Does Cyber Crucible comply with Saudi Arabia's PDPL?

Short answer: Cyber Crucible has reviewed its operations against Saudi Arabia's Personal Data Protection Law, uses SDAIA-approved Standard Contractual Clauses for any transfer of Saudi-origin personal data, and can be deployed entirely inside the Kingdom with zero cross-border flow. It collects only system and security telemetry — never file contents, documents, email, or communications.

What the law requires

PDPL took effect 14 September 2023 with a grace period to 14 September 2024. Saudi Arabia maintains among the strongest localization preferences in the Gulf, and the Saudi Data & AI Authority (SDAIA) supervises. Transfers out of the Kingdom require a recognized safeguard plus, in most cases, a Transfer Risk Assessment.

What specifically applies here

- **SDAIA pre-approved SCCs** are used for any transfer of Saudi-origin personal data to the United States, adopted without modification apart from required fields, and extended to any onward sub-processor.
- **A Transfer Risk Assessment** has been completed following SDAIA's structured guidance — data flows, destination legal regime, controls, residual risk, documented mitigations.
- **Processor role** — Cyber Crucible normally acts as processor under a written DPA; the Saudi customer is controller.
- **Article 33 local representative** — as processor, that obligation sits with you as controller.

The cleanest route

Given the localization preference, the fully on-premises air-gapped deployment is the strongest answer: all backend management inside your own physically secured racks, zero outbound telemetry. Where nothing crosses the border, transfer obligations do not arise.

> SCCs and the TRA available from **dpo@cybercrucible.com**. Status at time of writing — confirm current requirements with local counsel.

Revision #2
Created 2026-07-21 19:00:01 UTC by Dennis Underwood
Updated 2026-07-21 19:33:08 UTC by Dennis Underwood