COMMANDERS ACT

Fiche contractuelle de « Mesures de protection des données »

TOM

Technical and Organizational Measures

2022

I. INTRODUCTION

Ce document énumère toutes les mesures que nous avons mises en œuvre dans l'infrastructure et les processus de Commanders Act afin de garantir un niveau élevé de sécurité pour les données dont nous avons la charge.

II. ACCES PHYSIQUE

Notre infrastructure est hébergée par Amazon Web Services.

Tous les serveurs contenant des données sont hébergés sur la région française (eu-west-3). AWS assure un haut niveau de sécurité pour ses centres de données.

Pour plus d'informations, cliquez ici: https://aws.amazon.com/compliance/data-center/controls/

L'hébergement est également possible dans les Datacenters Equinix France (optionnel et soumis à facturation).

III. ACCES AU SYSTEME

Seuls les employés de Claranet et l'équipe informatique de Commanders Act peuvent accéder à nos serveurs.

Claranet étant notre gestionnaire d'infrastructure, ils ont accès à l'infrastructure via un réseau de gestion sécurisé.

Les employés de Commanders Act qui ont accès à l'infrastructure ne peuvent se connecter que via un VPN ou une IP restreinte.

La sécurité de l'accès au système est assurée par :

- Temporisation automatique de l'utilisateur
- Surveillance continue de la sécurité de l'infrastructure
- Contrôle d'accès basé sur les rôles, mis en œuvre de manière cohérente avec le principe du moindre privilège.
- L'accès aux serveurs hôtes, applications, bases de données, routeurs, commutateurs, etc. est enregistré.
- Les mots de passe doivent respecter ces règles :

    - o Longueur minimale de 10 caractères, et au moins un caractère spécial
    - o Renouvellement du mot de passe tous les 3 mois
- Examen régulier des risques de sécurité par des employés internes et des auditeurs tiers
- Délivrance et conservation des codes d'identification

IV. ACCÈS AUX DONNÉES ET SAISIE DES DONNÉES

Les données de nos clients sont stockées dans des bases de données partagées avec une séparation logique.

Outre les accès administrateurs couverts par le chapitre précédent, les données sont uniquement accessibles via notre interface web, à l'adresse suivante https://app.commandersact.com

La sécurité de l'accès aux données est assurée par :

- Accès individuel accordé par vérification de l'email
- Politique en matière de mots de passe :
- o Au moins 9 caractères
- o Au moins 1 chiffre
- o Au moins 1 caractère majuscule
- o Au moins 1 caractère spécial
- o Différents des 10 derniers mots de passe
- o Renouvellement tous les 3 mois maximum
- Droits d'accès différenciés
- Tous les accès sont enregistrés
- Toutes les modifications sont enregistrées
- La suppression des données est logique (pour les données supprimables via l'interface).
- WAF (Cloudflare)

Tous les formulaires de notre interface sont protégés contre les attaques CSRF.

Nos produits offrent la possibilité de rendre les données collectées pseudonymes. Nous pouvons par exemple obfusquer les adresses IP ou crypter les données personnelles (algorithme SHA256).

V. TRANSFERT DE DONNEES

Notre plateforme est destinée à collecter et à envoyer des données. Nous avons mis en place différents moyens de communication entre notre infrastructure et les actifs externes. Les données peuvent être transférées via :

- Web data collection (http hits)
- API
- FTP/SFTP

Les données ne doivent jamais être transférées par e-mail ou par des médias physiques, sauf recommandation spécifique d'un client.

Le niveau de sécurité du transfert de données dépend des données. Différents niveaux de sécurité peuvent être appliqués et cumulés.

La sécurité du transfert des données est assurée par :

- Cryptage des données critiques
- Tunnels (VPN)
- Sécurité du transport (SSL, restriction IP)
- Contrôle des données (somme de contrôle)
- Logging

VI. DISPONIBILITE DES DONNEES

Notre plateforme est conçue pour offrir une haute disponibilité de service, y compris la disponibilité des données.

La disponibilité des données est assurée par :

- Redondance des serveurs et redondance des disques durs (technologie RAID)
- Infrastructure de bâtiment double
- Alimentation électrique ininterrompue (UPS)
- Connexions Internet multiples
- Réseau sécurisé (pare-feu)
- Procédures de sauvegarde jusqu'à un mois de conservation
- Exclusion de logiciels, serveurs à tâche unique

Notre infrastructure est conçue pour être évolutive. Tous les services de collecte de données sont évolutifs et la plupart d'entre eux sont désormais auto-évolutifs. Cela signifie que le nombre de serveurs varie automatiquement en fonction du trafic entrant.

Notre infrastructure est également complètement industrialisée. Nous utilisons Terraform et Ansible pour déployer notre infrastructure. En cas d'urgence, nous pouvons facilement déployer nos services n'importe où et avoir le moins d'interruption de service possible.

VII. ISOLATION DES DONNEES

Les données que nous stockons et traitons sont la propriété de nos clients. Notre infrastructure est conçue pour éviter les fuites et pour garantir que les données sont traitées conformément à leur signification.

L'isolation des données est assurée par :

- Concept de client interne appelé "site".
- Isolation des bases de données
- Séparation de l'environnement de production et de développement
- Séparation des données de production et de test

VIII. CONTACT

Samuel Font – CIO
samuel.font@commandersact.com
+33 6 26 01 69 89