How does Cyber Crucible support the newer 2025–2026 state privacy laws?

Short answer: A wave of comprehensive state privacy laws took effect across 2025 and 2026 — including New Jersey, Delaware, Iowa, Nebraska, New Hampshire, Tennessee, Minnesota, Maryland, and, in 2026, Indiana, Kentucky, and Rhode Island. They share a common structure, and Cyber Crucible's processor role and no-collection design support all of them the same way: little personal data in custody, contractually limited processing, and reasonable security.

The common structure these laws share

- A required processor contract limiting the vendor to the controller's instructions.
- Data-minimization and purpose-limitation duties.
- Consumer rights (access, deletion, opt-out), increasingly with universal opt-out signals.
- Reasonable security safeguards and breach notification.

Why one answer covers the set

Because Cyber Crucible never collects customer content, credentials, or keys and processes on the endpoint, the obligations that vary between states — mostly about handling and disclosing personal data — have very little to attach to. A single, consistent data processing agreement supports the set. Maryland's law is worth noting for its stricter data-minimization standard, which the no-collection design supports well.

The honest boundary

State thresholds and effective dates change, and this is not legal advice; a controller should confirm which laws apply to it. Cyber Crucible holds no state "certification" — it supports the controller's obligations. Documentation is available from **dpo@cybercrucible.com**.

Revision #2
Created 2026-07-23 15:18:48 UTC by Dennis Underwood
Updated 2026-07-23 18:20:14 UTC by Dennis Underwood