Zahlreiche neue Datenschutzgesetze in den US-Bundesstaaten

Schwierige Datenschutz-Compliance in den USA

Dr. Axel Spies ist Rechtsanwalt bei Morgan Lewis & Bockius in Washington DC und Mitherausgeber der MMR.

Die Unternehmen kommen mit ihrer Datenschutz-Compliance kaum mehr nach: Neue nicht nur auf einen Sektor abzielende US-Datenschutzgesetze gibt es mittlerweile in Virginia, Colorado, Connecticut, Utah und Kalifornien (CCPA und neuerdings ergänzend der CPRA). Diese Gesetze sind entweder schon in Kraft oder werden in naher Zukunft in Kraft treten. Andere US-Bundesstaaten werden folgen. Ein allgemeines Modell, das als Vorbild für die Datenschutz-Compliance gelten kann, hat sich noch nicht herausgebildet.

Lesedauer: 16 Minuten

I. US-Bundesgesetz American Data Privacy Protection Act weiter in der Diskussion

Es wäre nicht nur für die Europäer schön, wenn wirklich nach Jahren der Verhandlungen im Kongress endlich etwas geschehen würde, aber ein den Gesetzen dieser Einzelstaaten nachgestaltetes, vielversprechendes Bundesgesetz (American Data Privacy Protection Act – ADPPA)[1] kommt im US-Kongress u.a. wegen des Ergebnisses der Zwischenwahlen 2022 und einem internen politischen Fingerhakeln[2] nicht vom Fleck. Der Energie- und Handelsausschuss des Repräsentantenhauses billigte den Gesetzesentwurf des ADPPA am 20.7.2022, aber das gesamte US-Repräsentantenhaus hat bislang noch nicht über den Entwurf abgestimmt. Es bleibt in der Schwebe. Der ADPPA würde für die meisten Einrichtungen gelten, auch für gemeinnützige Organisationen und Common Carrier, die von der Federal Communications Commission geregelt werden. Für Verantwortliche, die als „große Dateninhaber" (large data holder) definiert sind[3] und bestimmte Schwellenwerte erreichen,[4] und für Dienstleister, die Daten im Auftrag anderer Einrichtungen nutzen, gibt es zusätzlichen Anforderungen. Für Individuen, die im „nicht kommerziellen Zusammenhang" Daten verarbeiten, gilt der ADDPA nicht. Der sachliche Anwendungsbereich umfasst Informationen, die eine Person „identifizieren oder mit ihr verbunden oder vernünftigerweise mit einer Person verknüpft oder verknüpfbar" sind.

Ohne hier auf die Einzelheiten des ADPPA eingehen zu wollen: Der Anwendungsbereich und die Rechtsfolgen der DS-GVO und des ADPPA sind unterschiedlich. Der US-Gesetzgeber ist sich durchaus der DS-GVO bewusst, geht aber in vielen Bereichen im ADPPA eigene Wege. Die Definition des „Verarbeitens" in Sec. 2 (26) ADPPA ist zB nicht identisch mit der viel detaillierteren Definition desselben Begriffs in Art. 3 Nr. 2 DS-GVO und für den wichtigen Begriff „affirmative express consent" im ADPPA findet man leider in der DS-GVO keine Entsprechung. Bei manchen Bestimmungen des ADPPA halten politische Erwägungen der USA Einzug. Der Gesetzentwurf sieht zB vor, dass die betroffenen Unternehmen u.a. offenlegen müssen, ob sie die Daten der Volksrepublik China, Russland, dem Iran oder Nordkorea zugänglich machen.[5] Der Gesetzentwurf würde auch kleine und mittlere Unternehmen, die bestimmte Größen- und Datenerhebungsschwellenwerte erreichen, von der Einhaltung bestimmter Anforderungen befreien. So können diese Unternehmen zB auf die Aufforderung eines Verbrauchers, seine Daten zu korrigieren, reagieren, indem sie die Daten gleich löschen, anstatt sie zu korrigieren; sie wären von den meisten Datensicherheitsanforderungen des Gesetzentwurfs befreit. Vorschriften zum internationalen Datentransfer aus den USA heraus gibt es im AD-PPA nicht. Die DS-GVO widmet dem Thema bekanntlich ein ganzes Kapitel V.

