

## Mesures de sécurité organisationnelles et techniques

(Article 32 du RGPD)

### ACD GROUPE

*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 GROUPE a mis en œuvre 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 GROUPE 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](#).

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

Traitements réalisés en tant que sous-traitant



- ACD Groupe 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.

Registre des traitements



- **Data sur les serveurs** : dès la fin du contrat AOD
- **Data archivées** : 6 ans suivant la politique de rétention des sauvegardes définie entre ACD Groupe 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.

Durée de conservation des données



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

Localisation des données personnelles hébergées



- La relation entre ACD Groupe 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 Groupe s'engage à vérifier qu'ils soient conformes aux exigences du RGPD.

Contrôle des sous-traitants



- **Au niveau des DataCenters** : sécurités incendie, sismique, inondation, détection d'intrusion volumétrique, contrôle d'accès avec double authentification et dispositif de surveillance.
- **Au niveau des sites d'ACD Groupe** : sécurité incendie, contrôle par badge, alarme anti-intrusion et télésurveillance.

Contrôle des accès physiques 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 Groupe** : Accès par login / mot de passe pour chacun des intervenants habilités.

Contrôle des accès informatiques aux données personnelles



- La connexion à **i-Suite Expert** 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 Groupe.

Chiffrement des données à caractère personnel



- Une durée de rétention comprise entre **48 heures et 7 jours** en fonction des serveurs.

#### Journalisation



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

#### Sauvegardes des données à caractère personnel



- **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 GROUPE :** Une procédure de gestion des demandes de droit des personnes concernées.

#### Procédure de réponse aux droits des personnes concernées



- **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 Groupe :** Une procédure de gestion des violations de données personnelles avec sensibilisation du personnel.

#### Procédure de notification en cas de violation des données personnelles



- **Au niveau des DataCenters :** Procédure de gestion des incidents et procédure de gestion des changements (interne).
- **Au sein d'ACD Groupe :** Une procédure de gestion des demandes clients et une procédure en cas de contrôle CNIL (interne) 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 :** Limitation des rôles "Admin" Plan d'audit externe Procédure d'accompagnement tiers.
- **Au sein des outils d'ACD Groupe :** Accès restreints pour les livraisons des mises à jour fonctionnelles et techniques.

#### Gestion des comptes administrateurs



- **Au niveau des DataCenters :** Dossier d'architecture complet
- **Au sein des services d'ACD Groupe :** Utilisateurs Admin technique pour effectuer les mises à jour et/ou paramétrages sans accès aux données personnelles des clients.

#### Protection des infrastructures informatiques



- Le présent document relatif aux mesures de sécurité techniques et organisationnelles peut être amené à évoluer. La dernière mise à jour a été effectuée le 31 juillet 2020.