47. Jahrgang

datenschutz-berater.de

DSB 01/2023

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Editorial

Stichwort des Monats

Datenschutz im Fokus

Aktuelles aus den Aufsichtsbehörden

Rechtsprechung

ISSN 0170-7256

dfv Mediengruppe

Bettina Blawert

Der neue California Privacy Rights Act (CPRA) – „DSGVO 2.0" in Kalifornien?

Datenschutz und USA: Das sind zwei Begriffe, die – zumindest aus europäischer Sicht – nicht unbedingt miteinander einhergehen. Spätestens seit Schrems II sind die Problematiken rund um den Datentransfer in die USA jedem Datenschützer geläufig. Der derzeitige Versuch, die Datenübermittlung durch ein neues „Privacy Shield", das „transatlantic data privacy framework" (TADPF), auf rechtlich sichere Füße zu stellen, verdeutlicht, wie unterschiedlich Datenschutz in den USA gehandhabt wird. Kalifornien möchte nun Vorreiter im amerikanischen Datenschutzrecht sein und hat den CPRA auf den Weg gebracht, der auffallend viele Parallelen zur DSGVO aufzeigt. Schlechte Kopie oder ein großer Schritt im kalifornischen Datenschutz?

Einführung

Bereits 2020 ist in Kalifornien der California Consumer Protection Act (CCPA) in Kraft getreten. Dieser behandelt vor allem den Verkauf und die Erhebung personenbezogener Daten und wurde als „GDPR light" gehandelt. Allerdings ließen viele Regelungen im CCPA Spielraum für Interpretationen. Das führte zu einer Rechtsunsicherheit, die nun durch den California Privacy Rights Act (CPRA) beseitigt werden soll. Der CPRA ist – salopp gesagt – ein Zusatz zum CCPA. Er baut auf dem CCPA auf und hat diesen geändert und erweitert.

Der CPRA wurde am 03. November 2020 verabschiedet und trat am 01. Januar 2023 in Kraft. Er soll ab dem 01. Juli 2023 durchgesetzt werden.

Dabei weist der CPRA viele Ähnlichkeiten zur DSGVO auf. Hat Kalifornien damit die „DSGVO 2.0" erschaffen?

In diesem Beitrag sollen die Neuerungen vorgestellt und Parallelen zur DSGVO aufgezeigt werden. Des Weiteren wird dargestellt, was sich für europäische Unternehmen damit ändert.

Neuer Unternehmensbegriff

Zunächst wurde der Anwendungsbereich des Datenschutzgesetzes durch eine Änderung des Unternehmensbegriffs modifiziert.

Beide Gesetze haben zwar gemeinsam, dass sie für Unternehmen mit einem Jahresbruttoumsatz von mehr als 25 Millionen Dollar gelten. Während unter den CCPA jedoch Unternehmen fallen, die mindestens 50 % ihres Jahresumsatzes mit dem Verkauf personenbezogener Verbraucherdaten erzielen, erweitert der CPRA den Anwendungsbereich auf Unternehmen, die mindestens 50 % ihres Jahresumsatzes mit dem Verkauf oder der Weitergabe personenbezogener Verbraucherdaten erwirtschaften. Diese Vergrößerung des Anwendungsbereichs wird allerdings dadurch relativiert, dass die erforderliche Anzahl der von dem Verkauf bzw. der Weitergabe betroffenen Verbraucher von 50.000 auf 100.000 pro Jahr erhöht wird.

„DSGVO 2.0": DSGVO-Grundsätze

Besonders auffallend ist die teilweise wortgleiche Aufnahme einiger aus der DSGVO bekannter Grundsätze für die Datenverarbeitung.

