Für Artikel siehe unten

THOMAS HOEREN / STEFAN PINELLI

Das neue kalifornische Datenschutzrecht am Maßstab der DS-GVO

Auswirkungen des CCPA auf global agierende europäische Unternehmen

Informationspflichten

Zum 1.1.2020 wird das Datenschutzrecht des US-Bundesstaats Kalifornien grundlegend geändert. Zu diesem Zeitpunkt tritt der California Consumer Privacy Act von 2018 (CCPA) in Kraft, verbunden mit weitreichenden Pflichten für Unternehmen im Umgang mit personenbezogenen Daten. Der Beitrag stellt diese neue Regelung kurz dar. Im Weiteren wird der neue Rechtsstand in Kalifornien umrissen, mit dem Leitbild der Datenschutzgrundverordnung (DS-GVO) verglichen und ein kurzer Ausblick auf die Auswirkungen des CCPA auf global agierende Unternehmen mit Sitz oder einer Niederlassung in der EU gegeben. Lesedauer: 23 Minuten

I. Geschichte

Kalifornien ist seit jeher ein vom Datenschutz geprägter Bundesstaat. So ist in der kalifornischen Verfassung ein unentziehbares Grundrecht auf den Schutz der Privatsphäre verankert (Privacy).[1] I.Ü. hatte Kalifornien auch bedingt durch diesen Verfassungsauftrag immer schon diverse Regelungen zum Persönlichkeitsrecht, soweit es personenbezogene Daten betraf.[2] Im Kern ging es dabei jedoch stets mehr um den Schutz der individuellen Privatsphäre der Bürger als um den Schutz von Daten.[3]

Das neue Gesetz kam nunmehr durch eine Initiative der kalifornischen Bürger zu Stande. Diese wollten neue Datenschutzregeln im Wege eines Volksentscheids, vor allem aus Angst um die Bedrohung der Persönlichkeitsrechte im Nachgang zu dem, auch in den USA als in seinen Folgen dramatisch eingeschätzten Facebook-Skandal. Das dazu notwendige Bürgerbegehren hatten bereits 600.000 Einwohner unterzeichnet.[4] Um einem Gesetz kraft Volksabstimmung zuvorzukommen, verabschiedeten die Parlamentarier sehr schnell erste Entwürfe und brachten das Gesetzgebungsverfahren zügig zum Abschluss.[5] Sowohl Demokraten als auch Republikaner unterstützten das Gesetz.[6] Dadurch war der Gesetzgeber in der Lage, wieder die Handlungs- und damit auch die Gestaltungshoheit über das Gesetzgebungsverfahren zu gewinnen; die Verbraucherschutzverbände waren ihrerseits froh, auf diese Art vom Gesetzgeber die Bestätigung für die Berechtigung ihrer Forderungen zu erhalten. Binnen sieben Tagen wurde ein umfangreiches Gesetz, das kompliziert und qualitativ in Teilen überarbeitungsfähig entworfen wurde, durch das Parlament „gejagt". Außerdem hat man in weiten Teilen – und insofern einem Prinzip der DS-GVO folgend – wichtige Fragen delegiert, hier auf den „Attorney General"[7]. Die Entwürfe der Verbraucherverbände waren deutlich strenger als das Gesetz. So sollten ursprünglich die Unternehmen gezwungen werden, die Identität, insbesondere den Namen und die Kontaktdaten von dritten Unternehmen, offenzulegen, die Nutzerdaten, z.B. von *Facebook*, in 2017 gekauft hatten.[8] In der verabschiedeten Fassung des Gesetzes müssen die Unternehmen nunmehr nur die Kategorien der dritten Unternehmen mitteilen. Das Gesetz stand auch schon in seiner Vorfassung, die zur Volksabstimmung vorlag, unter kritischer Begutachtung der Technologieunternehmen und Banken. Diese kritisierten den Gesetzesentwurf als zu weitreichend und zu teuer, da das Gesetz zu kostspieligen Compliance-Maßnahmen und Dokumentationspflichten führe.

II. Systematik des CCPA

Der California Consumer Privacy Act (CCPA)[9] ist in verschiedene Sektionen unterteilt. Section 2 gibt die Erwägungsgründe des Gesetzgebers in amtlicher Form wieder. Section 3 enthält das eigentliche Gesetz, das dem Civil Code hinzugefügt wird, wobei die Pflichten und Rechte im Vordergrund stehen (Section 1798.100 bis 1798.135 CCPA). Die langen Gesetzesdefinitionen finden sich in Section 1798.140 CCPA wieder. Unklar ist, worauf sich diese Definitionen beziehen: nur auf die zuvor eingeführten Rechte oder auch auf die nach dem Definitionsteil eingeführten Strafen. Ausnahmebestimmungen finden sich zentral in Section 1798.145 CCPA, bevor das Gesetz mit umfangreichen Sanktionen schließt (Section 1798.150 und 1798.155 CCPA).

III. Geschützte Daten

1. Der Begriff der Einwohner

Nach dem Gesetz sind alle Einwohner von Kalifornien geschützt. Der Schutz gilt nicht nur für Verbraucher, sondern auch für jeden Kalifornier in seiner Rolle als Patient, Mieter, Student oder Teil der Familie.[10] Das Erfordernis des kalifornischen Wohnsitzes aus Section 1798.140 (g) CCPA wird in Titel 18, Section 17014 des California Code of Regulations definiert. Danach erfasst der Begriff „Residenz" jedes Individuum, das sich in dem Staat für einen mehr als zeitweiligen oder vorübergehenden Zweck aufhält, sowie jedes Individuum, das seinen Wohnsitz im Staat hat und diesen nur aus vorübergehenden oder zeitweiligen Gründen verlässt.

