Internationale Leitfäden zum Anbieterrisiko

Länderspezifische Antworten zum Lieferantenrisiko über die bestehenden Leitfäden für den Golf, Afrika und EU/UK hinaus — Kanada, Australien, Indien, Singapur, Japan, Brasilien, Schweiz, Neuseeland, Südkorea und Türkei. Legt klar dar, was Cyber Crucible vorhält und wie die Architektur jedes Regelwerk unterstützt.

Erfüllt Cyber Crucible die Anforderungen von Kanadas PIPEDA und dem Gesetz 25 von Québec?

Kurze Antwort: Cyber Crucible unterstützt die Verpflichtungen eines kanadischen Unternehmens im Rahmen von PIPEDA und dem Gesetz 25 von Québec in erster Linie dadurch, dass die Verarbeitung auf dem Endpunkt erfolgt und keine Kundeninhalte, Zugangsdaten oder Schlüssel erfasst werden – sodass sich nur wenige personenbezogene Informationen im Verantwortungsbereich befinden, die geschützt, offengelegt oder übermittelt werden müssten. Es agiert als Dienstanbieter unter der Kontrolle des Unternehmens, wobei eine Auftragsverarbeitungsvereinbarung zur Verfügung steht.

Wie es sich einfügt

- **Rechenschaftspflicht und Schutzmaßnahmen.** Starke Verschlüsselung, Zugriffskontrolle und lokale Verarbeitung unterstützen den Grundsatz der Sicherheitsvorkehrungen von PIPEDA.
- **Besonderheiten des Gesetzes 25.** Die stufenweisen Reformen in Québec führten Meldepflichten bei Datenschutzverletzungen, Datenschutz durch Voreinstellung (Privacy-by-Default) sowie Regeln für Übermittlungen außerhalb Québecs ein; das Design ohne Datenerfassung mit Möglichkeit zur lokalen Verarbeitung unterstützt Präferenzen zur Datenresidenz und begrenzt das Risiko bei Übermittlungen.
- **Unterstützung bei Vorfällen.** Zeitnahe Informationen zu Vorfällen helfen dem Unternehmen, die Meldepflichten von PIPEDA und dem Gesetz 25 zu erfüllen.

Die ehrliche Grenze

Die Compliance liegt in der Verantwortung des Unternehmens; Cyber Crucible ist eine unterstützende Kontrolle und ein Auftragsverarbeiter. Es verfügt über keine kanadische Zertifizierung. Eine Auftragsverarbeitungsvereinbarung sowie entsprechende Dokumentation sind über **dpo@cybercrucible.com** erhältlich.

Erfüllt Cyber Crucible den australischen Privacy Act und die APPs?

Kurze Antwort: Cyber Crucible unterstützt die Verpflichtungen einer australischen Organisation im Rahmen des Privacy Act 1988 und der Australian Privacy Principles durch Datenminimierung — es werden keine Kundeninhalte, Zugangsdaten oder Schlüssel erfasst — sowie durch lokale Verarbeitung auf dem Endgerät. Dies unterstützt unmittelbar APP 11 (Sicherheit personenbezogener Informationen) und begrenzt die Risiken im Zusammenhang mit grenzüberschreitender Offenlegung gemäß APP 8.

Wie die Ausrichtung erfolgt

- **APP 11 Sicherheit** — Verschlüsselung, Zugriffskontrolle und autonomer Endpunktschutz.
- **APP 8 grenzüberschreitend** — Die On-Premises-Bereitstellung hält personenbezogene Informationen dort in Australien, wo dies erforderlich ist; keine Kundeninhalte werden zur Sicherheitsverarbeitung ins Ausland übertragen.
- **Unterstützung bei Datenschutzverletzungen** — Vorfallinformationen zur Unterstützung der Verpflichtungen im Rahmen des Notifiable Data Breaches-Schemas.

Hinweise zur Anbieterauswahl

Das australische Sanktionssystem für schwerwiegende oder wiederholte Datenschutzverstöße wurde erheblich verschärft, wodurch die Prüfung von Anbietern strenger geworden ist. Der minimale Datenfußabdruck hält das Risiko auf Anbieterseite gering. Dokumentation ist auf Anfrage erhältlich.