II. Kalifornien geht allein einen Schritt weiter

Ob mit oder ohne ADDPA, für die betroffenen Unternehmen gilt: Allein schon das Nachhalten, welche US-Gesetze ab wann für wen gelten, ist sehr aufwändig. Die Schwellenwerte für die Anwendung sind unterschiedlich und die aus den Gesetzen resultierenden Rechte und Pflichten weichen voneinander ab. In Kalifornien gelten bis Ende 2022 folgende drei alternativen Schwellenwerte, egal wo das Unternehmen seinen Sitz hat, solange das Unternehmen nur „Geschäft" (Business) in Kalifornien tätigt:

■ Bruttojahresumsatz von mindestens 25 Mio. USD oder

■ Verarbeitung der persönlichen Daten von 50.000 oder mehr kalifornischen Einwohnern, Haushalten oder Geräten oder

■ Erzielung von 50% oder mehr ihres Jahresumsatzes aus dem „Verkauf" (buy, receive, share or sell) personenbezogener Daten von Einwohnern Kaliforniens.

Diese Schwellenwerte haben sich zum 1.1.2023 etwas geändert: Um den zweiten Schwellenwert zu erreichen, müssen Unternehmen ab 2023 jährlich die personenbezogenen Daten von 100.000 oder mehr Verbrauchern oder Haushalten kaufen, verkaufen oder weitergeben.[6] Der umstrittene Begriff „Geräte" (devices) fällt dann weg. Auch europäische Unternehmen können von diesen Gesetzen betroffen sein, da der Sitz des Unternehmens für die Anwendbarkeit der Gesetze keine Rolle spielt. Vielmehr kommt es darauf an, wessen Daten von der Verarbeitung betroffen sind. Der Schwerpunkt liegt auf den Verbrauchern im jeweiligen Bundesstaat, denn die genannten Gesetze sind weiterhin im Kern Verbraucherschutzgesetze. Der kalifonische CPRA[7] stellt klar, dass auch die Muttergesellschaft betrof-

fen ist und Maßnahmen ergreifen muss, wenn die kontrollierte Tochtergesellschaft in Kalifornien Kunden hat; ein gemeinsames Warenzeichen reicht dafür nach dem Gesetzestext schon aus.[8] Das bedeutet: „Hausaufgaben" für die Muttergesellschaft.

III. Umsetzung für europäische Unternehmen aufwändig

Besonders in den US-Bundestaaten, in denen eine direkte Klagemöglichkeit der Betroffenen per Gesetz besteht (right of private action), besteht ein erhebliches Risiko für Unternehmen, die sich nicht an die einschlägigen Datenschutzgesetze halten – gerade weil deren Webseiten so leicht auffindbar sind. Die Gesetze werden in den meisten Fällen von den jeweils zuständigen Generalstaatsanwälten (attorney general) durchgesetzt.

In Kalifornien hat eine neue unabhängige Datenschutzbehörde, die California Privacy Protection Agency (CPPA), ihre Arbeit aufgenommen, die ihrerseits Durchsetzungsbefugnisse hat.[9] Sammelklagen gegen bestimmte Unternehmen sind in Kalifornien nach dem kalifornischen Datenschutzrecht schon anhängig.[10] Die Schadenssummen bei Sammelklagen in den USA können hoch sein, wenn man der Erfahrung aus anderen Bereichen trauen darf.

Daneben gibt es weitere zahlreiche Datenschutzregeln in den USA, die sektorspezifisch sind. Sie decken zB den Online-Bereich ab. Der Gesundheitsbereich und der Finanzbereich folgen seit eh und je eigenen Gesetzen.[11] Auch bei einem Bruch der Datensicherheit (Datenpanne) sind in den USA zahlreiche Spezialgesetze einschlägig.[12] Zur Umsetzung kommen für die betroffenen Unternehmen u.a. folgende Maßnahmen in Frage:

■ Anpassung der Datenschutzerklärungen an die Erfordernisse des jeweiligen Bundesstaats;

■ Aufsetzen eines internen Compliance-Systems für diejenigen Betroffenen, die ihre Rechte ausüben;

■ Anpassung der internen Richtlinien an die jeweiligen Erfordernisse der Bundesstaaten sowie

■ Training des Personals.

