# Datenschutz in den USA

*Eduardo Isaac Soto Barrera, Jurist (Mexiko), Mag. iur. (Mx), Mag. iur. (D), Hannover*
*Antonia Herfurth, Rechtsanwältin, Hannover und München*

*August 2021*

Die USA sind Heimat der wertvollsten und mächtigsten Technologieunternehmen der Welt. Der Grund, warum diese Unternehmen so erfolgreich sind, ist, dass sie gewaltige Mengen an personenbezogenen Daten ihrer Nutzer sammeln. Die europäische Datenschutzgrundverordnung (*DSGVO*) ist weit bekannt; sie regelt die Verarbeitung personenbezogener Daten. Die US-amerikanischen Datenschutzbestimmungen hingegen sind kaum bekannt. Daher vermittelt dieses Compact einen Überblick über die Datenschutzlandschaft in den USA.

**Gesetzgebung auf Bundesebene**

In den USA gibt es kein umfassendes Bundesdatenschutzgesetz, im Gegensatz zur DSGVO in der EU. Daher gibt es auch keine Regulierungsbehörde, die für die Überwachung des Datenschutzrechts zuständig ist. Die Federal Trade Commission (*FTC*) ist für die Durchsetzung von Datenschutz- und Datensicherheitsanforderungen zuständig, aber in erster Linie eine Wettbewerbsbehörde mit der zusätzlichen Zuständigkeit für Verbraucherschutz. Allerdings existieren Datenschutzvorschriften für einzelne Sektoren wie Wirtschaft und Handel, Gesundheit und Finanzen.

*Gesetzgebung basierend auf der nationalen Sicherheit*

Der USA Freedom Act von 2015 besagt, dass US-Behörden Telekommunikationsdaten nicht speichern dürfen, sondern nur Telekommunikationsanbieter. Behörden dürfen jedoch auf Daten zugreifen, wenn von der betroffenen Person eine potenzielle Gefahr ausgeht. Der Foreign Intelligence Surveillance Act von 1978 (*FISA*) bildet die rechtliche Grundlage für die Datensammlung im Ausland durch US-Geheimdienste. Der FISA legt Voraussetzungen fest, unter denen personenbezogene Daten zur Terrorismusbekämpfung verarbeitet werden dürfen.

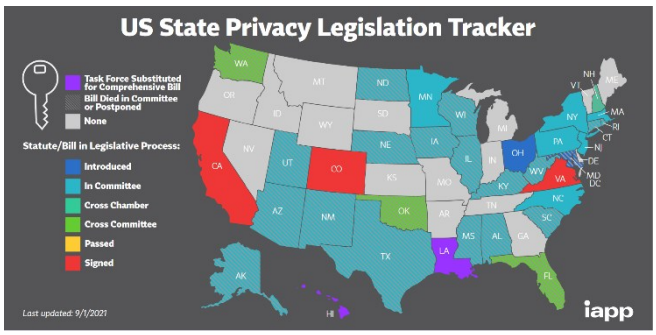
*Gesetzgebung basierend auf Datenschutz*

Der Fair Credit Reporting Act von 1970 (*FCRA*) regelt den Umgang mit Informationen, die von Verbrauchermeldeagenturen wie Kreditbüros, medizinischen Informationsunternehmen und Mieterüberwachungsdiensten gesammelt werden. Der Privacy Act von 1974 schützt personenbezogene Daten, die von Bundesbehörden in Aufzeichnungssystemen gespeichert werden. Das Gesetz legt Regeln für die Verarbeitung von Daten durch die Behörden fest und garantiert Einzelpersonen Rechte wie den Zugang zu ihren Daten und die Berichtigung im Falle von Ungenauigkeiten. Der Electronic Communications Privacy Act von 1986 (*ECPA*) wurde ursprünglich erlassen, um