Umgekehrt ist das Gesetz nicht anwendbar, wenn der gesamte Bereich der Geschäftsaktivitäten in Zusammenhang mit kalifornischen Einwohnern ausgeschlossen ist. Für weltweit tätige Konzerne kann jedenfalls nicht von vorneherein ausgeschlossen werden, dass sich ihre Geschäftsaktivitäten gleichfalls auf Kalifornier beziehen. Von daher ist das Gesetz auch für weltweit operierende Konzerne einschlägig.

2. Verbraucher

Das Gesetz ist insoweit irreführend, als es durchgängig von Verbrauchern oder Konsumenten spricht (z.B. in Section 1798.100 CCPA). Allerdings ist der Begriff „Konsument" legaldefiniert in Section 1798.140 (g) CCPA und umfasst jede natürliche Person, die Einwohner von Kalifornien ist. Der Anwendungsbereich geht daher weit über den Konsumentenschutz hinaus und meint jede Kommunikation bezogen auf eine natürliche Person. Dementsprechend gibt die Gesetzesbegründung in Section 2 an, dass Personen auch hinsichtlich der Information zum Wohnort oder zum Fahrverhalten, Schlafverhalten, biometrischen oder Gesundheitsinformationen u.Ä. geschützt sind. Insofern umfasst das Gesetz nach der Legaldefinition in Section 1798.140 (o) (1) (A) CCPA auch IP-Adressen, E-Mail-Adressen, Sozialversicherungsnummern oder die Nummer des Führerscheins. Der Personenbezug ist sehr weit formuliert (Section 1798.140 (o) (1) CCPA) als jede Information, die geeignet ist, mit einem Konsumenten oder Haushalt (dazu weiter unten) in Verbindung gebracht zu werden. Umgekehrt sind akkreditierte, anonymisierte Daten ausgenommen (Section 1798.145 (a) (5) CCPA).

3. Persönliche Informationen und Haushalte

Fraglich ist, wie weit das Erfordernis der persönlichen Information auszulegen ist. Die Gesetzeslage ist alles andere als klar. Im Abschnitt zu den Legaldefinitionen (Section 1798.140 CCPA)

---

1 Art. I Section 1 California Constitution, abrufbar unter: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CONS&division=&title=&part=&chapter=&article=I.

2 S. dazu die gute Übersicht von Senatorin *Jackson, Hannah-Beth* im Senate Judiciary Committee, abrufbar unter: https://digitalcommons.law.scu.edu/historical/1748/.

3 Vgl. *Schwartz, Paul M.*, Preemption and Privacy, 118 Yale L.J., 2009, S. 908 ff.

4 *Wakabayashi, Daisuke*, California Passes Sweeping Law to Protect Online Privacy, abrufbar unter: https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html; s.a. *Spies*, ZD-Aktuell 2018, 06156.

5 *Kramer Levin Naftalis & Frankel LLP*, United States: The California Consumer Privacy Act Of 2018: Summary And Comparison To GDPR, abrufbar unter: http://www.mondaq.com/unitedstates/x/724858/Dodd-Frank+Wall+Street+Reform+Consumer+Protection+Act/The+California+Consumer+Privacy+Act+of+2018+Summary+and+Comparison+to+GDPR; s.a. https://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml?bill_id=201720180AB375.

6 S. dazu: https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html; https://twitter.com/AsmEdChau/status/1012421315507073025?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1012421315507073025&ref_url=https%3A%2F%2Fwww.theverge.com%2F2018%2F6%2F28%2F17509720%2Fcalifornia-consumer-privacy-act-legislation-law-vote.

7 Nimmt Aufgaben eines Justizministers und Generalstaatsanwalts für den jeweiligen US-Bundesstaat wahr.

8 Section 1789.101 (a) der Initiative "The California Consumer Privacy Act of 2018", S. 3, abrufbar unter: https://oag.ca.gov/system/files/initiatives/pdfs/17-0039%20%28Consumer%20Privacy%20V2%29.pdf.

9 S. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375; vgl. hierzu auch *Determann*, ZD 2018, 443.

10 *Determann, Lothar*, Broad data and business regulation, abrufbar unter: https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/.

findet sich ein Hinweis auf Haushalte unter der Überschrift „aggregierte Konsumenteninformationen" (a), die eben nicht Daten mit Bezug zu einem einzelnen Konsumenten oder zu einem Haushalt umfassen. Das Gesetz wird umgekehrt nach Section 1798.140 (o) (1) CCPA auf jede Information bezogen, die einen Bezug zu einem besonderen Konsumenten oder Haushalt hat. Problematisch ist dabei jedoch, wie der Bezug zum Haushalt zu verstehen ist. *Determann* versteht diese Regelung weit und bezieht sie auch auf Informationen über Mehrpersonenhaushalte ohne spezifische Namensnennung der Personen. Dann wären auch Zähler für den Wasser- oder Stromverbrauch ebenso umfasst wie Internetprotokolle.[11] Unterstützt wird diese Auslegung durch die Definition des Identifizierungssystems in Section 1798.140 (x) CCPA als Teil der Legaldefinition in Section 1798.140 (o) (1) (A) CCPA (unique identifier). Solche Identifizierungssysteme sollen alle Informationen umfassen, die genutzt werden können, um einen Konsumenten oder eine Familie zu identifizieren. Der Begriff der „Familie" ist an dieser Stelle definiert als ein Elternteil mit einem minderjährigen Kind. Nicht geregelt ist der Fall, dass ein minderjähriges Kind in einem anderen Bundesstaat als die Eltern seinen Wohnsitz nimmt. In Section 1798.140 (g) CCPA wird dann der Begriff des „Verbrauchers" bzw. „Konsumenten" als zumindest auch durch Identifizierungssysteme identifizierbar umfassend definiert. Dadurch wird in dem durchaus komplizierten Gesetz klargestellt, dass die Regelung auch für nicht personenbezogene Daten einer ganzen Familie zur Anwendung kommt. Insofern unterscheidet sich die Rechtslage nach diesem Gesetz entscheidend von der DS-GVO, die für solche Fälle von vornherein nicht gilt.