Bei der Umsetzung der Gesetze mittels dieser Maßnahmen kann es für die betroffenen Unternehmen leicht zu Missverständnissen kommen. Es kann durchaus vorkommen, dass in einer Unternehmensgruppe bei der Erarbeitung eines Konzepts zur Umsetzung Verständnisschwierigkeiten aufkommen, weil allein schon die in den Gesetzen verwendeten Begriffe nicht identisch sind mit dem, was ein Verantwortlicher aus der EU gewohnt ist. Die Definitionen im geplanten ADPPA wurden schon genannt. Es gibt leider überall juristische Fußangeln. Der kalifornische CPRA definiert zB den Begriff „Verkauf" (sale) weiter als es der Wortsinn nahelegt: „verkaufen", „Verkauf" oder „verkauft" bedeutet im CPRA „den Verkauf, die Vermietung, die Freigabe, die Offenlegung, die Verbreitung, die Zurverfügungstellung, die Übertragung oder die anderweitige mündliche, schriftliche, elektronische oder sonstige Übermittlung der persönlichen Daten eines Verbrauchers durch das Unternehmen an ein anderes Unternehmen oder einen Dritten gegen Geld oder eine andere Gegenleistung."[13]

Ein anderes Paradebeispiel dafür, dass man mit dem Wortsinn häufig nicht weiterkommt, ist die Definition von personenbezogene Daten (personal information), für die es im CCPA[14] folgende Ausnahme gibt: „Personal Information" umfasst keine öffentlich zugänglichen Informationen. Für die Zwecke dieses Absatzes bedeutet „öffentlich zugänglich" Informationen, die rechtmäßig aus Aufzeichnungen von Bundes-, Landes- oder Kommunalbehörden zugänglich gemacht werden. „Öffentlich zugänglich" umfasst nicht „biometrische Informationen, die von einem Unternehmen über einen Verbraucher ohne dessen Wissen gesammelt wurden."[15] Bei der Verarbeitung von biometrischen Daten ist zur Zeit der Illinois Biometric Information Privacy Act[16] das in den USA strengste Gesetz und nicht etwa der CCPA/CPRA.

Diese beiden Beispiele zeigen, dass es wenig Sinn macht, die gewohnten DS-GVO-Standards eins zu eins in die USA übertragen zu wollen. Das liegt nicht nur an den verschiedenen Rechtsbegriffen. Die US-Datenschutzgesetze können auch strenger (oder zumindest spezifischer) sein als die einschlägig bekannten Datenschutzgesetze in Europa, indem zB nach kalifornischem Recht ein Opt-out-Button für die Verbraucher bei einem „Sale" seiner Daten auf der Webseite gut sichtbar installiert werden muss.[17] Die Datenschutzerklärungen können damit für weltweit tätig Unternehmen dadurch noch länger und unübersichtlicher werden und zu (aufklappbaren) Akkordeon-Lösungen oder Datenschutzerklärungen in zahlreichen Sprachen mit mehreren Ebenen führen. Keine einfache Aufgabe gerade für kleinere Unternehmen, die gerne ihre Produkte weltweit anbieten wollen.

Die am Ende des Beitrags befindliche Tabelle stellt die verabschiedeten allgemeinen Datenschutzgesetze in den Bundesstaten Kalifornien, Colorado, Utah und Virginia gegenüber.

IV. Privacy Shield 2.0/Phoenix aus der Asche?

Am 7.10.2022 hat Präsident Biden eine Executive Order (EO)[18] und ein Memorandum zur Presidential Directive PPD-28[19] veröf-

fentlicht, um es den Europäern nach dem Schrems-II-Urteil des EuGH[20] zu erleichtern, einen Nachfolger des Privacy Shield (Trans-Atlantic Data Privacy Framework) zu finden. Max Schrems und seine Organisation NOYB kritisierten die Maßnahmen umgehend – wenig überraschend.[21] Ihm

wurde auf dem IAPP Europe Data Protection Congress (DPC) deshalb u.a. „mangelnder Respekt" vor der ausländischen Rechtsordnung vorgeworfen. Wie dem auch sei, die EO ist bindend, aber ein Bundesgesetz, das viele fordern, ist es nicht. Dies ist aber kein grundsätzliches Hindernis, weil die Adäquanz-Entscheidung eine Klausel zur Aussetzung enthalten könnte, wenn ein US-Präsident die EO widerruft oder wesentlich abändert.

