurance) fordern häufig Data Breach Policies und haben eigene Vorgaben.

12 California Code, Civil Code – CIV § 1798.140 (ad) (1) "Sell", "selling", "sale" or "sold" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration. (2) For purposes of this title, a business does not sell personal information when: (A) A consumer uses or directs the business to intentionally: (i) Disclose personal information. (ii) Interact with one or more third parties. (B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information or limited the use of the consumer's sensitive personal information for the purposes of alerting persons that the consumer has opted out of the sale of the consumer's personal information or limited the use of the consumer's sensitive personal information ... – Durch Mergers, Bankrott usw. verursachte Datentransfers sind auch vom „Sale" ausgeschlossen.

13 FTC Office of Technology, Zusammenfassung v. 16.3.2023, abrufbar unter: https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking.

14 Der VPPA ist ein Bundesgesetz (ursprünglich von 1988), das es jedem Videodiensteanbieter verbietet, wissentlich personenbezogene Daten über „Mieter, Käufer oder Abonnenten von Waren oder Dienstleistungen" des Videodiensteanbieters ohne deren Zustimmung offenzulegen: 18 U.S. Code § 2710 – Wrongful disclosure of video tape rental or sale records.

15 Capture and Use of Biometric Information, abrufbar unter: https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm.

16 Vgl. https://lawfilesext.leg.wa.gov/biennium/2023-24/Pdf/Bills/Session%20Laws/House/1155-S.SL.pdf?q=20230509084942.

Aktionsfeld	Kommentare
Müssen Verträge, die einen Datentransfer an Dienstleister oder Verantwortliche vorsehen, angepasst werden?	■ Vorsicht: Die Vorgaben in einzelnen Bundesstaaten können über das hinausgehen, was Art. 26 und 28 DS-GVO von den Parteien verlangen. ■ In Kalifornien zB schreiben die CPPA-Regeln vor, dass ein Dienstleister oder Auftragnehmer personenbezogene Daten nur für die „spezifischen Geschäftszwecke" speichern, verwenden oder offenlegen darf, die im schriftlichen Vertrag nach dem CCPA zwischen dem Unternehmen und dem Dienstleister oder Auftragnehmer festgelegt sind. ■ Darüber hinaus gibt es eng definierte zusätzliche legitime Zwecke der Auftragsdatenverarbeitung, die nicht im Vertrag vereinbart werden müssen, zB „zur internen Verwendung durch den Dienstleister oder Auftragnehmer, um die Qualität der für das Unternehmen bereitgestellten Dienstleistungen zu steigern oder zu verbessern." Oder zur Aufdeckung von betrügerischen Handlungen und eines Bruchs der Datensicherheit.[17]
Welche zusätzlichen internen Richtlinien (policies) sind für das US-Geschäft erforderlich?	Zu erwägen sind für die USA u.a. folgende interne Richtlinien: ■ Data Retention Policy ■ Online Media Policy ■ Data Access Policy ■ BYOD Policy

Dr. Axel Spies
ist Rechtsanwalt in der Kanzlei Morgan, Lewis & Bockius in Washington DC und Mitherausgeber der ZD.

17 CCPA Regulations § 7050 (b) (4) und (5).

SEBASTIAN SCHWEDA / ULF NADARZINSKI

Müssen Verantwortliche ein Empfängerverzeichnis führen?

Auslegung der Rechtsgedanken zur Auskunftspflicht über Datenempfänger aus dem EuGH-Urteil

Betroffenenrechte
Transparenz
Offenlegung
Dokumentationspflicht
Datenminimierung

■ Mit seiner Entscheidung in der Rs. Österreichische Post (ZD 2023, 271) hat der EuGH klargestellt, dass Betroffene idR ein Recht haben, vom Verantwortlichen Auskunft über die konkreten Empfänger ihrer Daten zu erhalten. Anders ist dies nur dann, wenn diese nicht identifiziert werden können. Dies kann laut EuGH insbesondere bei künftigen Offenlegungen der Fall sein, wenn die Empfänger noch nicht bekannt sind. Wann aber ist davon auszugehen, dass Empfänger vergangener Offenlegungen nicht mehr identifizierbar sind? Kann sich der Verantwortliche darauf berufen, dass ihm dazu keine Informationen mehr vorliegen? Oder muss er ein eigenes Verzeichnis pflegen, aus dem sich für jede betroffene Person ergibt, wem ihre Daten offengelegt wurden? Die Autoren argumentieren, dass sich aus der DS-GVO keine Pflicht ableiten lässt, die konkreten Empfänger für jede betroffene Person für mögliche Auskunftsbegehren vorzuhalten. Wenn der Verantwortliche diese Information daher nicht zu anderen Zwecken gespeichert hat, verlangt das EuGH-Urteil nach dieser Auslegung auch nicht, dass er Betroffenen die konkreten Empfänger mitteilen muss.

■ In its decision in the Österreichische Post case (ZD 2023, 271), the ECJ clarified that data subjects generally have a right to receive information from the controller about the specific recipients of their data. This is only different if they cannot be identified. According to the ECJ, this can be the case for future disclosures if the recipients are not yet known. But when can we assume that recipients of past disclosures are no longer identifiable? Can the controller rely on the fact that he no longer has any information about them? Or does he have to maintain his own directory, from which it is clear for each data subject to whom his data has been disclosed? The authors argue that no obligation can be derived from the GDPR to keep the specific recipients for each data subject for possible requests for access. Therefore, if the controller has not stored this information for other purposes, the ECJ ruling, according to this interpretation, does not require it to inform data subjects of the specific recipients.
Lesedauer: 19 Minuten

I. Die Entscheidung des EuGH

Mit seinem Urteil v. 12.1.2023 in der Rs. RW gegen Österreichische Post AG (im Folgenden: Österreichische Post)[1] hat der EuGH klargestellt, dass Verantwortliche auf Verlangen Betroffener gem. Art. 15 Abs. 1 lit. c DS-GVO[2] grundsätzlich auch Auskunft darüber erteilen müssen, gegenüber welchen konkreten Empfängern personenbezogene Daten offengelegt worden sind oder noch werden.

Damit entschied der EuGH zu Vorlagefragen des ÖOGH im Zusammenhang mit der Klage eines Betroffenen gegen die Österreichische Post. Diese hatte auf seinen Auskunftsantrag hin zu-

1 EuGH ZD 2023, 271 – Österreichische Post.
2 VO (EU) 2016/679 des Europäischen Parlaments und des Rates v. 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG (ABl. L 119 v. 4.5.2016, 1, ABl. L 314 v. 22.11.2016, 72, ABl. L 127 v. 23.5.2018, 2).