USA: Der neue Delaware Personal Data Privacy Act

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

Die Reihe im Newsdienst ZD-Aktuell zu den US-Datenschutzgesetzen wird fortgesetzt: Am 12.9.2023 unterzeichnete der Gouverneur von Delaware, John Carney, den Delaware Personal Data Privacy Act (DPDPA). Wie in den anderen 12 Bundestaaten mit ähnlichen Gesetzen schützt der DPDPA die Datenschutzrechte von Verbrauchern in Delaware und regelt die Erhebung, Nutzung und Weitergabe ihrer personenbezogenen Daten durch Unternehmen, die in Delaware Geschäfte machen. Auf den Sitz des Unternehmens kommt es nicht an. Der DPDPA ist für europäische Unternehmen trotz der eher geringen Größe des Bundesstaates interessant, weil viele US-Tochterunternehmen in Delaware ihren Sitz haben und dort evtl. auch geschäftlich tätig sind. Der DPDPA tritt am 1.1.2025 in Kraft.

Der DPDPA (House Bill No. 154) folgt mit Abweichungen dem Modell des Virginia Consumer Data Protection Act (ZD-Aktuell 2021, 05047), der auch andere staatliche Datenschutzgesetze wie den Texas Data Privacy and Security Act (ZD-Aktuell 2023, 01232) maßgeblich beeinflusst hat.

1. Geltungsbereich

Der DPDPA gilt für Unternehmen, die in Delaware geschäftlich tätig sind oder Produkte oder Dienstleistungen herstellen, die sich an Einwohner von Delaware richten, und einen oder mehrere der folgenden Schwellenwerte erfüllen:

es werden personenbezogene Daten von mind. 35.000 Verbrauchern (dh natürlichen Personen) in Delaware kontrolliert oder verarbeitet, ausgenommen personenbezogene Daten, die ausschließlich zum Zweck der Abwicklung eines Zahlungsvorgangs kontrolliert oder verarbeitet werden; oder

- •es werden personenbezogene Daten von mind. 10.000 Verbrauchern in Delaware kontrolliert oder verarbeitet und mehr als 20 % ihrer Bruttoeinnahmen aus dem „Verkauf" (s. u.) ihrer personenbezogenen Daten erwirtschaftet.

Wie die Datenschutzgesetze von Virginia und Texas schließt auch der DPDPA Personen, die in einem kommerziellen (B2B) oder arbeitsrechtlichen Kontext handeln, von der Definition des Begriffs „Verbraucher" aus. Anderes gilt zB in Kalifornien nach dem CCPA (ZD-Aktuell 2022, 01364). Darüber hinaus werden durch den DPDPA wie in den anderen bundesstaatlichen Gesetzen auch solche Informationen vom Anwendungsbereich ausgenommen, die durch andere Bundesdatengesetze geschützt sind, darunter der Health Insurance Portability and Accountability Act (HIPPA) und der Gramm-Leach-Bliley Act.

2. Verbraucherrechte wie in der DS-GVO

Das Gesetz gewährt den Verbrauchern einige aus der DS-GVO wohlbekannte Rechte in Bezug auf ihre personenbezogenen Daten, darunter das Recht:

sich zu vergewissern, ob ein Verantwortlicher ihre personenbezogenen Daten verarbeitet, und Zugang zu diesen Daten zu erhalten, es sei denn, dies würde ein Geschäftsgeheimnis preisgeben;

- •Berichtigung von unrichtigen Angaben in ihren personenbezogenen Daten zu verlangen;

Löschung von personenbezogenen Daten, die von ihnen zur Verfügung gestellt oder über sie erhoben wurden;

- •eine Kopie ihrer personenbezogenen Daten in einem übertragbaren und nutzbaren Format zu erhalten;

eine Liste der Kategorien von Dritten zu erhalten, an die der für die Verarbeitung Verantwortliche die personenbezogenen Daten weitergegeben hat und

- •das Recht der Verarbeitung der personenbezogenen Daten für gezielte Werbung, den Verkauf personenbezogener Daten oder einem Profiling zu widersprechen.

Die Verbraucher können ihre Rechte über ein sicheres und zuverlässiges Kommunikationsmittel ausüben, das von dem für die Verarbeitung Verantwortlichen eingerichtet wurde, oder indem sie einen Bevollmächtigten benennen, zB eine Plattform oder eine Online-Technologie, der in ihrem Namen bestimmte Verarbeitungen untersagt. Die Verantwortlichen müssen Verbraucheranfragen ohne unangemessene Verzögerung innerhalb von 45 Tagen beantworten und können eine angemessene Gebühr erheben. Sie können es ablehnen, Anfragen zu bearbeiten, die offensichtlich unbegründet, übertrieben oder wiederholend sind. Die Verantwortlichen müssen außerdem ein Verfahren vorsehen, mit dem die Verbraucher gegen ihre Entscheidungen Widerspruch einlegen und sich an das Justizministerium von Delaware wenden können, um eine Beschwerde einzureichen.