Im Wesentlichen ergeben sich durch die Maßnahmen folgende Änderungen gegenüber dem Privacy Shield auf US-Seite:

1. Die EO schafft einen „mehrstufigen Mechanismus" für Personen aus „qualifizierten Staaten und Organisationen der regionalen Wirtschaftsintegration, wie sie gemäß der EO benannt werden", um eine unabhängige und verbindliche Überprüfung von Ansprüchen zu gewährleisten, dass ihre persönlichen Daten durch US-Spionagemaßnahmen erfasst wurden. Dieser Mechanismus besteht aus

■ einem Beauftragten für den Schutz der bürgerlichen Freiheiten im Büro des Direktors der nationalen Nachrichtendienste (CLPO) für die erste Untersuchung einer individuellen Beschwerde und

■ im Falle eines Rechtsmittels einem Datenschutz-Überprüfungsgericht (Data Protection Review Court – DPRC), das auf Antrag der betroffenen Person oder eines Mitglieds der Intelligence Community eine unabhängige und verbindliche Überprüfung der Entscheidungen des CLPO vornimmt. Das Weiße Haus erklärt, dass die Richter des DPRC von außerhalb der US-Regierung rekrutiert werden und über einschlägige Erfahrungen auf dem Gebiet des Datenschutzes und der nationalen Sicherheit verfügen müssen. Sie sollen die Beschwerden unabhängig prüfen und sind vor Abberufung geschützt. Der Beschwerdeführer ist selbst nicht am DPRC-Verfahren direkt beteiligt. Stattdessen wählt das DPRC für jeden Fall einen speziellen Interessensvertreter aus, der den Beschwerdeführer in der Angelegenheit vertritt.

2. Die EO hebt die vom EuGH (Schrems II) kritisierte[22] Presidential Directive PPD-28 auf, „mit Ausnahme der Abschnitte 3 und 6 dieser Richtlinie und des als Verschlusssache eingestuften Anhangs zu dieser Richtlinie, die weiterhin in Kraft bleiben."

3. Ein Civil Liberties Oversight Board wird die Richtlinien und die Verfahren der Intelligence Community überprüfen, um sicherzustellen, dass sie mit der EO übereinstimmen. Vorgesehen ist eine jährliche Überprüfung, einschließlich der Überprüfung, ob die Intelligence Community den Feststellungen und Entscheidungen des DPRC vollständig nachgekommen ist.

Ob diese Maßnahmen, die weiter gehen als das Ombudsperson-System des Privacy Shield,[23] für die Adäquanz aus Sicht der EU ausreichen, ist derzeit unklar. Auf EU-Seite bedarf es diverser Schritte, um einen Angemessenheitsbeschluss herbeizuführen.[24] Der Europäische Datenschutzausschuss (EDSA) muss eine unverbindliche Stellungnahme abgeben, kann weitere Dokumente anfordern und das EU-Parlament kann eine formelle Stellungnahme abgeben. Ein Ausschuss, der sich aus Vertretern der EU-Mitgliedstaaten zusammensetzt, muss dann den Vorschlag mit qualifizierter Mehrheit billigen. Dieser Prozess[25] dürfte frühestens im März 2023 mit einer zusätzlichen Umsetzungsfrist von einigen Monaten abgeschlossen sein.

Die neuen Regeln sind kompliziert und zT Neuland. Es ist zu vermuten, dass die EU-Kommission in die Abfassung des Texts der Maßnahmen im Vorfeld so eng eingebunden war, um weitere Schwierigkeiten vor Gericht zu vermeiden. Ob die Fundamentalkritik von NOYB, dass das DPRC kein unabhängiges Gericht iSd Schrems-II-Entscheidung und von Art. 47 GRCh sei, stichhaltig ist, muss am Ende vielleicht doch wieder der EuGH klären. Aus US-Sicht zieht die Kritik nicht: Ähnliche in die Executive eingegliederte Gerichte wie der DPRC gibt es in den USA bereits seit langem (zB das

Board of Immigration Appeals[26] des Justizministeriums). Der Ombudsmann des Privacy Shield war ein politischer Beamter.[27] Das wird beim DPRC mit seinen unabhängigen Richtern anders sein.

