

USA: CCPA-Aktualisierungen der Leitlinien des kalifornischen Attorney General

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

Am 7.2.2020 veröffentlichte der kalifornische Generalstaatsanwalt (Attorney General – AG) einen überarbeiteten 32-seitigen Entwurf ihrer Leitlinien zum kalifornischen Datenschutzgesetz (CCPA). Drei Tage später veröffentlichte der AG dann noch eine weitere Version, verbunden mit der Erklärung, dass die Vorversion versehentlich Überarbeitungen ausgelassen hatte. Die Öffentlichkeit hatte bis zum 25.2.2020 Zeit, Kommentare zu den aktualisierten Leitlinien abzugeben. Trotz früherer Erklärungen des AG, dass er nicht mit vielen Änderungen an den Entwürfen rechne, weisen die aktualisierten Entwürfe doch nunmehr erhebliche und zum großen Teil sinnvolle Änderungen auf.

Die wichtigsten Änderungen betreffen folgende Bereiche:

1. Überarbeitete Definitionen von Personal Information

Zu den wichtigsten Klarstellungen gehört, dass der AG die von vielen kritisierte Definition von „Haushalten“ präzisiert. Es reicht nicht aus, dass die Personen nur dieselbe Adresse haben, sondern sie müssen auch ein gemeinsames Gerät oder eine gemeinsame Dienstleistung des Unternehmens nutzen und als Personen mit demselben Konto oder mit eindeutigen Online-IDs identifiziert werden.

Interessant ist auch, dass die Angabe, ob es sich bei den Informationen um „Personal Information“ handelt, davon abhängt, wie die Informationen gespeichert werden. Wenn eine IP-Adresse beim Verarbeiter nicht in angemessener Weise mit einem bestimmten Verbraucher oder Haushalt in Verbindung gebracht werden kann, handelt es sich nicht um „Personal Information“. Wörtlich heißt es: „if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be „personal information“ (vgl. Abschnitt 999.302).

Der *EuGH* hat u. a. in der Rs. Breyer (ZD 2017, ZD Jahr 2017 Seite 24 m. Anm. *Klar/Kühling*) entschieden, dass dynamische IP-Adressen personenbezogene Daten sind. Damit dürfen Webseitenbetreiber sie nach der DS-GVO nur verarbeiten, wenn sie die strengen Vorgaben des Datenschutzes einhalten. Es kann demnach durchaus passieren, dass nach dem CCPA Daten nicht unter die Definition fallen, die dann nach Art. EWG_DSGVO Artikel 4 Nr. EWG_DSGVO Artikel 4 Nummer 1 DS-GVO personenbezogene Daten sind und vielleicht auch umgekehrt.

2. Privacy Policy v. Notice of Collection

Die aktualisierte AG-Stellungnahme stellt klar, dass ein Hinweis zum Zeitpunkt der Sammlung (Notice of Collection – § 999.305) etwas anders ist als eine Datenschutzrichtlinie. Ein Unternehmen muss zum Zeitpunkt der Erhebung, ähnlich wie in Art. EWG_DSGVO Artikel 13 und EWG_DSGVO Artikel 14 DSGVO, dem Verbraucher eine Mitteilung zukommen lassen, wenn es persönliche Informationen direkt von ihm sammelt. Die Benachrichtigung muss den Verbraucher darüber informieren, welche persönlichen Daten gesammelt werden und wie das Unternehmen sie verwenden wird. Wenn ein Unternehmen die persönlichen Daten von Verbrauchern online erfasst, kann es einen auffälligen Link zu dem Hinweis auf der Einführungsseite der Unternehmenswebsite und auf allen Webseiten, auf denen persönliche Daten erfasst werden, anbringen.

Hingegen beschreibt die Datenschutzrichtlinie die Praktiken des Unternehmens in Bezug auf die Sammlung, die Verwendung, die Weitergabe und den „Verkauf“ (sale) von persönlichen Daten. Die aktualisierten Verordnungsentwürfe erlauben es den Unternehmen nach wie vor, eine Datenschutzrichtlinie als Notice of Collection zum Zeitpunkt der Sammlung zu verwenden, indem sie auf den entsprechenden Abschnitt in der Datenschutzrichtlinie per Link verweisen. Das dürfte die Umsetzung vereinfachen.

3. Hinweise bei mobilen Anwendungen/Apps

Ebenfalls praktisch wichtig: Wenn ein Unternehmen personenbezogene Daten über eine mobile Anwendung sammelt, kann es auf der Download-Seite der mobilen Anwendung und innerhalb der Anwendung einen Link zum Datenschutzhinweis (und zu den Opt-out-Anforderungen) bereitstellen, z. B. über das Einstellungsmenü der Anwendung oder App. Wenn ein Unternehmen persönliche Daten telefonisch oder von Person zu Person sammelt, kann es die Mitteilung der Hinweise sogar mündlich abgeben.

