USA: Neues kalifornisches Datenschutzgesetz CCPA als Vorreiter

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

Wie kürzlich berichtet (ZD-Aktuell 2018, 06156), wurde für den Bundestaat Kalifornien im November im Rahmen der allgemeinen Wahlen für November eine Volksbefragung (ballot initiative) angesetzt, um ein neues Datenschutzgesetz auf den Weg zu bringen. Diese Volksbefragung hätte einschneidende Änderungen und Dokumentationspflichten für in Kalifornien tätige Unternehmen mit sich gebracht. Auch Unternehmen, die ihren Sitz nicht in Kalifornien haben, sind betroffen. Als Reaktion hat das Parlament am 27.6.2018 kurz vor Ablauf der Rücknahmefrist für die Volksbefragung den California Consumer Privacy Act (CCPA) verabschiedet, der weniger belastend für die Industrie ist und Rechtssicherheit schaffen soll. Die International Association of Privacy Professionals (IAPP) schätzt, dass allein in den USA mehr als 500.000 große und kleine Unternehmen vom CCPA betroffen sind.

Der Gouverneur von Kalifornien, *Jerry Brown,* unterzeichnete das Gesetz, das manche als „Mini-DS-GVO" bezeichnen, noch am selben Tage. Trotz seiner gegenüber der Volksbefragung zu Gunsten der Industrie abgemilderten Vorschriften wird der CCPA zu einschneidenden Maßnahmen und Compliance-Aktivitäten bei Unternehmen zu Gunsten von Verbraucherrechten führen, die sich durchaus mit der DS-GVO in manchen Bereichen messen können. Viele Unternehmen mit Geschäftsaktivitäten in Kalifornien müssen deshalb sehr bald ihre Praktiken neu bewerten und ihre Geschäftsprozesse bis zum 1.1.2020 als Stichtag anpassen.

1. Wer muss sich an den CCPA halten?

Das Gesetz enthält hierfür drei kumulative Kriterien. Der CCPA gilt für:

- jede gemeinnützige Organisation oder juristische Person, die in Kalifornien geschäftlich tätig ist (ohne dass es auf den Sitz des Unternehmens ankommt) und
- die von Verbrauchern personenbezogene Informationen (s.u.), entweder direkt oder durch einen Dritten in ihrem Auftrag, sammelt und
- die allein oder gemeinsam mit anderen die Zwecke der Verarbeitung dieser personenbezogenen Informationen bestimmt.

Für diese Adressaten des CCPA gelten folgende drei Schwellenwerte:

- Das Unternehmen hat einen jährlichen Bruttoumsatz von mehr als US-$ 25 Mio. oder
- das Unternehmen kauft jährlich, erhält, verkauft oder übermittelt für kommerzielle Zwecke personenbezogene Informationen von zusammengerechnet 50.000 oder mehr Verbrauchern, Haushalten oder Geräten oder
- das Unternehmen generiert mindestens 50 % seiner jährlichen Einnahmen aus dem Verkauf von personenbezogenen Informationen von Verbrauchern.

Der CCPA beschränkt sich nicht auf die Daten von Unternehmen, die elektronisch oder über das Internet gesammelt werden, und gilt daher wie die DS-GVO für eine Vielzahl von Unternehmen, die keine Online-Präsenz haben.

2. Was sind „personenbezogene Informationen" (PI)?

Die CCPA-Definition von personenbezogenen Informationen (PI) ist wie schon in der Volksbefragung breiter angelegt als z.B. die Definition in dem bestehenden Gesetz in Kalifornien über den Bruch der Datensicherheit (Kalifornisches Gesetzbuch Abschnitt 1798.82). Die Definition schließt alle Informationen ein, die „einen Verbraucher oder Haushalt bezeichnen, sich darauf beziehen, verweisen, in der Lage sind [dem Verbraucher oder Haushalt] zugeordnet zu werden oder vernünftigerweise direkt oder indirekt mit einem bestimmten Verbraucher oder Haushalt verknüpft werden können." Diese Einzelheiten sind in einer nicht abschließend gemeinten Liste von elf Datenkategorien (Namen, (IP-)-Adressen, Standortdaten usw.) aufgeführt. Ausdrücklich ausgeschlossen von dieser Definition ist jede „aggregierte Verbraucherinformation", die definiert ist als

- Daten, die „nicht mit einem Verbraucher oder Haushalt, unter anderem über ein Gerät verbunden sind oder vernünftigerweise verknüpfbar sind" sowie
- alle „öffentlich zugänglichen Informationen von Bund, Bundesstaat oder lokaler Regierung."

