USA: California Consumer Privacy Act (CCPA) steht zur Abstimmung

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

Während sich die Unternehmen in der EU und viele US-Unternehmen mit Geschäftsaktivitäten in Europa auf die Einhaltung der Datenschutzbestimmungen der DS-GVO konzentrieren, werden die Kalifornier bald die Möglichkeit bekommen, für ein umfassendes Datenschutzrecht zu votieren, das viele DS-GVO-Prinzipen (z. B. Auskunftsrechte) widerspiegelt. Kalifornien ist seit langem der Trendsetter für „Privacy"-Gesetze in den USA.

Am 3.5.2018 gaben Befürworter des California Consumer Privacy Act (CCPA) bekannt, dass sie die erforderlichen Unterschriften gesammelt haben, um über die Gesetzesmaßnahme am 6.11.2018 zusammen mit einer Volksabstimmung abzustimmen.

Mit dem Wahlzettel verbundene Volksabstimmungen am Wahltag (ballot initiatives) sind in Kalifornien und anderen US-Bundesstaaten häufig. Die Gesetzesmaßnahme hat fast doppelt so viele Unterschriften (über 600.000) auf sich vereint als erforderlich sind. Dies legt nahe, dass die Wähler bei den Wahlen im November 2018 für den CCPA votieren werden.

1. Annäherung an die DS-GVO

Der CCPA enthält viele aus der DS-GVO bekannte Prinzipen. Das Gesetz wird den Verbrauchern in Kalifornien das Recht geben, auf Anfrage ähnlich wie nach Art. 15 DS-GVO über Datensammlungen informiert zu werden, die ein vom Gesetz abgedecktes Unternehmen über sie sammelt, verkauft oder offenlegt. Die Unternehmen müssen dem Konsumenten auf Anfrage auch mitteilen, an wen die Informationen verkauft oder weitergegeben wurden. Die Verbraucher erhalten auch das Recht, den Verkauf oder die Offenlegung ihrer persönlichen Informationen (PI) zu verhindern (Opt-out).

Das Gesetz wird für alle Unternehmen gelten, die in Kalifornien Geschäfte tätigen (auch ausländische Unternehmen), wenn sie einen der folgenden Schwellenwerte erreichen:

- jährliche Brutto-Umsätze von mehr als US$ 50 Mio;
- jährliche Verkäufe von persönlichen Informationen von Datensätzen von über mehr als 120.000 Verbrauchern oder Geräten mit PI, sowie
- 50% oder mehr der jährlichen Einnahmen werden aus dem Verkauf von solchen PI erzielt.

Bemerkenswert ist, dass die Definition des CCPA von persönlichen Informationen (PI) viel umfassender ist als die Definition von „persönlichen Informationen" gemäß dem geltenden kalifornischen Gesetz zur Meldung bei Bruch der Datensicherheit (Kalifornisches Zivilgesetzbuch § 1798.82). Die CCPA-Definition deckt alle Informationen ab, die Verbraucher „identifizieren, sich auf sie beziehen, beschreiben [oder] die mit einem bestimmten Verbraucher oder Gerät vernünftigerweise direkt oder indirekt in Verbindung gebracht werden können." Die weitere Definition umfasst 12 Mindestkategorien von Informationen über Verbraucher und minderjährige Kinder des Verbrauchers. Während einige der aufgezählten Kategorien nicht überraschend sind (Name, Adresse, E-Mail-Adresse und Sozialversicherungsnummer oder Führerscheinnummer), sprengt die Definition von PI den in den USA üblichen Standard und geht in mancher Hinsicht über die Definition in Art. 4 Abs. 1 DS-GVO hinaus. Zu PI gehören z.B. kommerzielle Informationen, die

Produkte oder Dienstleistungen umfassen, die bereitgestellt, erhalten oder in Betracht gezogen werden, sowie Daten über Kauf- oder Konsumgewohnheiten oder -tendenzen und biometrische Daten, Browser-/Suchverlauf, Geolokalisierung und alle hieraus gezogenen Schlussfolgerungen auf Grund solcher Informationen. Aus dem Gesetzeswortlaut ist nicht klar ersichtlich, welcher Personenbezug vorliegen muss.

2. Datenschutzverletzungen und CCPA-Durchsetzung

Der neue CCPA sieht vor, dass die vom Gesetz umfassten Unternehmen zivilen Strafen (civil penalites) unterliegen, wenn sie von einem Bruch der Datensicherheit betroffen sind (§ 1798.82 (g) des Kalifornischen Zivilgesetzbuches), soweit die in § 1798.82 (h) aufgelisteten persönlichen Informationen der Verbraucher davon berührt sind. Die Sanktionen beziehen sich auf das Versäumnis eines Unternehmens, angemessene Sicherheitsverfahren und -praktiken einzuführen und aufrechtzuerhalten, und zwar unabhängig davon, ob der Verbraucher tatsächlich einen Geld- oder Vermögensverlust infolge des Verstoßes erlitten hat.

Ein Verbraucher in Kalifornien wird künftig in der Lage sein, eigene rechtliche Schritte gegen ein Unternehmen einzuleiten, das gegen den CCPA verstößt – wenn es die oben genannten Datenschutzrechte des Verbrauchers missachtet oder ein Bruch der Datensicherheit durch die Nichtumsetzung angemessener Sicherheitsmaßnahmen gemäß den Kalifornischen Gesetzen erfolgt (§ 1798.82). Ein CCPA-Verstoß führt in diesen Fällen dann zu einem gesetzlichen Schadensersatz, unabhängig davon, ob dem Verbraucher tatsächlich ein Geld- oder Sachverlust entstanden ist. Der CCPA bemisst den gesetzlichen Schadensersatz i.H.v. US$ 1.000,- oder den tatsächlichen Schaden für jede Verletzung durch ein Unternehmen. Bei Kenntnis oder vorsätzlichen Verletzungen liegt der gesetzliche Schaden zwischen US$ 1.000,- und US$ 3.000,- oder der tatsächliche Schaden, je nachdem, welcher höher ist, für jeden Verstoß des Unternehmens.

