

Länder-Compliance-Leitfäden

Antworten nach Rechtsordnung — was das Datenschutzrecht jedes Landes konkret vorschreibt und wie die Architektur von Cyber Crucible dem gerecht wird. Golfregion, Afrika, Europa und Vereinigtes Königreich.

- [Erfüllt Cyber Crucible das saudi-arabische PDPL?](#)
- [Erfüllt Cyber Crucible das Datenschutzrecht der VAE?](#)
- [Erfüllt Cyber Crucible das bahrainische Datenschutzgesetz?](#)
- [Erfüllt Cyber Crucible das katarische Datenschutzgesetz?](#)
- [Erfüllt Cyber Crucible das Datenschutzgesetz Omans?](#)
- [Kuwait verfügt über kein umfassendes Datenschutzgesetz – was bedeutet das für die Auswahl von Anbietern?](#)
- [Erfüllt Cyber Crucible das kenianische Datenschutzgesetz \(Data Protection Act\)?](#)
- [Erfüllt Cyber Crucible die Anforderung Nigerias zur Datenlokalisierung?](#)
- [Erfüllt Cyber Crucible die südafrikanische POPIA?](#)
- [Erfüllt Cyber Crucible das ägyptische Datenschutzgesetz?](#)
- [Erfüllt Cyber Crucible das ghanaische Datenschutzgesetz \(Data Protection Act\)?](#)
- [Erfüllt Cyber Crucible die Anforderungen Sambias zur Datenlokalisierung?](#)
- [Erfüllt Cyber Crucible das ruandische Datenschutzgesetz?](#)
- [Erfüllt Cyber Crucible das marokkanische Datenschutzgesetz?](#)
- [Welche Datenschutzanforderungen gelten in Libyen?](#)
- [Erfüllt Cyber Crucible die Vorgaben der DSGVO?](#)
- [Erfüllt Cyber Crucible die Vorgaben der UK GDPR?](#)

Erfüllt Cyber Crucible das saudi-arabische PDPL?

Kurze Antwort: Cyber Crucible hat seine Betriebsabläufe im Hinblick auf das saudi-arabische Personal Data Protection Law (PDPL) überprüft, verwendet von der SDAIA genehmigte Standardvertragsklauseln für jede Übermittlung personenbezogener Daten saudi-arabischen Ursprungs und kann vollständig innerhalb des Königreichs ohne jeglichen grenzüberschreitenden Datenfluss eingesetzt werden. Es werden ausschließlich System- und Sicherheitstelemetriedaten erfasst — niemals Dateiinhalte, Dokumente, E-Mails oder Kommunikation.

Was das Gesetz vorschreibt

Das PDPL trat am 14. September 2023 in Kraft, mit einer Übergangsfrist bis zum 14. September 2024. Saudi-Arabien verfügt über eine der strengsten Lokalisierungspräferenzen im Golfraum, und die Saudi Data & AI Authority (SDAIA) fungiert als Aufsichtsbehörde. Übermittlungen aus dem Königreich hinaus erfordern eine anerkannte Schutzmaßnahme sowie in den meisten Fällen eine Transfer Risk Assessment (Risikobewertung der Übermittlung).

Was hier konkret gilt

- **Von der SDAIA vorab genehmigte SCCs** werden für jede Übermittlung personenbezogener Daten saudi-arabischen Ursprungs in die Vereinigten Staaten verwendet, unverändert übernommen — abgesehen von erforderlichen Feldern — und auf jeden weiteren Unterauftragsverarbeiter ausgeweitet.
- **Eine Transfer Risk Assessment** wurde gemäß den strukturierten Vorgaben der SDAIA durchgeführt — Datenflüsse, Rechtsordnung des Bestimmungslandes, Kontrollen, Restrisiko, dokumentierte Minderungsmaßnahmen.
- **Rolle als Auftragsverarbeiter** — Cyber Crucible tritt in der Regel als Auftragsverarbeiter im Rahmen einer schriftlichen Vereinbarung zur Auftragsverarbeitung (DPA) auf; der saudi-arabische Kunde ist der Verantwortliche.
- **Örtlicher Vertreter nach Artikel 33** — als Auftragsverarbeiter liegt diese Pflicht bei Ihnen als Verantwortlichem.

Der sauberste Weg

Angesichts der Lokalisierungspräferenz ist die vollständig On-Premises betriebene, luftisolierte (air-gapped) Bereitstellung die stärkste Lösung: die gesamte Backend-Verwaltung erfolgt innerhalb Ihrer eigenen physisch gesicherten Racks, ohne ausgehende Telemetriedaten. Wo nichts die Grenze überschreitet, entstehen keine Übermittlungspflichten.

“ SCCs und die TRA sind über **dpo@cybercrucible.com** erhältlich. Stand zum Zeitpunkt der Erstellung — bitte aktuelle Anforderungen mit lokalem Rechtsbeistand bestätigen.

Erfüllt Cyber Crucible das Datenschutzrecht der VAE?

Kurze Antwort: Ja, im Rahmen derselben Architektur — minimale Datenerfassung, lokale Verarbeitung und Bereitstellungsoptionen, bei denen die Daten das Land nie verlassen. Ein VAE-spezifischer Punkt ist wichtig: Wenn Ihr Unternehmen im DIFC oder ADGM ansässig ist, gilt ein anderes Regime als das föderale Recht.