die Befugnis der US-Regierung zum Abhören von Telefongesprächen zu erweitern. Durch mehrere Änderungen wurden die Befugnisse der Regierung teilweise eingeschränkt, jetzt enthält das Gesetz auch Vorschriften zum Schutz privater elektronischer Kommunikation vor unbefugtem staatlichen Zugriff. Der Computer Fraud and Abuse Act von 1986 legt Regeln zur Cybersicherheit fest, wie z. B. den Schutz vor unbefugtem oder übermäßigem Zugriff auf einen Computer. Die Verarbeitung personenbezogener Gesundheitsdaten wird durch den Health Insurance Portability and Accountability Act von 1996 (*HIPAA*) geregelt. Die Datenschutz- und Sicherheitsanforderungen für Finanzinstitute sind im Gramm-Leach-Bliley Act von 1999 festgelegt. Der Children's Online Privacy Protection Act aus dem Jahr 2000 schützt die Privatsphäre von Kindern, indem er sich auf die Art und Weise konzentriert, wie Betreiber von kommerziellen Websites und Online-Diensten Kinder gezielt adressieren.

**Gesetzgebung auf staatlicher Ebene**

Da kein Bundesdatenschutzgesetz existiert, haben die Staaten eigene Datenschutzgesetze erlassen – bereichsspezifische und umfassende. Hinsichtlich der umfassenden Gesetze befinden sich die Staaten jedoch an unterschiedlichen Punkten der Entwicklung. Während Maine und Nevada zum Beispiel keine Datenschutzgesetze haben, sind sie in New York und North Carolina in Vorbereitung und wurden in Kalifornien, Colorado und Virginia sogar bereits unterzeichnet.




Quelle: https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Map.pdf.

Das Vorbild ist jedoch Kalifornien. Es hat sein Datenschutzgesetz, den California Consumer Privacy Act (*CCPA*), an die DSGVO angelehnt. Mit seinem Inkrafttreten im Januar 2020 führte der CCPA neue Nutzerrechte ein. Die Datenschutzaktivistengruppe *Californians for Consumer Privacy* hielt den CCPA jedoch für nicht streng genug und initiierte daher ein strengeres Gesetz. Der neue California Consumer Privacy Rights Act (*CPRA*) wird am 1. Januar 2023 in Kraft treten und noch strenger sein als die DSGVO.

Dieses Compact betrachtet den CCPA und den CPRA näher, nicht nur, weil sie an der Spitze der US-Datenschutzgesetze stehen, sondern auch, weil Kalifornien das Zentrum der mächtigsten Technologieunternehmen der Welt ist, die erhebliche Datenmengen sammeln. Wenn Unternehmen in den USA tätig sein wollen, können sie die kalifornischen Datenschutzgesetze kaum ignorieren und tendieren daher dazu, diese als Standard zu nehmen.

*Das Vorbild – California Consumer Privacy Act*

Der CCPA ist anwendbar, wenn ein Unternehmen oder eine Organisation in Kalifornien geschäftlich tätig ist; ein „Geschäft“ erfordert eine gewinnorientierte Tätigkeit. Er ist auch anwendbar, wenn ein Unternehmen nicht in Kalifornien ansässig ist, aber personenbezogene Daten von in Kalifornien wohnhaften Verbrauchern sammelt. Das Unternehmen muss nicht nur in Kalifornien geschäftlich tätig sein, sondern entweder im vorangegangenen Kalenderjahr jährliche Bruttoeinnahmen von mehr als $ 25.000.000 erzielt haben *oder* allein oder gemeinsam jährlich personenbezogene Daten von 50.000 oder mehr Verbrauchern, Haushalten oder Geräten zu kommerziellen Zwecken kaufen, empfangen, verkaufen oder weitergeben *oder* 50 % oder mehr von seinen jährlichen Einnahmen aus dem Verkauf personenbezogener Verbraucherdaten erzielen.

Wenn ein Unternehmen unter den CCPA fällt, stellt das Gesetz den Verbrauchern mehrere Rechte zur Verfügung, wie das Recht auf Auskunft darüber, wel-

che personenbezogenen Daten ein Unternehmen gesammelt und schließlich an Dritte weitergegeben hat, und das Recht auf Zugang (Datenübertragbarkeit). Darüber hinaus hat der Einzelne das Recht, den Verkauf personenbezogener Daten an Dritte durch einen Opt-out-Mechanismus zu untersagen, und das Recht, personenbezogene Daten löschen zu lassen.