Erfüllt Cyber Crucible die Anforderungen des indischen Digital Personal Data Protection Act (DPDP)?

Kurze Antwort: Cyber Crucible unterstützt die Pflichten eines Data Fiduciary im Rahmen des indischen Digital Personal Data Protection Act, indem es als Datenverarbeiter (Data Processor) fungiert, der im Wesentlichen keine personenbezogenen Daten erhebt und die Verarbeitung auf dem Endpunkt durchführt. Da Kundeninhalte niemals erfasst werden, ist die Angriffsfläche für die Pflichten zu Einwilligung, Zweckbindung und Löschung in seinem Verantwortungsbereich minimal.

Wie die Ausrichtung erfolgt

- **Rolle als Verarbeiter** im Rahmen eines Vertrags mit dem Data Fiduciary.
- **Datenminimierung** — es werden keine Kundeninhalte, Zugangsdaten oder Schlüssel erfasst.
- **Sicherheitsvorkehrungen und Unterstützung bei Sicherheitsverletzungen** zur Erfüllung der Pflichten des Data Fiduciary.

Hinweise zur Anbieterauswahl

Indien hat im November 2025 die DPDP Rules, 2025 bekannt gegeben, wobei die materiellen Pflichten schrittweise über die folgenden rund 18 Monate in Kraft treten. Die operativen Details (Einwilligungsmanagement, Meldung von Sicherheitsverletzungen, grenzüberschreitende Mechanismen) treten daher erst nach und nach in Kraft. Eine On-Premises-Bereitstellung unterstützt in der Zwischenzeit Präferenzen hinsichtlich des Datenstandorts (Data Residency). Cyber Crucible verfügt über keine indische Zertifizierung und unterstützt die Pflichten des Data Fiduciary, übernimmt sie jedoch nicht. Dokumentation ist auf Anfrage erhältlich.

Erfüllt Cyber Crucible die Anforderungen des singapurischen PDPA?

Kurzantwort: Cyber Crucible unterstützt die Verpflichtungen einer Organisation gemäß dem singapurischen Personal Data Protection Act als Datenintermediär, der auf dem Endpunkt verarbeitet und keine Kundeninhalte, Zugangsdaten oder Schlüssel erfasst. Die Protection- und Transfer-Limitation-Verpflichtungen haben kaum Angriffspunkte, da sich nur minimale personenbezogene Daten in seiner Obhut befinden.

Wie dies übereinstimmt

- **Rolle als Datenintermediär** im Rahmen eines schriftlichen Vertrags.
- **Schutzverpflichtung (Protection Obligation)** — Verschlüsselung, Zugriffskontrolle und Endpunktprävention.
- **Transferbeschränkung (Transfer Limitation)** — On-Premises-Bereitstellung und kein Offshore-Transfer von Kundeninhalten zur Sicherheitsverarbeitung.

Hinweise zur Anbieterauswahl

Der singapurische PDPA enthält eine verpflichtende Regelung zur Meldung von Datenschutzverletzungen; zeitnahe Vorfallsinformationen unterstützen diese. Eine Vereinbarung zur Auftragsdatenverarbeitung ist auf Anfrage erhältlich.

Erfüllt Cyber Crucible die Anforderungen des japanischen APPI?

Kurzantwort: Cyber Crucible unterstützt die Pflichten eines Unternehmens gemäß dem japanischen Gesetz zum Schutz personenbezogener Informationen (Act on the Protection of Personal Information, APPI), indem Daten minimiert und lokal verarbeitet werden. Es werden keine Kundeninhalte, Zugangsdaten oder Schlüssel erfasst, sodass die Vorschriften zur Handhabung, zur Weitergabe an Dritte und zur grenzüberschreitenden Übermittlung in seinem Verantwortungsbereich nur minimale Angriffsfläche bieten.

