Quais leis estaduais dos EUA sobre privacidade e segurança afetam a seleção de fornecedores de segurança?

Resposta curta: Um conjunto crescente e fragmentado de leis estaduais dos EUA impõe obrigações que se estendem aos fornecedores de uma empresa — leis abrangentes de privacidade (Califórnia, Virgínia, Colorado, Texas, entre outras), regras setoriais como o New York DFS Part 500 para o setor financeiro, exigências de segurança de dados como o Massachusetts 201 CMR 17.00, leis sobre dados biométricos como o Illinois BIPA, e estatutos de notificação de violação de dados em todos os estados. O elemento comum é que o comprador deve confirmar que seu fornecedor de segurança minimiza os dados, contrata de forma adequada e protege tudo o que manuseia.

O que essas leis geralmente exigem de um fornecedor

- Um contrato por escrito (acordo de processamento de dados) que limite o fornecedor às instruções do cliente.
- Minimização de dados e limitação de finalidade.
- Salvaguardas de segurança razoáveis e notificação imediata em caso de violação.
- Suporte aos direitos do consumidor (acesso, exclusão) quando dados pessoais forem processados.

Por que a Cyber Crucible atende a isso de forma estrutural

Como a Cyber Crucible nunca coleta conteúdo, credenciais ou chaves do cliente e realiza o processamento no endpoint, as obrigações de maior risco têm pouco a que se aplicar — há uma quantidade mínima de dados pessoais sob sua custódia. Um acordo de processamento de dados e a documentação de suporte estão disponíveis em **dpo@cybercrucible.com**. As páginas deste livro abordam as regras estaduais específicas que um avaliador tem maior probabilidade de citar.

Revision #1
Created 2026-07-24 06:04:20 UTC by Dennis Underwood
Updated 2026-07-24 06:04:21 UTC by Dennis Underwood