

Regionaler Datenschutz und Compliance

Wie Cyber Crucible Datenschutzgesetze in der Golfregion, Afrika, Europa und darüber hinaus unterstützt — Rollen von Verantwortlichem und Auftragsverarbeiter, grenzüberschreitende Datenübermittlungen, Datenresidenz, sensible Daten und lokale Vertretung.

- [Warum verlangen so viele nationale Datenschutzgesetze dasselbe?](#)
- [Welche Golfstaaten verfügen über Datenschutzgesetze, und wie unterscheiden sie sich?](#)
- [Wie wirken sich afrikanische Datenschutzgesetze auf die Auswahl von Sicherheitsanbietern aus?](#)
- [Was gilt in Europa und im Vereinigten Königreich?](#)
- [Ist Cyber Crucible ein Verantwortlicher oder ein Auftragsverarbeiter für Daten?](#)
- [Wie werden grenzüberschreitende Datenübertragungen gehandhabt?](#)
- [Erfasst Cyber Crucible sensible personenbezogene Daten?](#)
- [Welche Schutzmaßnahmen schützen personenbezogene Daten, die von Cyber Crucible verarbeitet werden?](#)
- [Muss ich einen lokalen Vertreter benennen?](#)
- [Wie fordere ich Compliance-Dokumentation an?](#)

Warum verlangen so viele nationale Datenschutzgesetze dasselbe?

Kurze Antwort: Weil die meisten modernen Datenschutzgesetze demselben Rahmenwerk nachempfunden sind. Ob saudisches PDPL, VAE, Bahrain, Katar, Oman, Kenia, Nigeria, Südafrika oder die DSGVO der EU – sie laufen alle auf dieselben Kernanforderungen hinaus: nur das Notwendige erheben, es absichern, transparent sein, die Rollen von Verantwortlichem und Auftragsverarbeiter definieren und die grenzüberschreitende Übermittlung kontrollieren.

Die gemeinsame Struktur

Nahezu jedes Regelwerk dieser Familie stellt dieselben fünf Fragen:

1. **Was ist Ihre Rechtsgrundlage** für die Verarbeitung personenbezogener Daten?
2. **Wie wenig können Sie erheben** und dennoch den Zweck erreichen?
(Datenminimierung)
3. **Wie wird es abgesichert** – technisch, vertraglich, organisatorisch?
4. **Wer ist Verantwortlicher und wer ist Auftragsverarbeiter**, und ist das schriftlich festgehalten?
5. **Wohin gehen die Daten**, und welche Schutzmaßnahmen gelten für eine grenzüberschreitende Übermittlung?

Der Wortlaut und die Schwellenwerte unterscheiden sich. Die Architektur, die erforderlich ist, um diese Fragen gut zu beantworten, unterscheidet sich nicht.

Warum das für ein Sicherheitsprodukt wichtig ist

Die meisten Sicherheitstools erzeugen Compliance-Aufwand, weil sie kontinuierlich Endpoint-Telemetriedaten – oft einschließlich Kontodetails und Dateiartefakten – an eine Anbieter-Cloud in einer anderen Rechtsordnung übermitteln. Das ist eine fortlaufende grenzüberschreitende Übermittlung, die in jedem dieser Regelwerke begründet, dokumentiert und verteidigt werden muss.

Die Antwort von Cyber Crucible ist strukturell und nicht verfahrenstechnisch:

- **Inhalte, Zugangsdaten, Schlüssel und Tokens werden niemals erfasst**, sodass die risikoreichsten Kategorien schon durch das Design fehlen.
- **Die Analyse erfolgt lokal auf dem Endpoint**, sodass der Schutz keine Datenbewegung erfordert.
- **Die Bereitstellung kann vollständig air-gapped erfolgen**, wodurch keinerlei ausgehende Telemetriedaten entstehen – was bedeutet, dass von vornherein keine Übermittlung zu bewerten ist.