Diese Definition reicht weit über die herkömmlichen Definitionen von personenbezogenen in den USA hinaus und deckt u.a. den Bereich der Social Media ab. Problematisch ist, dass der Begriff „Haushalt" nirgendwo im Gesetz definiert ist.

3. Welche Rechte hat der Verbraucher in Kalifornien nach dem CCPA?

Der CCPA eröffnet den Verbrauchern in Kalifornien neue, aus der DS-GVO schon bekannte Wege, um ihre PI zu schützen, ihre Weitergabe zu kontrollieren und Auskunft zu verlangen. Zu nennen sind folgende Rechte:

- **Recht, die Kategorien von Informationen zu erfahren**, die ein Unternehmen über den Verbraucher sammelt, verkauft, erhebt, verarbeitet oder und an wen diese Informationen verkauft oder weitergegeben werden, sowie das Recht, diesen Verkauf oder diese Weitergabe von PI des Verbrauchers zu verhindern.
- **Recht auf eine Kopie** „spezifischer Teile" von PI über den Verbraucher, die das Unternehmen gesammelt hat, die kostenlos innerhalb von 45 Tagen per Post oder elektronisch zur Verfügung gestellt werden müssen.
- **Recht auf Vergessen-Werden** beinhaltet, dass ein Unternehmen die PI löschen muss (und einen Drittanbieter mit Datenzugang entsprechend anweisen muss).
- **Recht auf ein Opt-out** vor Verhinderung eines Verkaufs von personenbezogenen Informationen an Dritte, wobei das Unternehmen an einen „klaren und deutlichen" Link mit dem aussagekräftigen Titel „Do Not sell my Personal Information" auf der Homepage des Unternehmens posten muss.
- **Recht auf Nicht-Diskriminierung** von Verbrauchern, die ihre Rechte unter dem CCPA gegenüber einem Unternehmen ausüben.

Der CCPA gibt den betroffenen kalifornischen Verbrauchern das Recht, bis zu zweimal in jedem 12-Monatszeitraum die „spezifischen Teile" der PI, die ein Unternehmen bezüglich dieser Person gesammelt hat, sowie die Kategorien von PI, die dort gesammelt wurden, ähnlich wie in Art. 15 DS-GVO anzufordern. Nur verifizierbare Anfragen müssen bearbeitet werden. Wenn die PI in einem gängigen elektronischen Format bereitgestellt werden, müssen sie portierbar sein und, ähnlich wie nach der DS-GVO, soweit technisch machbar, in einem leicht verwendbaren Format bereitgestellt werden, das es dem Verbraucher ermöglicht, diese Informationen ungehindert an ein anderes Unternehmen weiterzugeben. Das Gesetz gibt keine klare Aussage darüber, ob Unternehmen jeden einzelnen Fall offenlegen müssen, in dem personenbezogene Daten erscheinen, oder ob eine allgemeine Auflistung, die doppelte Quellen ausschließt, ausreicht.

Das genannte Recht auf Vergessen-Werden sollte im Vergleich mit der einschlägigen DS-GVO-Vorschrift nicht überbewertet werden, da der CCPA neun Ausnahmen enthält, darunter die Verarbeitung für interne Zwecke, „die den Erwartungen des Verbrauchers angemessen entsprechen" oder die „in rechtmäßiger Weise mit dem Kontext in Einklang stehen, in dem die Informationen bereitgestellt wurden." Die betroffenen Unternehmen werden sich wahrscheinlich hierauf berufen.

Die Unternehmen können personenbezogene Daten an Dritte oder Dienstleister für geschäftliche Zwecke weitergeben, soweit und solange es ein schriftlicher Vertrag solchen Parteien untersagt, PI zu verkaufen oder für nicht vom Vertrag abgedeckte Zwecke zu nutzen. Darüber hinaus verbietet der CCPA eine Vereinbarung oder Bestimmung, die die Rechte des Verbrauchers gemäß dem CCPA beschränkt oder aufhebt, einschließlich das Recht auf Rechtsmittel zur Durchsetzung, Schiedsverfahren und Sammelklage mit Bezug auf die CCPA-Rechte.

