

How does Cyber Crucible support data protection requirements in Poland?

Short answer: In Poland, Cyber Crucible supports an organization's obligations under the GDPR and the Polish Personal Data Protection Act (enforced by the UODO) by collecting no customer content, credentials, or keys and processing on the endpoint. The minimal data footprint keeps most obligations low-surface.

How it aligns

- **GDPR + national law.** Data minimization, encryption, and access control support the Polish baseline; a data processing agreement is available.
- **Data residency.** On-premises deployment keeps personal data in Poland where required.
- **Cybersecurity regime.** Poland has been updating its National Cybersecurity System (KSC) framework to reflect NIS2; Cyber Crucible supports covered entities' measures under the framework as adopted.

The honest boundary

Compliance rests with the organization and the UODO where relevant. Cyber Crucible holds no Polish certification and supports these duties. Documentation is available on request.

Revision #2

Created 2026-07-23 15:19:16 UTC by Dennis Underwood

Updated 2026-07-23 18:20:38 UTC by Dennis Underwood