Dieser letzte Punkt ist der entscheidende. Der größte Teil der Compliance-Schwierigkeiten in dieser Kategorie entsteht durch grenzüberschreitenden Datenfluss. Ein Produkt, das mit null ausgehender Telemetrie arbeiten kann, **beseitigt die Frage, anstatt sie zu beantworten**.

“ **Keine Rechtsberatung.** Diese Seiten beschreiben, wie das Produkt konzipiert ist, um Sie bei der Erfüllung Ihrer Pflichten zu unterstützen. Das Datenschutzrecht ändert sich, und für mehrere der unten genannten Regelwerke werden noch Vorschriften erlassen. Überprüfen Sie die aktuellen Anforderungen mit Ihrem eigenen Rechtsberater und Datenschutzbeauftragten.

Welche Golfstaaten verfügen über Datenschutzgesetze, und wie unterscheiden sie sich?

Kurze Antwort: Fünf der sechs GCC-Staaten verfügen mittlerweile über umfassende Datenschutzgesetze — Saudi-Arabien, die VAE, Bahrain, Katar und Oman. Kuwait bildet die Ausnahme und verfolgt stattdessen einen sektoralen Ansatz. Die Unterschiede liegen vor allem in der Strenge der Einwilligungsanforderungen, der Präferenz für Datenlokalisierung und dem Übermittlungsmechanismus.

Das regionale Bild

Rechtsraum	Status	Unterscheidungsmerkmal
Saudi-Arabien	PDPL in Kraft (volle Wirksamkeit ab September 2024)	Stärkste Präferenz für Lokalisierung; von der SDAIA genehmigte SCCs
VAE	Bundesdekret-Gesetz 45/2021	DSGVO-ähnliche Rechtsgrundlagen; DIFC und ADGM betreiben eigenständige Regelwerke
Bahrain	In Kraft seit 2019	Stark an der DSGVO orientiert; extraterritoriale Reichweite; ausgereifte Durchsetzung
Katar	In Kraft seit 2017	Früheste Regelung in der Region; stärker einwilligungszentriert
Oman	Volle Wirksamkeit 5. Februar 2026	Orientiert sich an DSGVO-Grundsätzen; Übergangsfrist läuft aus
Kuwait	Kein umfassendes Gesetz	Nur sektoral — CITRA-Regelung für Telekommunikation und IT

Status zum Zeitpunkt der Veröffentlichung; bitte mit lokaler Rechtsberatung bestätigen.

Die wichtigste Unterscheidungsachse

In der Praxis unterscheiden sich diese Regelwerke vor allem in zwei Punkten:

- **Strenge der Einwilligung.** Katar und Saudi-Arabien tendieren zu einem einwilligungszentrierten Ansatz. Die VAE erlauben eine breitere Palette an Rechtsgrundlagen, näher an der DSGVO.
- **Präferenz für Lokalisierung.** Saudi-Arabien ist hier am strengsten; die VAE und Katar verfolgen einen stärker risikobasierten, schutzmaßnahmenorientierten Ansatz.

Warum eine Architektur alle sechs beantwortet

Die Regelwerke sind sich beim Mechanismus uneinig, stimmen aber in der Substanz überein: das Minimum erheben, es absichern, kontrollieren, wohin es gelangt.

Da Cyber Crucible niemals Schlüssel, Zugangsdaten, Token oder Inhalte erhebt und air-gapped mit null ausgehender Telemetrie betrieben werden kann, fällt die Antwort auf die Frage „Welche personenbezogenen Daten hält dieser Anbieter, und wohin gelangen sie?“ in jedem dieser Regelwerke kurz aus. Wer die strengste Anforderung — Saudi-Arabien — erfüllt, deckt die übrigen mit ab.

Oman hat kurzfristig Priorität für alle, die ihren Stack noch nicht überprüft haben, angesichts des Termins im Februar 2026.

“ Länderspezifische Details finden sich in den **Country Compliance Guides**.

Wie wirken sich afrikanische Datenschutzgesetze auf die Auswahl von Sicherheitsanbietern aus?