4. Welche Informationen muss eine Datenschutzerklärung nach dem CCPA mindestens beinhalten?

Die betroffenen Unternehmen müssen – entweder auf ihren Websites oder anderweitig schriftlich – bestimmte Informationen über ihre Praktiken bei der Sammlung von Verbraucherdaten offenlegen und die Informationen mindestens einmal jährlich aktualisieren. Trotz aller auch in Europa geäußerter genereller Kritik, dass die bis dato bestehenden Datenschutzerklärungen zu ausführlich seien und selten gelesen werden, verlangt der CCPA, dass diese Privacy Policies noch mehr Details als bisher enthalten müssen. Abzudecken sind folgende Informationen:

- Eine Beschreibung der Verbraucherrechte nach dem CCPA.
- Instruktionen, wie ein Verbraucher Zugriffsanfragen an das Unternehmen senden kann.
- Die Kategorien von PI, die das Unternehmen in den vorangegangenen 12 Monaten über den Verbraucher gesammelt hat und sammeln wird.
- Listen mit den Kategorien der PI, die das Unternehmen in den vorangegangenen 12 Monaten für geschäftliche Zwecke verkauft oder veröffentlicht hat (oder ein Statement, dass das Unternehmen diese Information nicht verkauft oder offengelegt hat).

5. Welche Opt-out-Rechte hat der Verbraucher?

Der CCPA ist ein Opt-out-Gesetz. Verbraucher können den „Verkauf" ihrer PI an eine dritte Partei ablehnen, und wenn sie dies tun, ist ein Unternehmen für mind. 12 Monate daran gehindert, diese Verbraucher zu bitten, ihr Opt-out zurückzuziehen. Der Begriff „Verkauf" ist weit definiert als

„Verkauf, Vermietung, Freigabe, Offenlegung, Verbreitung, Bereitstellung, Übertragung oder anderweitige mündliche, schriftliche oder elektronische oder anderweitige Übermittlung der persönlichen Daten eines Verbrauchers durch das Unternehmen an ein anderes Unternehmen oder eine dritte Partei für Geld oder andere vermögenswerte Gegenleistung." Kein Opt-out-Recht gibt es für die Weitergabe personenbezogener Daten an Dienstleister, welche die Informationen benötigen und denen vertraglich untersagt ist, diese für ihre eigenen Zwecke zu verwenden.

6. Welche Neuerungen gibt es bei Datenpannen?

Der CCPA schafft ein individuelles Klagerecht für den Verbraucher und gesetzlichen Schadensersatz, wenn es zu einem Bruch der Datensicherheit kommt und seine PI betroffen sind. Dies wird voraussichtlich zu einer Zunahme der Privacy-Rechtsstreitigkeiten in Kalifornien führen. Der Verbraucher kann eine Zivilklage erheben, wenn ein Unternehmens gegen die Pflicht zu angemessenen Sicherheitsmaßnahmen verstoßen hat. In diesen Fällen kann der Verbraucher folgende Beträge einklagen: entweder den gesetzlichen Schadensersatz i. R. v. US-$ 100,- bis US-$ 750,- pro Verbraucher und Vorfall oder den tatsächlichen Schaden, wenn dieser nachweisbar höher ist. Ein Unterlassungsanspruch und anderer gerichtlich angeordneter einstweiliger Rechtsschutz stehen auch zur Verfügung. Vor Klageerhebung eine Zivilklage nach dem CCPA muss der Verbraucher das Unternehmen mit einer „ausdrücklichen schriftlichen Erklärung" abmahnen und ihm 30 Tage Zeit zur Abhilfe gewähren. Dafür ist eine „ausdrückliche schriftliche [Abhilfe-] Erklärung" des Unternehmens erforderlich. Wenn ein betroffenes Unternehmen unter Verstoß gegen die ausdrückliche schriftliche Erklärung weiterhin das Rechts verletzt, kann der Verbraucher auch rückwirkend den gesetzlichen Schadensersatz für jeden Verstoß einklagen.

Jeder Kläger nach dem CCPA muss innerhalb von 30 Tagen nach Einreichung der Klage das kalifornische Justizministerium davon benachrichtigen. Das kalifornische Justizministerium kann dann eigene Maßnahmen zur Verfolgung der Verletzung ergreifen.