Was das Gesetz verlangt

Das föderale VAE-Dekretgesetz Nr. 45 von 2021 begründet den föderalen Rahmen zum Schutz personenbezogener Daten. Es lässt eine breitere Palette rechtmäßiger Grundlagen zu als die eher zustimmungszentrierten Regelungen am Golf und verfolgt bei grenzüberschreitenden Datenübermittlungen einen risikobasierten, schutzmaßnahmenorientierten Ansatz anstelle strikter Datenlokalisierung. Die Umsetzung hängt von den Durchführungsverordnungen ab — ein Bereich, der sich weiterentwickelt hat, sodass Sie den aktuellen Stand prüfen sollten.

Die Frage der Freizonen

Hier stolpern viele. Das DIFC (Dubai International Financial Centre) und das ADGM (Abu Dhabi Global Market) betreiben eigene, vom föderalen Recht getrennte Datenschutzregime. Wenn Ihr Unternehmen in einer dieser Zonen ansässig ist, gelten andere Vorschriften und eine andere Aufsichtsbehörde.

Klären Sie, welcher Rahmen für Sie maßgeblich ist, bevor Sie einen Anbieter bewerten — die Antwort bestimmt, was Sie nachweisen müssen.

Was hier konkret gilt

- **Flexibilität bei der Rechtsgrundlage** — die breitere Palette an Grundlagen bedeutet, dass eine Argumentation im Stil des berechtigten Interesses für sicherheitsbezogene Verarbeitung in der Regel praktikabler ist als in eher zustimmungszentrierten Regelungen.
- **Schutzmaßnahmen bei Übermittlungen** — regionales Staging hält die Verarbeitung innerhalb der VAE; eine Air-Gapped-Bereitstellung schließt Übermittlungen vollständig aus.

- **Rolle als Auftragsverarbeiter** im Rahmen eines schriftlichen DPA, gemäß Ihren dokumentierten Anweisungen.

“ Stand zum Zeitpunkt der Erstellung — bestätigen Sie die aktuellen Anforderungen, einschließlich der Durchführungsverordnungen und der Anwendbarkeit für Freizonen, mit lokalem Rechtsbeistand.

Erfüllt Cyber Crucible das bahrainische Datenschutzgesetz?

Kurzantwort: Ja. Das bahrainische Gesetz orientiert sich stark am DSGVO-Modell und hat extraterritoriale Reichweite, sodass dieselben Kontrollen, die die DSGVO erfüllen, auch hier gelten – minimale Datenerhebung, dokumentierte Rolle als Auftragsverarbeiter, starke Sicherheitsvorkehrungen und kontrollierte Übermittlung.

Was das Gesetz vorschreibt

Bahrain verfügt seit 2019 über ein eigenständiges Datenschutzgesetz. Es gilt oft als eines der klarsten und ausgereiftesten in der Golfregion, mit starken Rechten der betroffenen Personen, expliziten Rechenschaftspflichten und **extraterritorialer Anwendung** – das heißt, es kann auch Anbieter außerhalb Bahrains erfassen, die Daten von in Bahrain ansässigen Personen verarbeiten.

Was hier konkret gilt

Die extraterritoriale Reichweite ist der entscheidende Punkt. Sie bedeutet, dass sich die Frage nicht nur darauf beschränkt, ob *Sie* die Vorgaben einhalten, sondern auch, ob Ihre Anbieter dies tun.

- **Rechenschaftspflicht** – die Liste der ausgeschlossenen Daten (keine Schlüssel, Anmeldedaten, Tokens oder Inhalte) ist explizit und dokumentiert und nicht nur allgemein beschrieben, was genau den Rechenschaftspflichten entspricht.
- **Rechte der betroffenen Personen** – in der Praxis hier begrenzt, da Verhaltenselektrometriedaten pseudonymisiert werden und Inhalte nie erfasst werden, sodass der Umfang personenbezogener Daten, die Gegenstand von Rechteinfragen sein könnten, minimal ist.
- **Übermittlung** – regionale Zwischenspeicherung oder Air-Gapped-Bereitstellung.

Warum die Ausrichtung an der DSGVO hilft

Da sich das bahrainische Gesetz eng an der DSGVO orientiert, lässt sich die DSGVO-Zuordnung nahezu direkt übertragen. Wenn Ihre Organisation bereits eine DSGVO-Anbieterbewertung durchgeführt hat, lässt sich der Großteil davon übernehmen.

“ Stand zum Zeitpunkt der Erstellung – bitte mit lokalem Rechtsberater bestätigen.

Erfüllt Cyber Crucible das katarische Datenschutzgesetz?

Kurze Antwort: Ja. Katars Regelwerk ist stärker einwilligungszentriert als das seiner Nachbarländer, was eine minimale Datenerhebung besonders wertvoll macht – je weniger personenbezogene Daten verarbeitet werden, desto geringer ist der Einwilligungsaufwand.

Was das Gesetz vorschreibt

Katar verfügt seit 2017 über ein eigenständiges Datenschutzgesetz und zählt damit zu den frühesten in der Region. Es folgt einem strengeren, einwilligungszentrierten Modell im Vergleich zur breiteren Palette an Rechtsgrundlagen der VAE, verbunden mit einem risikobasierten Ansatz bei Schutzmaßnahmen für Übermittlungen.

Warum Einwilligungszentrierung dieser Architektur zugutekommt

In einem einwilligungszentrierten Regelwerk ist jede Kategorie personenbezogener Daten, die Sie verarbeiten, eine Kategorie, für die Sie möglicherweise eine Rechtsgrundlage benötigen. Das macht *das Nicht-Erheben* von Daten wesentlich wertvoller als deren bloßen Schutz.