Kurze Antwort: Die meisten afrikanischen Rechtsordnungen schränken die grenzüberschreitende Übermittlung ein, und mehrere gehen noch weiter mit strikter Datenlokalisierung — Nigeria und Sambia verlangen, dass personenbezogene Daten im Land gespeichert werden. Das schließt cloudabhängige Sicherheitstools strukturell aus, nicht nur vertraglich.

Das regionale Bild

Rechtsordnung	Rahmenwerk	Position zum Verlassen von Daten aus dem Land
Nigeria	Data Protection Act 2023	Lokalisierung — personenbezogene Daten von Bürgern müssen in Nigeria gespeichert werden
Sambia	Data Protection Act, Teil X	Lokalisierung — Abschnitt 70 verlangt Speicherung auf einem Server innerhalb Sambias
Kenia	Data Protection Act 2019	Übermittlung eingeschränkt; sensible Daten benötigen Zustimmung und Schutzmaßnahmen
Südafrika	POPIA (2013)	Zustimmung oder Zielland mit im Wesentlichen ähnlichem Schutz
Ägypten	Datenschutzgesetz	Vorherige Genehmigung für Übermittlung erforderlich
Ruanda	Von der NCSA beaufsichtigtes Gesetz	Sektorale Lokalisierung — Banken müssen Primärdaten in Ruanda vorhalten
Ghana	Datenschutzrahmenwerk	Bemerkenswerte Ausnahme — keine zusätzlichen grenzüberschreitenden Bedingungen
Marokko	Gesetz 09-08 + Dekret 2-09-165	Von der CNDP beaufsichtigt; etabliertes Regime

Rechtsordnung	Rahmenwerk	Position zum Verlassen von Daten aus dem Land
Libyen	Noch kein umfassendes Rahmenwerk	Souveränität ist eine kommerzielle, keine rechtliche Entscheidung

Stand zum Zeitpunkt der Erstellung; bitte mit örtlicher Rechtsberatung bestätigen.

Das Muster, das man verstehen sollte

Es zeigen sich drei unterschiedliche Modelle, die jeweils unterschiedliche Anforderungen an einen Anbieter stellen:

1. **Vorgaben zum Speicherort** (Nigeria, Sambia; Ruanda für den Bankensektor). Verträge und Verschlüsselung erfüllen diese Anforderungen nicht — nur der physische Speicherort der Daten zählt.
2. **Bedingte Übermittlung** (Kenia, Südafrika). Zulässig mit Schutzmaßnahmen, Zustimmung oder Angemessenheit — eine Bewertung, die Sie nachweisen müssen.
3. **Genehmigungspflichtige Übermittlung** (Ägypten). Vorherige Genehmigung, mit Risiken hinsichtlich Zeitpunkt und Verlängerung.

Sektorale Vorschriften fügen häufig zusätzliche Lokalisierungsanforderungen hinzu, insbesondere im Finanzdienstleistungssektor.

Warum dies eine lokale Verarbeitungsarchitektur begünstigt

Ein Sicherheitsprodukt, das darauf ausgelegt ist, Endpunkt-Telemetriedaten an eine Anbieter-Cloud zu senden, exportiert von Natur aus personenbezogene Daten als Voraussetzung für seine Funktionsweise. Unter Modell 1 ist dies nicht behebbar.

Cyber Crucible analysiert am Endpunkt und kann vollständig On-Premises betrieben werden, ohne ausgehende Telemetriedaten — so verlassen die Daten nie das Unternehmen, und die Frage der Übermittlung stellt sich gar nicht erst.

“ Länderspezifische Details finden Sie in den **Country Compliance Guides**.

Was gilt in Europa und im Vereinigten Königreich?

Kurze Antwort: Die EU-DSGVO und die UK-DSGVO, die sich eng aneinander orientieren. Die praktischen Kontrollen sind identisch; die Hauptabweichung besteht darin, welches Instrument internationale Übermittlungen regelt – die EU-Standardvertragsklauseln (SCCs) gegenüber dem britischen IDTA oder Addendum.