Wie die Übereinstimmung erreicht wird

- **Sichere Handhabung** — Verschlüsselung, Zugriffskontrolle und Endpunktschutz.
- **Grenzüberschreitende Übermittlung** — Der On-Premises-Einsatz unterstützt den Verbleib personenbezogener Daten in Japan; für die Sicherheitsverarbeitung werden keine Kundeninhalte ins Ausland übertragen.
- **Unterstützung bei Vorfällen** — Informationen zu Vorfällen zur Unterstützung der APPI-Meldepflichten.

Hinweise zur Anbieterauswahl

Die Änderungen des APPI haben die Meldepflichten bei Datenschutzverletzungen sowie die Vorschriften für grenzüberschreitende Übermittlungen verschärft; der minimale Datenfußabdruck hält die Verpflichtungen des Anbieters gering. Dokumentation ist auf Anfrage erhältlich.

Erfüllt Cyber Crucible die brasilianische LGPD?

Kurze Antwort: Cyber Crucible unterstützt die Pflichten eines Verantwortlichen im Rahmen der brasilianischen Lei Geral de Proteção de Dados (LGPD) als Betreiber (Auftragsverarbeiter), der auf dem Endpunkt verarbeitet und keine Kundendaten, Zugangsdaten oder Schlüssel erfasst. Die meisten LGPD-Pflichten – Rechtsgrundlage, Rechte der betroffenen Personen, Übermittlungsregeln – haben nur geringe Relevanz, da sich kaum personenbezogene Daten in der Obhut von Cyber Crucible befinden.

Wie die Ausrichtung erfolgt

- **Rolle als Betreiber** vertraglich, Verarbeitung gemäß den Anweisungen des Verantwortlichen.
- **Sicherheitsmaßnahmen** — Verschlüsselung, Zugriffskontrolle und autonome Endpunktprävention.
- **Unterstützung bei Sicherheitsvorfällen** für die Meldepflichten des Verantwortlichen gegenüber der ANPD.

Hinweise zur Anbieterauswahl

Die ANPD ist zunehmend aktiv bei der Durchsetzung und bei Leitlinien zu Datenübermittlungen; eine On-Premises-Bereitstellung unterstützt Präferenzen hinsichtlich des Datenstandorts. Cyber Crucible verfügt über keine brasilianische Zertifizierung und unterstützt die Pflichten des Verantwortlichen. Dokumentation ist auf Anfrage erhältlich.

Erfüllt Cyber Crucible die revidierte FADP der Schweiz?

Kurze Antwort: Cyber Crucible unterstützt die Verpflichtungen einer Schweizer Organisation im Rahmen des revidierten Bundesgesetzes über den Datenschutz (revFADP), indem Daten minimiert und lokal auf dem Endpunkt verarbeitet werden. Da keine Kundeninhalte, Zugangsdaten oder Schlüssel erfasst werden, ergeben sich in seinem Verantwortungsbereich nur minimale Berührungspunkte mit den Sicherheits-, Verarbeitungsverzeichnis- und Übermittlungspflichten.

Wie die Ausrichtung erfolgt

- **Auftragsverarbeiter-Rolle** im Rahmen einer Vereinbarung zur Auftragsverarbeitung.
- **Security by Design** — Verschlüsselung, Zugriffskontrolle und Endpunktschutz unterstützen die Datensicherheitspflicht der revFADP.
- **Grenzüberschreitende Übermittlung** — Die On-Premises-Bereitstellung hält personenbezogene Daten dort, wo dies erforderlich ist, in der Schweiz; für Übermittlungen stehen Standardvertragsklauseln (SCCs) zur Verfügung.

Hinweise zur Anbieterauswahl

Die revFADP orientiert sich eng an der DSGVO, sodass ein Großteil der DSGVO-Unterstützung von Cyber Crucible ebenfalls gilt. Dokumentation, einschließlich SCCs, ist auf Anfrage erhältlich.

Erfüllt Cyber Crucible die Anforderungen des neuseeländischen Privacy Act 2020?

Kurzantwort: Cyber Crucible unterstützt die Verpflichtungen einer neuseeländischen Behörde gemäß dem Privacy Act 2020, indem keine Kundeninhalte, Zugangsdaten oder Schlüssel erfasst werden und die Verarbeitung auf dem Endpunkt erfolgt. Die Information Privacy Principles – insbesondere Speicherung und Sicherheit (IPP 5) sowie grenzüberschreitende Offenlegung (IPP 12) – weisen nur eine minimale Angriffsfläche auf, da sich kaum personenbezogene Informationen im Verantwortungsbereich befinden.