Cyber Crucible erfasst niemals Verschlüsselungsschlüssel, Anmeldedaten, Sitzungstoken oder Dateiinhalte. Verhaltensbezogene Telemetriedaten werden pseudonymisiert, sofern sie eine Person identifizieren könnten, und die Telemetriequellen sind konfigurierbar, sodass Sie die Erfassung weiter einschränken können.

Das Ergebnis ist, dass die Einwilligungsfläche für das Sicherheitstool selbst ungewöhnlich klein ist.

Übermittlung

Regionales Staging hält die Verarbeitung nahe an oder innerhalb der jeweiligen Rechtsordnung; eine air-gapped Bereitstellung eliminiert grenzüberschreitende Datenflüsse vollständig.



Stand zum Zeitpunkt der Erstellung – bitte mit lokalem Rechtsbeistand bestätigen.

Erfüllt Cyber Crucible das Datenschutzgesetz Omans?

Kurze Antwort: Ja — und Oman ist derzeit die zeitkritischste Rechtsordnung am Golf. Omans Gesetz zum Schutz personenbezogener Daten tritt nach einer zweijährigen Übergangsfrist am **5. Februar 2026** vollständig in Kraft, sodass Anbieterlösungen, die bisher standardmäßig konform waren, nun in den Anwendungsbereich fallen.

Was das Gesetz vorschreibt

Omans Gesetz orientiert sich eng an den Grundsätzen der DSGVO und berücksichtigt gleichzeitig lokale Anforderungen an Einwilligung und Datenverarbeitung. Die zweijährige Übergangsfrist endet am 5. Februar 2026; ab diesem Zeitpunkt wird vollständige Compliance erwartet.

Warum dies jetzt für die Anbieterauswahl relevant ist

Übergangsfristen folgen einem vorhersehbaren Muster: Organisationen verschieben die Überprüfung ihrer Anbieter bis kurz vor die Frist und stellen dann fest, dass ein Sicherheitswerkzeug, das kontinuierlich Endpunkt-Telemetriedaten in eine andere Rechtsordnung überträgt, unter der neuen Regelung nur schwer zu rechtfertigen ist.

Wenn Sie Ihre Lösungen im Hinblick auf den Februar 2026 überprüfen, lohnt es sich, jedem Endpunkt-Anbieter folgende Fragen zu stellen:

1. Welche personenbezogenen Daten werden konkret und im Einzelnen erfasst?
2. Wo werden diese Daten verarbeitet, und kann dies in Oman erfolgen?
3. Welcher Übertragungsmechanismus kommt zum Einsatz, falls die Daten das Land verlassen?
4. Kann die Lösung ganz ohne ausgehende Telemetriedaten betrieben werden?

Die Antworten von Cyber Crucible lauten: klar definierte Ausschlüsse (keine Schlüssel, Anmeldedaten, Token oder Inhalte); die Verarbeitung erfolgt lokal auf dem Endpunkt; eine regionale Zwischenspeicherung ist verfügbar; und ja — die air-gapped Bereitstellung erzeugt keinerlei ausgehende Telemetriedaten.

Stand zum Zeitpunkt der Erstellung — bitte den aktuellen Status sowie mögliche Fristverlängerungen mit lokalem Rechtsbeistand bestätigen.

Kuwait verfügt über kein umfassendes Datenschutzgesetz – was bedeutet das für die Auswahl von Anbietern?

Kurze Antwort: Kuwait hat einen gezielten sektoralen Ansatz gewählt, anstatt ein umfassendes nationales Datenschutzgesetz zu erlassen, wobei die CITRA-Regulierung regelt, wie der Telekommunikations- und IT-Sektor mit Nutzerinhalten umgeht. Das macht Datensouveränität zu einer geschäftlichen und sicherheitsrelevanten Entscheidung und nicht zu einer Compliance-Pflicht – aber die Entscheidung ist dennoch von Bedeutung.

Die aktuelle Lage

Kuwait bleibt die bemerkenswerte Ausnahme unter den großen Golfstaaten, da es über kein umfassendes nationales Gesetz zum Schutz personenbezogener Daten verfügt. Stattdessen adressiert die CITRA-Regulierung den Umgang mit Nutzerinhalten speziell in den Bereichen Telekommunikation und IT.

Warum „kein Gesetz“ nicht dasselbe ist wie „kein Risiko“

Drei Gründe, warum Organisationen in Kuwait dies dennoch sorgfältig abwägen:

1. **Sektorale Regeln gelten weiterhin.** Wer im Telekommunikations- oder IT-Bereich tätig ist, unterliegt aktiven CITRA-Anforderungen.
2. **Vertragspartner setzen eigene Bedingungen durch.** Multinationale Partner, Versicherer und Kunden verlangen vertraglich häufig eine GDPR-äquivalente Handhabung, unabhängig vom lokalen Recht.
3. **Regulierung kommt in der Regel doch.** Jeder andere GCC-Staat hat inzwischen ein umfassendes Gesetz erlassen. Die Wahl von Anbietern, die bereits strengere Regelwerke

erfüllen, vermeidet eine spätere erzwungene Migration.

Die praktische Position

Da Cyber Crucible niemals Schlüssel, Anmeldedaten, Tokens oder Inhalte erfasst und vollständig air-gapped bereitgestellt werden kann, erfüllt es die strengsten Regelwerke der Region. Die Wahl von Cyber Crucible in Kuwait bedeutet, dieses Problem gar nicht erst zu haben, wenn sich die Gesetzeslage ändert.

