

¿Qué leyes estatales de EE. UU. sobre privacidad y seguridad afectan la selección de proveedores de seguridad?

Respuesta breve: Un mosaico cada vez mayor de leyes estatales de EE. UU. impone obligaciones que se trasladan a los proveedores de una empresa — leyes integrales de privacidad (California, Virginia, Colorado, Texas y otras), normas sectoriales como el New York DFS Part 500 para servicios financieros, mandatos de seguridad de datos como Massachusetts 201 CMR 17.00, leyes biométricas como Illinois BIPA, y estatutos de notificación de brechas en todos los estados. El hilo común es que un comprador debe confirmar que su proveedor de seguridad minimiza los datos, contrata de manera adecuada y protege todo lo que maneja.

Qué exigen generalmente estas leyes a un proveedor

- Un contrato escrito (acuerdo de procesamiento de datos) que limite al proveedor a las instrucciones del cliente.
- Minimización de datos y limitación de la finalidad.
- Medidas de seguridad razonables y notificación oportuna de brechas.
- Soporte para los derechos del consumidor (acceso, eliminación) cuando se procesan datos personales.

Por qué Cyber Crucible responde a la mayor parte de esto de manera estructural

Debido a que Cyber Crucible nunca recopila contenido del cliente, credenciales o claves, y procesa en el endpoint, las obligaciones de mayor riesgo tienen poco margen de aplicación — hay una cantidad mínima de datos personales bajo su custodia. Un acuerdo de procesamiento de datos y la documentación de respaldo están disponibles a través de **dpo@cybercrucible.com**. Las páginas

de este libro abordan las normas estatales específicas que un revisor probablemente citará.

Revision #1

Created 2026-07-24 02:05:35 UTC by Dennis Underwood

Updated 2026-07-24 02:05:35 UTC by Dennis Underwood