Die beiden Regelwerke

	EU-DSGVO	UK-DSGVO + DPA 2018
Aufsichtsbehörde	Nationale Datenschutzbehörden / EDPB	Information Commissioner's Office (ICO)
Übermittlungsinstrument	EU-Standardvertragsklauseln	International Data Transfer Agreement, oder UK Addendum zu den EU-SCCs
Grundsätze, Rechtsgrundlagen, Pflichten der Verarbeiter	Weitgehend identisch	Weitgehend identisch

Was das in der Praxis bedeutet

Organisationen, die in beiden Regelwerken tätig sind, müssen beide erfüllen, aber die zugrunde liegenden Kontrollen überschneiden sich fast vollständig. Für ein Regelwerk durchgeführte Anbieterbewertungen lassen sich auf das andere übertragen, wobei lediglich das Übermittlungsinstrument ausgetauscht wird.

Warum die anderen Regelwerke in diesem Buch hier ebenfalls von Bedeutung sind

Die DSGVO ist die Vorlage, an der sich die meisten neueren Datenschutzgesetze weltweit orientieren. Bahrain und Oman bilden sie eng nach; Kenia, Nigeria und Südafrika übernehmen ihre Struktur. Arbeit, die zur Erfüllung der DSGVO geleistet wird, ist anderswo selten vergeblich –

deshalb bewerten Organisationen, die in mehreren dieser Märkte tätig sind, Anbieter in der Regel anhand des strengsten anwendbaren Regelwerks statt jedes einzeln.

“ Länderspezifische Details finden Sie in den **Country Compliance Guides**.

Ist Cyber Crucible ein Verantwortlicher oder ein Auftragsverarbeiter für Daten?

Kurze Antwort: In den meisten Engagements agiert Cyber Crucible als **Auftragsverarbeiter** im Auftrag des Kunden, der der Verantwortliche ist. Der Kunde legt die Zwecke und Mittel der Verarbeitung fest; Cyber Crucible verarbeitet Daten nur gemäß den dokumentierten Anweisungen des Verantwortlichen, im Rahmen einer schriftlichen Auftragsverarbeitungsvereinbarung (Data Processing Agreement).

Warum diese Unterscheidung wichtig ist

Fast jedes Regelwerk in dieser Familie — PDPL, GDPR und deren Ableitungen — verteilt Pflichten nach Rolle. Verantwortliche entscheiden, warum und wie Daten verarbeitet werden, und tragen die schwerwiegenden Pflichten: die Information betroffener Personen, die Bearbeitung von Rechteinfragen und in manchen Fällen die Registrierung.

Auftragsverarbeiter müssen rechtmäßigen Anweisungen folgen und die Daten schützen. Unter PDPL würde ein Auftragsverarbeiter, der Daten über die Anweisungen des Verantwortlichen hinaus nutzt, selbst als Verantwortlicher behandelt werden — weshalb der Umfang vertraglich festgelegt und nicht der Auslegung überlassen wird.

In der Praxis

Cyber Crucible arbeitet im Rahmen einer schriftlichen Auftragsverarbeitungsvereinbarung oder eines Dienstleistungsvertrags, der den Umfang der Verarbeitung festlegt, und verwendet oder speichert Daten nicht außerhalb dieser Anweisungen weiter.

Da es sich normalerweise um einen Auftragsverarbeiter handelt, liegen die verantwortlichenspezifischen Pflichten bei Ihnen: die Information betroffener Personen über die Verarbeitung, die Beantwortung von Rechteinfragen und Ähnliches.

Die Ausnahme

Nur wenn Cyber Crucible personenbezogene Daten für eigene Zwecke verarbeiten würde, wäre es ein Verantwortlicher, und würde dann vollständige Verantwortlichen-Pflichten übernehmen, einschließlich Registrierung und Einwilligung, sofern zutreffend. Das ist nicht das Betriebsmodell.

