Comment Cyber Crucible soutient-il les exigences en matière de protection des données et de sécurité en Allemagne ?

Réponse courte : En Allemagne, Cyber Crucible soutient les obligations d'une organisation au titre du RGPD et de la loi fédérale sur la protection des données (BDSG) en ne collectant aucun contenu client, identifiant ou clé, et en traitant les données au niveau du terminal. Pour les organisations relevant du régime de cybersécurité allemand (le cadre de la loi BSI, dans le cadre de sa transposition de NIS2), la conception permettant un traitement local et un déploiement sur site soutient leurs obligations en matière de sécurité et de chaîne d'approvisionnement.

Comment cela s'aligne

- **RGPD + BDSG.** La minimisation des données, le chiffrement et le contrôle des accès soutiennent le socle allemand de protection des données ; un accord de traitement des données est disponible.
- **Résidence des données.** Le déploiement sur site conserve les données personnelles en Allemagne lorsque cela est requis ; aucun contenu client n'est transféré à l'étranger pour le traitement de sécurité.
- **Régime de cybersécurité.** L'Allemagne a transposé progressivement NIS2 dans le cadre de sa loi BSI ; Cyber Crucible soutient les mesures de gestion des risques et de sécurité de la chaîne d'approvisionnement des entités concernées.

La limite honnête

La conformité relève de la responsabilité de l'organisation et, le cas échéant, de son délégué à la protection des données et de l'autorité de contrôle compétente. Cyber Crucible ne détient aucune certification allemande et soutient ces obligations sans s'y substituer. La documentation est disponible sur demande.

Revision #1
Created 2026-07-24 07:20:21 UTC by Dennis Underwood

Updated 2026-07-24 07:20:21 UTC by Dennis Underwood