“ Stand zum Zeitpunkt der Erstellung – aktuelle sektorale Anforderungen bitte mit lokalem Rechtsbeistand bestätigen.

Erfüllt Cyber Crucible das kenianische Datenschutzgesetz (Data Protection Act)?

Kurze Antwort: Ja. Kenias Data Protection Act 2019 beschränkt die grenzüberschreitende Übermittlung auf Länder mit angemessenen Schutzmaßnahmen und wendet für sensible personenbezogene Daten eine strengere Regel an. Cyber Crucible erhebt überhaupt keine sensiblen personenbezogenen Daten und kann so eingesetzt werden, dass keine Daten Kenia verlassen.

Was das Gesetz vorschreibt

Die Abschnitte 48 und 49 des Data Protection Act 2019 untersagen die Übermittlung personenbezogener Daten in ein Land, das keine angemessenen Datensicherheitsvorkehrungen aufweist, wobei mehrere zulässige Grundlagen bestehen, darunter die Angemessenheit (Adäquanz).

Die strengere Regel, auf die es ankommt: Die Übermittlung *sensibler* personenbezogener Daten ist nur zulässig, wenn die betroffene Person eingewilligt hat **und** angemessene Schutzmaßnahmen bestehen. Beide Bedingungen, nicht nur eine.

Warum die Regel zu sensiblen Daten der entscheidende Punkt ist

Diese doppelte Anforderung ist operativ nur schwer zu erfüllen — für jedes betroffene Individuum fortlaufend eine individuelle Einwilligung einzuholen und nachzuweisen, und das für ein Sicherheitswerkzeug.

Cyber Crucible umgeht dies: **Es werden keine sensiblen personenbezogenen Daten erhoben.** Weder biometrische, gesundheitsbezogene oder genetische Daten; noch Daten, die Rückschlüsse auf die rassische oder ethnische Herkunft, religiöse Überzeugungen oder politische Meinungen zulassen. Die Telemetriedaten beschreiben Systemverhalten und Sicherheitsereignisse, nicht persönliche Merkmale.

Wo Verhaltenstelemetrie indirekt eine Person identifizieren könnte, werden Identifikatoren pseudonymisiert oder maskiert.

Übermittlung

Durch die regionale Zwischenspeicherung (Staging) bleibt die Verarbeitung innerhalb Kenias. Der Air-Gapped-Einsatz erzeugt keinerlei ausgehende Telemetriedaten, sodass die Abschnitte 48–49 nicht zur Anwendung kommen.

“ Stand zum Zeitpunkt der Erstellung — bitte mit lokalem Rechtsbeistand bestätigen.

Erfüllt Cyber Crucible die Anforderung Nigerias zur Datenlokalisierung?

Kurze Antwort: Ja — und dies ist die Rechtsordnung, in der die Architektur am wichtigsten ist. Nigerias Data Protection Act 2023 sieht eine Anforderung zur Datenlokalisierung vor: Personenbezogene Daten nigerianischer Bürger müssen innerhalb Nigerias gespeichert werden. Die On-Premises-Bereitstellung von Cyber Crucible hält alles innerhalb Ihrer eigenen Infrastruktur, im Land selbst, mit null ausgehender Telemetrie.

Was das Gesetz verlangt

Die Abschnitte 41–43 des Nigeria Data Protection Act 2023 legen Bedingungen für grenzüberschreitende Übermittlungen fest, einschließlich Schutzmaßnahmen im Zielland und der Einwilligung der betroffenen Person. Über diese Bedingungen hinaus **schreibt Nigeria eine Lokalisierungspflicht vor** — personenbezogene Daten nigerianischer Bürger müssen innerhalb Nigerias gespeichert werden. Branchenspezifische Vorschriften im Finanzsektor fügen weitere Lokalisierungspflichten hinzu.

Warum die meisten Sicherheitsanbieter hier Schwierigkeiten haben

Dies ist das klarste Beispiel für eine Regelung, die cloudabhängige Endpunktsicherheit konstruktionsbedingt nicht erfüllen kann. Ein Tool, dessen Architektur darauf beruht, „Telemetriedaten am Endpunkt zu sammeln und zur Analyse an unsere Cloud zu senden“, verlagert strukturell personenbezogene Daten aus Nigeria heraus, um überhaupt funktionsfähig zu sein. Vertragliche Schutzmaßnahmen lösen keine Anforderung zum Speicherort.

Warum diese Architektur die Anforderung erfüllt

- **Die Analyse erfolgt lokal.** Die Bedrohungsbewertung und -abwehr erfolgt am Endpunkt, typischerweise in unter 200 Millisekunden. Für den Schutz ist keine Cloud-Rückmeldung erforderlich.
- **Das Backend kann vollständig im Land betrieben werden.** Das On-Premises-Modell führt die gesamte Verwaltungssoftware innerhalb Ihrer eigenen physisch gesicherten Racks aus.
- **Null ausgehende Telemetrie** in der abgeschotteten (air-gapped) Konfiguration — nichts verlässt das System, daher wird nichts im Ausland gespeichert.
- **Ohnehin weniger zu lokalisieren** — Schlüssel, Zugangsdaten, Tokens und Dateiinhalte werden von vornherein nicht erfasst.