Wie werden grenzüberschreitende Datenübertragungen gehandhabt?

Kurze Antwort: Über den von der jeweiligen Rechtsordnung anerkannten Mechanismus – von der SDAIA genehmigte Standardvertragsklauseln für saudische Daten, gleichwertige vertragliche Schutzmaßnahmen anderswo – gestützt durch eine abgeschlossene Transfer Risk Assessment. Oder gänzlich vermieden, indem so bereitgestellt wird, dass keine Daten eine Grenze überschreiten.

Der vertragliche Weg

Für personenbezogene Daten saudischen Ursprungs verwendet Cyber Crucible von der SDAIA vorab genehmigte SCCs, die unverändert übernommen werden – abgesehen von erforderlichen Feldern –, in Kundenverträge oder DPAs integriert und auf jede nachgelagerte Übertragung an Unterauftragsverarbeiter ausgeweitet werden.

Andere Rechtsordnungen erkennen vergleichbare Mechanismen an – Angemessenheitsbeschlüsse, Standardklauseln oder Einwilligung plus Schutzmaßnahmen. Die gemeinsame Anforderung besteht darin, dass der Importeur vertraglich zu Schutzmaßnahmen verpflichtet ist, die dem Recht des Exportlandes gleichwertig sind.

Die Transfer Risk Assessment

Wenn die Übertragung auf Schutzmaßnahmen wie SCCs beruht oder sensible Daten betrifft, ist in der Regel eine Risikobewertung erforderlich. Cyber Crucible hat eine TRA durchgeführt, die die Art der Datenflüsse, das Rechtssystem des Zielstaates, die vorhandenen technischen und organisatorischen Kontrollen sowie Restrisiken bewertet – mit dokumentierten Abhilfemaßnahmen wie Datenminimierung, Verschlüsselung, vertraglichen Regelungen und Vorfallsbehandlung.

Der architektonische Weg

Vertragliche Mechanismen steuern eine Übertragung. Keine Übertragung durchzuführen, beseitigt sie.

- **Air-gapped vor Ort** – keinerlei ausgehende Telemetrie, sodass überhaupt keine Übertragung stattfindet.
- **Regionales Staging** – Infrastruktur so positioniert, dass die Verarbeitung innerhalb Ihrer Rechtsordnung verbleibt.

Für Rechtsordnungen mit Lokalisierungsanforderungen – Nigeria ist das klarste Beispiel – ist dies oft die einzig saubere Lösung.

“ Dokumentation verfügbar unter **dpo@cybercrucible.com**.

Erfasst Cyber Crucible sensible personenbezogene Daten?

Kurze Antwort: Nein. Cyber Crucible erfasst keine der Kategorien, die diese Gesetze als sensibel definieren – biometrische, gesundheitsbezogene oder genetische Daten oder Daten, die die rassische oder ethnische Herkunft, religiöse Überzeugungen oder politische Meinungen offenbaren. Die Telemetrie konzentriert sich auf Systemverhalten und Sicherheitsereignisse, nicht auf personenbezogene Merkmale.

Warum diese Kategorie gar nicht relevant wird

Die Aufgabe der Software besteht darin, festzustellen, ob ein *Programm* sich bösartig verhält. Dafür ist keinerlei Wissen über eine *Person* erforderlich. Sensible personenbezogene Daten spielen in der Erkennungslogik keine Rolle und werden daher nicht erfasst.

Warum dies überproportional wichtig ist

Sensible Daten unterliegen in praktisch jedem Regelwerk der strengsten Behandlung – ausdrückliche Einwilligung, zusätzliche Schutzmaßnahmen, obligatorische Risikobewertungen vor einer Übermittlung und in manchen Rechtsordnungen Registrierungspflichten, die andernfalls nicht bestehen würden.

