Does Cyber Crucible comply with Morocco's data protection law?

Short answer: Yes. Morocco's Law No. 09-08 and its implementing decree govern personal data processing, supervised by the CNDP. The same controls apply — minimal collection, documented processor role, strong safeguards, and in-country or air-gapped deployment where preferred.

What the law requires

Morocco's framework rests on **Law No. 09-08** on the protection of individuals with regard to the processing of personal data, together with implementing **Decree No. 2-09-165**. The **CNDP** (Commission Nationale de contrôle de la protection des Données à caractère Personnel) is the supervisory authority, and is active in international cooperation on emerging issues including AI.

What specifically applies here

Morocco's regime is among the more established in North Africa, with a functioning authority and notification/authorization procedures that vary by processing type. Practical implications for vendor assessment:

- **Enumerate what is collected.** Cyber Crucible's excluded-data list is explicit — no keys, credentials, tokens, or content — which supports notification accuracy.
- **Processor role** under a written DPA on documented instructions.
- **Transfer** — regional staging or air-gapped deployment; the latter removes the question.

For organizations operating across the Maghreb

Requirements differ considerably between Morocco, Tunisia, Algeria, and Libya. Selecting a vendor that meets the strictest applicable regime — rather than assessing each separately — is usually the lower-effort path.

> Status at time of writing — confirm with local counsel.

Revision #2
Created 2026-07-21 19:00:14 UTC by Dennis Underwood
Updated 2026-07-21 19:33:20 UTC by Dennis Underwood