

USA: Neues Datenschutzgesetz in Oregon

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

Der Riegel von Gesetzen auf Bundesstaatsebene zum Schutz der Privatsphäre von Verbrauchern in den Vereinigten Staaten kann man nunmehr Oregon hinzufügen. Am 22.6.2023 verabschiedete das Repräsentantenhaus von Oregon den Oregon Consumer Privacy Act (OCA). Sobald die Gouverneurin das Gesetz wie erwartet unterzeichnet, soll der OCA am 1.7.2024 in Kraft treten.

Ganz nach dem Vorbild der Vorlagen von Connecticut und Virginia gilt der OCA für jedwede (auch ausländische) Person, die in Oregon geschäftlich tätig ist oder Produkte/Dienstleistungen für Einwohner von Oregon anbietet und

- personenbezogene Daten von 100.000 oder mehr Verbrauchern in Oregon verarbeitet oder kontrolliert oder
- personenbezogene Daten von 25.000 oder mehr Verbrauchern in Oregon kontrolliert oder verarbeitet und über 25 % des Bruttoumsatzes aus dem Verkauf dieser Daten erzielt.

Ein „Verbraucher“ ist eine natürliche Person, die in Oregon ansässig ist und in einer anderen Eigenschaft als in einem gewerblichen oder beruflichen Kontext handelt. Wie bei den meisten anderen staatlichen Datenschutzgesetzen bedeutet dies, dass Mitarbeiter und Business-to-Business-Kontakte ausdrücklich von der Definition des Begriffs „Verbraucher“ und damit vom OCA ausgenommen sind – anders als zB in Kalifornien.

„Personenbezogene Daten“ sind alle Daten, abgeleitete („derived“) Daten oder eindeutigen Identifikatoren, die mit einem Verbraucher oder einem Gerät verknüpft sind oder vernünftigerweise mit einem Verbraucher oder einem Gerät verknüpft werden können, das einen oder mehrere Verbraucher in einem Haushalt identifiziert, mit ihm verknüpft ist oder vernünftigerweise mit ihm in Verbindung gebracht werden kann.“ Der Begriff schließt anonymisierte Daten sowie öffentlich zugängliche Informationen aus. Letzteres gilt auch für Informationen, von denen der für die Verarbeitung Verantwortliche vernünftigerweise annimmt, dass sie der Öffentlichkeit von einem Verbraucher rechtmäßig zugänglich gemacht wurden.

Der OCA gilt wie andere bundesstaatliche Datenschutzgesetze u. a. nicht für öffentliche Körperschaften und Regierungsbehörden, Versicherer (einschließlich Versicherungsproduzenten und -berater iSd Gesetzes von Oregon) sowie nicht-kommerzielle Aktivitäten, die von einem Verleger, Redakteur, Reporter oder einer ähnlichen Rolle im Journalismus und einem von der Federal Communications Commission (FCC) lizenzierten Radio- oder Fernsehsender ausgeführt werden.

Der OCA erlegt den Datenverantwortlichen iRd staatlichen Verbraucherschutzgesetze zahlreiche „Standard“-Verpflichtungen auf. Konkret müssen die für die Verarbeitung Verantwortlichen zB ihre Verarbeitung personenbezogener Daten auf das Maß zu beschränken, das für die dem Verbraucher mitgeteilten Zwecke der Verarbeitung angemessen, relevant und notwendig ist; sie müssen auch Maßnahmen ergreifen, um angemessene Sicherheitsvorkehrungen zum Schutz der personenbezogenen Daten zu treffen, die sich unter ihrer Kontrolle befinden und mehr.

Interessant: Der OCA verlangt von den Verantwortlichen ausdrücklich, dass sie die – in der für einen Bruch der Datensicherheit geltende Vorschrift ORS 646A.622 – beschriebenen Sicherheitsvorkehrungen einhalten. Mit dieser dynamischen Verweisung ist der OCA strenger als diverse andere bundesstaatliche Gesetze zum Schutz der Privatsphäre von Verbrauchern, die keine solche konkrete Vorgabe machen.

Weitere Verpflichtungen der Verantwortlichen sind:

- Bereitstellung eines wirksamen Verfahrens für Verbraucher zum Widerruf der Einwilligung. Wenn der Verbraucher seine Einwilligung widerruft, stellt der für die Verarbeitung Verantwortliche die Verarbeitung innerhalb von 15 Tagen ein.
- Diskriminierungsverbot der Verbraucher bei der Ausübung ihrer Rechte;
- Einwilligungserfordernis vor der Verarbeitung sensibler Daten und bevor personenbezogene Daten zum Zwecke gezielter Werbung, Profiling oder des „Verkaufs“ personenbezogener Daten einer Person (ähnlich definiert wie in Kalifornien) verarbeitet werden,
- besondere Vorschriften zum Schutz von Minderjährigen,
- Bereitstellung einer Datenschutzerklärung, die angemessen zugänglich, klar und aussagekräftig ist und den Verantwortlichen klar identifiziert.