Wie die Ausrichtung erfolgt

- **IPP 5 Sicherheit** — Verschlüsselung, Zugriffskontrolle und autonomer Endpunktschutz.
- **IPP 12 grenzüberschreitende Übermittlung** — Die On-Premises-Bereitstellung hält personenbezogene Informationen in Neuseeland; für die Sicherheitsverarbeitung werden keine Kundeninhalte ins Ausland übertragen.
- **Unterstützung bei Sicherheitsvorfällen** für die Verpflichtungen der Behörde zur Meldung meldepflichtiger Datenschutzverletzungen.

Hinweise zur Anbieterauswahl

Der Privacy Act 2020 hat eine verpflichtende Meldepflicht bei Sicherheitsverletzungen sowie Compliance-Mitteilungen eingeführt; zeitnahe Informationen zu Vorfällen unterstützen beides. Dokumentation ist auf Anfrage erhältlich.

Unterstützt Cyber Crucible das südkoreanische PIPA?

Kurze Antwort: Cyber Crucible unterstützt die Verpflichtungen einer Organisation im Rahmen des südkoreanischen Personal Information Protection Act (PIPA) — eines der strengeren Regelwerke weltweit — indem Daten und Verarbeitung auf dem Endpunkt minimiert werden. Es werden keine Kundeninhalte, Anmeldedaten oder Schlüssel erfasst, sodass die Verpflichtungen zu Einwilligung, Handhabung und grenzüberschreitender Datenübermittlung nur minimale Berührungspunkte in seinem Verantwortungsbereich haben.

Wie die Ausrichtung erfolgt

- **Rolle als Auftragsverarbeiter** gemäß Vertrag, nach Weisung des Verantwortlichen.
- **Starke Schutzmaßnahmen** — Verschlüsselung, Zugriffskontrolle und Endpunktprävention unterstützen die anspruchsvollen Sicherheitsanforderungen von PIPA.
- **Grenzüberschreitende Übermittlung** — die On-Premises-Bereitstellung unterstützt den Verbleib personenbezogener Daten in Korea; für die Sicherheitsverarbeitung werden keine Kundeninhalte ins Ausland übertragen.

Hinweise zur Anbieterauswahl

PIPA sieht erhebliche Sanktionen und detaillierte Sicherheitsanforderungen vor; der minimale Datenfußabdruck und die On-Premises-Option halten das anbieterseitige Risiko gering. Dokumentation ist auf Anfrage erhältlich.

Erfüllt Cyber Crucible die Vorgaben des türkischen KVKK?

Kurze Antwort: Cyber Crucible unterstützt die Pflichten eines Verantwortlichen (data controller) gemäß dem türkischen Gesetz zum Schutz personenbezogener Daten (KVKK), indem keine Kundeninhalte, Zugangsdaten oder Schlüssel erfasst werden und die Verarbeitung auf dem Endgerät erfolgt. Registrierungs-, Sicherheits- und Übermittlungspflichten haben eine minimale Angriffsfläche, da sich nur wenige personenbezogene Daten in der Obhut des Unternehmens befinden.

Wie die Ausrichtung erfolgt

- **Rolle als Auftragsverarbeiter** gemäß Vertrag.
- **Sicherheitsmaßnahmen** — Verschlüsselung, Zugriffskontrolle und Endpoint-Prävention unterstützen die Anforderung des KVKK an technische Maßnahmen.
- **Grenzüberschreitende Übermittlung** — die On-Premises-Bereitstellung unterstützt die Präferenzen zur Datenresidenz gemäß den türkischen Übermittlungsregeln.

Hinweise zur Anbieterauswahl

Die Übermittlungsregelungen des KVKK sowie die VERBIS-Registrierungspflichten liegen beim Verantwortlichen; Cyber Crucible unterstützt diese Pflichten, übernimmt sie jedoch nicht. Dokumentation ist auf Anfrage erhältlich.