Welche EU-Vorschriften wirken sich neben der DSGVO auf die Auswahl eines Sicherheitsanbieters aus?

Kurze Antwort: Neben der DSGVO prägen zunehmend drei EU-Regelwerke die Auswahl von Anbietern: DORA (operative Resilienz für Finanzunternehmen und deren IKT-Dienstleister), NIS2 (Cybersicherheitspflichten für wesentliche und wichtige Einrichtungen, einschließlich der Sicherheit der Lieferkette) und das EU-KI-Gesetz (risikoabgestufte Vorschriften für KI-Systeme). Jedes dieser Regelwerke verlagert Pflichten in Richtung der Anbieter. Das Design von Cyber Crucible — keine Erfassung von Kundeninhalten, lokale Verarbeitung, Option zum On-Premises-Betrieb — unterstützt die Pflichten des Kunden im Rahmen all dieser Regelwerke, ohne dass Cyber Crucible eine Compliance im Namen des Kunden beansprucht.

Die Landschaft im Überblick

- **DSGVO** — die Grundlage für die Verarbeitung personenbezogener Daten in der gesamten EU. Siehe die Country Compliance Guides für die Seite zur DSGVO.
- **DORA** — gilt ab dem 17. Januar 2025 für Finanzunternehmen und, wichtig, für deren IKT-Drittdienstleister.
- **NIS2** — die Mitgliedstaaten sollten die Richtlinie bis Oktober 2024 in nationales Recht umsetzen; Stand 2026 haben dies die meisten getan, während mehrere die nationale Gesetzgebung noch abschließen.
- **EU-KI-Gesetz** — risikoabgestufte Pflichten, die bis 2026–2027 schrittweise in Kraft treten.

Wie Cyber Crucible dazu passt

Das wiederkehrende Thema ist das Risiko der Lieferkette und von Drittanbietern. Da Cyber Crucible keine Kundeninhalte, Zugangsdaten oder Schlüssel erfasst und vollständig innerhalb der Grenzen des Kunden betrieben werden kann, verringert es die Angriffsfläche, die diese Regelwerke eindämmen sollen. Die Seiten in diesem Buch behandeln jedes Regelwerk sowie die größeren Mitgliedstaaten. Dokumentation ist erhältlich unter **dpo@cybercrucible.com**.

Revision #1
Created 2026-07-24 04:58:35 UTC by Dennis Underwood
Updated 2026-07-24 04:58:35 UTC by Dennis Underwood