Unternehmen, die unter den CCPA fallen, müssen bestimmte Anforderungen erfüllen, z.B. müssen sie personenbezogene Daten sicher aufbewahren (Datensicherheit), sie müssen auf ihrer Website zwei Möglichkeiten zur Kontaktaufnahme anbieten und Verbraucheranfragen innerhalb von 45 Tagen beantworten. Außerdem müssen sie die Verbraucher über ihre Online-Datenschutzrichtlinien informieren und auf ihrer Website ein für die Verbraucher leicht erkennbares Opt-out-Tool (*"Do not sell my info"-Button*) einrichten. Der CCPA sieht auch einen besonderen Schutz für Minderjährige vor.

Wichtig ist, dass das Gesetz nur Verbraucher in Kalifornien schützt.

*Ein Schritt weiter – California Consumer Privacy Rights Act*

Durch den CPRA wird der Anwendungsbereich teilweise geändert. Ein Unternehmen fällt unter das Gesetz, wenn es allein oder in Kombination mit anderen Unternehmen jährlich die personenbezogenen Daten von *100.000 oder mehr* Verbrauchern oder Haushalten kauft, verkauft oder weitergibt. Im Vergleich zum CCPA müssen personenbezogene Daten von 100.000 Verbrauchern betroffen sein, nicht mehr nur von 50.000. Das Gesetz erweitert jedoch den Anwendungsbereich, indem es festlegt, dass ein Unternehmen auch dann unter den CPRA fällt, wenn es 50 % oder mehr seiner jährlichen Einnahmen aus dem Verkauf *oder der Weitergabe* personenbezogener Daten von Verbrauchern erzielt. Hier hat der kalifornische Gesetzgeber die Tätigkeit der „Weitergabe" hinzugefügt.

Mit dem CPRA wurde eine Behörde zur Umsetzung und Durchsetzung des Gesetzes eingerichtet, die California Privacy Protection Agency (*CPPA*) – die erste ihrer Art in den USA.

Bereits bestehende Rechte werden geändert und neue Rechte eingeführt, wie das Recht auf Berichtigung unrichtiger personenbezogener Daten oder das Recht auf Einschränkung der Verwendung sensibler personenbezogener Daten. Darüber hinaus kodifiziert der CPRA die Grundsätze der Zweckbindung, der Speicherbegrenzung und der Datenminimierung, die bereits aus der DSGVO bekannt sind.

*DSGVO vs. CCPA vs. CPRA*

In der folgenden Tabelle werden die Bestimmungen der DSGVO, des CCPA und des CPRA verglichen:


Quelle: https://www.linkedin.com/posts/dltsays_ccpa-gdpr-cpra-activity-6606221910663663616-e8vv.

**Datenübermittlung zwischen der EU und den USA**

Die DSGVO ist derzeit eines der strengsten Datenschutzgesetze der Welt und erschwert die Verarbeitung personenbezogener Daten aus der EU in einem Drittland.

*Safe Harbour und Privacy Shield*

In den letzten 20 Jahren war die Übermittlung personenbezogener Daten zwischen der EU und den USA dank des *Safe-Harbour-Abkommens* und des *Privacy Shields* unproblematisch. Beide Abkommen ermöglichten eine sichere und damit freie Übermittlung von Daten. Mit der *Schrems I*-Entscheidung im Jahr 2015 erklärte der Europäische Gerichtshof Safe Harbour jedoch für ungültig. Dessen Nachfolgeregelung, das Privacy Shield, erklärte der Gerichtshof im Jahr 2020 mit der *Schrems II*-Entscheidung für ungültig. Seitdem betrachtet die EU die USA wieder als unsicheres Drittland.

*Aktuelle Lösungen*

Aus Sicht der EU kann die Übermittlung personenbezogener Daten in die USA nur auf Grundlage anderer, von der EU festgelegter, Mechanismen erfolgen: verbindliche interne Datenschutzvorschriften (*BCR)* und Standardvertragsklauseln (*SCC*).