4. Richtlinien zur Zugänglichkeit der Bekanntmachungen

Der aktualisierte Entwurf des AG verlangt, dass alle Online-Bekanntmachungen und Datenschutzrichtlinien für den CCPA den Web Content Accessibility Guidelines Version 2.1 des *World Wide Web Consortium* folgen. Diese neue Anforderung soll die Zugänglichkeit für Verbraucher mit Behinderungen besser berücksichtigen.

5. Bearbeitung von Anfragen von Verbrauchern

Der aktualisierte AG-Entwurf stellt auch klar, dass die Unternehmen glücklicherweise keine drei Methoden für den Empfang von Verbraucheranfragen beibehalten müssen. Ein Unternehmen, das ausschließlich online tätig ist und eine direkte Beziehung zu einem Verbraucher hat, von dem es „Personal Information“ sammelt, muss nur eine E-Mail-Adresse angeben, um Anfragen entgegenzunehmen. Alle anderen Unternehmen müssen zwei Methoden für den Empfang von Anfragen bereitstellen (z. B. auch eine gebührenfreie Telefonnummer).

Die Unternehmen bekommen auch eine längere Frist, um den Erhalt einer Anfrage zu bestätigen (nunmehr 10 Arbeitstage). Der Verordnungsentwurf verlängerte auch die Frist, um einen Antrag auf Opt-out nachzukommen, von 15 Tagen auf 15 Geschäftstage. Außerdem können Unternehmen nun einen Antrag auf Kenntnisnahme oder Löschung ablehnen, wenn der Antrag nicht innerhalb von 45 Tagen überprüft werden kann. Wenn ein Unternehmen einen Antrag auf Löschung nicht verifizieren kann, muss es den nicht verifizierten Antrag nicht mehr als Antrag auf Opt-out behandeln.

6. Diensteanbieter

Alle Diensteanbieter können nach dem AG die persönlichen Daten ihrer Kunden in bestimmten Fällen für zusätzliche Zwecke über den eigentlichen Dienstleistungszweck hinaus verwenden. Insbesondere darf ein Diensteanbieter die persönlichen Daten seiner Kunden verwenden, um:

- einen Subunternehmer zu beauftragen, der sich an den CCPA hält,
- seine Dienstleistungen intern zu verbessern (mit der Rückausnahme des Profiling),
- Gesetze oder gesetzliche Verpflichtungen einzuhalten,
- einen Bruch der Datensicherheit zu untersuchen oder
- eigene Rechtsansprüche zu verteidigen oder abzuwehren.

Die Entwürfe des AG revidieren auch die Verpflichtung eines Diensteanbieters, auf das Recht des Verbrauchers auf Kenntnisnahme zu reagieren: ein Dienstleistungsanbieter muss der Anfrage im Namen des Verantwortlichen voll nachkommen. Er kann als Alternative den Verbraucher aber auch darüber informieren, dass er der Anfrage nicht nachkommen kann, weil sie an einen Diensteanbieter geschickt wurde. Ein Diensteanbieter ist nicht verpflichtet, dem Verbraucher die Kontaktinformationen zur Verfügung zu stellen, wie der Verbraucher den Verantwortlichen erreichen kann.

7. Schaltfläche für das Opt-out

Unternehmen können den vorgeschlagenen Opt-out-Button (mit der Maus zu bewegenden Schieber) links neben dem Link „Meine persönlichen Daten nicht verkaufen“ oder „Do not sell my information“ einfügen. Die Verwendung der Opt-out-Schaltfläche ist optional. Es gilt jedoch weiterhin, dass die Verwendung der Schaltfläche nicht die Verpflichtung eines Unternehmens ersetzt, ggf. den Textlink „Meine persönlichen Daten nicht verkaufen“ in Englisch auf der Website zu platzieren.

Wenn die *Generalstaatsanwaltschaft* nach dem Ablauf der Kommentierungsfrist am 25.2.2020 nur unwesentliche Änderungen an den Verordnungsentwürfen vornimmt, gibt es keine weitere Ankündigungs- und Kommentarfrist. In diesem Fall werden die Vorschriften dem *Office of Administrative Law* vorgelegt, das dann 30 Arbeitstage Zeit hat, um zu überprüfen, ob die Anforderungen des Verwaltungsverfahrens eingehalten wurden.

Weiterführende Links

Vgl. auch *Spies*, ZD-Aktuell 2019, ZDAKTUELL Jahr 06781 m. w. Nw.