Zweckbindung

Ähnlich dem Zweckbindungsgrundsatz gem. Art. 5 Abs. 1 lit. b DSGVO muss die Verarbeitung der erhobenen Daten nach dem CPRA mit „den angemessenen Erwartungen des Verbrauchers" übereinstimmen. Das bedeutet, das Unternehmen muss vor der Verarbeitung prüfen, ob der Verbraucher mit der Datenverarbeitung zu dem angegebenen Zweck rechnet. „Reasonable expectations" sind dem europäischen Datenschutzrecht nicht fremd. Sie sind beispielsweise in Erwägungsgrund 47 DSGVO als Kriterium für die Bewertung überwiegender berechtigter Interessen gemäß Art. 6 Abs. 1 S. 1 lit. f) DSGVO verankert. Bei der Bewertung, ob der Verbraucher die Datenverarbeitung erwartet, müssen folgende Kriterien herangezogen werden:

- Die Beziehung zwischen dem Verbraucher und dem Unternehmen
- Art, Beschaffenheit und Umfang der personenbezogenen Daten, die das Unternehmen zu sammeln oder zu verarbeiten beabsichtigt
- Die Quelle, aus der die personenbezogenen Daten stammen
- Art der Datenverarbeitung

Beispiel: Wenn ein Verbraucher einem Unternehmen Informationen zur Verfügung stellt, um eine bestimmte Dienstleistung in Anspruch zu nehmen, erwartet er nicht, dass dieselben personenbezogenen Daten für ein anderes Produkt oder eine andere Dienstleistung, die von dem Unter-

nehmen oder seiner Tochtergesellschaft angeboten werden, verwendet werden.
- Die Beteiligung von Dritten an der Erhebung und Verarbeitung der Daten und ob die Weiterleitung der Daten an diese Dritte für den Verbraucher offensichtlich ist

Beispiel: Der Verbraucher erwartet nicht, dass die Daten an einen Dritten weitergeleitet werden, wenn er mit diesem Dritten nie interagiert hat oder die Rolle des Dienstleisters im Rahmen der Datenverarbeitung nicht offensichtlich ist.

Datenminimierung

Ein weiterer aus Art. 5 Abs. 1 lit. c DSGVO bekannter Grundsatz begegnet man auch im CPRA: Die Datenminimierung. Es gilt dabei Folgendes zu beachten:
- Es dürfen nur die Daten verarbeitet werden, die für die Erreichung des angegeben Zwecks „vernünftigerweise notwendig" sind.
- Es müssen mögliche negative Auswirkungen der Datenverarbeitung auf den Verbraucher berücksichtigt werden und
- zusätzliche Sicherheitsvorkehrungen getroffen werden, um diese möglichen negativen Auswirkungen zu minimieren.
- Hat der Verbraucher die Möglichkeit, die Art und Weise der Datenverarbeitung auszuwählen, muss die Auswahl der Optionen gleichwertig sein. Das bedeutet, die Option mit dem höheren Schutzniveau darf nicht schwieriger auswählbar sein als die Option mit dem geringeren Schutzniveau.

Speicherbegrenzung

Ebenso wie die Datenminimierung hat auch der Grundsatz der Speicherbegrenzung seinen Weg in den CPRA gefunden. Danach dürfen personenbezogene Daten nur so lange aufbewahrt werden, wie es zur Erfüllung des angegeben Zwecks „vernünftigerweise erforderlich" ist.

Sensible Daten

Neben den aus der DSGVO bekannten Grundsätzen wird der CPRA auch um eine uns bekannte Kategorie erweitert. Während der CCPA sensible Daten lediglich erwähnt, vergrößert der CPRA den Umfang der „sensitive personal information" und schafft somit eine neue Kategorie personenbezogener Daten, die besonders schützenswert sind. Dies weist Ähnlichkeiten zu Art. 9 DSGVO auf. Der CPRA gibt den kalifornischen Verbrauchern mehr Kontrolle darüber, wie Unternehmen besonders sensible Daten verarbeiten. Zu den „sensitive personal information" zählen:
- Daten aus staatlichen Ausweisen (z. B. Sozialversicherungsnummer, Führerschein oder Reisepassnummer)
- Bankdaten (z. B. Kreditkarten- und Anmeldedaten)
- „präzise Geolokalisierung"
- Daten zu rassischer oder ethnischer Herkunft
- Daten zu religiöser oder philosophischer Überzeugung
- Mitgliedschaft in einer Gewerkschaft
- Inhalt nicht öffentlicher Mitteilungen (Post, E-Mail und Textnachrichten)
- genetische Daten
- biometrische Daten
- Gesundheitsdaten
- Informationen über das Sexualleben oder die sexuelle Ausrichtung

Damit geht der CPRA sogar noch ein Stück weiter als Art. 9 DSGVO und nimmt beispielsweise Bankdaten, Daten aus Ausweisdokumenten und „precise geolocation" in die Kategorie der besonders sensiblen Daten auf.

