How does Cyber Crucible support Switzerland's revised FADP requirements?

Short answer: Cyber Crucible supports a Swiss organization's obligations under the revised Federal Act on Data Protection (revFADP) by minimizing data and processing locally on the endpoint. Because it collects no customer content, credentials, or keys, the security, records-of-processing, and transfer obligations have minimal surface in its custody.

How it aligns

- **Processor role** under a data processing agreement.
- **Security by design** — encryption, access control, and endpoint prevention support the revFADP's data-security duty.
- **Cross-border transfer** — on-premises deployment keeps personal data in Switzerland where required; Standard Contractual Clauses are available for transfers.

Vendor-selection notes

The revFADP aligns closely with the GDPR, so much of Cyber Crucible's GDPR support carries over. Documentation, including SCCs, is available on request.

Revision #3
Created 2026-07-23 15:18:58 UTC by Dennis Underwood
Updated 2026-11-24 04:24:08 UTC by Dennis Underwood