“ Stand zum Zeitpunkt der Erstellung — bestätigen Sie die aktuellen Anforderungen, einschließlich der Vorschriften für den Finanzsektor, bei örtlichen Rechtsberatern.

Erfüllt Cyber Crucible die südafrikanische POPIA?

Kurze Antwort: Ja. POPIA schränkt die grenzüberschreitende Übermittlung ein, sofern das Zielland keinen im Wesentlichen vergleichbaren Schutz bietet oder die betroffene Person nicht zustimmt. Cyber Crucible minimiert von vornherein die verarbeiteten Daten und kann so eingesetzt werden, dass überhaupt keine Übermittlung stattfindet.

Was das Gesetz verlangt

Der südafrikanische Protection of Personal Information Act (2013) untersagt die Übermittlung personenbezogener Informationen außerhalb des Landes ohne die Zustimmung der betroffenen Person, es sei denn, die Empfängerjurisdiktion unterliegt einem Gesetz, das einen im Wesentlichen vergleichbaren Schutz bietet.

Was hier konkret gilt

Der Test des „im Wesentlichen vergleichbaren Schutzes“ ist eine Bewertung, die Sie belegen können müssen. Zwei Faktoren erleichtern diese Bewertung:

1. **Der Umfang ist gering.** Verschlüsselungsschlüssel, Anmeldedaten, Sitzungstoken und Dateiinhalte werden niemals erfasst. Was verbleibt, ist Verhaltenstelemetrie, pseudonymisiert dort, wo sie eine Person identifizieren könnte.
2. **Vertragliche Schutzmaßnahmen** — die Verarbeitung erfolgt im Rahmen einer schriftlichen DPA mit Bestimmungen zu Sicherheit, Vertraulichkeit und Verstoßmeldung, die auch auf jeden Unterauftragsverarbeiter ausgeweitet werden.

Oder den Test ganz vermeiden

Regionales Staging hält die Verarbeitung in Südafrika. Der luftgetrennte (air-gapped) Einsatz erzeugt überhaupt keinen ausgehenden Datenfluss, wodurch die Übermittlungsbestimmungen schlicht nicht greifen — in der Regel ein schnellerer Weg als der Nachweis der Angemessenheit.

Stand zum Zeitpunkt der Erstellung — bitte mit lokalem Rechtsbeistand bestätigen.

Erfüllt Cyber Crucible das ägyptische Datenschutzgesetz?

Kurze Antwort: Ja. Ägypten verlangt eine vorherige Genehmigung für grenzüberschreitende Übermittlungen personenbezogener Daten – eine deutlich höhere Hürde als vertragliche Schutzmaßnahmen. Cyber Crucible kann so eingesetzt werden, dass keine Übermittlung stattfindet, wodurch das Genehmigungserfordernis entfällt, anstatt es erfüllen zu müssen.

Was das Gesetz verlangt

Ägyptens Datenschutzrahmen verlangt eine **vorherige Genehmigung** für Übermittlungen personenbezogener Daten außerhalb des Landes. Das ist ein genehmigungsbasiertes Modell und kein schutzmaßnahmenbasiertes: Man kann nicht einfach vertragliche Schutzmaßnahmen einführen und fortfahren.

Warum das Genehmigungsmodell die Anbieterauswahl verändert

Bei einem schutzmaßnahmenbasierten Modell ist ein Anbieter mit starken Vertragsklauseln praktikabel. Bei einem genehmigungsbasierten Modell ist jeder grenzüberschreitende Datenfluss ein Verwaltungsverfahren mit Zeitplanung, Ermessensspielraum und Erneuerungsrisiko.

Ein Sicherheitstool, das kontinuierlich Telemetriedaten exportiert, erzeugt einen fortlaufenden Datenfluss, für den diese Genehmigung gültig bleiben muss. Läuft die Genehmigung ab oder ändern sich die Bedingungen, wird der normale Betrieb des Tools zu einem Compliance-Problem.

Die naheliegende Antwort

Die luftisolierte On-Premises-Bereitstellung erzeugt keinerlei ausgehende Telemetriedaten – es wird nichts übermittelt, sodass keine Genehmigung erforderlich ist. Regionale Staging-Umgebungen halten die Verarbeitung lokal, sofern ein Hybridmodell bevorzugt wird.

Die Kategorien, die am ehesten regulatorische Aufmerksamkeit auf sich ziehen – Schlüssel, Anmeldedaten, Tokens, Dateiinhalte – werden unabhängig von der Bereitstellungsart niemals erfasst.

Stand zum Zeitpunkt der Erstellung – aktuelle Anforderungen und das Genehmigungsverfahren bitte mit lokalem Rechtsbeistand bestätigen.

Erfüllt Cyber Crucible das ghanaische Datenschutzgesetz (Data Protection Act)?

Kurze Antwort: Ja, und Ghana ist im Vergleich unkompliziert. Ghana zeichnet sich unter den afrikanischen Rechtsordnungen dadurch aus, dass es **keine** zusätzlichen Anforderungen an grenzüberschreitende Übermittlungen stellt, die über seine allgemeinen Datenschutzpflichten hinausgehen — es gelten also die üblichen Kontrollen ohne ein besonderes Übermittlungsregime.

Was das Gesetz vorschreibt

Ghana verfügt über einen etablierten Datenschutzrahmen mit einer Aufsichtsbehörde. Analysen afrikanischer Rechtsordnungen identifizieren Ghana durchgängig als Ausnahme: Anders als die meisten seiner Nachbarländer legt es keine zusätzlichen Bedingungen speziell für den grenzüberschreitenden Datenaustausch fest.

