



CHARTRE DE CONFIDENTIALITÉ ET PROTECTION DES DONNÉES

CyberWall Belgique – SOC IA SOUVERAIN

Dernière mise à jour : Janvier 2026

1. PRÉAMBULE ET ENGAGEMENT SOUVERAIN

CyberWall Belgique place la protection de la vie privée et la sécurité des données au cœur de sa mission. Notre infrastructure est conçue selon le principe de Souveraineté Numérique Totale.

Contrairement aux solutions basées sur des technologies extra-européennes, CyberWall Belgique garantit qu'aucune donnée traitée n'est soumise au Cloud Act américain ou à toute autre législation d'ingérence étrangère.

2. IDENTITÉ DU RESPONSABLE DE TRAITEMENT

Le traitement des données est assuré par :
CyberWall Belgique (MLN Partenaires)
Avenue Reine Elisabeth 170/1, 5300 Andenne
Numéro d'entreprise : BE0754.899.926
Email de contact : info@cyberwalldefender.com
Email DPO : privacy@cyberwalldefender.com

3. NATURE DES DONNÉES COLLECTÉES

Dans le cadre de nos services de SOC IA, nous collectons deux types de données :

- **Données de contact** : Nom, entreprise, email et téléphone via nos formulaires d'audit.

- **Données techniques (Logs de sécurité)** : Flux réseaux, journaux d'événements systèmes et télémétrie des agents (Layer 0) nécessaires à la détection des cybermenaces.

4. TRAITEMENT PAR L'INTELLIGENCE ARTIFICIELLE (LLAMA3)

Le traitement de vos logs par notre moteur cognitif IA (Layer 2) respecte les règles suivantes :

- **Anonymisation** : Les données sont traitées de manière à identifier des schémas d'attaque (intentions) et non des comportements personnels.
- **Non-Entraînement** : Vos données ne sont jamais utilisées pour entraîner des modèles d'IA tiers ou globaux. Chaque analyse reste confinée à votre instance de sécurité.
- **Hébergement** : L'inférence IA est réalisée exclusivement sur nos serveurs souverains OVHcloud.

5. LOCALISATION ET SÉCURITÉ DU STOCKAGE

Toutes les données sont stockées au sein de l'Union Européenne (Belgique/France) sur des infrastructures certifiées **ISO/IEC 27001**. Nous utilisons des protocoles de chiffrement de pointe (AES-256) pour garantir l'intégrité de vos rapports de sécurité mensuels.

6. FINALITÉS DU TRAITEMENT

Les données sont traitées exclusivement pour :

1. La détection et la neutralisation des cyberattaques en temps réel (1.2s).
2. La génération de rapports d'audit et de posture de sécurité.
3. La réponse aux obligations légales (ex: conformité NIS2 pour les entités concernées).

7. DURÉE DE CONSERVATION

Les logs de sécurité sont conservés par défaut pour une durée de 30 jours afin de permettre l'investigation post-incident (Forensics), sauf demande contraire ou obligation légale spécifique.

8. VOS DROITS (RGPD)

Conformément au RGPD, vous disposez des droits suivants :

- Droit d'accès et de rectification.
- Droit à l'effacement de vos données de contact.
- Droit à la limitation du traitement.

Pour exercer ces droits, contactez notre DPO à l'adresse : **privacy@cyberwalldefender.com**.

9. IMMUNITÉ JURIDIQUE

CyberWall Belgique certifie n'utiliser aucun sous-traitant technique soumis au droit américain (Cloud Act), garantissant que vos données ne peuvent être consultées par des tiers sans mandat judiciaire européen exécutoire en Belgique.