7. Welche Ausnahmen vom CCPA gibt es?

Obwohl der CCPA an sich ähnlich wie die DS-GVO sehr viele Bereiche abdeckt, enthält das Gesetz einige wichtige Ausnahmen. Bundes-, Staats- oder lokale Gesetze dürfen nicht verletzt werden. Den Anordnungen im Rahmen einer Straf- oder behördlichen Ermittlung, Vorladung oder Dokumentenvorlage muss das Unternehmen weiter nachkommen. Die Datennutzung zur Verteidigung eigener Rechtsansprüche ist weiter erlaubt. Unbeschränkt durch das Gesetz ist die Datenverarbeitung auch für die Zusammenarbeit mit Strafverfolgungsbehörden und für die Ausübung oder Verteidigung rechtlicher Ansprüche. CCPA gilt ebenfalls nicht für Gesundheitsinformationen, die nach dem California Confidentiality of Medical Information Act und dem Bundesgesetz Health Insurance Portability and Availabilty Act (HIPAA) geregelt sind. Im Finanzbereich gilt der CCPA nicht für Daten, die nach dem Gramm-Leach-Bliley Act (GLBA) und seinen Ausführungsvorschriften verarbeitet werden, allerdings nur insoweit, als Widersprüche zwischen dem GLBA und CCPA bestehen. Ist das nicht der Fall, müssen sich die Unternehmen im Finanzbereich an den CCPA halten.

8. Wie sollten sich Unternehmen auf den CCPA vorbereiten?

Mit dem CCPA ist der Gesetzgeber der o.g. Volksbefragung (ballot initiative) quasi in letzter Minute zuvorgekommen. Unternehmen in Europa sollten wissen, dass das Gesetz nicht nur für

Unternehmen gilt, die ihren Sitz in Kalifornien haben. Damit hat der CCPA allein angesichts der Größe und Bedeutung dieses Bundesstaats Ausstrahlungswirkung weit über die Grenzen von Kalifornien hinaus. Da die Besucher einer Website zum genannten Schwellenwert der Verbraucher, Haushalte oder Geräte beitragen, wird die Schwelle von 50.000 wahrscheinlich auch für kleine Unternehmen leicht erreicht, vor allem, wenn ein Verbraucher mehrere Endgeräte hat.

Die Planung für die Einhaltung des CCPA erfordert einen erheblichen Zeit- und Ressourceneinsatz, ähnlich wie bei der DS-GVO. Die Bemühungen von Organisationen, die sich auf die Einhaltung der DS-GVO vorbereitet haben, werden sich im Hinblick auf die Vorbereitung zur Einhaltung des CCPA auszahlen, allerdings zusätzliche Arbeit erforderlich machen. Die Anforderungen des CCPA unterscheiden sich in vielen wichtigen Punkten von der DS-GVO und machen zusätzliche Prozesse und Mechanismen notwendig. Als nächste Schritte möglichst bald vor dem Erreichen des Stichtags zum 1.1.2020 werden die Unternehmen einige interne und externe Maßnahmen implementieren müssen, wie etwa folgende Prozesse und Leitlinien für:

- erforderliche CCPA-Benachrichtigungen und Mechanismen für die Opt-out- Rechte,
- das Recht, Vergessen zu werden nach dem CCPA,
- den Zugang der Betroffenen zu ihren Verbraucherdaten auf Anfrage in einem „leicht verwendbaren Format"
- Vereinbarungen mit Dienstleistern, damit auch diese CCPA-konform sind, sowie
- interne Schulungsmaßnahmen.

Auch Unternehmen, die sich derzeit an die bestehenden kalifornischen Datenschutzgesetze wie den California Online Protection Act halten, werden mit erheblichen Compliance-Aufwand konfrontiert werden. Während die Nutzung eines Incident-Response-Plans für den Bruch der Datensicherheit schon seit einiger Zeit für Kalifornien „Best Practice" ist, unterstreichen die neuen gesetzlichen Schäden und zivilrechtlichen Strafen des CCPA die Notwendigkeit eines durchdachten und umfassenden Ansatzes, um die Risiken eines Bruchs der Datensicherheit in den Griff zu bekommen, auch wenn es in Kalifornien keine Datenschutzbehörde i. S. d. DS-GVO gibt. Angesichts des hektischen Aktivismus, mit dem der CCPA vom Gesetzgeber gegen die laufende Uhr der Volksbefragung in knapp einer Woche verabschiedet worden ist und der schon jetzt festgestellten redaktionellen Fehler im Gesetz ist es sehr wahrscheinlich, dass einige Änderungen am CCPA vor dem 1.1.2020 vorgenommen werden müssen.