4. Geräte

Unklar ist auch die Rechtslage zur Anwendung des neuen Systems auf Geräte. Von Anfang an wurde die Notwendigkeit gesehen, auch den Bereich des Internet of Things mit zu regeln. Ausdrücklich wurde auf die schwierigen datenschutzrechtlichen Probleme beim Einsatz etwa elektronischer Stromzähler hingewiesen. Vorbild des kalifornischen Gesetzes ist die hierzu geplante Regelung in der ePrivacy-Verordnung der EU. „Geräte" werden in Section 1798.140 (j) CCPA definiert als physische Objekte, die man mit dem Internet direkt oder indirekt oder mit einem anderen Gerät verbinden kann. Der Internetbezug ist also nicht zwingend erforderlich. Es reicht aus, zwei Geräte miteinander zu verbinden. Wieso das Gesetz solche Fälle umfasst, bleibt unbeantwortet. Dies ist vielleicht auch der unklaren Regelungstechnik im Gesetz selbst geschuldet. Gerätedaten werden sonst nur als Teil der Legaldefinition der aggregierten Verbraucherinformation angesprochen (Section 1798.140 (a) CCPA). Ansonsten taucht der Bezug zu den Geräten im Text selbst nicht auf. Daher gilt Section 1798.140 (o) (1) CCPA, wonach es darauf ankommt, ob die Informationen direkt oder indirekt auf einen spezifischen Verbraucher oder Haushalt bezogen werden können.

Die Definition des CCPA von persönlichen Informationen ist folglich viel umfassender als die Definition von persönlichen Informationen etwa nach dem geltenden kalifornischen Gesetz zur Data Breach Notification (California Civil Code Section 17098.82). Es reicht schon die indirekte Verbindungsmöglichkeit mit einem bestimmten Verbraucher oder Gerät aus. Damit unterfallen, wie bereits ausgeführt, zahlreiche Daten, die bei der Nutzung eines Produkts entstehen, dem kalifornischen Datenschutzsystem.

5. Öffentlich zugängliche Informationen

Ausgenommen vom notwendigen Personenbezug sind gem. Section 1798.140 (o) (2) CCPA z.B. öffentlich verfügbare Informationen. Hier hat man im Gegensatz zu den Legaldefinitionen versucht, den Spagat zwischen Datenschutzrecht und Informationsinteressen der Öffentlichkeit zu regeln. Öffentlich zugänglich heißt hiernach, dass die Information aus Bundes-, Staats- und sonstigen Datenbanken auf lokaler Verwaltungsebene rechtmäßig zugänglich gemacht wird.

Wiederum ausgeschlossen von der öffentlichen Zugänglichmachung sind biometrische Informationen, die ein Unternehmen über einen Konsumenten ohne dessen Wissen sammelt. Nicht öffentlich zugänglich sind Informationen, die aus Regierungsdatenbanken stammen und für einen Zweck genutzt werden, der nicht kompatibel mit dem ursprünglichen Zweck der Datenerhebung ist. Verhindert werden soll dadurch, dass zweckentfremdete Daten in Regierungsdatenbanken landen und dann vom Datenschutzrecht ausgenommen sind. Das Gesetz vermengt den Zweckbindungsgrundsatz mit der Legaldefinition von Daten. Wer also künftig Daten aus Regierungsdatenbanken nutzt, kann sich nicht darauf verlassen, dass diese per se nicht dem Datenschutzrecht unterliegen. Dadurch entstehen erhebliche Komplikationen. Ferner sollen öffentlich zugängliche Daten die Konsumenteninformationen, die aggregiert sind, nicht umfassen.[12] Diese überflüssige Ausnahme dürfte dadurch bedingt sein, dass aggregierte Daten von vornherein nicht unter das Datenschutzrecht fallen. Da aggregierte Daten in der Regel keinen Personenbezug aufweisen, sind sie vom Datenschutzrecht nicht erfasst.[13] Für das Datenschutzrecht ist diese Kategorie anerkannt. Da der CCPA auch auf einen „particular consumer or household" abstellt, scheint diese Annahme aber problemlos übertragbar zu sein.

