Datenschutz in den USA

4.2

Überraschende Einblicke für deutsche Unternehmen

Autor
Julian Banse

Datenschutz und die USA – auf den ersten Blick keine offensichtliche Verbindung. Viele denken bei den Vereinigten Staaten an wirtschaftliche Freiheit, Technologie-Giganten und Innovation, aber kaum an datenschutzrechtliche Vorschriften.

Tatsächlich gibt es in den USA Datenschutzgesetze, die nicht zentral auf Bundesebene geregelt sind, sondern von den einzelnen Bundesstaaten. Das bedeutet für Unternehmen, die auf dem US-Markt tätig sind: Sie müssen individuell prüfen, welche Regelungen in den jeweiligen Bundesstaaten gelten – von Kalifornien bis Texas.

Überraschend ist, dass selbst wirtschaftsliberale Staaten wie Texas eigene Datenschutzgesetze eingeführt haben. Während Texas im Vergleich zu Kalifornien weniger strikte Datenschutzvorschriften hat, gibt es dennoch relevante Bestimmungen, insbesondere für sensible Daten. Der Schutz personenbezogener Informationen gewinnt zunehmend an Bedeutung, und auch Verbraucherinnen und Verbraucher erhalten mehr Rechte, darunter die Möglichkeit, der Nutzung ihrer Daten zu widersprechen.

Für deutsche Unternehmen, die an die einheitlichen Vorgaben der EU-Datenschutz-Grundverordnung (DSGVO) gewöhnt sind, stellt dieser föderale Ansatz eine Herausforderung dar. Während die DSGVO einen kohärenten Rahmen vorgibt, gleicht der Datenschutz in den USA einem Mosaik verschiedener Gesetze und Bestimmungen.
2025 wird diese Komplexität weiter zunehmen: Neue Datenschutzgesetze treten in Staaten wie Maryland, Minnesota und Tennessee in Kraft. Diese beinhalten spezifische Anforderungen an Datenminimierung und verpflichten Unternehmen zu detaillierten Bewertungen der Datenverarbeitung.

Texas als Fallbeispiel für Datenschutzgesetze in den USA

Ein aufschlussreiches Beispiel für Datenschutzgesetze auf Staatsebene ist Texas. Der Bundesstaat verabschiedete 2023 das Texas Data Privacy and Security Act (TDPSA), das am 1. Juli 2024 in Kraft trat. Dies zeigt, dass Datenschutz auch in Staaten mit wirtschaftsliberaler Prägung als relevantes Regulierungsgebiet anerkannt wird.
Allerdings ist das TDPSA weniger umfassend als die DSGVO oder das kalifornische CCPA/CPRA. Während die DSGVO in vielen Fällen eine vorherige Einwilligung (Opt-in) erfordert, basiert das TDPSA auf einem Opt-out-Prinzip: Verbraucherinnen und Verbraucher müssen aktiv widersprechen, wenn sie der Nutzung ihrer Daten nicht zustimmen. Dennoch setzt Texas auf eine strenge Durchsetzung seiner Datenschutzgesetze, insbesondere bei Verstößen gegen den Schutz biometrischer Daten.

So wurde Meta wegen der unrechtmäßigen Nutzung biometrischer Daten mit einer Strafe von 1,4 Milliarden US-Dollar belegt. Diese Strafe resultierte allerdings nicht aus dem TDPSA, sondern aus dem bereits seit 2009 bestehenden Texas Biometric Privacy Act. Dies verdeutlicht, dass Datenschutzverstöße in den USA durchaus ernsthafte finanzielle Konsequenzen nach sich ziehen können – allerdings abhängig von der spezifischen Rechtsgrundlage und dem betroffenen Bundesstaat.

Kalifornien nahm mit dem 2018 verabschiedeten California Consumer Privacy Act (CCPA) eine Vorreiterrolle ein. Der Erfolg des CCPA zeigte, dass Datenschutzgesetze Verbraucherinnen und Verbraucher schützen und Unternehmen klare Richtlinien bieten können. Dieser Impuls führte auch in Texas dazu, Datenschutz als wirtschaftlich relevante Frage zu betrachten.

Die politische Dimension des Datenschutzes in den USA

Viele deutsche Beobachterinnen und Beobachter könnten vermuten, dass Datenschutzgesetze unter einer neuen US-Regierung zurückgenommen werden könnten. Doch auf Staatsebene ist das unwahrscheinlich, da der Datenschutz in den Zuständigkeitsbereich der Bundesstaaten fällt. Die meisten dieser Gesetze bleiben unabhängig von der Bundesregierung bestehen.

Darüber hinaus existieren in den USA bereits seit Jahren bundesweite Datenschutzvorschriften für spezifische Bereiche, etwa der Health Insurance Portability and Accountability Act (HIPAA) für Gesundheitsdaten oder der Gramm-Leach-Bliley Act (GLBA) für Finanzdaten. Diese Vorschriften zeigen, dass Datenschutz in den USA nicht ausschließlich eine Angelegenheit der Bundesstaaten ist.

Worauf deutsche Unternehmen achten müssen

Ein zentrales Merkmal der US-amerikanischen Regelungen ist, dass Datenschutzgesetze je nach Bundesstaat unterschiedlich ausgestaltet sind. Unternehmen müssen daher prüfen, in welchen Staaten sie tätig sind und welche Vorschriften für sie gelten.

Ein weiterer wichtiger Punkt ist die Differenzierung zwischen Verbraucherdaten und Geschäftsdaten. Viele US-Datenschutzgesetze wie der CCPA oder das TDPSA betreffen primär personenbezogene Daten von Verbraucherinnen und Verbrauchern. In einigen Bundesstaaten gibt es jedoch Regelungen, die auch für B2B-Daten relevant sein können, etwa im Bereich biometrischer Daten.

Drei zentrale Maßnahmen für deutsche Unternehmen:

1. Klarheit über die Anwendbarkeit:
   Unternehmen sollten prüfen, ob ihre Tätigkeiten im jeweiligen Staat unter die lokalen Datenschutzgesetze fallen. Diese definieren oft spezifische Schwellenwerte, z. B. zur Anzahl betroffener Personen oder zum Umsatz.

2. Unterscheidung zwischen Verbraucherdaten und B2B-Daten:
   Es ist essenziell, die eigenen Datenflüsse zu kategorisieren. Datenschutzgesetze wie der CCPA oder das TDPSA betreffen in erster Linie Verbraucherdaten, können jedoch auch bestimmte Geschäftsdaten einschließen.

3. Prozesse für Datenanfragen etablieren:
   Viele US-Datenschutzgesetze verpflichten Unternehmen, Anfragen von Betroffenen, z. B. zu Auskunft, Korrektur oder Löschung, innerhalb einer bestimmten Frist zu bearbeiten. Dafür sollten klare interne Prozesse sowie leicht zugängliche Kontaktpunkte geschaffen werden.

Für deutsche Unternehmen bedeutet dies, dass ein detailliertes Verständnis der jeweiligen Datenschutzregelungen der Bundesstaaten notwendig ist, um rechtlich sicher und effizient zu agieren. Die US-Datenschutzlandschaft ist zwar komplex, kann jedoch mit sorgfältiger Planung und klaren Prozessen erfolgreich bewältigt werden.