US-amerikanische Leitfäden zum Anbieterrisiko nach Bundesstaat und Branche

Wie Cyber Crucible die Datenschutz- und Sicherheitsgesetze der US-Bundesstaaten sowie branchenspezifische Vorschriften aus Sicht der Anbieterauswahl unterstützt — New York DFS, Kalifornien, Texas, Virginia, Colorado, Massachusetts, Illinois und Pennsylvania. Legt klar dar, was Cyber Crucible vorweisen kann und was nicht.

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 illinoische 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.

Wie unterstützt Cyber Crucible die Cybersicherheitsanforderungen von New York DFS Part 500?

Kurzantwort: Für ein Finanzinstitut, das unter New York DFS Part 500 (23 NYCRR 500) fällt, unterstützt Cyber Crucible mehrere erforderliche Kontrollen – Multi-Faktor-Authentifizierung, Verschlüsselung, Zugriffskontrollen und Incident Response – und reduziert gleichzeitig das Drittanbieterrisiko, da es die durch die Vorschrift geschützten nichtöffentlichen Informationen niemals erhebt. Cyber Crucible ist im Sinne der Vorschrift ein Drittanbieter (Third-Party Service Provider), keine erfasste Einrichtung (Covered Entity) selbst.

Unterstützte Kontrollen

- **Zugriffskontrollen und MFA** für das Management-Dashboard, abgesichert durch starke Authentifizierung.
- **Verschlüsselung** von Daten während der Übertragung und im Ruhezustand.
- **Incident Response** im Rahmen eines dokumentierten Breach-Response-Prozesses, mit einer vertraglich zugesicherten Benachrichtigungsfrist – zur Unterstützung der 72-Stunden-Meldepflicht der erfassten Einrichtung gegenüber der DFS.
- **Reduzierung des Drittanbieterrisikos** durch Datenminimierung: Es werden keine nichtöffentlichen Informationen erhoben.

Die ehrliche Grenze

Die Verpflichtungen von Part 500 – Benennung eines CISO, Risikobewertung, die jährliche Zertifizierung – liegen bei der erfassten Einrichtung. Cyber Crucible liefert Kontrollnachweise für die Third-Party-Service-Provider-Richtlinie der Einrichtung (500.11). Cyber Crucible ist keine erfasste Einrichtung und besitzt keine „Zertifizierung“ nach Part 500. Nachweise werden im Rahmen einer NDA bereitgestellt.

Wie unterstützt Cyber Crucible die Anbieterpflichten nach dem kalifornischen CCPA/CPRA?

Kurzantwort: Cyber Crucible agiert als Dienstleister ("service provider") im Sinne des CCPA/CPRA und ist vertraglich verpflichtet, Daten ausschließlich nach den Anweisungen des Kunden zu verarbeiten; personenbezogene Daten werden weder verkauft noch weitergegeben ("shared"). Da im Wesentlichen von vornherein keine personenbezogenen Daten erfasst werden, haben die Verbraucherrechte und Datenverarbeitungspflichten in der Obhut von Cyber Crucible kaum Angriffsfläche.

Wie die Ausrichtung erfolgt

- **Rolle als Dienstleister** im Rahmen eines schriftlichen Vertrags, der eine sekundäre Nutzung untersagt.
- **Kein Verkauf oder Weitergabe** personenbezogener Daten.
- **Unterstützung der Verbraucherrechte** (Zugriff, Löschung), da keine personenbezogenen Daten vorgehalten werden, die andernfalls durchsucht oder gelöscht werden müssten.

Hinweise zur Anbieterauswahl

Der California Privacy Rights Act hat die vertraglichen Anforderungen an Dienstleister verschärft und zusätzliche Pflichten für sensible personenbezogene Daten ("sensitive personal information") eingeführt; Cyber Crucible erfasst keine sensiblen personenbezogenen Daten. Eine CCPA-konforme Datenverarbeitungsvereinbarung ist auf Anfrage erhältlich.

Wie unterstützt Cyber Crucible den Texas Data Privacy and Security Act (TDPSA)?

Kurze Antwort: Im Rahmen des Texas Data Privacy and Security Act fungiert Cyber Crucible als Auftragsverarbeiter, gebunden durch eine Vereinbarung zur Auftragsverarbeitung, und unterstützt den Verantwortlichen bei Sicherheits- und Betroffenenanfragen. Durch das Design zur Datenminimierung – es werden keine Kundeninhalte, Zugangsdaten oder Schlüssel erfasst – gibt es nur wenige personenbezogene Daten zu verarbeiten, was die Pflichten des Verantwortlichen vereinfacht.