Die Ergebnisse der Untersuchung sind jedenfalls intern bindend – sie sind nicht nur Empfehlungen an die Sicherheitsbehörden wie beim Ombudsmann.[28] Allerdings sind drei Einschränkungen bemerkenswert:

■ Der CLPO befasst sich nur mit „qualifizierte(n) Beschwerden, die von der zuständigen Behörde eines qualifizierten Staates in Bezug auf US-Signalaufklärungstätigkeiten übermittelt werden"; diese werden „auf einen erfassten Verstoß gegen das Recht der Vereinigten Staaten hin überprüft und erforderlichenfalls geeignete Abhilfemaßnahmen."[29] Das bedeutet praktisch: Der Betroffene aus Europa kann wie schon beim Ombudsperson-System nicht den CLPO direkt anrufen, sondern nur die zuständige Datenschutzbehörde. Und er muss eine „covered violation" des US-Recht rügen.[39] Mit diesem Mechanismus werden Probleme des US-Prozessrechts für den ausländischen Beschwerdeführer (standing) umschifft.[31] Das Problem des „standing" besteht iÜ auch im neuen ADPPA, wenn er verabschiedet wird. Er gilt nur für eine „natürliche Person mit Wohnsitz in den Vereinigten Staaten" (gleich welcher Nationalität), schützt also nicht Betroffene iSd DS-GVO in Europa.[32] Damit dürfte der ADPPA für die Prüfung der Angemessenheit des Datenschutzes verglichen mit der EU kaum eine Rolle spielen.

■ Das Beschwerdeverfahren ist kein Antrag auf Datenauskunft iSv Art. 15 DS-GVO. CLPO und DPRC haben zwei Möglichkeiten, um dem Beschwerdeführer zu antworten: „es gibt keine Überwachung" oder „ja, es gab ein Problem und es wurde gelöst." Eine Liste mit den Daten, die US-Sicherheitsbehörden über

ihn gespeichert haben, erhält er nicht. Dies ist sinnvoll, weil ansonsten das Beschwerdeverfahren missbraucht werden könnte, um Kenntnisse über die US-Geheimdienste zu sammeln.

Übersicht: Allgemeine Datenschutzgesetze in bestimmten US-Bundesstaaten (Stand 12/2022)

	US-BUNDESSTAAT	Kalifornien (CPRA)	Kalifornien (CCPA)	Colorado Privacy Act (CPA)[33]	Utah Consumer Privacy Act (UCPA)[34]	Virginia Consumer Data Protection Act (VCDPA)[35]
Anwendbarkeit	**Inkrafttreten**	1.1.2023	1.1.2020	1.7.2023	31.12.2023	1.1.2023
Rechte der Betroffenen	Recht auf Datenzugang	X	X	X	X	X
	Recht auf Berichtigung	X		X		X
	Recht auf Löschung	X	X	X	X	X
	Recht auf Verarbeitungsbeschränkung	X			X	X
	Recht auf Portabilität	X	X	X		X
	Recht auf Opt-out	X	X	X	X beschränkt	X

	US-BUNDESSTAAT	Kalifornien (CPRA)	Kalifornien (CCPA)	Colorado Privacy Act (CPA)[33]	Utah Consumer Privacy Act (UCPA)[34]	Virginia Consumer Data Protection Act (VCDPA)[35]
Anwendbarkeit	**Inkrafttreten**	1.1.2023	1.1.2020	1.7.2023	31.12.2023	1.1.2023
	Private Right of Action	X	X			
	Recht gegen automatisierte Entscheidungstreffung	X		X		X
	Allgemeines Private Right of Action – Klagerecht	X	X			
	Recht auf Anfechtung einer Entscheidung, die den Datenzugang (Access Request) versagt.			X		X
Anforderungen an den Verarbeiter	Privacy Notice-Transparenzerfordernis	X	X	X	X	X
	Benachrichtigungspflicht bei einem Bruch der Datensicherheit					
	Impact Assessments geregelt oder erforderlich	X		X		X
	Diskriminierungsverbot bei der Ausübung der Rechte	X	X	X	X	X
	Zweckbegrenzung bei der Verarbeitung	X	X	X	X	X
	Data Processing Agreements erforderlich	X	X	X	X	X
	Zweckbegrenzung	X	X	X		X
	Korrekturfrist bei Verstößen			X (60 Tage)	X (30 Tage)	X (30 Tage)
	Pflicht zur Datenminimisierung	X		X	X	X