6. Medizinische Daten

Eine Ausnahme bilden medizinische Informationen. Informationen, die von dem California Confidentiality of Medical Information Act oder dem U.S. Health Insurance Portability and Accountability Act erfasst werden, sind von der Regelung des CCPA ausgenommen.[14]

7. Adressaten der Regelung

Das Gesetz gilt weltweit für alle Unternehmen, die personenbezogene Daten der Einwohner Kaliforniens verarbeiten oder beziehen. Es ist ausdrücklich nicht nur auf den Bereich des Internets bezogen, sondern gilt für jede Sammlung und jeden Verkauf personenbezogener Daten durch ein Unternehmen (Section 1798.175 CCPA). Es gilt in gleicher Weise für den kleinen Pizzashop wie für große IT-Unternehmen. Allerdings muss gem. Section 1798.140 (c) (1) CCPA zusätzlich eine von drei Voraussetzungen erfüllt sein.

■ Zunächst gilt das Gesetz nur für Unternehmen, die jährlich Einnahmen i.H.v. US-$ 25 Mio. oder mehr erzielen (Section 1798.140 (c) (1) (A) CCPA). Fraglich ist, ob dies nur auf die Einnahmen in Kalifornien bezogen ist oder ob darüber hinaus globale Einnahmen erfasst werden und ob Konzernergebnisse Berücksichtigung finden.[15] Die DS-GVO sieht Sanktionen bezogen auf den weltweit erzielten Jahresumsatz vor. Ähnlich sieht das der California Civil Code in Section 1714.43 (a) (1). Andere Gesetze in Kalifornien stellen ausdrücklich auf die Beschränkung

11 S. *Determann* (o. Fußn. 10).

12 Section 1798.140 (a) (5) CCPA.

13 *Klar/Kühling*, in: Kühling/Buchner (Hrsg.), DSGVO – BDSG, 2. Aufl. 2018, DS-GVO Art. 4 Nr. 1 Rdnr. 15, 16; *Helfrich*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, 46. EL Januar 2018, Teil 16.1 Rdnr. 29 ff.

14 *Epstein Becker & Green P.C.*, How Will the New California Consumer Privacy Act of 2018 Affect Your Business?, abrufbar unter: https://www.healthlawadvisor.com/2018/07/05/how-will-the-new-california-consumer-privacy-act-of-2018-will-affect-your-business/.

15 S. *Determann* (o. Fußn. 10), sowie *Determann, Lothar*, California Privacy Law – Practical Guide and Commentary U.S. Federal and California Law, 3rd edition 2018.

hinsichtlich kalifornischer Einnahmen ab.[16] Getreu der Zielrichtung des Gesetzes wird man aber davon ausgehen können, dass nur Umsätze in Kalifornien aus dem Geschäft mit kalifornischen Einwohnern gezählt werden.

- Alternativ gilt das Gesetz für Unternehmen, deren Datenverarbeitung jährlich mindestens 50.000 Kalifornier betrifft (Section 1798.140 (c) (1) (B) CCPA). Diese Summe wird leicht überschritten, wenn man sich klarmacht, dass zu den relevanten Größen auch IP-Adressen gehören.[17] Im Bereich des Internets werden also auch global agierende Unternehmen regelmäßig an den Vorgaben des kalifornischen Sonderrechts gemessen werden.
- Schließlich gilt das Gesetz auch für Unternehmen, die mehr als 50% ihrer jährlichen Einnahmen aus dem Verkauf von personenbezogenen Informationen kalifornischer Einwohner erhalten (Section 1798.140 (c) (1) (C) CCPA). Ein „Verkauf" umfasst gem. Section 1798.140 (t) (1) CCPA jede Nutzung der Daten gegen Geld oder eine andere wertbezogene Gegenleistung.

Wenn ein Unternehmen kommerziell komplett außerhalb Kaliforniens tätig ist, muss es sich gem. Section 1798.145 (a) (6) CCPA indes nicht den Vorschriften des CCPA unterwerfen. Das setzt jedoch voraus, dass sich das Unternehmen jeglicher Datenverarbeitung sowie wiederholten und sukzessiven Transaktionen in Kalifornien enthält.[18] Erfasst wird somit letztlich jedes Unternehmen mit wirtschaftlicher Aktivität in Kalifornien.[19] Alle Unternehmen aus der EU, die einen Absatzmarkt in Kalifornien haben, müssen somit die Vorgaben der CCPA hinsichtlich ihrer Geschäftsaktivität in Kalifornien beachten. An dieser Stelle könnte ein Konflikt zur „Supremacy Clause" der amerikanischen Verfassung bestehen.[20] Diese legt den Vorrang von US-Bundesrecht vor dem Recht der Bundesstaaten fest. Insbesondere schränkt diese Regelung die Bundesstaaten darin ein, datenschutzrechtliche Regelungen zu treffen, die Unternehmen außerhalb des jeweiligen Bundesstaats betreffen.[21] Allerdings vermeidet der CCPA eine solche Regelung gerade. Auf Bundesebene existiert in den USA der Privacy Act von 1974, der sich allerdings nur an öffentliche Stellen richtet.[22] Darüber hinaus gibt es Regulierungen für einzelne Sektoren, wie den Right to Financial Privacy Act 1978, jedoch kein allgemeingültiges Datenschutzgesetz, mit denen im Einzelfall ein Konflikt des CCPA bestehen könnte. CCPA bezieht sich explizit nur auf wirtschaftliche Aktivitäten in Kalifornien und exkludiert alle weiteren wirtschaftlichen Aktivitäten der Unternehmen. Allerdings bestimmt das US-Bundesrecht im Foreign Account Tax Compliance Act einige Grenzen, die durch bundesstaatlichen Datenschutz nicht überschritten werden dürfen.[23]

8. Pflichten des Gesetzes

Kommt das Gesetz zur Anwendung, treffen die Unternehmen eine Reihe von Verhaltenspflichten.

