

USA: Weitere neue Datenschutzgesetze in Indiana, Montana und Tennessee

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

Die jüngste Flut von Datenschutzgesetzen auf bundesstaatlicher Ebene hält an. Wie mehrfach erläutert, haben Kalifornien, Colorado, Connecticut, Utah, Virginia und Iowa jeweils eigene Datenschutzgesetze für Verbraucher, die entweder bereits in Kraft sind oder im Laufe des Jahres in Kraft treten werden. Nunmehr haben die US-Gesetzgeber in drei weiteren Bundesstaaten – Indiana, Montana und Tennessee – eigene Datenschutzgesetze verabschiedet. Das Verbraucherdatenschutzgesetz von Indiana wurde am 1.5.2023 unterzeichnet, womit Indiana der siebte US-Bundesstaat ist, der ein solches Gesetz verabschiedet hat. Die Parlamente von Montana und Tennessee haben ihrerseits Datenschutzgesetze für diese Bundesstaaten verabschiedet, die voraussichtlich sehr bald von den jeweiligen Gouverneuren unterzeichnet werden. Vor einem Monat wurde wie berichtet (Spies ZD-Aktuell 2023, [01124](#)) Iowa zum sechsten Staat, der ein umfassendes Datenschutzgesetz zum Zweck des Verbraucherschutzes verabschiedet hat.

Indiana

Das neue Gesetz in Indiana ([ICDPA](#)) ist nach erster Einschätzung eher unternehmensfreundlich und ist dem Datenschutzgesetz von Virginia nachgestaltet (ZD-Aktuell 2021, [05047](#)). Es wird erst am 1.1.2026 in Kraft treten, so dass die betroffenen Unternehmen genügend Zeit für ihre Compliance haben.

Geltungsbereich: Der ICDPA gilt für (auch ausländische) Unternehmen, die in Indiana geschäftlich tätig sind oder Produkte oder Dienstleistungen anbieten, die sich an Einwohner von Indiana richten, aber – ähnlich wie in anderen Bundesstaaten mit Ausnahme von Kalifornien – nur dann, wenn das Unternehmen während eines Kalenderjahres die personenbezogenen Daten von 100.000 Einwohnern von Indiana kontrolliert oder verarbeitet oder wenn es die personenbezogenen Daten von mindestens 25.000 Einwohnern von Indiana kontrolliert oder verarbeitet oder wenn es mehr als 50 % seiner Bruttoeinnahmen aus dem Verkauf dieser Daten erzielt. Gemeinnützige Organisationen, staatliche Einrichtungen, höhere Bildungseinrichtungen, öffentliche Versorgungsbetriebe und deren angeschlossene Dienstleistungsunternehmen sowie Einrichtungen, die dem Gramm-Leach-Bliley Act (GLBA) oder dem Health Insurance Portability and Accountability Act (HIPAA) unterliegen, sind vom Gesetz ausgenommen. Weitere enge Ausnahmen gelten je nach Kategorie der verarbeiteten Daten.

- **Verbraucherrechte:** Wie in anderen Bundesstaaten räumt der ICDPA ab seinem Inkrafttreten den Einwohnern des Bundesstaats eine Reihe von Datenschutzrechten ein: das Recht auf Auskunft, auf Datenberichtigung, auf Löschung, auf Datenzugang und das Recht, gezielte Werbung, den Verkauf persönlicher Daten und die Profilerstellung abzulehnen. Kopien der spezifischen Informationen, die als Antwort auf ein Auskunftersuchen zur Verfügung gestellt werden, müssen in einem leicht verwendbaren Format zur Verfügung gestellt werden, dass deren Übermittlung ermöglicht. Die für die Verarbeitung Verantwortlichen müssen auf Anfragen innerhalb von 45 Tagen antworten, können diese Frist jedoch um weitere 45 Tage verlängern, wenn dies nach angemessener Benachrichtigung des Verbrauchers erforderlich ist.

Grundsätze der Verarbeitung: Das ICDPA enthält eine Reihe von allgemeinen „Datenverarbeitungsgrundsätzen“ wie die aus der DS-GVO benannte Zweckbindung und die generelle Pflicht zur Datenminimierung. Die erfassten Unternehmen werden verpflichtet, die Erhebung personenbezogener Daten auf Daten zu beschränken, die „angemessen, relevant und im Hinblick auf die Zwecke, für die diese Daten verarbeitet werden, vernünftigerweise erforderlich sind.“ Die Verwendung und Weitergabe personenbezogener Daten muss ebenfalls „vernünftigerweise notwendig und verhältnismäßig“ zum Zweck der Verarbeitung sein und „angemessen, relevant und begrenzt auf das, was in Bezug auf den spezifischen Zweck notwendig ist.“ Für die Verarbeitung bestimmter Kategorien sensibler Daten wird eine Zustimmung des Betroffenen erfordert.

- **Datenschutz-Folgenabschätzungen (DPIA):** Nach dem ICDPA muss ein für die Verarbeitung Verantwortlicher, wenn er gezielte Werbung (Profiling), die Verarbeitung sensibler Daten oder Verarbeitungstätigkeiten mit erhöhtem Schadensrisiko durchführt, eine Datenschutz-Folgenabschätzung (DPIA) vorweisen. Eine einzelne Datenschutzfolgenabschätzung kann mehrere Verarbeitungsvorgänge abdecken, wenn diese DPIA ähnliche Tätigkeiten umfassen. Ein Verantwortlicher kann sich je nachdem auf eine existierende DPIA berufen, die zur Einhaltung eines anderen Gesetzes oder einer anderen Verordnung erstellt wurde. Der Generalstaatsanwalt von Indiana kann ebenfalls eine Kopie einer DPIA anfordern, wenn diese für eine Untersuchung/ Ermittlung relevant ist.