Wie die Ausrichtung erfolgt

- **Rolle als Auftragsverarbeiter** im Rahmen einer TDPSA-konformen Vereinbarung zur Auftragsverarbeitung.
- **Unterstützung bei Sicherheit und Datenschutzverletzungen** gegenüber dem Verantwortlichen.
- **Minimaler Umfang personenbezogener Daten**, wodurch das Risiko und der Reaktionsaufwand reduziert werden.

Hinweise zur Anbieterauswahl

Der TDPSA gilt umfassend für Unternehmen, die in Texas tätig sind. Da Cyber Crucible im Wesentlichen keine personenbezogenen Daten verarbeitet und vor Ort (on-premises) eingesetzt werden kann, unterstützt es sowohl die Sicherheits- als auch die Datenresidenz-Präferenzen, die ein Käufer in Texas möglicherweise hat. Dokumentation ist auf Anfrage erhältlich.

Wie unterstützt Cyber Crucible das Datenschutzgesetz für Verbraucher von Virginia (VCDPA)?

Kurze Antwort: Cyber Crucible unterstützt die VCDPA-Pflichten eines Verantwortlichen als Auftragsverarbeiter im Rahmen einer Auftragsverarbeitungsvereinbarung und hilft bei Datensicherheitspflichten sowie bei Anfragen zu Verbraucherrechten. Durch das Design ohne Datenerfassung hält das Unternehmen kaum bis gar keine personenbezogenen Daten vor, was die Verarbeitungs- und Reaktionslast des Verantwortlichen gering hält.

Wie die Ausrichtung erfolgt

- **Pflichten als Auftragsverarbeiter** — Unterstützung bei Sicherheit, Verletzungsmeldungen und Datenschutz-Folgenabschätzungen.
- **Datenminimierung** — keine Erfassung von Kundendaten, Anmeldeinformationen oder Schlüsseln.
- **Zweckbindung** — Verarbeitung ausschließlich nach Anweisung des Verantwortlichen.

Hinweise zur Anbieterauswahl

Das VCDPA verlangt von Verantwortlichen, Auftragsverarbeiter vertraglich zu binden und für risikoreichere Verarbeitungen Bewertungen durchzuführen; der minimale Umfang personenbezogener Daten vereinfacht beides. Eine Auftragsverarbeitungsvereinbarung ist auf Anfrage erhältlich.

Wie unterstützt Cyber Crucible den Colorado Privacy Act (CPA)?

Kurzantwort: Cyber Crucible agiert als Auftragsverarbeiter im Sinne des Colorado Privacy Act, gebunden durch eine Auftragsverarbeitungsvereinbarung, die es verpflichtet, den Anweisungen des Verantwortlichen zu folgen, bei der Sicherheit zu unterstützen und die Rechte der Verbraucher zu fördern. Da so gut wie keine personenbezogenen Daten erfasst werden, haben die meisten CPA-Verpflichtungen nur minimale Relevanz für den Verwahrungsbereich.

Wie die Ausrichtung erfolgt

- **Rolle als Auftragsverarbeiter** mit vertraglich begrenzter Verarbeitung.
- **Unterstützung bei der Sicherheit** und bei Vorfällen für den Verantwortlichen.
- **Unterstützung der Verbraucherrechte**, indem keine personenbezogenen Daten gespeichert werden, die andernfalls in den Anwendungsbereich fallen würden.

Hinweise zur Anbieterauswahl

Der CPA verlangt Datenschutz-Folgenabschätzungen für risikoreichere Verarbeitungen und die Einhaltung universeller Opt-out-Mechanismen auf Ebene des Verantwortlichen; der minimale Datenumfang hält die Anbieterseite einfach. Dokumentation ist auf Anfrage erhältlich.

Wie unterstützt Cyber Crucible Massachusetts 201 CMR 17.00 (WISP)?

Kurze Antwort: Massachusetts 201 CMR 17.00 verlangt von jeder Organisation, die personenbezogene Daten eines Einwohners von Massachusetts verarbeitet, ein schriftliches Informationssicherheitsprogramm (Written Information Security Program) mit spezifischen Schutzmaßnahmen zu unterhalten. Cyber Crucible unterstützt das WISP eines Kunden durch Verschlüsselung, Zugriffskontrolle und Überwachung – und verringert die eigene Risikoexposition des Kunden, da Cyber Crucible im Wesentlichen keine personenbezogenen Daten vorhält.