a) Informationspflicht

Die betroffenen Unternehmen müssen demnach auf Anfrage mitteilen, welche Kategorien und spezifischen Daten sie über den Betroffenen sammeln (Section 1798.100 (a) CCPA).[24] Entscheidend ist der Akt der Sammlung („collect"). Das Gesetz nimmt für sich nicht in Anspruch, die Zulässigkeit der Sammlung zu klären, sondern setzt diese als zulässig voraus. Die Sammlung ist legaldefiniert in Section 1798.140 (e) CCPA. Die Definition ist sehr weit und umfasst jeden Akt des Empfangs von oder des Zugangs zu persönlichen Informationen eines Konsumenten, einschließlich des aktiven oder passiven Empfangs solcher Informationen sowie der Verhaltensbeobachtung.

Dazu muss das Unternehmen vor oder bei der Sammlung der personenbezogenen Daten den Konsumenten über die Kategorien der personenbezogenen Daten und die Zwecke der Datenverarbeitung informieren.[25] Dafür bedarf es allerdings einer spezifischen Anfrage des Betroffenen (Section 1798.100 (c) CCPA). Hierzu muss die Gesetzesdefinition in Section 1798.140 (y) CCPA herangezogen werden, die wieder auf die Richtlinien des „Attorney General" nach Section 1798.185 (a) (7) CCPA verweist. Diese Richtlinien umfassen etwa die Frage, wie eine Anfrage behandelt wird, die über ein passwortgeschütztes Konto gestellt wird, das vom Verbraucher bei dem Unternehmen geführt wird, während er in das Konto eingeloggt ist.

Dann muss die Information unverzüglich und kostenlos an den Konsumenten herausgegeben werden, entweder per Post oder E-Mail in einer einfach lesbaren Form. Eine Pflicht zur Information ist begrenzt auf zwei Antworten innerhalb von zwölf Monaten. Wenn die Information nur einmal für eine Transaktion gebraucht und nicht verkauft wird, besteht die Pflicht nicht (Section 1798.110 (d) (1) CCPA).

b) Spezifische Informationspflicht

Unklar ist wieder einmal die Regelungstechnik bezogen auf die anderen Pflichten. So soll der Konsument nach Section 1798.110 CCPA das Recht haben, eine Fülle von Informationen zu den gespeicherten personenbezogenen Daten zu erhalten. Fraglich ist dabei, wie sich die Informationspflicht nach Section 1798.110 CCPA zu der allgemeinen Informationspflicht nach Section 1798.100 CCPA verhält. Man kann die beiden Informationspflichten als separat bestehend oder die spezifische Regelung in Section 1798.110 CCPA als Konkretisierung von Section 1798.100 CCPA betrachten. Die Lösung liegt in dem Wort Verkauf („sell"), für den nur Section 1798.115 CCPA gilt. Daraus ergibt sich, dass die Informationspflicht an dieser Stelle speziell den Fall des Verkaufs von Daten im weiteren Sinne umfasst.

Jedenfalls kann der Konsument von jedem informationsverarbeitenden Unternehmen über die Kategorien der persönlichen Informationen, die Kategorien der Quellen, den Zweck der Datenverarbeitung und die Kategorien der Dritten, an welche Daten ggf. übermittelt werden, Auskunft verlangen. Voraussetzung ist wieder eine qualifizierte Anfrage des Konsumenten.

c) Widerspruchsrechte

Nutzer von Internetangeboten und Homepages sollen die Möglichkeit erhalten, den Verkauf ihrer persönlichen Daten zu untersagen (Section 1798.120 (a) CCPA).[26] Ein Verkauf liegt nach der Legaldefinition bei einer Weitergabe von personenbezogenen Daten durch das Unternehmen an ein drittes Unternehmen gegen Geld oder andere Wertzuwendung vor. Die Möglichkeit des Widerspruchs wird in Section 1798.120 (a) CCPA als das „right to opt out" bezeichnet. Im Umkehrschluss gilt, dass ein Weiter-

16 So etwa der California Revenue and Taxation Code in Section 17942 (a) (2), abrufbar unter: http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=RTC&sectionNum=17942.

17 *Goldman, Eric*, An Introduction to the California Consumer Privacy Act (CCPA), S. 2, abrufbar unter: https://poseidon01.ssrn.com/delivery.php?ID=963020092123086109008083125066027073033078047010022006094075126002102112011202611250070060580390441111130281250000871260700041001230820690480921061250670941110810310350930151221061011181100650081191220971130861211040010900240930891211110310240801261118EXT=pdf.

18 Doch bleiben Zweifel an der verfassungsrechtlichen Zuständigkeit und Zulässigkeit; s. *Goldman* (o. Fußn. 17).

19 S. *Goldman* (o. Fußn. 17).

20 U.S. Const. art. VI, cl. 2; *Determann, Lothar*, California Privacy Law, S. 10, abrufbar unter: https://iapp.org/media/pdf/publications/IAPP-California-Privacy-Law-2018-SAMPLE.pdf.

21 *Determann* (o. Fußn. 20).

22 *Schwartz, Paul M.*, Preemption and Privacy, 118 Yale L.J. 902 (2008), S. 913.

23 *Schwartz, Paul M.*, Preemption and Privacy, 118 Yale L.J. 902 (2008), S. 921.

24 *Goldman* (o. Fußn. 17), S. 4.

25 *Goldman* (o. Fußn. 17), S. 4.