Unternehmen sind verpflichtet, die Verbraucher darüber zu informieren, ob sie sensible Daten verkaufen oder weitergeben, wie lange sie aufbewahrt und zu welchen Zwecken sie verarbeitet werden.

Durch die Kategorisierung der Daten als besonders schützenswert ist insbesondere bei der Datenverarbeitung von sensiblen Daten auf die vorgenannten Grundsätze zu achten.

Aber keine Regel ohne Ausnahme: Die Daten dürfen immer dann uneingeschränkt verarbeitet werden, wenn keine Rückschlüsse auf Charaktereigenschaften des Verbrauchers geschlossen werden können.

Beispiel: Auf einer Webseite werden Artikel zu Gesundheitsinformationen bereitgestellt. Über die Suchfunktion kann der Website-Nutzer für ihn interessante Artikel suchen. Die bei der Suche angegebenen Stichworte können nach dem CPRA weiterverarbeitet werden, da dadurch keine Rückschlüsse auf Eigenschaften des Betroffenen gezogen werden können.

Rechte der Betroffenen

Die Rechte der betroffenen Personen sind Dreh- und Angelpunkt der DSGVO. Ohne die Möglichkeit der Betroffenen, die Verarbeitung ihrer Daten zu überprüfen, berichtigen oder zu limitieren, würden die Grundsätze der Datenverarbeitung leerlaufen. Auch der CPRA gibt kalifornischen Verbrauchern nun erweiterte Betroffenenrechte an die Hand.

Recht auf Auskunft

Bereits das Recht auf Auskunft des CCPA hat weitreichende Ähnlichkeiten zu Artikel 15 DSGVO.

Die betroffene Person hat den Anspruch, ein Auskunftsersuchen gegenüber dem jeweiligen Unternehmen zu stellen und unter anderem zu erfahren, welche personenbezoge-

nen Daten aus welchen Quellen zu welchen Zwecken verarbeitet werden.

Während sich dieses Auskunftsrecht nach dem CCPA nur auf personenbezogene Daten bezogen hat, die in den letzten 12 Monaten erhoben wurden, sieht der CPRA vor, dass auch Daten über diesen 12-Monats-Zeitraum hinaus beauskunftet werden müssen. Unternehmen müssen die Verbraucher außerdem nun vor der Datenerhebung über dieses Auskunftsrecht informieren.

Recht auf Datenübermittlung

Das Recht auf Auskunft wird im CPRA dadurch ergänzt, dass den kalifornischen Verbrauchern ein Recht auf Datenübermittlung eingeräumt wird. Das bedeutet, sie können verlangen, dass das jeweilige Unternehmen bestimmte personenbezogene Daten an ein anderes Unternehmen weitergibt. Auch diesen Anspruch kennen wir als Recht auf Datenübertragbarkeit aus Art. 20 DSGVO.

Recht auf Löschung

Das Recht auf Löschung personenbezogener Daten, sobald der angegebene Zweck erreicht ist, erwähnte schon der CCPA. Der CPRA erweitert die Regelungen nun dergestalt, dass Unternehmen Verbraucher über diesen Anspruch vor Datenerhebung informieren müssen. Der CPRA verlangt weiter, dass Unternehmen Dienstleister, Auftragnehmer und Dritte über Löschungsanträge von Verbrauchern informieren.

Eine Löschpflicht besteht allerdings dann nicht, wenn die Daten notwendig sind, um Transaktionen abzuschließen, Garantien zu erfüllen, Produkte zurückrufen oder andere Verpflichtungen erfüllen zu können.

