

Which US state privacy and security laws affect security-vendor selection?

Short answer: A growing patchwork of US state laws imposes obligations that flow down to a company's vendors — comprehensive privacy acts (California, Virginia, Colorado, Texas, and others), sector rules like New York DFS Part 500 for financial services, data-security mandates like Massachusetts 201 CMR 17.00, biometric laws like Illinois BIPA, and breach-notification statutes in every state. The common thread is that a buyer must confirm its security vendor minimizes data, contracts appropriately, and secures what it touches.

What these laws generally ask of a vendor

- A written contract (data processing agreement) limiting the vendor to the customer's instructions.
- Data minimization and purpose limitation.
- Reasonable security safeguards and prompt breach notification.
- Support for consumer rights (access, deletion) where personal data is processed.

Why Cyber Crucible answers most of this structurally

Because Cyber Crucible never collects customer content, credentials, or keys and processes on the endpoint, the highest-risk obligations have little to bite on — there is minimal personal data in its custody. A data processing agreement and supporting documentation are available from **dpo@cybercrucible.com**. The pages in this book address the specific state rules a reviewer is most likely to cite.

Revision #2

Created 2026-07-23 15:18:34 UTC by Dennis Underwood

Updated 2026-07-23 18:20:02 UTC by Dennis Underwood