26 *Goldman* (o. Fußn. 17), S. 5.

verkauf ohne weiteres zulässig ist, wenn der Nutzer von diesem Recht keinen Gebrauch gemacht hat (für Minderjährige unter 16 Jahren gelten allerdings Sonderregelungen). Es ist jedoch zu beachten, dass die Nutzer – wie im Weiteren noch beschrieben – umfassend über ihre Rechte und Möglichkeiten vom Unternehmen informiert werden müssen und ihnen die Opt-out-Möglichkeit als einfach zugänglich präsentiert werden muss. Zu dem Begriff „Verkauf" zählt nach Section 1798.140 (t) (2) (D) CCPA nicht der Bereich gesellschaftsrechtlicher Transaktionen wie Mergers & Acquisitions. I.Ü. fehlt es an einer Weitergabe an einen Dritten im Falle der Auftragsdatenverarbeitung.

Im Rahmen der erwähnten Informationspflichten sollen Betreiber von Internetseiten gem. Section 1798.135 (a) (1) CCPA u.a. einen Link mit den Worten „Do Not Sell My Personal Information" anbieten, durch den die Nutzer ohne großen Aufwand den Weiterverkauf ihrer Daten untersagen können.[27] Nach dem Widerspruch ist der Verkauf der Daten verboten. Die Entscheidung ist mindestens zwölf Monate lang zu respektieren. Erst danach darf das Unternehmen den Betroffenen um eine erneute Einwilligung bitten. Die Unternehmen können eine getrennte zusätzliche Homepage für kalifornische Konsumenten vorhalten, die die notwendigen Links und Informationen bereitstellt.

Aus Section 1798.120 (c) und (d) CCPA ergibt sich diesbezüglich eine Sonderstellung für Minderjährige unter 16 Jahren. Genau umgekehrt zur Grundregel dürfen ihre Daten nicht weiterverkauft werden, wenn die Unternehmen nicht eine ausdrückliche Ermächtigung dazu erhalten haben.[28] Im Gegensatz zur Opt-out-Lösung lässt sich dies als Opt-in-System klassifizieren.[29] Eine solche Ermächtigung kann für 13- bis 16-jährige Nutzer von diesen selbst abgegeben werden, für alle Nutzer unter 13 Jahren müssen die gesetzlichen Vertreter einwilligen.[30] Damit unterscheidet sich der CCPA von der DS-GVO, die für jegliche Verarbeitung von Daten aller Personen unter 16 Jahren ein Einverständnis des gesetzlichen Vertreters vorsieht.[31] Diese Bestimmungen zur Minderjährigkeit gelten, solange das Unternehmen tatsächliche Kenntnis von der Minderjährigkeit des Konsumenten hat.[32] Wird das Alter des Konsumenten willentlich missachtet, wird angenommen, dass das Unternehmen Kenntnis vom Alter des Konsumenten hatte.[33] Auch an diesem Punkt unterscheidet sich der CCPA von der DS-GVO, die für alle Personen unter 16 Jahren ein Einverständnis des gesetzlichen Vertreters vorsieht.[34] Unternehmen können für die Zustimmung von gesetzlichen Vertretern ein Formular für die Einverständniserklärung vorsehen, das per Post, Fax oder Scan zurückgesandt werden kann.[35]

d) Löschungspflichten

Nach Section 1798.105 CCPA kann der Konsument die Löschung aller persönlichen Informationen verlangen.[36] Das Unternehmen[37] muss dann alle persönlichen Informationen aus ihren Datenbeständen löschen und alle Service-Provider auffordern, dies ebenfalls zu tun. Umfangreiche Ausnahmen gelten, wenn die Daten notwendig für den Geschäftszweck oder den Service-Provider sind, um die Transaktion zur Durchführung des Vertrags zu beenden, Sicherheitsprobleme aufzudecken, Störungen zu beheben oder der Informationsfreiheit Rechnung zu tragen.[38] Ferner ist die Datenverarbeitung auch trotz des Widerspruchsrechts zur Durchführung von Forschung im öffentlichen Interesse auf der Basis einer ursprünglichen Zustimmung oder wenn die Daten für lediglich interne Zwecke gebraucht werden oder zur Durchführung einer Rechtsverpflichtung notwendig sind, erlaubt. Die US-amerikanische Literatur spricht hier in Anlehnung zur DS-GVO vom „Recht auf Vergessenwerden".[39] Allerdings sind die Ausnahmen von dem Recht weiter gefasst als in der EU. Die Parallele zur EU passt insofern nicht.

9. Sanktionen und Bußgelder

Gem. Section 1798.155 CCPA drohen Unternehmen Strafen bis zu US-$ 7.500,– pro vorsätzlicher Verletzung der Datenschutzpflichten oder US-$ 2.500,– für fahrlässige Verletzungen, wenn das Unternehmen nach einer Warnung nicht binnen 30 Tagen reagiert. Diese Ansprüche können durch den „Attorney General"[40] geltend gemacht werden. 20% der Strafzahlungen sollen dabei direkt dem *Justizministerium* zur weiteren Verfolgung von Verstößen zu Gute kommen.