	US-BUNDESSTAAT	Kalifornien (CPRA)	Kalifornien (CCPA)	Colorado Privacy Act (CPA)[33]	Utah Consumer Privacy Act (UCPA)[34]	Virginia Consumer Data Protection Act (VCDPA)[35]
Anwendbarkeit	**Inkrafttreten**	1.1.2023	1.1.2020	1.7.2023	31.12.2023	1.1.2023
	Besondere Regelungen für sensitive Daten	X		X		X
Datenschutz und Datenminimierung	Überwachung der Implementierung (Data Protection Program)	X		X	X	X
	Regelungen zur Datenlöschung					
	Reguliert „Sale" der Daten	Opt-out	Opt-out	X	X	Opt-out (Opt-in bei sensiblen Daten)
	Notifizierungspflichten bei Bruch der Datensicherheit		X			
Pflichten ggü. Dritten	Pflichten für Dienstleister-Service Providers (SP)	X		X	X	X
	Datenschutzprogramm für Third-Party SP			X		X
Biometrische Daten	Reguliert die Sammlung und/oder Speicherung	X	X	X	X	X
	Anmerkungen:	Ändert den CCPA und fügt u.a. neue Rechte und Verfahrensanforderungen hinzu; gilt ab dem 1.1.2023 nunmehr auch für B2B und für Arbeitnehmerdaten.	Derzeit gültig, aber wird durch den CPRA zum 1.1.2023 geändert und ergänzt.		Das bislang verarbeiterfreundlichste Datenschutzgesetz.	Am 11.4.2022 unterzeichnete der Gouverneur ein Gesetz mit Änderungen des VCDPA (HB 381). Es sieht eine Ausnahme vom Recht des Verbrauchers auf Löschung vor, wenn der Verantwortliche Verbraucher

	US-BUNDESSTAAT	Kalifornien (CPRA)	Kalifornien (CCPA)	Colorado Privacy Act (CPA) 33	Utah Consumer Privacy Act (UCPA)34	Virginia Consumer Data Protection Act (VCDPA)35
Anwendbarkeit	**Inkrafttreten**	1.1.2023	1.1.2020	1.7.2023	31.12.2023	1.1.2023
						daten von einer anderen Quelle als dem Verbraucher erhalten hat.

■ Die neuen Regeln für das Beschwerdeverfahren greifen nur ein, wenn es eine Reziprozität des Beschwerdemechanismus seitens der EU-Staaten (oder eines Drittstaats wie Großbritannien)

gibt.33 Dafür bedarf es einer näher bestimmten Entscheidung (designation of qualifying state) des Justizministers. Das ist neu, aber im Ergebnis juristisch schwer angreifbar.

Um das Thema nur kurz zu erwähnen: Die EO enthält spezifische Vorgaben für allgemeine Datensammlungen (bulk collection), insbesondere deren „necessity" und „proportionality", die noch genauer analysiert werden müssen. Diese Begriffe sind entgegen der Ansicht von Schrems, Brink u.a. im US-Rechtskreis bekannt. In den vorgeschlagenen Umsetzungsregeln des kalifornischen CCPA zB findet man die Begriffe „necessary" und „proportionate" mit näheren Erläuterungen und Beispielen.34 Die US-Regierung hat die Aussagen des EuGH in der Rs. Schrems II zur „bulk collection" mehrfach angezweifelt.35 Sie sei in bestimmten Fällen zur Terrorismus- und Verbrechensbekämpfung notwendig. Die europäischen Gerichte müssen demnach über die aktuelle Rechtslage Beweis aufnehmen.

4. Fazit zum jetzigen Zeitpunkt: Die neue EO wird schon jetzt einen positiven Einfluss auf die Transfer Impact Assessments (TIA) für die USA haben, die allerdings weiterhin erforderlich sein werden – jedenfalls solange es keine rechtskräftige Adäquanzentscheidung der EU gibt. Bußgelder, wenn keine TIA vorliegt, sind weiter möglich. Wie immer man zu der EO steht, die ein Präsident theoretisch jederzeit durch eine neue EO widerrufen kann, es steht fest: In die neuen US-Regeln wurde viel Arbeit investiert und ihre Umsetzung ist noch nicht abgeschlossen.

Schnell gelesen …

■ Während in den USA ein allgemeines Bundesdatenschutz (ADPPA) weiter auf sich warten lässt, haben einzelne Bundesstaaten eigene allgemeine Datenschutzgesetze erlassen.

