Which EU rules affect selecting a security vendor, beyond GDPR?

Short answer: Beyond the GDPR, three EU regimes increasingly shape vendor selection: DORA (operational resilience for financial entities and their ICT providers), NIS2 (cybersecurity obligations for essential and important entities, including supply-chain security), and the EU AI Act (risk-tiered rules for AI systems). Each pushes obligations toward vendors. Cyber Crucible's design — no customer content collected, local processing, on-premises option — supports a customer's obligations under all of them, without Cyber Crucible claiming compliance on the customer's behalf.

The landscape at a glance

- **GDPR** — the baseline for personal-data processing across the EU. See the Country Compliance Guides for the GDPR page.
- **DORA** — applies from 17 January 2025 to financial entities and, importantly, to their ICT third-party service providers.
- **NIS2** — member states were to transpose it by October 2024; as of 2026 most have, while several were still finalizing national law.
- **EU AI Act** — risk-tiered obligations phasing in through 2026–2027.

How Cyber Crucible fits

The recurring theme is supply-chain and third-party risk. Because Cyber Crucible collects no customer content, credentials, or keys and can run entirely within the customer's boundary, it reduces the surface these regimes are written to control. The pages in this book address each regime and the larger member states. Documentation is available from **dpo@cybercrucible.com**.

Revision #2
Created 2026-07-23 15:19:05 UTC by Dennis Underwood
Updated 2026-07-23 18:20:29 UTC by Dennis Underwood