Das bedeutet nicht, dass die Übermittlung unreguliert ist — die allgemeinen Pflichten hinsichtlich rechtmäßiger Verarbeitung, Sicherheit und Rechten der betroffenen Personen gelten weiterhin. Es bedeutet lediglich, dass keine gesonderte Genehmigungs- oder Angemessenheitshürde zu überwinden ist.

Was hier konkret gilt

Da die Übermittlungsfrage vereinfacht ist, reduziert sich die Bewertung auf die üblichen Punkte:

- **Was wird erhoben?** Nur System- und Sicherheitstelemetriedaten. Keine Schlüssel, Anmeldedaten, Tokens oder Inhalte.
- **Wie wird es geschützt?** TLS 1.3 bei der Übertragung, JWE-Payload-Verschlüsselung pro Agent, Verschlüsselung im Ruhezustand, rollenbasierte Zugriffskontrolle.
- **Wer ist verantwortlich?** Cyber Crucible fungiert als Auftragsverarbeiter im Rahmen einer schriftlichen Auftragsverarbeitungsvereinbarung (DPA) gemäß Ihren dokumentierten Anweisungen.

Souveränität bleibt dennoch bedenkenswert

Auch ohne Übermittlungsbeschränkung bleibt eine landesinterne oder abgeschottete (air-gapped) Bereitstellung möglich — und Organisationen, die regionale Kunden bedienen, bevorzugen dies häufig, da benachbarte Rechtsordnungen erheblich strenger sind.

“ Stand zum Zeitpunkt der Erstellung — bitte mit lokalem Rechtsbeistand bestätigen.

Erfüllt Cyber Crucible die Anforderungen Sambias zur Datenlokalisierung?

Kurze Antwort: Ja. Das sambische Datenschutzgesetz (Data Protection Act) verpflichtet Verantwortliche, personenbezogene und besonders sensible personenbezogene Daten in einem Rechenzentrum oder auf einem Server **innerhalb Sambias** zu verarbeiten und zu speichern. Die On-Premises-Bereitstellung von Cyber Crucible erfüllt dies direkt — das Backend läuft innerhalb Ihrer eigenen Infrastruktur, im jeweiligen Land.

Was das Gesetz verlangt

Teil X des sambischen Datenschutzgesetzes regelt die grenzüberschreitende Übermittlung, und Abschnitt 70 verpflichtet einen Datenverantwortlichen, personenbezogene und besonders sensible personenbezogene Daten in einem Rechenzentrum oder auf einem Server innerhalb Sambias zu verarbeiten und zu speichern.

Dies ist eine **Vorgabe zum Speicherort**, kein Test von Schutzmaßnahmen. Vertragliche Schutzmaßnahmen erfüllen diese Anforderung nicht.

Warum dies die meisten cloudbasierten Sicherheitstools ausschließt

Ein Anbieter, dessen Produkt den Versand von Endpunkt-Telemetriedaten an eine Cloud-Region außerhalb Sambias erfordert, kann Abschnitt 70 nicht durch bessere Verträge oder Verschlüsselung erfüllen. Die Anforderung betrifft, *wo sich die Daten physisch befinden*.

Warum diese Architektur die Anforderung erfüllt

- **On-Premises-Backend** — die gesamte Verwaltungssoftware läuft auf Servern, die Sie selbst kontrollieren, innerhalb Sambias.

- **Lokale Analyse** — die Bewertung von Bedrohungen und deren Abwehr erfolgt direkt am Endpunkt, sodass der Schutz niemals von einem Dienst außerhalb des Landes abhängt.
- **Keine ausgehende Telemetrie** in der abgeschotteten (Air-Gapped-)Konfiguration.
- **Minimaler Umfang** — Schlüssel, Anmeldedaten, Tokens und Inhalte werden niemals erfasst, sodass der Umfang der personenbezogenen Daten, die unter Abschnitt 70 fallen, von vornherein gering ist.

“ Stand zum Zeitpunkt der Erstellung — bitte mit lokalem Rechtsbeistand abstimmen, einschließlich etwaiger branchenspezifischer Vorschriften.

Erfüllt Cyber Crucible das ruandische Datenschutzgesetz?

Kurze Antwort: Ja. Das ruandische Datenschutzgesetz wird von der National Cyber Security Authority beaufsichtigt, und sektorspezifische Vorschriften fügen Lokalisierungspflichten hinzu — insbesondere für lizenzierte Banken, die Primärdaten innerhalb Ruandas vorhalten müssen. Die On-Premises-Bereitstellung erfüllt beide Anforderungen.

Was das Gesetz vorschreibt

Ruanda hat ein Datenschutzgesetz erlassen, wobei die **National Cyber Security Authority (NCSA)** als Aufsichtsbehörde benannt wurde; ihre Datenschutzabteilung nahm im März 2022 ihre Arbeit auf.

Neben dem allgemeinen Gesetz fügt eine sektorale Regulierung eine Lokalisierungspflicht hinzu: Die Cybersicherheitsregulierung verlangt von durch die Zentralbank lizenzierten Banken, Primärdaten innerhalb des ruandischen Staatsgebiets vorzuhalten.

Warum die sektorale Vorschrift am wichtigsten ist

Für Finanzdienstleistungen in Ruanda stellt die Lokalisierungspflicht für Banken in der Regel die maßgebliche Einschränkung dar — sie ist strenger und spezifischer als die allgemeinen Datenschutzbestimmungen. Ein Sicherheitsprodukt, das auf den Endpunkten einer Bank eingesetzt wird, verarbeitet Daten, die darunter fallen.