Recht auf Berichtigung

Neu hinzugekommen ist das Recht auf Berichtigung. Demnach dürfen – ganz wie nach Art. 16 DSGVO – betroffene Personen verlangen, dass über sie erhobene unrichtige Daten berichtigt werden.

Automatisierte Entscheidungsfindung

In Bezug auf die automatisierte Entscheidungsfindung enthält der CPRA sogar zwei neue Regelungen:

Das Recht zu erfahren, ob die eigenen personenbezogenen Daten Teil automatisierter Entscheidungsfindung sind und das Recht, diese automatisierte Entscheidungsfindung abzulehnen.

Beim Auskunftsrecht zu automatisierter Entscheidungsfindung können die kalifornischen Einwohner nicht nur Aufklärung verlangen, ob eine automatisierte Entscheidungsfindung stattfindet. Sie müssen auf Wunsch auch darüber informiert werden, wie die Logik dieser Entscheidungsprozesse und wie das darauf basierende Ergebnis aussehen.

Dienstleister

Das Vertragsrecht wurde im CPRA ebenfalls angepasst. Er enthält eine neue Regelung, die ähnlich der Verpflichtung zum Abschluss eines Auftragsverarbeitungsvertrages nach Art. 28 DSGVO ist. Nach dem CPRA gelten Auftragnehmer nicht als solche, sofern sie keinen Vertrag hierüber geschlossen haben. Salopp gesagt: Der Auftragsverarbeiter ist erst dann einer, wenn er einen entsprechenden Vertrag vorlegen kann.

Des Weiteren muss in diesem Vertrag die Verpflichtung niedergelegt sein, den Verantwortlichen bei Betroffenenanfragen zu unterstützen. Auch das kommt uns aus Art. 28 Abs. 3 S. 2 lit. e DSGVO bekannt vor.

Neue Regelungen

Außerdem enthält der CPRA einige weitere neue Regelungen, die nicht direkt an die DSGVO angelehnt, aber deshalb nicht weniger wichtig sind:

Dark Patterns

Unternehmen sind verpflichtet, sogenannte „Dark Patterns“ zu vermeiden. „Dark Pattern“ ist ein Design, das darauf ausgelegt ist, den Benutzer zu Handlungen zu verleiten, die seinen Interessen entgegenlaufen. Gemeint ist, den Benutzer zu animieren, eine Einstellung vorzunehmen, die seine Daten weniger schützt als er es eigentlich will. Erst dieses Jahr veröffentlichte der EDSA eine Richtlinie zum Umgang mit solchen „Dark Patterns“ („Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them“). Dies verdeutlicht die weltweite Relevanz dieses Themas und macht die Aufnahme in den CPRA umso verständlicher.

Demnach müssen Unternehmen Datenschutzeinstellungen so gestalten, dass die Wahlmöglichkeiten der Verbraucher nicht beeinflusst werden.

Beispiel: Wenn sich der Verbraucher erst durch eine Reihe aufpoppender Fenster klicken muss, bevor er beispielsweise Cookies ablehnen kann, handelt es sich um „Dark Patterns“. Denn die Wahlmöglichkeiten des Verbrauchers wurden beeinflusst. Ist es einfacher, die Cookies zu akzeptieren, wird er eher diese Auswahl betätigen als die datenschutzfreundlichere Alternative der Ablehnung.

Dabei ist die objektive Betrachtung des Designs ausschlaggebend. Es ist nicht entscheidend, ob ein Unternehmen die Absicht hatte, den Verbraucher zu einer Auswahlmöglichkeit zu drängen. Der Vorsatz kann bei der Auslegung, ob es sich um „Dark Patterns“ handelt, allerdings herangezogen werden.

Außerdem muss die abgegebene Einwilligung – ganz so, wie wir es bereits kennen – frei, spezifisch, informiert und unmissverständlich erteilt werden.

Rechte für Minderjährige

Neben der Einhaltung des Children's Online Privacy Protection Act (COPPA) verlangt der CPRA, dass ein Unternehmen, Verzeichnisse über die Einholung der jeweiligen Einwilligungen führt. Bei Kindern unter 13 Jahren ist das die Einwilligung der Erziehungsberechtigten. Bei Minderjährigen zwischen 13 und 16 Jahren ist das ihre eigene Einwilligung.