BCRs bilden einen Rahmen für die unternehmensinterne Verarbeitung personenbezogener Daten. Auf der Grundlage ihrer BCRs können internationale Unternehmen personenbezogene Daten weltweit übermitteln, auch wenn der empfangende Teil des Unternehmens in einem unsicheren Drittland ansässig ist.

SCCs sind Standardklauseln, die die – interne und externe – Übermittlung personenbezogener Daten in unsichere Drittländer erlauben. Sie können von der Website der Europäischen Kommission heruntergeladen und frei verwendet werden. Sie dürfen jedoch nicht geändert oder ergänzt werden, sondern müssen in der von der Kommission veröffentlichten Fassung verwendet werden. Da Teile der bestehenden SCCs 30 Jahre alt sind, hat die Kommission am 4. Juni 2021 einen modernisierten Satz herausgegeben.

**Ausblick**

Das US-Datenschutzrecht ist ein Flickenteppich. Anstelle eines umfassenden Bundesdatenschutzgesetzes gibt es zahlreiche bereichspezifische Gesetze auf Bundes- und Staatenebene. Es gibt weder eine eigene Datenschutzbehörde noch eine einheitliche Definition des Begriffs „persönliche Informationen“. Es wird kritisiert, dass einige der bestehenden Gesetze so alt sind, dass sie der aktuellen digitalen Situation nicht mehr gerecht werden und persönliche Informationen nicht wirklich schützen, sondern US-Behörden zahlreiche Schlupflöcher bieten, um doch an Informationen zu gelangen.

Aus diesem Grund wird in den USA bereits seit vielen Jahren ein Bundesdatenschutzgesetz diskutiert. Vor allem große internationale Unternehmen unterstützen die Harmonisierung. Da Kalifornien seinen Datenschutz vorantreibt, ist zu erwarten, dass der Bundesgesetzgeber folgen wird. So wie die EU und die USA an einem neuen Rahmen für die sichere Übermittlung personenbezogener Daten zwischen ihnen arbeiten.

## IMPRESSUM

### HERAUSGEBER

HERFURTH & PARTNER Rechtsanwaltsgesellschaft mbH
Luisenstr. 5, D-30159 Hannover
Fon 0511-30756-0 Fax 0511-30756-10
Mail info@herfurth.de, Web www.herfurth.de

Hannover · Göttingen · Brüssel
Member of the ALLIURIS GROUP, Brussels

### REDAKTION

Leitung: Ulrich Herfurth, Rechtsanwalt, zugelassen in Hannover und Brüssel (verantw.)

Mitarbeit: Angelika Herfurth, Rechtsanwältin, FA Familienrecht; Sibyll Hollunder-Reese, M.B.L. (HSG), Rechtsanwältin; Günter Stuff, Steuerberater; Xiaomei Zhang, Juristin (China), Mag. iur. (D); Thomas Gabriel, Rechtsanwalt; JUDr. Yvona Rampáková, Juristin (CR); Dr. Jona Aravind Dohrmann, Rechtsanwalt; Prof. Dr. jur. Christiane Trüe LL.M. (East Anglia); Dr. jur. Reinhard Pohl, Rechtsanwalt; Konstantin Kuhle, Rechtsanwalt; Antonia Herfurth, Rechtsanwältin; Eduardo Isaac Soto Barrera, Master of Law (Mexiko); Tobias Wundram, Rechtsanwalt; Stephanie Reese, Rechtsanwältin

### KORRESPONDENTEN

u.a. Amsterdam, Athen, Brüssel, Budapest, Helsinki, Istanbul, Kopenhagen, Lissabon, London, Luxemburg, Mailand, Madrid, Moskau, Oslo, Paris, Stockholm, Warschau, Wien, Zug, New York, Toronto, Mexico City, Sao Paulo, Buenos Aires, New Delhi, Peking, Tokio.

### VERLAG

CASTON GmbH, Law & Business Information
Luisenstr. 5, D-30159 Hannover,
Fon 0511 - 30756-50 Fax 0511 - 30756-60
Mail info@caston.info; Web www.caston.info