Ferner droht gem. Section 1798.150 (a) (1) (A) CCPA ein gesetzlicher Schadensersatz von US-$ 100,– bis 750,– pro Einwohner und Vorfall, wenn Unternehmen Datendiebstahl oder anderen Formen des Datenverlusts zum Opfer fallen. Erstmals taucht an dieser Stelle die Notwendigkeit zu einem angemessenen Konzept der Datensicherheit auf. Allerdings bleibt es beim bloßen Hinweis, Unternehmen mögen „reasonable security procedures" entwickeln und pflegen. Der Ausgleich kann aber auch auf eine andere durch das Gericht festgelegte Art und Weise gewährt werden. Diese Regelungen bieten dem Verbraucher ein individuelles Klagerecht, sodass er diese Ansprüche selbst durchsetzen kann. Zudem ist es möglich, die Ansprüche im Wege von Sammelklagen geltend zu machen, wenn die Zahl der Betroffenen so groß ist, dass Einzelklagen unpraktikabel wären.

Die genannten Summen in Section 1798.155 CCPA scheinen mangels Einzelfallspielraum starre Höchstgrenzen zu sein. Die gesetzlichen Schadensersatzansprüche in Section 1798.150 CCPA können in der Summe überschritten werden, wenn der tatsächliche Schaden beim Verbraucher die genannten Grenzen übersteigt.[41] Sie gelten unabhängig davon, ob der Verbraucher tatsächlich einen Geld- oder Vermögensverlust infolge des Verstoßes erlitten hat. Die Höhe des festgesetzten Schadensersatzes mag im Vergleich zur DS-GVO sehr niedrig erscheinen. Man muss sich aber immer die Gefahr vergegenwärtigen, dass der Schadensersatz in seiner Höhe nachträglich durch den Gesetzgeber hochgesetzt werden kann. Zu denken ist auch an den Imageschaden in den USA, der gerade für global agierende Unternehmen äußerst sensibel ist.

---

27 S. dazu auch: https://www.hipaajournal.com/california-passes-gdpr-style-data-privacy-law/.

28 Section 1798.120 (d) CCPA.; s.a. *Mathews, Kristen J./Bowman, Courtney M.*, The California Consumer Privacy Act of 2018, abrufbar unter: https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/; *Kramer Levin Naftalis & Frankel LLP* (o. Fußn. 5).

29 Section 1798.120 (d) CCPA; s.a. *Kramer Levin Naftalis & Frankel LLP* (o. Fußn. 5).

30 S. o. Fußn. 29.

31 *Kramer Levin Naftalis & Frankel LLP* (o. Fußn. 5).

32 Section 1798.120 (d) CCPA.

33 Section 1798.120 (d) CCPA; s.a. *Goldman* (o. Fußn. 17), S. 5.

34 *Kramer Levin Naftalis & Frankel LLP* (o. Fußn. 5).

35 *Determann, Lothar*, Analysis: The California Consumer Privacy Act of 2018, abrufbar unter: https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/.

36 *Goldman* (o. Fußn. 17), S. 4.

37 Der CCPA trifft keine Aussagen darüber, wer im Unternehmen für die Einhaltung der gesetzlichen Pflichten aus dem CCPA verantwortlich zu sein hat; scheinbar wird dies den Unternehmen zur eigenen Ausgestaltung überlassen.

38 *Goldman* (o. Fußn. 17), S. 4.

39 So etwa *Grant, Amy*, The California Consumer Privacy Act of 2018 (AB 375): What You Need to Know, abrufbar unter: https://www.tripwire.com/state-of-security/featured/california-consumer-privacy-act-2018/.

40 Section 1798.150 CCPA; *De la Torre, Lydia*, GDPR matchup: The California Consumer Privacy Act 2018, abrufbar unter: https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/.

41 S. Wortlaut Section 1798.150 (a) (1) (A) CCPA „whichever is greater"; *Spies*, ZD-Aktuell 2018, 04318.

10. Verhalten bei Datenpannen bzw. Datenmissbrauchsfällen

Für Datenmissbrauchsfälle ist ausnahmsweise ein gerichtliches Vorgehen des Einzelnen vorgesehen.[42] Zunächst muss der Konsument jedoch das Unternehmen über die Datenpanne in Kenntnis setzen und diesem die Möglichkeit geben, die Datenpanne innerhalb von 30 Tagen zu beheben. Erst wenn der Konsument nicht innerhalb von 30 Tagen eine schriftliche Benachrichtigung erhält, dass die Datenpanne behoben wurde, ist es ihm erlaubt, gerichtlich dagegen vorzugehen.[43] Allerdings kann der Konsument sein Begehren erst verfolgen, wenn er den Attorney General über das Begehren informiert hat und dieser nach Ablauf von sechs Monaten nicht aktiv geworden ist.[44] Der Attorney General muss innerhalb von 30 Tagen nach Einreichen der Klage informiert werden.[45] Vorgesehen ist ein gesetzlicher Schadensersatzanspruch in einer Höhe zwischen US-$ 100,– und 750,– pro Konsument, pro Vorfall oder tatsächlicher Schadensersatz, je nachdem was höher ist.[46] Auch die Möglichkeiten zur Feststellungs- bzw. Unterlassungsklage sind gegeben.[47]

IV. CCPA und DS-GVO

Angesichts des neuen kalifornischen Gesetzes drängt sich die Frage auf, ob europäische Unternehmen durch Erfüllung der Vorgaben der DS-GVO auch die kalifornischen Sonderbestimmungen erfüllt haben.[48] Grundsätzlich kann nicht ohne weiteres von einer automatischen Einhaltung ausgegangen werden. Unbekannt in Europa sind die von dem CCPA geforderte Art der Offenlegung von Daten und die Kooperation mit den Verbrauchern i.R.d. Geltendmachung ihrer Rechte. Insbesondere erwähnenswert ist hier die Anforderung an Unternehmen, Möglichkeiten zum Widerspruchsrecht hinsichtlich des Weiterverkaufs direkt auf der Internetseite zur Verfügung zu stellen.

