Welche Schutzmaßnahmen schützen personenbezogene Daten, die von Cyber Crucible verarbeitet werden?

Kurze Antwort: Verschlüsselung während der Übertragung und im Ruhezustand, Pseudonymisierung von Identifikatoren, soweit möglich, rollenbasierte Zugriffskontrolle, Schlüsselverwaltung mit Rotation, Audit-Protokollierung und regelmäßige Schwachstellen-Scans – abgesichert durch vertragliche Regelungen in den Auftragsverarbeitungsverträgen (DPAs) der Kunden sowie durch ein internes Informationssicherheitsprogramm.

Technisch

- Personenbezogene Daten werden **bei der Übertragung** (TLS 1.3) und **im Ruhezustand** verschlüsselt.
- Pro-Agent-JSON-Web-Encryption der operativen Nutzdaten unter Verwendung eindeutiger Schlüsselpaare.
- Sensible Identifikatoren werden, wo immer möglich, pseudonymisiert oder anonymisiert.
- Der Zugriff wird durch Authentifizierung und rollenbasierte Berechtigungen kontrolliert.
- Richtlinien zur kryptografischen Schlüsselverwaltung stellen sicher, dass Schlüssel sicher gespeichert und regelmäßig rotiert werden.
- Protokollierung und Auditierung von Zugriffen und administrativen Aktionen zur Erkennung unbefugter Aktivitäten.
- Regelmäßige Schwachstellen-Scans und Sicherheitstests.

Vertraglich

Kundenverträge und DPAs enthalten Bestimmungen zu Datensicherheit, Vertraulichkeit und Meldung von Sicherheitsverletzungen. Unterauftragsverarbeiter werden nur im Rahmen schriftlicher Vereinbarungen eingesetzt, die gleichwertige Schutzmaßnahmen vorschreiben. Mitarbeiter und Auftragnehmer sind durch gegenseitige Vertraulichkeitsvereinbarungen (NDAs) gebunden.

Organisatorisch

Ein Informationssicherheits-Managementprogramm regelt die laufende Einhaltung der Vorgaben, einschließlich Sicherheitsschulungen für relevante Mitarbeiter, dokumentierter Reaktion auf Vorfälle, Verfahren zur Datenaufbewahrung und -löschung sowie regelmäßiger interner Audits.

Zu Zertifizierungen — klar formuliert

Das Sicherheitsprogramm von Cyber Crucible ist **an anerkannten Branchenrahmenwerken ausgerichtet**. **Cyber Crucible verfügt derzeit nicht über eine ISO 27001- oder SOC 2-Zertifizierung, und eine Zertifizierung ist derzeit nicht geplant.**

Ausrichtung bedeutet, dass die Kontrollen den in diesen Rahmenwerken beschriebenen Praktiken folgen. Es bedeutet nicht, dass ein externer Auditor diese bewertet und zertifiziert hat, und dies sollte in Ihrer eigenen Compliance-Dokumentation nicht so dargestellt werden. Wenn Ihr Beschaffungsprozess zertifizierte Nachweise erfordert, wird diese Anforderung derzeit nicht erfüllt – wenden Sie sich an **dpo@cybercrucible.com**, um zu besprechen, welche Dokumentation verfügbar ist.

Revision #1
Created 2026-07-24 04:45:23 UTC by Dennis Underwood
Updated 2026-07-24 04:45:23 UTC by Dennis Underwood