Wie unterstützt Cyber Crucible die Datenschutz- und Sicherheitsanforderungen in Deutschland?

Kurze Antwort: In Deutschland unterstützt Cyber Crucible die Verpflichtungen einer Organisation gemäß der GDPR und dem Bundesdatenschutzgesetz (BDSG), indem keine Kundeninhalte, Zugangsdaten oder Schlüssel erfasst werden und die Verarbeitung auf dem Endgerät erfolgt. Für Organisationen, die dem deutschen Cybersicherheitsregime unterliegen (der BSI-Gesetzesrahmen, im Zuge der Umsetzung von NIS2), unterstützt das Design mit lokaler Verarbeitung und On-Premises-Fähigkeit deren Sicherheits- und Lieferkettenverpflichtungen.

Wie die Ausrichtung erfolgt

- **GDPR + BDSG.** Datenminimierung, Verschlüsselung und Zugriffskontrolle unterstützen den deutschen Datenschutzstandard; eine Datenverarbeitungsvereinbarung ist verfügbar.
- **Datenresidenz.** Die On-Premises-Bereitstellung hält personenbezogene Daten dort, wo es erforderlich ist, in Deutschland; keine Kundeninhalte werden zur Sicherheitsverarbeitung ins Ausland übertragen.
- **Cybersicherheitsregime.** Deutschland setzt NIS2 in seinen BSI-Gesetzesrahmen um; Cyber Crucible unterstützt die Risikomanagement- und Lieferkettenmaßnahmen betroffener Einrichtungen.

Die ehrliche Grenze

Die Compliance liegt bei der Organisation und, soweit relevant, bei ihrem Datenschutzbeauftragten und der zuständigen Aufsichtsbehörde. Cyber Crucible verfügt über keine deutsche Zertifizierung und unterstützt diese Pflichten, übernimmt sie jedoch nicht. Dokumentation ist auf Anfrage erhältlich.

Revision #1
Created 2026-07-24 04:59:20 UTC by Dennis Underwood
Updated 2026-07-24 04:59:20 UTC by Dennis Underwood