Durchsetzung: Eine eigene Datenschutzbehörde gibt es auch in Indiana nicht (anders in Kalifornien mit der schon aktiven CPPA – Spies ZD-Aktuell 2021, [05130](#); MMR 2023, [69](#)). Der ICDPA wird durch den Generalstaatsanwalt durchgesetzt. Diese Befugnis ermöglicht es dem Generalstaatsanwalt, zivilrechtliche Ermittlungsaufforderungen zu erlassen, wenn ein begründeter Verdacht auf einen Verstoß besteht, sowie einstweilige Verfügungen und zivilrechtliche Strafen von bis zu 7.500 USD pro Verstoß zu verhängen. Für Verantwortliche und Verarbeiter gilt eine 30-tägige Gnadenfrist zur Behebung des Verstoßes (cure period). Der Generalstaatsanwalt als De-facto-Datenschutzbehörde hat außerdem die Möglichkeit, ist aber nicht verpflichtet, vor Inkrafttreten des Gesetzes auf ihrer Website „eine Liste von Ressourcen für die für die Verarbeitung Verantwortlichen, einschließlich Mustern für Datenschutzhinweise und -erklärungen“ bereitzustellen, um die für die Verarbeitung Verantwortlichen bei ihren Bemühungen um die Einhaltung der neuen Vorschriften zu unterstützen.

- **Montana und Tennessee**

Die Parlamente der Bundesstaaten Tennessee und Montana haben kürzlich ihre eigenen Datenschutzgesetze verabschiedet, die nun den jeweiligen Gouverneuren zur Unterschrift vorliegen.

Das **Verbraucherdatenschutzgesetz von Montana (MCDPA)** wäre nach Unterzeichnung durch den Gouverneur das erste der drei Gesetze, das dann schon am 1.10.2024 in Kraft treten würde. Wie der ICDPA und der TIPA verlangt der MCDPA eigene Datenschutzbewertungen für „Verarbeitungstätigkeiten, die ein erhöhtes Schadensrisiko für einen Verbraucher darstellen.“ Zwar wird auch hier die Kontrolle über personenbezogene Daten als Kriterium für die Anwendbarkeit herangezogen, doch liegt die Schwelle mit 50.000 Verbrauchern in Montana niedriger als bei den meisten anderen Gesetzen in diesem Bereich, was wohl mit der geringen Einwohnerzahl des Bundesstaates zusammenhängt. Das Gesetz von Montana verlangt von den Unternehmen, dass sie die universellen Opt-out-Einstellungen des Browsers (dh Global Privacy Control) anerkennen. Das MCDPA sieht zwar eine 60-tägige Gnadenfrist für die Behebung von Mängeln vor, die Bestimmung läuft jedoch schnell am 1.4.2026 aus; die Generalstaatsanwaltschaft des Bundesstaats ist für die

Durchsetzung zuständig. Die Definition des Begriffs „Einwilligung“ stellt außerdem klar, dass „eine unter Verwendung von Dark Pattern erlangte Zustimmung“ nicht ausreicht. Gedacht ist Lockvogel-Taktik getarnte Werbung, versteckte Kosten, Freundschaftsspam, Verhinderung von Preisvergleichen und sonstige Irreführung – dh Designelemente, die Besucher der Webseite absichtlich verwirren, in die Irre führen oder täuschen, damit sie unbeabsichtigte und möglicherweise für sie schädliche Entscheidungen treffen.

Der neue **Tennessee Information Protection Act (TIPA)** würde seinerseits nach Unterschrift am 1.12.25 in Kraft treten. Viele seiner Bestimmungen spiegeln die bereits erlassenen bundestaatlichen Gesetze wider, wie etwa:

Die Definition der Anwendbarkeit auf der Grundlage der Kontrolle über die personenbezogenen Daten von Verbrauchern (Schwellenwerte) und der Einnahmen aus dem wie in anderen Bundesstaaten weit definierten „Verkauf“ (sale) personenbezogener Daten;

- der Übertragung der ausschließlichen Durchsetzungsbefugnis an den Generalstaatsanwalt des Bundesstaats (keine eigene Datenschutzbehörde);

Ausnahmen für personenbezogene Daten, die unter die Spezialgesetze HIPAA, GLBA, FERPA und den Children's Online Privacy Protection Act (COPPA) fallen;

- Datenzugang und Antwort auf Anfragen zu den Rechten der Betroffenen innerhalb von 45 Tagen;

erforderliche DPIAs für bestimmte Verarbeitungstätigkeiten.

- Eine interessante Neuerung des TIPA im Vergleich zu anderen Gesetzen ist ein Passus, dass erfasste Verantwortliche und Auftragsverarbeiter „ein schriftliches Datenschutzprogramm erstellen, pflegen und einhalten müssen, das dem Datenschutzrahmen (Privacy Framework) des National Institute of Standards and Technology entspricht.“ Dieses bekannte NIST Privacy Framework ist eigentlich eine freiwillige Maßnahme. Sie müssen dann das Programm innerhalb eines Jahres nach jeder Änderung des NIST-Rahmens aktualisieren.

Weiterführende Links

S. jew. 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 2022, [01191](#); ZD-Aktuell 2022, [01392](#); ZD-Aktuell 2022, [01396](#) und ZD-Aktuell 2023, [01010](#); ZD-Aktuell 2023, [01050](#); ZD-Aktuell 2023, [01124](#) sowie MMR-Aktuell 2020, [426334](#) und MMR 2022, [839](#) und MMR 2023, [69](#).