¿Cómo respalda Cyber Crucible los requisitos de protección de datos y seguridad en Alemania?

Respuesta breve: En Alemania, Cyber Crucible respalda las obligaciones de una organización en virtud del GDPR y la Ley Federal de Protección de Datos (BDSG) al no recopilar contenido, credenciales ni claves de los clientes, y al procesar en el endpoint. Para las organizaciones que están dentro del alcance del régimen de ciberseguridad de Alemania (el marco de la Ley BSI, en su adopción de la NIS2), el diseño de procesamiento local con capacidad de implementación local (on-premises) respalda sus obligaciones de seguridad y de cadena de suministro.

Cómo se alinea

- **GDPR + BDSG.** La minimización de datos, el cifrado y el control de acceso respaldan la base de protección de datos alemana; hay disponible un acuerdo de procesamiento de datos.
- **Residencia de datos.** La implementación local (on-premises) mantiene los datos personales en Alemania cuando así se requiere; ningún contenido del cliente se transfiere al extranjero para el procesamiento de seguridad.
- **Régimen de ciberseguridad.** Alemania ha estado transponiendo la NIS2 a su marco de la Ley BSI; Cyber Crucible respalda las medidas de gestión de riesgos y de cadena de suministro de las entidades cubiertas.

El límite honesto

El cumplimiento recae en la organización y, cuando corresponda, en su responsable de protección de datos (DPO) y en la autoridad supervisora competente. Cyber Crucible no posee ninguna certificación alemana y respalda estas obligaciones, en lugar de asumirlas. La documentación está disponible a solicitud.

Revision #1
Created 2026-07-24 02:09:31 UTC by Dennis Underwood
Updated 2026-07-24 02:09:31 UTC by Dennis Underwood