Neue Datenschutzbehörde

Während der CCPA von der kalifornischen Generalstaatsanwaltschaft durchgesetzt wird, nimmt mit dem CPRA eine neue Durchsetzungsbehörde ihre Arbeit auf: die California Privacy Protection Agency (CPPA). Diese wird mit Ermittlungs-, Durchsetzungs- und Regelungsbefugnissen ausgestattet.

Neue Bußgelder

Der CPRA aktualisiert die Sanktionen des CCPA und sieht nun auch Bußgelder für Verstöße vor, bei denen es um personenbezogene Daten von Personen unter 16 Jahren geht. Diese Bußgelder können ebenfalls bis zu 7.500 Dollar betragen. Des Weiteren können nun neben dem Verantwortlichen auch dessen Dienstleister haftbar gemacht werden.

Während Unternehmen der Zahlung von Bußgeldern unter dem CCPA noch entgehen konnten, indem sie die Verstöße innerhalb von 30 Tagen nach Benachrichtigung durch den Generalstaatsanwalt abstellten, entfällt dieses Möglichkeit unter dem CPRA.

Opt-in/Opt-out

Schon nach dem CCPA hatten Verbraucher das Recht, dem Verkauf ihrer Daten zu widersprechen. Der CPRA geht nun noch weiter und führt dieses Widerspruchsrecht auch für die bloße Weitergabe der Daten ein.
Unternehmen sind außerdem verpflichtet, mindestens 12 Monate zu warten, bevor sie nach einer verweigerten Zustimmung bzw. nach einem Opt-out erneut nach einem Opt-in fragen dürfen.

Neue Anforderungen an Websites

Mit dem CPRA und dem Grundsatz der Datenminimierung müssen Websites künftig folgenden Links anbieten:

- „Do Not Sell or Share My Personal Information" (statt wie bisher nur „Do Not Sell")
- „Limit the Use of My Sensitive Personal Information"

Alternativ kann auch ein einziger „deutlich gekennzeichneter Link" verwendet werden, der es den Verbrauchern leicht ermöglicht, dem Verkauf oder der Weitergabe personenbezogener Daten zu widersprechen und gleichzeitig die Verwendung oder Offenlegung ihrer sensiblen personenbezogenen Daten einzuschränken.

Der Link zu sensiblen Daten ist nur dann nicht erforderlich, wenn die gesammelten sensiblen Informationen nur zu den in den Datenschutzinformationen angegeben Zwecken verarbeitet werden. Auf den kann man ebenfalls verzichten, wenn durch die Daten keine Rückschlüsse auf die Eigenschaften des Verbrauchers gezogen werden können.

Was bedeutet das für europäische Unternehmen?

Europäische Unternehmen, die in Kalifornien tätig sind und in den oben aufgezeigten Anwendungsbereich fallen, werden größtenteils mit den Anforderungen vertraut sein. Die DSGVO ist nach wie vor strenger als das kalifornische Datenschutzrecht und so sind nur in manchen Fällen Anpassungen erforderlich.

Unternehmen sollten dennoch wachsam sein und ihre Abläufe auf Datenschutz-Compliance hin prüfen und gegebenenfalls Änderungen auf der Webseite oder in ihren Datenverarbeitungsprozessen vornehmen, um Sanktionen und Bußgeldern zu entgehen.

Der CPRA ist das bisher strengste Datenschutzgesetz in den USA. Auch wenn er nicht das Schutzniveau der DSGVO erreicht, ist er ihr zumindest ein Stück nähergekommen. Die „DSGVO 2.0" ist der CPRA demnach nicht geworden. Und dennoch: Ein Schritt in die richtige Richtung.

Autorin: **Bettina Blawert (CIPP/E) ist Rechtsanwältin bei Spirit Legal in Leipzig. Sie ist auf Datenschutzrecht spezialisiert und berät vor allem Unternehmen im Bereich des betrieblichen Datenschutzes.**