Quais regras da UE afetam a seleção de um fornecedor de segurança, além do GDPR?

Resposta curta: Além do GDPR, três regimes da UE moldam cada vez mais a seleção de fornecedores: o DORA (resiliência operacional para entidades financeiras e seus prestadores de TIC), o NIS2 (obrigações de cibersegurança para entidades essenciais e importantes, incluindo a segurança da cadeia de suprimentos) e o EU AI Act (regras escalonadas por risco para sistemas de IA). Cada um deles impõe obrigações aos fornecedores. O design da Cyber Crucible — sem coleta de conteúdo do cliente, processamento local, opção on-premises — apoia as obrigações do cliente em relação a todos eles, sem que a Cyber Crucible reivindique conformidade em nome do cliente.

Panorama geral

- **GDPR** — a base para o processamento de dados pessoais em toda a UE. Consulte os Guias de Conformidade por País para a página do GDPR.
- **DORA** — aplica-se a partir de 17 de janeiro de 2025 a entidades financeiras e, de forma importante, aos seus prestadores terceirizados de serviços de TIC.
- **NIS2** — os Estados-Membros deveriam transpô-lo até outubro de 2024; a partir de 2026, a maioria já o fez, embora vários ainda estivessem finalizando a legislação nacional.
- **EU AI Act** — obrigações escalonadas por risco, em fase de implementação até 2026–2027.

Como a Cyber Crucible se encaixa

O tema recorrente é o risco de cadeia de suprimentos e de terceiros. Como a Cyber Crucible não coleta conteúdo do cliente, credenciais ou chaves, e pode operar inteiramente dentro do perímetro do cliente, ela reduz a superfície que esses regimes foram elaborados para controlar. As páginas deste livro abordam cada regime e os principais Estados-Membros. A documentação está disponível em **dpo@cybercrucible.com**.

Revision #1
Created 2026-07-24 06:07:37 UTC by Dennis Underwood
Updated 2026-07-24 06:07:37 UTC by Dennis Underwood