Kenia beispielsweise erlaubt die Übermittlung sensibler personenbezogener Daten nur dann, wenn die betroffene Person eingewilligt hat **und** angemessene Schutzmaßnahmen bestehen. Ein Anbieter, der niemals sensible Daten erfasst, umgeht diesen Weg vollständig.

Datenminimierung

Es werden ausschließlich die personenbezogenen Daten erfasst, die für den Sicherheitszweck unbedingt erforderlich sind. Kunden können zudem selbst festlegen, welche Telemetriequellen erfasst werden, und Felder, die für die Bedrohungserkennung nicht wesentlich sind, werden ausgeschlossen oder umgehend verworfen.

Welche Schutzmaßnahmen schützen personenbezogene Daten, die von Cyber Crucible verarbeitet werden?

Kurze Antwort: Verschlüsselung während der Übertragung und im Ruhezustand, Pseudonymisierung von Identifikatoren, soweit möglich, rollenbasierte Zugriffskontrolle, Schlüsselverwaltung mit Rotation, Audit-Protokollierung und regelmäßige Schwachstellen-Scans – abgesichert durch vertragliche Regelungen in den Auftragsverarbeitungsverträgen (DPAs) der Kunden sowie durch ein internes Informationssicherheitsprogramm.

Technisch

- Personenbezogene Daten werden **bei der Übertragung** (TLS 1.3) und **im Ruhezustand** verschlüsselt.
- Pro-Agent-JSON-Web-Encryption der operativen Nutzdaten unter Verwendung eindeutiger Schlüsselpaare.
- Sensible Identifikatoren werden, wo immer möglich, pseudonymisiert oder anonymisiert.
- Der Zugriff wird durch Authentifizierung und rollenbasierte Berechtigungen kontrolliert.
- Richtlinien zur kryptografischen Schlüsselverwaltung stellen sicher, dass Schlüssel sicher gespeichert und regelmäßig rotiert werden.
- Protokollierung und Auditierung von Zugriffen und administrativen Aktionen zur Erkennung unbefugter Aktivitäten.
- Regelmäßige Schwachstellen-Scans und Sicherheitstests.

Vertraglich

Kundenverträge und DPAs enthalten Bestimmungen zu Datensicherheit, Vertraulichkeit und Meldung von Sicherheitsverletzungen. Unterauftragsverarbeiter werden nur im Rahmen schriftlicher Vereinbarungen eingesetzt, die gleichwertige Schutzmaßnahmen vorschreiben. Mitarbeiter und Auftragnehmer sind durch gegenseitige Vertraulichkeitsvereinbarungen (NDAs) gebunden.

Organisatorisch

Ein Informationssicherheits-Managementprogramm regelt die laufende Einhaltung der Vorgaben, einschließlich Sicherheitsschulungen für relevante Mitarbeiter, dokumentierter Reaktion auf Vorfälle, Verfahren zur Datenaufbewahrung und -löschung sowie regelmäßiger interner Audits.

Zu Zertifizierungen — klar formuliert

Das Sicherheitsprogramm von Cyber Crucible ist **an anerkannten Branchenrahmenwerken ausgerichtet. Cyber Crucible verfügt derzeit nicht über eine ISO 27001- oder SOC 2-Zertifizierung, und eine Zertifizierung ist derzeit nicht geplant.**

Ausrichtung bedeutet, dass die Kontrollen den in diesen Rahmenwerken beschriebenen Praktiken folgen. Es bedeutet nicht, dass ein externer Auditor diese bewertet und zertifiziert hat, und dies sollte in Ihrer eigenen Compliance-Dokumentation nicht so dargestellt werden. Wenn Ihr Beschaffungsprozess zertifizierte Nachweise erfordert, wird diese Anforderung derzeit nicht erfüllt – wenden Sie sich an **dpo@cybercrucible.com**, um zu besprechen, welche Dokumentation verfügbar ist.

Muss ich einen lokalen Vertreter benennen?