Wie die Ausrichtung erfolgt

- **Technische Schutzmaßnahmen** — Verschlüsselung bei der Übertragung und im Ruhezustand, starke Authentifizierung und Zugriffskontrolle entsprechen den Anforderungen der Regulierung an Computersysteme.
- **Endpunktschutz und Überwachung** unterstützen die Anforderung an "angemessen aktuelle" Sicherheitssoftware.
- **Minimaler Datenfußabdruck** — die Verpflichtungen der Regulierung beziehen sich auf personenbezogene Daten; Cyber Crucible erhebt diese nicht.

Hinweise zur Anbieterauswahl

201 CMR 17.00 verlangt außerdem die vertragliche Überwachung von Drittanbietern. Eine Auftragsverarbeitungsvereinbarung sowie Kontrolldokumentationen sind auf Anfrage erhältlich.

Wie geht Cyber Crucible mit dem Illinois BIPA und Bedenken zu biometrischen Daten um?

Kurze Antwort: Cyber Crucible erfasst, speichert oder verarbeitet keine biometrischen Identifikatoren oder biometrischen Informationen und schafft somit nicht die Art von Risiko, die der Illinois Biometric Information Privacy Act (BIPA) adressieren soll. Es liegen keine biometrischen Daten in seiner Obhut, für die im Rahmen des Gesetzes eine Einwilligung erforderlich wäre oder die aufbewahrt oder vernichtet werden müssten.

Warum es keine BIPA-Relevanz gibt

- **Keine Erfassung biometrischer Daten.** Cyber Crucible analysiert Prozess- und Speicherverhalten, nicht Gesichter, Fingerabdrücke oder andere biometrische Identifikatoren.
- **Keine sensiblen personenbezogenen Daten.** Allgemeiner betrachtet erfasst Cyber Crucible keine biometrischen, gesundheitsbezogenen oder sonstigen besonderen Kategorien personenbezogener Daten.

Hinweise zur Anbieterauswahl

BIPA ist insbesondere wegen seines privaten Klagerechts und der gesetzlich festgelegten Schadensersatzansprüche bemerkenswert, weshalb Anbieter biometrischer Daten besonders genau geprüft werden; Cyber Crucible fällt jedoch nicht in diese Kategorie. Dies kann in der auf Anfrage verfügbaren Dokumentation zur Daten-Governance bestätigt werden.

Wie unterstützt Cyber Crucible das Datenschutzverletzungs-Meldegesetz von Pennsylvania?

Kurzantwort: Das Breach of Personal Information Notification Act von Pennsylvania (73 P.S. §2301, geändert durch Act 151 von 2022) verlangt, betroffene Einwohner – und bei größeren Sicherheitsverletzungen auch den Attorney General – nach einer Verletzung geschützter personenbezogener Informationen zu benachrichtigen. Cyber Crucible unterstützt die Verpflichtungen einer Organisation in Pennsylvania, indem es selbst keine personenbezogenen Informationen speichert und zeitnahe, beweiskräftige Vorfallsinformationen bereitstellt, damit die Organisation ihre gesetzlichen Fristen einhalten kann. Cyber Crucible hat seinen Hauptsitz in Pittsburgh, Pennsylvania.

Wie dies übereinstimmt

- **Keine gespeicherten personenbezogenen Informationen** — die Organisation behält die Kontrolle über jede Feststellung einer Sicherheitsverletzung und Benachrichtigung; es gibt keinen anbieterseitigen Datensatz, der verloren gehen könnte.
- **Zeitnahe Vorfallsinformationen** — der Vorfallreaktionsprozess ist so gestaltet, dass die Organisation die Fakten erhält, die sie benötigt, um innerhalb der vorgeschriebenen Frist zu benachrichtigen.
- **Erweiterte Definitionen berücksichtigt** — die Änderung von 2022 erweiterte die geschützten personenbezogenen Informationen (einschließlich medizinischer Daten und bestimmter Kombinationen von Zugangsdaten); durch den Verzicht auf Datenerfassung bleibt Cyber Crucible außerhalb dieser Kategorien.

Hinweise zur Anbieterauswahl

Bei Sicherheitsverletzungen, die mehr als 500 Einwohner von Pennsylvania betreffen, sieht die Änderung eine zusätzliche Benachrichtigung des Attorney General vor; die Aufgabe von Cyber Crucible besteht darin, diese Verpflichtung zu unterstützen, nicht sie festzustellen. Detaillierte Informationen zur Vorfallsbehandlung sind unter NDA verfügbar.