Die für die Verarbeitung Verantwortlichen müssen den Verbrauchern in Oregon auch bestimmte Auskunftsrechte, Berichtigungsrechte und Lösungsrechte einräumen. Der Gesetzestext enthält hier keine Überraschungen.

Wie bei anderen staatlichen Verbraucherschutzgesetzen sind in bestimmten Fällen Datenschutzfolgeabschätzungen verpflichtend. Die Verantwortlichen müssen den Nutzen der Verarbeitung für das Unternehmen, den Verbraucher und die Öffentlichkeit analysieren und gleichzeitig die Schäden und potenziellen Schadensbegrenzungen abwägen. Der OCA ermöglicht die Verwendung von Folgeabschätzungen, die nach anderen staatlichen Gesetzen durchgeführt wurden, um seinen eigenen Anforderungen gerecht zu werden, und verlangt keine rückwirkenden Folgeabschätzungen für Verarbeitungstätigkeiten, die vor dem Datum des Inkrafttretens des Gesetzes stattgefunden haben.

Der Generalstaatsanwalt von Oregon hat die ausschließliche Durchsetzungsbefugnis. Ein privates Klagerecht besteht in Oregon nicht. Es gibt auch keine unabhängige Datenschutzbehörde wie in Kalifornien. Vor der Einleitung eines Vollstreckungsverfahrens muss der Generalstaatsanwalt schriftlich eine Frist von 30 Tagen einräumen und Gelegenheit zur Richtigstellung geben. Wenn eine Durchsetzungsmaßnahme folgt, werden Verstöße gegen den OCA mit Geldstrafen von bis zu 7.500 USD pro Verstoß geahndet.

Fazit

Die Entwicklung zeigt einmal mehr, dass weiter längst nicht alle US-Bundesstaaten dem kalifornischen Modell folgen und teilweise eigene Wege gehen, u. a. nach den eher industriefreundlichen Vorgaben in Virginia, Texas und Utah. Diesem Modell folgt jetzt auch Oregon mit Nuancen. Interessant ist, dass Oregon bestimmte Datensicherheitsstandards vorschreibt. Auffällig ist der Terminus „abgeleitete Daten“ (derived data) in der o. g. Definition der personenbezogenen Daten. Im OCA wird er nicht definiert. „Abgeleitete Daten“ sind wohl diejenigen Daten, die aus anderen Daten extrapoliert werden und die mit einem oder mehreren Verbrauchern oder Haushalten verknüpft bleiben oder vernünftigerweise verknüpft werden können – ähnlich wie in Art. 4 Nr. 1 DS-GVO. Ein Bundesgesetz ist weiter nicht in Sicht. Die Lage hier in

den USA bleibt also unübersichtlich und verlangt von den Unternehmen in Europa mit Geschäft in den USA, eine Compliance an den einzelnen Bundesstaaten auszurichten.

Weiterführende Links

Vgl. hierzu Determann ZD 2018, [443](#); Horstmann ZD-Aktuell 2023, 01024 und Spies ZD 2023, [70](#). Damit haben derzeit neben Oregon derzeit folgende US-Staaten allgemeine Datenschutzgesetze: Kalifornien, Colorado, Connecticut, Utah, Virginia, Iowa, Indiana, Montana, Tennessee, Texas s. jeweils Spies ZD-Aktuell 2020, [04407](#); ZD-Aktuell 2020, 04414; ZD-Aktuell 2020, [07398](#); ZD-Aktuell 2021, [05047](#); ZD-Aktuell 2021, [05130](#); ZD-Aktuell 2021, [05257](#); ZD-Aktuell 2022, [01093](#); ZD-Aktuell 2022, [01177](#); ZD-Aktuell 2020, [01191](#); ZD-Aktuell 2020, 01392, ZD-Aktuell 2020, [01396](#) und ZD-Aktuell 2023, [01010](#); ZD-Aktuell 2023, [01050](#); ZD-Aktuell 2020, [01124](#); ZD-Aktuell 2020, [01184](#) sowie MMR-Aktuell 2020, [426334](#) und MMR 2022, [839](#) sowie MMR 2023, [69](#).