Kurze Antwort: In der Regel muss dies Ihre Organisation tun, nicht Cyber Crucible. Mehrere Regelwerke verlangen, dass Einrichtungen außerhalb des Landes, die personenbezogene Daten von Ansässigen verarbeiten, einen lokalen Vertreter benennen — und da Cyber Crucible üblicherweise als Auftragsverarbeiter agiert, liegt diese Pflicht bei Ihnen als Verantwortlichem.

Wie sich die Rollen aufteilen

- **Cyber Crucible als Auftragsverarbeiter (Regelfall):** Sie als Verantwortlicher benennen den lokalen Vertreter. Cyber Crucible kooperiert vollumfänglich bei lokalen Compliance-Pflichten.
- **Cyber Crucible als Verantwortlicher (Ausnahmefall):** Würde Cyber Crucible personenbezogene Daten für eigene Zwecke verarbeiten, würde es einen lokalen Vertreter in der jeweiligen Rechtsordnung stellen.

Artikel 33 des saudi-arabischen PDPL ist das eindeutigste Beispiel für diese Anforderung, doch ähnliche Bestimmungen finden sich in der gesamten von der DSGVO abgeleiteten Regelwerksfamilie.

Zur Registrierung von Verantwortlichen

Einige Regelwerke verlangen, dass bestimmte Verantwortliche sich bei der Aufsichtsbehörde registrieren — typischerweise öffentliche Stellen, Einrichtungen, deren Haupttätigkeit die Verarbeitung personenbezogener Daten ist, oder solche, die mit hochriskanten sensiblen Daten umgehen.

Das Kerngeschäft von Cyber Crucible ist Cybersicherheitssoftware und nicht die allgemeine Verarbeitung personenbezogener Daten, weshalb es nicht in diese Kategorien fällt. Registrierungs Vorschriften werden beobachtet, und bei einer Änderung der Rolle oder der Tätigkeiten würde die entsprechende Compliance sichergestellt.

Wie fordere ich Compliance-Dokumentation an?

Kurze Antwort: Wenden Sie sich an den Datenschutzbeauftragten unter **dpo@cybercrucible.com**. Verfügbare Dokumentation umfasst Standard Contractual Clauses, die Transfer Risk Assessment, Data Processing Agreements und die Data-Governance-Richtlinie — bereitgestellt vorbehaltlich angemessener Vertraulichkeitsmaßnahmen.

Was Sie anfordern können

- **Standard Contractual Clauses** — einschließlich der von der SDAIA vorab genehmigten Klauseln für Übermittlungen nach Saudi-Arabien.
- **Transfer Risk Assessment** — die abgeschlossene TRA, die Datenflüsse, das Rechtsregime des Zielstaats, Kontrollen und Abhilfemaßnahmen abdeckt.
- **Data Processing Agreement** — mit Definition des Verarbeitungsumfangs, der Sicherheitsbestimmungen, der Vertraulichkeit und der Meldung von Verstößen.
- **Data-Governance- und -Sharing-Richtlinie** — Erhebungsbeschränkungen, Schutz während der Übertragung und Verpflichtungen zur Nicht-Weitergabe an Dritte.

Was Sie in Ihre Anfrage aufnehmen sollten

Es beschleunigt den Vorgang erheblich, wenn Sie Ihre Jurisdiktion angeben, ob Sie als Verantwortlicher (Controller) auftreten, welches Deployment-Modell Sie prüfen (air-gapped, regional oder hybrid), und welche Anforderungen Ihre eigene Aufsichtsbehörde oder Ihr Auditor stellt.

Für hier nicht abgedeckte Jurisdiktionen

Die in diesem Leitfaden beschriebenen Regelwerke sind diejenigen, nach denen am häufigsten gefragt wird. Sollte Ihre Jurisdiktion nicht aufgeführt sein, sind die zugrunde liegenden Antworten in der Regel dieselben — minimale Datenerhebung, lokale Verarbeitung und im Land verfügbare Deployment-Optionen. Wenden Sie sich mit der konkreten Anforderung an den DPO, damit diese direkt geklärt werden kann.