■ Die Gesetze sind unterschiedlich, was die Compliance für alle betroffenen Unternehmen sehr erschwert.

■ Daneben gibt es in den USA zahlreiche Spezialgesetze, die zB regeln, was bei einem Bruch der Datensicherheit zu tun ist oder wie mit Online-Daten umzugehen ist. Besonders geregelt sind u.a. die Bereiche Gesundheit und Finanzen.

■ Europäische Unternehmen mit Geschäftsbeziehungen in die USA, die unter diese Gesetze fallen, können die gewohnten DS-GVO-Standards nicht eins zu eins auf die Datenverarbeitung in den USA übertragen.

■ Die neue Executive Order v. 7.10.2022 ist ein Schritt in die richtige Richtung. Ob sie vor den europäischen Gerichten bei der Überprüfung der Adäquanz Bestand hat, wird sich noch zeigen.

Dr. Axel Spies
ist Rechtsanwalt bei Morgan Lewis & Bockius in Washington DC und Mitherausgeber der MMR.

---

1 Lesenswerte Übersicht des Congressional Research Service CRS v. 31.8.22, abrufbar unter: https://crsreports.congress.gov/product/pdf/LSB/LSB10776.

2 Näheres: Pelosi opposes proposed American Data Privacy and Protection Act, seeks new preemption, abrufbar unter: https://iapp.org/news/a/pelosi-rejects-proposed-american-data-privacy-and-protection-act-seeks-new-compromise/.

3 Sec. 2 (21) – Definitions, abrufbar unter: https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-1178152rh.pdf (H. R. 8152), S. 18.

4 Die Schwelle liegt bei 5 Mio. Datensätzen, aber es kommen noch andere Voraussetzungen und Ausnahmen dazu.

5 Sec. 202 (b) (9) Transparency, abrufbar unter: https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-1178152rh.pdf.

6 Näheres unter https://cppa.ca.gov/faq.html.

7 California Privacy Rights Act v. 3.11.2020, auf Grund der ballot initiative v. 2019, abrufbar unter: https://iapp.org/media/pdf/resource_center/ca_privacy_rights_act_2020_ballot_initiative.pdf und hierdurch geänderter Gesetzestext des kalifornischen Datenschutzgesetzes, abrufbar unter: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5; s. Zusammenfassung Spies MMR 2022, 425 sowie näher Spies ZD-Aktuell 2022, 01364 und ZD-Aktuell 2022, 01392.

8 Sec. 1798.140: (c)(2) "Any entity that controls or is controlled by a business as defined in paragraph (1) and that shares common branding with the business. "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, servicemark, or trademark."; s.a. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

9 Webseite der Behörde, abrufbar unter: https://cppa.ca.gov/.

10 Kürzlich Seirafi et al v. Samsung Electronics America, Inc., Case 4:22-cv-05176-KAW, Northern District of California schon auf der Grundlage des CCPA – abrufbar unter: https://www.classaction.org/media/seirafi-et-al-v-samsung-electronics-america-inc.pdf.

11 Spies ZD-Aktuell 2018, 04318

12 Spies ZD 2015, 293 und ZD-Aktuell 2018, 04318; FTC RiLi, abrufbar unter: https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business und Übersicht über die einschl. Gesetze, abrufbar unter: https://info.digitalguardian.com/rs/768-OQW-145/images/the-definitive-guide-to-us-state-data-breach-laws.pdf.

13 Sec. 1798.140 (t) (1), abrufbar unter: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

14 California Consumer Privacy Act v. 2018, abrufbar unter: https://oag.ca.gov/privacy/ccpa; Zusammenfassung Spies ZD-Aktuell 2021, 05009; ZD-Aktuell 2022, 01364 und ZD-Aktuell 2021, 01392 (mwN).

15 Sec. 1798.140 (o) (2).

16 Abrufbar unter: https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

17 Näheres im CPPA FAQ "What rights do I have under the CCPA today", abrufbar unter: https://cppa.ca.gov/faq.html und FAQ des CA Attorney General: "Businesses that sell personal information are subject to the CCPA's requirement to provide a clear and conspicuous "Do Not Sell My Personal Information" link on their website that allows you to submit an opt-out request. Businesses cannot require you to create an account in order to submit your request. Businesses also should not require you to verify your identity, though they can ask you basic questions to identify which personal information is associated with you …", abrufbar unter: https://oag.ca.gov/privacy/ccpa#collapse7b - B 3.