Wie unterstützt Cyber Crucible den Connecticut Data Privacy Act (CTDPA)?

Kurze Antwort: Cyber Crucible fungiert im Rahmen des Connecticut Data Privacy Act als Auftragsverarbeiter, gebunden an eine Auftragsverarbeitungsvereinbarung, um nach den Anweisungen des Verantwortlichen zu handeln und bei Sicherheits- und Betroffenenanfragen zu unterstützen. Da keine Kundeninhalte, Zugangsdaten oder Schlüssel erfasst werden, haben die meisten CTDPA-Pflichten in dessen Verwahrungsbereich kaum Berührungspunkte.

Wie es sich einfügt

- **Rolle als Auftragsverarbeiter** mit vertraglich begrenzter Verarbeitung und einer Unterstützungspflicht gegenüber dem Verantwortlichen.
- **Datenminimierung** — keine Erfassung von Kundeninhalten, Zugangsdaten oder Schlüsseln.
- **Unterstützung bei Sicherheitsfragen und Datenschutzverletzungen** gegenüber dem Verantwortlichen.

Hinweise zur Anbieterauswahl

Der CTDPA verlangt, dass Verantwortliche Auftragsverarbeiter vertraglich binden, universelle Opt-out-Signale respektieren und Bewertungen für Verarbeitungen mit höherem Risiko durchführen; der minimale Umfang personenbezogener Daten hält die Anbieterseite einfach. Eine Auftragsverarbeitungsvereinbarung ist erhältlich unter **dpo@cybercrucible.com**.

Wie unterstützt Cyber Crucible den Utah Consumer Privacy Act (UCPA)?

Kurzantwort: Cyber Crucible fungiert im Rahmen des Utah Consumer Privacy Act als Auftragsverarbeiter und folgt dabei den dokumentierten Anweisungen des Verantwortlichen im Rahmen einer Datenverarbeitungsvereinbarung. Durch das Design ohne Datenerfassung befinden sich nur wenige personenbezogene Daten im Besitz des Unternehmens, auf die die Verarbeitungs- und Offenlegungsregeln des UCPA überhaupt Anwendung finden könnten.

Wie die Ausrichtung erfolgt

- **Rolle als Auftragsverarbeiter** im Rahmen eines Vertrags mit dem Verantwortlichen.
- **Datenminimierung** — es werden keine Kundendaten, Zugangsdaten oder Schlüssel erfasst.
- **Sicherheitsmaßnahmen** — Verschlüsselung, Zugriffskontrolle und Endpoint-Prävention.

Hinweise zur Anbieterauswahl

Der UCPA gilt im Allgemeinen als geschäftsfreundlicher als einige vergleichbare Gesetze anderer Bundesstaaten, verlangt aber dennoch Verträge mit Auftragsverarbeitern sowie angemessene Sicherheitsmaßnahmen; der minimale Datenfußabdruck unterstützt beides. Entsprechende Dokumentation ist auf Anfrage erhältlich.

Wie unterstützt Cyber Crucible den Oregon Consumer Privacy Act (OCPA)?

Kurzantwort: Cyber Crucible fungiert im Rahmen des Oregon Consumer Privacy Act als Auftragsverarbeiter und ist vertraglich verpflichtet, ausschließlich nach den Anweisungen des Verantwortlichen zu verarbeiten sowie bei Sicherheits- und Verbraucherrechtsanfragen zu unterstützen. Da im Wesentlichen keine personenbezogenen Daten erhoben werden, haben die meisten OCPA-Pflichten in seinem Verantwortungsbereich nur minimale Berührungspunkte.

Wie die Ausrichtung erfolgt

- **Pflichten des Auftragsverarbeiters** — Unterstützung bei Sicherheitsvorfällen, Reaktion auf Datenschutzverletzungen und Datenschutz-Folgenabschätzungen.
- **Datenminimierung** — es werden keine Kundeninhalte, Zugangsdaten oder Schlüssel erhoben.
- **Zweckbindung** — die Verarbeitung erfolgt ausschließlich nach Anweisung des Verantwortlichen.

