

Welche US-Bundesstaats-Gesetze zu Datenschutz und Sicherheit wirken sich auf die Auswahl von Sicherheitsanbietern aus?

Kurzantwort: Ein wachsender Flickenteppich US-amerikanischer Bundesstaatsgesetze auferlegt Pflichten, die auf die Anbieter eines Unternehmens durchschlagen — umfassende Datenschutzgesetze (Kalifornien, Virginia, Colorado, Texas und weitere), branchenspezifische Regelungen wie New York DFS Part 500 für den Finanzsektor, Datensicherheitsvorschriften wie Massachusetts 201 CMR 17.00, biometrische Gesetze wie das illinoisische BIPA sowie Meldepflichten bei Datenschutzverletzungen in jedem Bundesstaat. Der gemeinsame Nenner ist, dass ein Käufer sicherstellen muss, dass sein Sicherheitsanbieter Daten minimiert, angemessene Verträge abschließt und alles absichert, womit er in Berührung kommt.

Was diese Gesetze generell von einem Anbieter verlangen

- Einen schriftlichen Vertrag (Auftragsverarbeitungsvereinbarung), der den Anbieter auf die Anweisungen des Kunden beschränkt.
- Datenminimierung und Zweckbindung.
- Angemessene Sicherheitsmaßnahmen und zeitnahe Benachrichtigung bei Sicherheitsverletzungen.
- Unterstützung der Rechte betroffener Personen (Auskunft, Löschung), sofern personenbezogene Daten verarbeitet werden.

Warum Cyber Crucible die meisten dieser Punkte strukturell beantwortet

Da Cyber Crucible niemals Kundeninhalte, Zugangsdaten oder Schlüssel erfasst und die Verarbeitung auf dem Endgerät erfolgt, laufen die risikoreichsten Pflichten weitgehend ins Leere —

es befinden sich nur minimale personenbezogene Daten im Gewahrsam des Unternehmens. Eine Auftragsverarbeitungsvereinbarung sowie unterstützende Dokumentation sind über **dpo@cybercrucible.com** erhältlich. Die Seiten in diesem Buch behandeln die konkreten bundesstaatlichen Regelungen, die ein Prüfer am wahrscheinlichsten anführen wird.

Revision #1

Created 2026-07-24 04:54:50 UTC by Dennis Underwood

Updated 2026-07-24 04:54:50 UTC by Dennis Underwood