Does Cyber Crucible comply with India's Digital Personal Data Protection Act (DPDP)?

Short answer: Cyber Crucible supports a data fiduciary's obligations under India's Digital Personal Data Protection Act by acting as a data processor that collects essentially no personal data and processes on the endpoint. Because customer content is never collected, the consent, purpose-limitation, and erasure obligations have minimal surface in its custody.

How it aligns

- **Processor role** under contract with the data fiduciary.
- **Data minimization** — no customer content, credentials, or keys collected.
- **Security safeguards and breach support** for the fiduciary's obligations.

Vendor-selection notes

India notified the DPDP Rules, 2025 in November 2025, with substantive obligations phasing in over roughly the following 18 months, so the operational detail (consent management, breach reporting, cross-border mechanics) is still coming into force. On-premises deployment supports data-residency preferences in the meantime. Cyber Crucible holds no Indian certification and supports, rather than assumes, the fiduciary's duties. Documentation is available on request.

Revision #2
Created 2026-07-23 15:18:54 UTC by Dennis Underwood
Updated 2026-07-23 18:20:19 UTC by Dennis Underwood