Mesures de sécurité organisationnelles et techniques

(Article 32 du RGPD)

ACD

Ce document a pour objet de décrire les principales mesures de sécurité mises en place pour la protection des données.

Ce document a vocation à s'appliquer à toutes personnes ayant souscrit à l'offre ACD On Demand.

Pour toutes les personnes ayant acheté une licence, vous êtes responsables de la manière dont vous assurez la sécurité, la confidentialité, l'intégrité et la disponibilité des données.

PRÉAMBULE

En tant que sous-traitant, ACD a mis en oeuvre des mesures appropriées en matière de confidentialité, d'intégrité, de disponibilité et de fiabilité, ainsi que des procédures régulières d'examen, d'évaluation et d'appréciation.

Le présent document décrit les mesures techniques et organisationnelles qui s'appliquent à tous les services et clients ACD On Demand.

ACD a choisi le sous-traitant ultérieur COAXIS, certifié HDS - Hébergement de Données de Santé, pour le service d'hébergement afin de vous garantir un haut niveau de sécurité au niveau des données personnelles. Le service d'hébergement est composé de plusieurs DataCenters :

- Un DataCenter de production où sont hébergés les serveurs et les données en fonctionnement nominal ;
- Un DataCenter de sauvegarde dédié aux sauvegardes et à l'archivage des données.

Ce document est disponible sur notre site internet, sur la page de présentation de l'**offre AOD**.

Traitements réalisés en tant que sous-traitant

- **Hébergement** des données personnelles
- **Support technique** : assistance et maintenance
- **Installation et mises à jour** des produits

Registre des traitements

- **ACD** tient un **registre des traitements** en tant que responsable de traitement et en tant que Sous-traitant conformément à l'article **30.1** et **30.2** du **RGPD**

Durée de conservation des données

- **Data sur les serveurs** : dès la fin du contrat AOD
- **Data archivées** : 6 ans suivant la politique de rétention des sauvegardes définie entre **ACD** et **COAXIS-ASP**
- Restitution des données sur disques ou via un transfert de fichiers au plus tard le dernier jour du contrat, sur demande du client

Localisation des données personnelles hébergées

- **France** - Site de production à **Fauguerolles**
- **France** - Site de sauvegarde et archivage à **Fauguerolles**

Contrôle des sous-traitants

- La relation entre **ACD** et **COAXIS** est encadrée par un contrat d'hébergement
- Un avenant **RGPD** a été rédigé pour être conforme aux exigences du **RGPD** en matière de sous-traitance
- En cas de sous-traitants ultérieurs : **ACD** s'engage à vérifier qu'ils soient conformes aux exigences du **RGPD**.

Contrôle des accès physiques aux données personnelles

- **Au niveau des DataCenters** : sécurités incendie, sismique, inondation, détection d'intrusion volumétrique, contrôle d'accès avec double authentification et dispositif de surveillance incluant un enregistreur vidéo qui opère 24x7 avec une sauvegarde des enregistrements de 30 jours.
- **Au niveau des sites d'ACD** : sécurité incendie, contrôle par badge, alarme anti-intrusion et télésurveillance

Contrôle des accès informatiques aux données personnelles

- **Au niveau des DataCenters** : Accès administrateurs : double authentification via un mot de passe et une carte à puce
- **Au sein d'ACD** : Accès par login / mot de passe pour chacun des intervenants habilités

Chiffrement des données à caractère personnel

- La connexion à **i-Suite** est sécurisée via **https** (protocole TLS)
- La **GED** est chiffrée selon un algorithme AES sur 128 bits
- Possibilité de chiffrer les documents PDF au sein des outils développés par **ACD**

ACD
18 rue de la Milletière - Bât. Mermoz - 37100 TOURS ■ Tél. : 02.47.39.11.49
SIRET 528 553 654 00047 - SAS au capital de 6 114 638 €

Journalisation

- **Au niveau des DataCenters** : Une durée de rétention comprise entre **48 heures** et **7 jours** en fonction des serveurs.
- Journalisation centralisée et xDR et SOC Managé

Sauvegarde des données à caractère personnel

- Sauvegardes stockées dans un **bâtiment distinct** de la production
- **Sauvegardes toutes les 12 heures** conservées sur disque pendant 30 jours
- **Sauvegardes complète toutes les semaines** conservées sur bande pendant 1 an
- **Sauvegardes par mois** conservées sur bande pendant 6 ans

Procédure de réponse aux droits des personnes concernées

- **Au niveau des DataCenters** : Politique générale de la sécurité du SI, corpus documentaire associé de la charte informatique, du règlement intérieur, des clauses de confidentialité
- **Au sein d'ACD** : Une procédure de gestion des demandes de droit des personnes concernées

Procédure de notification en cas de violation des données personnelles

- **Au niveau des DataCenters** : Qualification de l'incident de sécurité RGPD par le RSSI et procédure de gestion d'un incident de sécurité
- **Au sein d'ACD** : Une procédure de gestion des violations de données personnelles avec sensibilisation du personnel

Procédure d'aide du responsable de traitement en cas d'audit ou réclamation de l'autorité de contrôles

- **Au niveau des DataCenters** : Procédure de gestion des incidents et procédure de gestion des changements (interne)
- **Au sein d'ACD** : Une procédure de gestion des demandes clients et une procédure en cas de contrôle CNIL (interne) avec sensibilisation du personnel

Gestion des comptes administrateurs

- **Au niveau des DataCenters** : Limitation des rôles « Admin »
  Plan d'audit externe
  Procédure d'accompagnement tiers
  Revue des habilitations mensuelles
  Stratégie de sécurité renforcée pour les comptes à privilège
- **Au sein d'ACD** : Accès restreints pour les livraisons des mises à jour fonctionnelles et techniques

Protection des infrastructures informatiques

- **Au niveau des DataCenters** :
  - **Incendie/fumée** : le datacenter de production est équipé d'un système anti-incendie comprenant 6 bouteilles de gaz ARGON 55. Les capteurs sont situés à trois niveaux différents. Des inspections régulières sont programmées par un organisme agréé.
  - **Inondation** : plancher technique ayant une élévation de 70 cm au-dessus du niveau du sol. Les fondations et la dalle du sous-plancher sont étanches
- **Au sein des services ACD** : Utilisateurs Admin technique pour effectuer les mises à jour et/ou paramétrages sans accès aux données personnelles des clients.

Sécurité

- **Au niveau des DataCenters** :
  - **COAXIS** dispose d'une PGSSSI notamment dans le cadre de la certification ISO27001 & HDS
  - **COAXIS** réalise régulièrement des audits de sécurité des SI
  - Un SOC (Security Operationnel Center) assure la sécurité opérationnelle et un COSEC (Comité de sécurité) est dédié aux aspects organisationnels et normatifs

Le présent document relatif aux mesures de sécurité techniques et organisationnelles peut être amené à évoluer.

La dernière mise à jour a été effectuée par **OPTIMEX DATA** le **24/04/2024**.

ACD
18 rue de la Milletière - Bât. Mermoz - 37100 TOURS ■ Tél. : 02.47.39.11.49
SIRET 528 553 654 00047 - SAS au capital de 6 114 638 €