



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 Assistance-Maintenance.

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 Assistance-Maintenance.

L'hébergement des données est géré uniquement par vos soins. ACD n'héberge pas les données pour votre compte.

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

Traitements réalisés en tant que sous-traitant

- ✓ **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

- ✓ **Documents contractuels :** 5 ans à compter de la fin de la relation contractuelle

Contrôle des sous-traitants

- ✓ 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 sites d'**ACD** : sécurité incendie, contrôle par badge, alarme anti-intrusion et télésurveillance

Contrôle des accès informatiques aux données personnelles

- ✓ **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**

Journalisation

- ✓ Journalisation des mises à jour depuis l'espace client
- ✓ Journalisation des jetons **i-Suite**
- ✓ Journalisation des erreurs des clients au niveau des logiciels

Sauvegarde des données à caractère personnel

- ✓ Deux types de rétention de sauvegarde des données dans le cadre de la maintenance et les migrations :
 - 30 jours en local au sein d'**ACD**
 - 30 jours au sein de OVH et purge automatique
- ✓ La rétention permet de répondre aux demandes et de gérer les délais

Prérequis

- ✓ **Au niveau d'ACD :** Les prérequis disponibles sur l'espace client demandent l'installation du serveur Web sur une DMZ et l'utilisation d'un certificat afin de chiffrer les informations d'authentification ainsi que le flux de données qui transitent sur internet

Procédure de réponse aux droits des personnes concernées

- ✓ **Au sein d'ACD :** Une procédure de gestion des demandes de droit des personnes concernées
- ✓ Réponse dans un délai raisonnable

Procédure de notification en cas de violation des données personnelles

- ✓ **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 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 sein d'ACD :**
Accès restreints pour les livraisons des mises à jour fonctionnelles et techniques

Protection des infrastructures informatiques

- ✓ **Au sein des services ACD :**
Utilisateurs Admin technique pour effectuer les mises à jour et/ou paramétrages sans accès aux données personnelles des clients

Gestion des accès aux données

- ✓ **Au sein des services ACD :**
L'accès aux données se fait au travers d'une authentification nécessitant un identifiant et un mot de passe. Chaque client ne peut accéder qu'à ses propres données. Le serveur Web ne stocke aucune donnée. C'est à travers le serveur Web que vous pouvez accéder à vos dossiers

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**.