Was hier konkret zutrifft

- **On-Premises-Bereitstellung** hält Primärdaten innerhalb Ruandas vor und erfüllt damit die Lokalisierungspflicht direkt.
- **Lokale Analyse** bedeutet, dass der Schutz nicht von einem Dienst außerhalb des Landes abhängt.
- **Übereinstimmung mit der Aufsichtsbehörde** — da die NCSA sowohl für Cybersicherheit als auch für Datenschutz zuständig ist, ist die Fähigkeit, in aufgeschlüsselter Form nachzuweisen, was ein Sicherheitstool erfasst, ungewöhnlich

nützlich.

“ Stand zum Zeitpunkt der Erstellung — bestätigen Sie die aktuellen allgemeinen und sektoralen Anforderungen bei örtlichem Rechtsbeistand.

Erfüllt Cyber Crucible das marokkanische Datenschutzgesetz?

Kurze Antwort: Ja. Das marokkanische Gesetz Nr. 09-08 und die dazugehörige Durchführungsverordnung regeln die Verarbeitung personenbezogener Daten und werden von der CNDP beaufsichtigt. Es gelten dieselben Kontrollen – minimale Datenerfassung, dokumentierte Rolle als Auftragsverarbeiter, starke Schutzmaßnahmen sowie eine Bereitstellung im Land oder air-gapped, sofern bevorzugt.

Was das Gesetz vorschreibt

Marokkos Rechtsrahmen beruht auf dem **Gesetz Nr. 09-08** zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zusammen mit der Durchführungsverordnung **Nr. 2-09-165**. Die **CNDP** (Commission Nationale de contrôle de la protection des Données à caractère Personnel) ist die Aufsichtsbehörde und beteiligt sich aktiv an der internationalen Zusammenarbeit zu aufkommenden Themen, einschließlich KI.

Was hier konkret gilt

Marokkos Regelung gehört zu den etablierteren in Nordafrika, mit einer funktionierenden Aufsichtsbehörde sowie Melde-/Genehmigungsverfahren, die je nach Art der Verarbeitung variieren. Praktische Auswirkungen für die Anbieterbewertung:

- **Auflisten, was erfasst wird.** Die Liste der ausgeschlossenen Daten von Cyber Crucible ist explizit – keine Schlüssel, Zugangsdaten, Tokens oder Inhalte –, was die Genauigkeit der Meldung unterstützt.
- **Rolle als Auftragsverarbeiter** im Rahmen einer schriftlichen Auftragsverarbeitungsvereinbarung (DPA) auf dokumentierte Anweisung.
- **Übermittlung** – regionale Zwischenspeicherung oder air-gapped Bereitstellung; Letzteres macht die Frage hinfällig.

Für Organisationen, die im gesamten Maghreb tätig sind

Die Anforderungen unterscheiden sich erheblich zwischen Marokko, Tunesien, Algerien und Libyen. Die Wahl eines Anbieters, der die strengste geltende Regelung erfüllt – anstatt jede einzeln zu bewerten – ist in der Regel der Weg mit dem geringeren Aufwand.

“ Stand zum Zeitpunkt der Erstellung – bitte mit lokalem Rechtsbeistand bestätigen.

Welche Datenschutzanforderungen gelten in Libyen?

Kurze Antwort: Libyen hat bisher keine umfassenden Datenschutzvorschriften entwickelt. Das macht Datensouveränität zu einer kommerziellen, sicherheitsbezogenen und vertragspartnerbezogenen Entscheidung und nicht zu einer lokalen Compliance-Pflicht — für Organisationen, die sensible Vorgänge abwickeln, bleibt es jedoch eine Entscheidung, die es wert ist, bewusst getroffen zu werden.

Die aktuelle Lage

Libyen hat noch keinen umfassenden Datenschutzrahmen erlassen. Es gibt kein Äquivalent zum saudischen PDPL, zum marokkanischen Gesetz 09-08 oder zum nigerianischen NDPA.

Warum Souveränität auch ohne lokales Gesetz weiterhin wichtig ist

1. Vertragspartner stellen Anforderungen. Internationale Partner, Versicherer, multinationale Kunden und Kapitalgeber verlangen vertraglich routinemäßig eine GDPR-äquivalente Handhabung, unabhängig vom lokalen Recht. Wer den strengeren Standard von Anfang an erfüllt, vermeidet spätere Neuverhandlungen.

2. Sensible Sektoren bergen ein eigenes Risiko. Energie, Telekommunikation, Finanzen und staatliche Einrichtungen ziehen unabhängig von der Datenschutzgesetzgebung Aufmerksamkeit auf sich. Wohin ein Sicherheitstool Telemetriedaten sendet — und wer dort Zugriff darauf erzwingen kann — ist eine echte operative Frage.

3. Regulierung folgt in der Regel nach. Nachbarländer in Nordafrika haben Rahmenwerke erlassen oder aktualisiert. Anbieterentscheidungen, die jetzt getroffen werden, gelten weiterhin, wenn sich die Position Libyens ändert.

Die praktische Einordnung

Da Cyber Crucible niemals Schlüssel, Zugangsdaten, Tokens oder Inhalte erfasst und vollständig air-gapped mit null ausgehender Telemetrie betrieben werden kann, erfüllt es die strengsten Regelwerke der Region. In Libyen ist dies eine Wahl und keine Verpflichtung — aber eine, die sich langfristig bewährt.