Unternehmen, die gegen die Vorschriften den neuen CCPA verstoßen, können auch durch Zivilklagen belangt werden, die vom kalifornischen *Generalstaatsanwalt* oder lokalen Staatsanwälten, wie z.B. Bezirksstaatsanwälten, eingeleitet werden. Die Maßnahme sieht zivilrechtliche Strafen von bis zu US$ 7.500,- pro Verstoß für vorsätzliche Verletzungen vor. Darüber hinaus kann jeder Hinweisgeber (Whistleblower) mit nicht-öffentlichen Informationen, dass ein Unternehmen die Maßnahme verletzt hat, mit seinen Informationen veranlassen, dass der *Generalstaatsanwalt* eine Zivilklage einreicht. Wenn der *Generalstaatsanwalt* dies ablehnt, kann der Whistleblower anstelle des *Generalstaatsanwalts* Zivilklage erheben.

3. Weiter Widerstand gegen den CCPA aus der Industrie

Der CCPA wird von vielen Technologieunternehmen, TK-Unternehmen, Banken, Kreditgenossenschaften und der Automobilindustrie sowie von einer Reihe von Handelsverbänden wie der *California Bankers Association*, dem *California Community Banking Network*, der *California Credit Union*, der *California New Car Dealers Association*, der *Allianz der Automobilhersteller, Inc*. und der *Handelskammer* abgelehnt. Die Gegner kritisieren, wie erwartet, den Gesetzesvorschlag als zu weitreichend und zu teuer, da er praktisch alle Informationen umfasse, die ein Unternehmen über einen Verbraucher verarbeite und über fast alle Branchen und Geschäftspraktiken hinweg Anwendung finde. Der CCPA sieht Ausnahmen für den Gesundheitsbereich (HIPAA) und die dort tätigen Unternehmen und die einschlägigen Consumer Reporting Agencies vor. Davon abgesehen gilt er für alle Branchen.

4. Compliance-Maßnahmen schon bald erforderlich

Wenn der CCPA verabschiedet wird, wird das Gesetz wahrscheinlich zu erheblichen Compliance-Herausforderungen in der Industrie führen und die Belastungen und Kosten sowie das Risiko von Rechtsstreitigkeiten erheblich erhöhen. Insbesondere müssen die betroffenen Unternehmen ähnlich wie nach der DS-GVO bestimme Informationen offenlegen und erklären, was sie speichern und welche PI der Verbraucher sie weitergeben, die dann für US-Sammelklagen genutzt werden könnten. Unternehmen, die in Kalifornien Geschäfte machen, müssen dann entweder einen separaten internen Prozess für den Umgang mit den persönlichen Daten der Bewohner des Staats einrichten, die etwa 12% der US-Bevölkerung ausmachen, oder den kalifornischen Standard landesweit anwenden. Der CCPA tritt nach der Volksabstimmung bei Annahme der „ballot intiative" am 7.11.2018, dem Tag nach der Wahl, in Kraft. Das Gesetz sieht eine Übergangsfrist von neun Monaten vor und wird nur für personenbezogene Daten gelten, die am oder nach dem 7.8.2019 gesammelt werden, also nicht rückwirkend.

Eine Komponente des CCPA, die am 7.11.2018 allerdings sofort wirksam wird, ist der genannte neue Haftungsstandard, der Durchsetzungsprozess und der gesetzliche Schadensersatz bei einem Bruch der Datensicherheit. Während die Implementierung eines intern getesteten Incident-Response-Plans schon seit einiger Zeit eine „Best Practice" ist, unterstreicht der CCPA die Notwendigkeit eines durchdachten und umfassenden Ansatzes für die Verletzung von Maßnahmen, da das Gesetz höchstwahrscheinlich zu einem Anstieg der Rechtsstreitigkeiten bei einem Bruch der Datensicherheit führen wird.

Fest steht schon jetzt: Die Planung der Einhaltung erfordert IT- und rechtliche Ressourcen und eine sorgfältige Prüfung der Optionen – durchaus vergleichbar mit dem Aufwand für die DS-GVO. Angesichts des breiten Informationsumfangs, der durch das Gesetz abgedeckt wird, ist es unwahrscheinlich, dass Unternehmen die Sammlung, den Verkauf und die Offenlegung von persönlichen Informationen derzeit in der erforderlichen umfassenden Weise dokumentiert haben. Unternehmen mit Geschäft in Kalifornien sollten deshalb schon jetzt darüber nachdenken, wie sie Informationen über den Verkauf oder die Weitergabe von persönlichen Verbraucherinformationen an Dritte organisieren, um die erforderlichen CCPA-Benachrichtigungen und Opt-out-Rechte bereitzustellen. Unternehmen, die derzeit den kalifornischen Privacy-Gesetzen wie dem Online Privacy Protection Act leidlich nachkommen, müssen möglicherweise neue CCPA-Regeln und Verfahrensschritte und Richtlinien über die nach gegenwärtigem Recht bestehenden verbraucherbezogenen Datenschutzhinweise hinaus entwickeln.

Weiterführende Links

Vgl. auch ZD 2018, 76; *Metz/Spittka*, ZD 2017, 361; *Spies*, ZD-Aktuell 2018, 04291und *Revolidis*, ZD-Aktuell 2017, 05598.