Auch die Definitionen der personenbezogenen Daten sind nicht identisch. Der CCPA setzt den Anwendungsbereich weiter und umfasst – insoweit teilweise ähnlich der geplanten ePrivacy-Verordnung – auch Daten, die nicht unter die DS-GVO fallen, wie z.B. Haushalts- und Gerätedaten.[49]

Weiter gefasst sind auch die Rechte von kalifornischen Einwohnern zur Löschung von Daten und zum Datenzugang.[50] Erneut kann hier die Möglichkeit innerhalb des CCPA erwähnt werden, Weiterverkäufe zu verbieten. Differenzierungen ergeben sich hinsichtlich der Rechte der Verbraucher auch bei den entsprechenden Ausnahmetatbeständen, die den Unternehmen einzelne Freiräume gewähren, sodass dahingehend große Vorsicht geboten ist. Insbesondere der Schutz der Meinungs- und Informationsfreiheit genießt in dem kalifornischen Gesetz eine höhere Stellung als auf EU-Ebene.[51]

Allerdings muss beachtet werden, dass das Schutzniveau der DS-GVO insgesamt trotzdem als vergleichsweise hoch angesehen werden kann, beruht es doch grundsätzlich auf einem Opt-in-System (Art. 5-7 DS-GVO) bei der grundsätzlichen Datenerhebung durch die Unternehmen. Der CCPA hingegen geht von einer grundsätzlichen Zulässigkeit mit der Möglichkeit des Widerspruchs aus (Opt-out-System).

Ferner schreibt der CCPA vor, dass Verbraucher keine Benachteiligungen auf Grund der Ausübung ihrer Rechte erfahren dürfen (Section 1798.125 CCPA). Danach ist es jedem Unternehmen unabhängig von dessen Größe verboten, die Lieferung von Gütern oder Dienstleistungen wegen Wahrnehmung der Rechte aus dem Gesetz zu verneinen oder auch nur verschiedene Preise für diese Angebote zu berechnen. Eine gleiche ausdrückliche Regelung gibt es in der DS-GVO nicht.

Weiterhin bleibt es in den USA dabei, dass es keine speziellen Datenschutzbehörden zur Verfolgung von Verstößen wie in Europa gibt. Zwar sieht Section 1798.160 (a) CCPA die Schaffung eines „Consumer Privacy Fund" vor, die Rechtsdurchsetzung soll jedoch durch Privat- und Sammelklagen und in Einzelfällen durch das *Justizministerium* selbst gewährleistet werden.

Zudem soll nach dem CCPA – anders als nach Art. 37-39 DS-GVO in Europa – auch weiterhin keine Pflicht für Unternehmen zur Bestellung eines Datenschutzbeauftragten bestehen.

V. Ausblick

Da auch die global agierenden europäischen Unternehmen mit Sitz oder Niederlassung in der EU in ihren Beziehungen zum Kunden – gerade im Internetgeschäft – vom CCPA erfasst werden können, werden sich die neuen Regelungen auch auf ihren Unternehmensalltag auswirken. Auf Grund der erhöhten Anforderungen an Unternehmen verglichen sowohl zum vorherigen Schutzniveau in Kalifornien als auch zum neuen Standard in der EU bedeutet dies, dass viele Datenverarbeitungsprozesse angepasst werden müssen, was mit einem hohen zeitlichen und finanziellen Aufwand verbunden ist.[52]

Es kommen auf viele Unternehmen deutlich erhöhte Compliance-Anforderungen und Dokumentationspflichten zu. Diese sind, wie gezeigt, nicht deckungsgleich mit den Pflichten nach der DS-GVO, sondern kommen zu den Vorgaben des EU-Rechts hinzu. Darüber hinaus überrascht, dass der Bereich Internet of Things jetzt in Kalifornien schon „datenschutzrechtlich" geregelt ist, während die europäischen Institutionen noch über der ePrivacy-Verordnung brüten.

Professor Dr. Thomas Hoeren
ist Direktor der zivilrechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM) an der Westfälischen Wilhelms-Universität Münster und Mitherausgeber der MMR.

Stefan Pinelli
ist Rechtsanwalt und Leiter der Hauptabteilung Digital Recht bei der Volkswagen AG in Wolfsburg.

42 *De la Torre* (o. Fußn. 40).
43 Section 1798.150 (b) (1) CCPA.
44 Section 1798.150 (b) (2), (3) CCPA.
45 Section 1798.150 (b) (2) CCPA.
46 Section 1798.150 (a) (1) (A) CCPA; *De la Torre* (o. Fußn. 40).
47 Section 1798.150 (a) (1) (B) CCPA.
48 *Kramer Levin Naftalis & Frankel LLP* (o. Fußn. 5).
49 *Determann* (o. Fußn. 10); *Kramer Levin Naftalis & Frankel LLP* (o. Fußn. 5).
50 *De la Torre* (o. Fußn. 40); *Kramer Levin Naftalis & Frankel LLP* (o. Fußn. 5).
51 *Determann, Lothar,* Kommunikationsfreiheit im Internet – Freiheitsrechte und gesetzliche Beschränkungen, 1999, S. 622.
52 *Determann* (o. Fußn. 10).