“ Stand zum Zeitpunkt der Erstellung — bitte die aktuelle Gesetzeslage vor einer Entscheidung mit lokalem Rechtsbeistand bestätigen.

Erfüllt Cyber Crucible die Vorgaben der DSGVO?

Kurze Antwort: Ja, und zwar von Grund auf konzipiert und nicht nur durch Richtlinien geregelt. Inhalte, Zugangsdaten, Verschlüsselungsschlüssel und Sitzungstoken werden niemals erfasst; die Analyse erfolgt auf dem Endgerät; Cyber Crucible agiert als Auftragsverarbeiter im Rahmen eines schriftlichen Auftragsverarbeitungsvertrags (DPA); und die Bereitstellungsoptionen sorgen dafür, dass personenbezogene Daten innerhalb der EU verbleiben — oder innerhalb Ihres eigenen Gebäudes.

Zuordnung zu den Grundsätzen der DSGVO

- **Datenminimierung (Art. 5)** — die ausgeschlossenen Datenkategorien sind konkret aufgeführt, nicht nur allgemein beschrieben. Die Telemetriedaten beschränken sich auf das für die Bedrohungserkennung erforderliche Maß und sind konfigurierbar.
- **Integrität und Vertraulichkeit (Art. 5, 32)** — TLS 1.3 bei der Übertragung, JWE-Verschlüsselung der Nutzdaten pro Agent, Verschlüsselung im Ruhezustand, rollenbasierte Zugriffskontrolle, Schlüsselrotation, Protokollierung (Audit-Logging).
- **Pflichten des Auftragsverarbeiters (Art. 28)** — schriftlicher Auftragsverarbeitungsvertrag mit klar definiertem Umfang; Verarbeitung ausschließlich auf dokumentierte Anweisung; Unterauftragsverarbeiter sind an gleichwertige Bedingungen gebunden.
- **Übermittlungen (Kapitel V)** — regionale Zwischenspeicherung innerhalb der EU oder eine abgeschottete (air-gapped) Bereitstellung, die Übermittlungen vollständig ausschließt.
- **Datenschutz durch Technikgestaltung (Art. 25)** — die stärkste mögliche Zusicherung: Die Kategorien mit dem höchsten Risiko werden nicht durch Richtlinien geschützt, sondern gar nicht erst erfasst.

Pseudonymisierung

Sofern verhaltensbezogene Telemetriedaten eine Person indirekt identifizierbar machen könnten, werden Identifikatoren pseudonymisiert oder maskiert — eine Schutzmaßnahme, die die DSGVO ausdrücklich anerkennt.

Was dies nicht leistet

Dies macht Ihre Organisation nicht automatisch DSGVO-konform. Ihre Pflichten hängen von Ihren eigenen Verarbeitungszwecken, Rechtsgrundlagen, Informationspflichten und Aufzeichnungen ab. Was dadurch entfällt, ist eine häufige Schwierigkeit: ein Sicherheitsanbieter, der fortlaufend personenbezogene Daten in ein Drittland exportiert.

Erfüllt Cyber Crucible die Vorgaben der UK GDPR?

Kurzantwort: Ja. Die UK GDPR und der Data Protection Act 2018 folgen eng der EU-DSGVO, sodass dieselbe Zuordnung gilt — minimale Datenerhebung, Auftragsverarbeiterrolle im Rahmen eines schriftlichen DPA, starke technische Schutzmaßnahmen sowie Bereitstellungsoptionen, die Daten im Vereinigten Königreich oder vollständig in Ihren eigenen Räumlichkeiten belassen.

Was gilt

Nach dem Austritt des Vereinigten Königreichs aus der EU gilt die UK GDPR gemeinsam mit dem Data Protection Act 2018, überwacht durch das Information Commissioner's Office (ICO). Die Grundsätze, Rechtsgrundlagen und Pflichten der Auftragsverarbeiter entsprechen weitgehend der EU-DSGVO.

Worauf Organisationen achten sollten

- **Internationale Datenübermittlungen** nutzen die eigenen Mechanismen des Vereinigten Königreichs — das International Data Transfer Agreement (IDTA) oder das UK Addendum zu den EU-SCCs, statt allein der EU-SCCs.
- **Doppelte Compliance** — Organisationen, die sowohl im Vereinigten Königreich als auch in der EU tätig sind, müssen beide Regelwerke erfüllen, wobei sich die praktischen Kontrollen nahezu vollständig überschneiden.

Was hier konkret gilt

Die Bewertung entspricht der für die EU-DSGVO, und die Antworten sind dieselben:

- Schlüssel, Anmeldedaten, Tokens und Dateiinhalte werden niemals erfasst.
- Die Analyse erfolgt am Endpunkt; der Schutz erfordert keine Datenübertragung.
- Regionales Staging im Vereinigten Königreich oder eine Air-Gap-Bereitstellung, die eine Übermittlung vollständig ausschließt.
- Auftragsverarbeiterrolle im Rahmen eines schriftlichen DPA, wobei Unterauftragsverarbeiter an gleichwertige Bedingungen gebunden sind.

Für das für Ihre Situation passende Übermittlungsinstrument wenden Sie sich an **dpo@cybercrucible.com**. Stand zum Zeitpunkt der Erstellung — aktuelle ICO-Leitlinien bitte mit rechtlichem Beistand bestätigen.