

How does Cyber Crucible support data protection and security requirements in Germany?

Short answer: In Germany, Cyber Crucible supports an organization's obligations under the GDPR and the Federal Data Protection Act (BDSG) by collecting no customer content, credentials, or keys and processing on the endpoint. For organizations in scope of Germany's cybersecurity regime (the BSI Act framework, as it takes on NIS2), the local-processing, on-premises-capable design supports their security and supply-chain obligations.

How it aligns

- **GDPR + BDSG.** Data minimization, encryption, and access control support the German data-protection baseline; a data processing agreement is available.
- **Data residency.** On-premises deployment keeps personal data in Germany where required; no customer content is transferred offshore for security processing.
- **Cybersecurity regime.** Germany has been transposing NIS2 into its BSI Act framework; Cyber Crucible supports covered entities' risk-management and supply-chain measures.

The honest boundary

Compliance rests with the organization and, where relevant, its data protection officer and the competent supervisory authority. Cyber Crucible holds no German certification and supports, rather than assumes, these duties. Documentation is available on request.

Revision #2

Created 2026-07-23 15:19:10 UTC by Dennis Underwood

Updated 2026-07-23 18:20:33 UTC by Dennis Underwood