3. Pflichten von Verantwortlichen und Auftragsverarbeiter

Nach dem DPDPA ergeben sich wenige Besonderheiten für Delaware. Das Gesetz erlegt den für die Verarbeitung „Verantwortlichen" und den „Auftragsverarbeitern" diverse aus der DS-GVO bekannte Pflichten auf. So muss ein Verantwortlicher die Erhebung und Verwendung personenbezogener Daten auf das Notwendige und mit den offengelegten Zwecken Vereinbare beschränken, die Zustimmung zur Verarbeitung sensibler Daten oder zum Verkauf personenbezogener Daten einholen, einen Datenschutzhinweis (mit bestimmten Pflichtangaben) und ein Verfahren für die Ausübung der Verbraucherrechte bereitstellen. Er darf Verbraucher, die ihre Rechte wahrnehmen, nicht diskriminieren. Ein Auftragsverarbeiter muss wie in der DS-GVO die Anweisungen des für die Verarbeitung Verantwortlichen befolgen, ihn bei der Erfüllung seiner Pflichten angemessen unterstützen sowie die Vertraulichkeit und Sicherheit der personenbezogenen Daten gewährleisten.

Das Gesetz verlangt, dass der Verantwortliche mit dem Auftragsverarbeiter einen Vertrag über die Verarbeitung personenbezogener Daten (vgl. den AVV nach der DS-GVO) abschließt. In diesen Verträgen müssen die Anweisungen, die Art, der Zweck und die Dauer sowie die Rechte und Pflichten beider Parteien in Bezug auf die Verarbeitung personenbezogener Daten eindeutig festgelegt werden. Diese Verträge müssen vorsehen, dass der Auftragsverarbeiter bestimmte Bedingungen einhalten muss, wie zB die Löschung oder Rückgabe personenbezogener Daten auf Anweisung des für die Verarbeitung Verantwortlichen, die Bereitstellung von Informationen zum Nachweis der Einhaltung der Vorschriften, die Möglichkeit des Widerspruchs durch den Verantwortlichen vor der Beauftragung von Unterauftragnehmern und die Ermöglichung von Audits durch den für die Verarbeitung Verantwortlichen oder einen unabhängigen Prüfer.

4. „Verkauf" von personenbezogenen Daten an Dritte

Wie in vielen anderen US-Datenschutzgesetzen ist der Terminus „Verkauf" (Sale) ein Schlüsselbegriff. Das Gesetz regelt den „Verkauf" personenbezogener Daten detailliert, indem es u. a. von den Verantwortlichen verlangt, die Verarbeitung in klarer und auffälliger Weise

offenzulegen. Er muss den Verbrauchern die Möglichkeit zu geben, dem „Verkauf" ihrer personenbezogenen Daten zu widersprechen (Opt-out – Opt-in bei bestimmten sensiblen Daten). Das Gesetz definiert wie zB in Kalifornien den „Verkauf" personenbezogener Daten weit, nämlich als die Übermittlung „personenbezogener Daten gegen Geld oder eine andere entgeltliche Gegenleistung durch den für die Verarbeitung Verantwortlichen an einen Dritten." Bestimmte Übermittlungen von Daten sind allerdings im Rahmen ihrer Notwendigkeit davon ausgenommen, wie:

Übermittlung an einen Auftragsdatenverarbeiter, sofern dies auf den Zweck dieser Verarbeitung beschränkt ist;

- •Übermittlung an einen Dritten zum Zwecke der Bereitstellung eines Produkts oder einer Dienstleistung, die der Verbraucher ausdrücklich angefordert hat;

Übermittlung an ein verbundenes Unternehmen des Verantwortlichen;

- •Übermittlung, wenn der Verbraucher den Verantwortlichen anweist, die personenbezogenen Daten weiterzugeben;

Übermittlung solcher personenbezogenen Daten, die der Verbraucher absichtlich über einen Kanal der Massenmedien der breiten Öffentlichkeit zugänglich gemacht hat und die nicht auf ein bestimmtes Publikum beschränkt waren sowie

- •Übermittlung an einen Dritten als Vermögenswert (Asset), der Teil einer Fusion, einer Übernahme, eines Konkurses oder einer Insolvenz ist.

Hinzu kommen diverse Vorschriften zum Kinderschutz. Das Gesetz verbietet es den Verantwortlichen auch, personenbezogene Daten ohne die Zustimmung der Eltern zu „verkaufen", wenn der Verbraucher jünger als 13 Jahre ist.

