

How does Cyber Crucible support data protection requirements in the Netherlands?

Short answer: In the Netherlands, Cyber Crucible supports an organization's obligations under the GDPR and the Dutch GDPR Implementation Act (enforced by the Autoriteit Persoonsgegevens) by minimizing data and processing on the endpoint. It collects no customer content, credentials, or keys, so most obligations have little surface in its custody.

How it aligns

- **GDPR + national implementation.** Encryption, access control, and data minimization support the Dutch baseline; a data processing agreement is available.
- **Data residency.** On-premises deployment keeps personal data in the Netherlands where required.
- **Cybersecurity regime.** The Netherlands' NIS2 transposition (the Cyberbeveiligingswet) was still being finalized as of 2026; Cyber Crucible supports covered entities' measures under the framework as adopted.

The honest boundary

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

Revision #2

Created 2026-07-23 15:19:13 UTC by Dennis Underwood

Updated 2026-07-23 18:20:35 UTC by Dennis Underwood