

# 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.

---

Revision #1

Created 2026-07-24 04:43:49 UTC by Dennis Underwood

Updated 2026-07-24 04:43:49 UTC by Dennis Underwood