Hinweise zur Anbieterauswahl

Das Gesetz Oregons ist bemerkenswert wegen seiner weiter gefassten Definition personenbezogener Daten und spezifischer Verbraucherrechte in Bezug auf namentlich genannte Dritte; der minimale Datenfußabdruck sorgt dafür, dass das Anbieterrisiko gering bleibt. Eine Auftragsverarbeitungsvereinbarung (Data Processing Agreement) ist auf Anfrage erhältlich.

Wie unterstützt Cyber Crucible den Washington My Health My Data Act?

Kurze Antwort: Der Washington My Health My Data Act regelt „Verbrauchergesundheitsdaten“ (consumer health data) umfassend und sieht ein privates Klagerecht vor, sodass Anbieter, die mit solchen Daten in Berührung kommen, einem realen Risiko ausgesetzt sind. Cyber Crucible erfasst keine Verbrauchergesundheitsdaten – es analysiert Prozess- und Speicherverhalten auf dem Endpunkt und nimmt niemals Kundeninhalte auf – und schafft somit nicht die Erfassungs- und Einwilligungsfläche, die das Gesetz regeln soll.

Warum es kaum Angriffsfläche gibt

- **Keine Erfassung von Verbrauchergesundheitsdaten.** Cyber Crucible sammelt keine gesundheitsbezogenen Inhalte, Identifikatoren oder Rückschlüsse.
- **Lokale Verarbeitung.** Die Analyse verbleibt auf dem Gerät; es gibt keinen beim Anbieter gespeicherten Gesundheitsdatensatz.
- **Kein Verkauf oder Weitergabe** personenbezogener Daten jeglicher Art.

Hinweise zur Anbieterauswahl

Das private Klagerecht des Gesetzes rückt Anbieter von Gesundheitsdaten in den Fokus der Prüfung; Cyber Crucible fällt jedoch nicht in diese Kategorie. Dies kann in der auf Anfrage verfügbaren Dokumentation zur Daten-Governance bestätigt werden. Dies stellt keine Rechtsberatung dar – eine erfasste Stelle sollte ihre eigenen Verpflichtungen mit rechtlichem Beistand prüfen.

Wie unterstützt Cyber Crucible die neueren US-Bundesstaaten-Datenschutzgesetze von 2025–2026?

Kurzantwort: Im Verlauf von 2025 und 2026 traten in mehreren US-Bundesstaaten umfassende Datenschutzgesetze in Kraft — darunter New Jersey, Delaware, Iowa, Nebraska, New Hampshire, Tennessee, Minnesota, Maryland sowie ab 2026 Indiana, Kentucky und Rhode Island. Sie folgen einer gemeinsamen Struktur, und die Rolle von Cyber Crucible als Auftragsverarbeiter sowie das Konzept der Nicht-Erfassung unterstützen alle diese Gesetze auf dieselbe Weise: geringer Bestand an personenbezogenen Daten, vertraglich begrenzte Verarbeitung und angemessene Sicherheit.

Die gemeinsame Struktur dieser Gesetze

- Ein vorgeschriebener Auftragsverarbeitungsvertrag, der den Anbieter auf die Weisungen des Verantwortlichen beschränkt.
- Pflichten zur Datenminimierung und Zweckbindung.
- Verbraucherrechte (Auskunft, Löschung, Widerspruch), zunehmend mit universellen Opt-out-Signalen.
- Angemessene Sicherheitsmaßnahmen und Benachrichtigung bei Datenschutzverletzungen.

Warum eine Antwort das gesamte Spektrum abdeckt

Da Cyber Crucible niemals Kundeninhalte, Zugangsdaten oder Schlüssel erfasst und die Verarbeitung auf dem Endpunkt erfolgt, gibt es für die zwischen den Bundesstaaten variierenden Pflichten — die sich meist auf den Umgang mit und die Offenlegung von personenbezogenen Daten beziehen — kaum Anknüpfungspunkte. Eine einzige, einheitliche Auftragsverarbeitungsvereinbarung deckt das gesamte Spektrum ab. Bemerkenswert ist das

Gesetz von Maryland mit seinem strengeren Standard zur Datenminimierung, den das Nicht-Erfassungskonzept gut unterstützt.

Die ehrliche Grenze

Schwellenwerte der Bundesstaaten und Inkrafttretensdaten ändern sich, und dies stellt keine Rechtsberatung dar; ein Verantwortlicher sollte prüfen, welche Gesetze auf ihn anwendbar sind. Cyber Crucible besitzt keine „Zertifizierung" eines Bundesstaates — es unterstützt die Pflichten des Verantwortlichen. Dokumentation ist erhältlich unter **dpo@cybercrucible.com**.