18 Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities, abrufbar unter: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-statessignals-intelligence-activities/; s.a. Dehmel/Ossmann-Magiera/Weiß MMR 2023, 17 – in diesem Heft.

19 National Security Memorandum on Partial Revocation of Presidential Policy Directive 28, abrufbar unter: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/.

20 EuGH MMR 2020, 597 mAnm Hoeren = ZD 2020, 511 mAnm Moos/Rothkegel – Schrems II.

21 Abrufbar unter: https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law; krit. auch der LfDI Baden-Württemberg, Dr. Stephan Brink – s. ZD-Aktuell 2022, 01389 mwN.

22 Paal/Kumkar MMR 2020, 73 mwN.

23 Abrufbar unter: https://www.state.gov/privacy-shield-ombudsperson/#:~:text=The%20Under%20Secretary%20of%20State,Union%20or%20Switzerland%20to%20the; allg. zu Privacy Shield s. von der Bussche/Voigt, Konzerndatenschutz/Spies, 2. Aufl. 2019, Teil 4, Kapitel 4.

24 S. FAQ der Kommission, abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045.

25 Näher Roßnagel in seinem Editorial ZD 2022, 305.

26 Abrufbar unter: https://www.justice.gov/eoir/board-of-immigration-appeals.

27 Krach, Under Secretary of State for Economic Growth, Energy, and the Environment.

28 Einzelheiten zur Ombudsperson: v.d. Bussche/Voigt, Konzerndatenschutz/Spies, 2019, Teil 4, Kap. 4 Rn. 25 und https://www.state.gov/privacy-shield-ombudsperson/sowie zum Verfahren https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0g.

29 EO, Sec. 3 (a). Signals Intelligence Redress Mechanism, abrufbar unter: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/.

39 Definiert in der EO in Sec. 4 (d) ebd.

31 Der Begriff ist schwer zu übersetzen – vielleicht mit „Klagebefugnis"; vgl. in Deutschland zur Grundrechtsbindung bei der Ausland-Ausland-Fernmeldeaufklärung nach dem BND-Gesetz – BVerfG Urt. v. 19.5.2020 – 1 BvR 2835/17; näher zu „standing" in den USA: Christakis/Propp/Swire (02/2022), abrufbar unter: https://europeanlawblog.eu/2022/02/16/eu-us-adequacy-negotiations-and-the-redress-challenge-how-to-create-an-independent-authority-with-effective-remedy-powers / mwN.

32 Sec. 2 Definition 16, abrufbar unter: https://www.congress.gov/bill/117th-congress/house-bill/8152/text#toc-H4B489C75371741CBAA5F38622BF082DE.

33 Colorado Privacy Act v. 8.7.2021, abrufbar unter: https://legiscan.com/CO/drafts/SB190/2021; Zusammenfassung Spies ZD-Aktuell 2021, 05257.

34 Utah Consumer Privacy Act v. 25.3.2022, abrufbar unter: https://le.utah.gov~-/2022/bills/static/SB0227.html; Zusammenfassung Spies ZD-Aktuell 2022, 01093.

35 Virginia Consumer Data Protection Act v. 3.3.2021, abrufbar unter: https://lis.virginia.gov/cgi-bin/legp604.exe?211+ful+SB1392ES1+pdf; Zusammenfassung Spies ZD-Aktuell 2021, 05047.

33 EO Sec. 2 (f) (i) Designation of qualifying state. "To implement the redress mechanism established by section 3 of this order, the Attorney General is authorized to designate a country or regional economic integration organization as a qualifying state for purposes of the redress mechanism established pursuant to section 3 of this order…"; Großbritannien hofft, bald auf diese Liste zu kommen, abrufbar unter: https://www.commerce.gov/news/press-releases/2022/10/us-uk-joint-statement-new-comprehensive-dialogue-technology-and-data.

34 CPPA Modified Text of Proposed Regulations: § 7002 – Restrictions on the Collection and Use of Personal Information, Section (d) und § 7027 Requests to Limit Use and Disclosure of Sensitive Personal Information, Sections (m) (2), (3), (4), (6) und (7) – abrufbar unter: https://cppa.ca.gov/meetings/materials/20221021_22_item3_modtext.pdf.

35 DoC /DoJ: Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II (September 2020), abrufbar unter: https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF, S. 13, 18.