5. Datenschutz-Folgenabschätzungen (DSFA)

Die DSFA (DPIA) in Delaware bergen einige Überraschungen für europäische Unternehmen. Das Gesetz geht in Teilen über das hinaus, was Art. 35 DS-GVO verlangt. Verantwortliche, welche die Daten von mindestens 100.000 Verbrauchern verarbeiten, mit Ausnahme von Daten, die ausschließlich zur Abwicklung eines Zahlungsvorgangs verarbeitet werden, müssen für jede ihrer Verarbeitungstätigkeiten, die ein erhöhtes Schadensrisiko für Verbraucher darstellen, eine DSFA durchführen. Zu diesen Tätigkeiten gehören:

die Verarbeitung personenbezogener Daten für gezielte Werbung;

- •der „Verkauf" (s. o.) von personenbezogenen Daten;

ein Profiling, das rechtliche oder erhebliche Auswirkungen hat; oder

- •die Verarbeitung (näher definierter) sensibler Daten.

Die DSFA müssen die Vorteile und Risiken der Verarbeitung sowie die Schutzmaßnahmen, die zur Verringerung der Risiken eingesetzt werden können, ermitteln und abwägen, wobei die berechtigten Erwartungen der Verbraucher sowie der Kontext und die Beziehung der Verarbeitung zu berücksichtigen sind. Der Generalstaatsanwalt (Attorney General) kann von einem Verantwortlichen verlangen, die DPIA/DSFA offenzulegen und diese dann selbst überprüfen.

6. Dark Pattern

Das Gesetz befasst sich auch explizit mit der Verwendung von Dark Patterns, dh Benutzeroberflächen oder Praktiken, die die Autonomie, Entscheidungsfreiheit oder Wahlmöglichkeiten der Benutzer manipulieren oder beeinträchtigen. Das Gesetz verbietet die

Verwendung von Dark Patterns, um die Zustimmung zur Verarbeitung personenbezogener Daten einzuholen. Es definiert die Zustimmung eng als eine klare, bestätigende Handlung, die eine frei gegebene, spezifische, informierte und eindeutige Zustimmung des Verbrauchers beinhaltet.

7. Durchsetzung

Der DPDPA wird vom Justizministerium des Bundesstaats Delaware durchgesetzt, das befugt ist, Verstöße gegen das Gesetz zu untersuchen und dann auch zu verfolgen. Eine unabhängige Datenschutzbehörde, wie sie mittlerweile in Kalifornien existiert (CCPA – ZD-Aktuell 2023, 01050), gibt es in Delaware nicht. Stellt das Justizministerium fest, dass ein Verstoß vorliegt, der jedoch behoben werden kann, muss es dem Verantwortlichen eine Mitteilung über den Verstoß zukommen lassen und ihm Gelegenheit geben, den Verstoß innerhalb einer Gnadenfrist von 60 Tagen zu beheben, bevor es eine Durchsetzungsmaßnahme einleitet. Die 60-Tage-Frist ist für auf diese Weise heilbare Verstöße nach dem 31.12.2025 nicht mehr zwingend. Nach diesem Datum kann das Justizministerium des Bundesstaats Delaware bei der Entscheidung, ob dem für die Verarbeitung Verantwortlichen eine Korrekturfrist eingeräumt wird, verschiedene Faktoren berücksichtigen, zB die Anzahl und Art der Verstöße, die Größe des Verantwortlichen sowie die Wahrscheinlichkeit und das Ausmaß des Schadens für die Verbraucher. Das Gesetz sieht an keiner Stelle ein privates Klagerecht vor. Stattdessen gilt ein Verstoß gegen das Gesetz als „ungesetzliche Praxis" iSd Delaware-Verbraucherschutzgesetzgebung, die vom Justizministerium in Delaware durchgesetzt werden kann.

8. Kurze Einordnung

Der DPDPA zeigt als bundesstaatliches Gesetz einmal mehr, dass sich Unternehmen nicht darauf verlassen können, mit der Compliance nach kalifornischem Recht alles für die anderen US-Bundesstaaten getan zu haben. Ein Beispiel: Im Gegensatz zu einigen anderen Bundesstaaten gilt der DPDPA für die meisten „Not for profits" und höheren Bildungseinrichtungen. In vielen US-Bundesstaaten scheint sich nicht der kalifornische Standard durchzusetzen, sondern der etwas unternehmensfreundlichere Ansatz von Virginia. Angesichts von knapp 1 Mio. Einwohnern in Delaware ist die Eingangsschwelle von 35.000 Verbrauchern relativ niedrig. Vorschriften zum Datenexport aus Delaware gibt es nicht.

Weiterführende Links

Vgl. hierzu auch Spies ZD-Aktuell 2023, 01298 mwN; Spies ZD-Aktuell 2023, 01326; Spies ZD-Aktuell 2023, 01232; Spies ZD-Aktuell 2022, 01364 und Spies ZD-Aktuell 2023, 01050.