Plan d'Assurance Sécurité Annexe « Service Gestion »

1. Introduction

Cette annexe est liée et indissociable à l' « ***ANNEXE CGV_PAS Dispositions du Plan d'Assurance Sécurité*** ».

2. Description

En tant que prestataire de solutions de gestion, la Société commercialise des applications contenant des Données à Caractère Personnel et fournit des prestations au Client et dans ce cadre peut y avoir accès.

L'accent sera mis sur les points qui justifient la mise en œuvre de mesures de sécurité.

Les solutions proposées étant liés aux systèmes et réseaux de son infrastructure, l'annexe « ANNEXE PAS Service Infogérance » est également applicable.

3. Mesures de sécurité

La Société se porte garant de l'intégrité et de la confidentialité des données qui lui sont confiées pendant toutes les phases de traitement des données concernant les applications de gestion sous sa charge.

3.1. Transfert des applications

Sauf demande expresse auprès de la Société, le Client réalisera les sauvegardes de ses informations et les gèrera de manière à permettre une reprise en cas d'incident lors de la bascule du système.

Le Client devra fournir à la Société :

- La liste des personnes autorisées ainsi que leurs habilitations et restrictions éventuelles pour l'utilisation de chaque application mais aussi pour l'accès aux services supports ;
- La liste des particularités, développements spécifiques s'il y a lieu, liens avec d'autres applications externes ;
- Toute instruction complémentaire que le Client jugerait utile.

3.2. Déplacement de données

Dans le cadre de ses interventions, la Société peut être amené à déplacer les données du Client.

Voici une liste non exhaustive de cas possibles :

- ***Changement de système d'exploitation ou de matériel***

La Société réalise une sauvegarde des données des applications de gestion du Client ou utilise une sauvegarde fournie par le Client et gère cette sauvegarde de manière à permettre une reprise en cas d'incident lors de la bascule du système. Le transfert se fait par l'intermédiaire de l'infrastructure du Client dans la mesure du possible.

Aucune copie n'est conservée par la Société à l'issue du transfert.

- ***Récupération de base pour réparation, test de paramétrage, développement spécifique, éditions personnalisées...***

La récupération de base ne se fait que sur accord express écrit du Client uniquement pour le traitement précis déterminé avec le Client.

Le Client doit documenter par écrit toute instruction spécifique concernant le traitement des données que doit effectuer la Société.

Une copie des données est effectuée et cryptée (AES-256) avec attribution d'un mot de passe complexe pour sa phase de transfert.

La Société a équipé ses consultants et techniciens Support de matériel avec option de chiffrement pour permettre le stockage sécurisé et l'exploitation de ce type de données.

Dans le cas où le transfert doit se faire via un canal non sécurisé, la transmission du mot de passe se fait de manière confidentielle par un autre canal.

Une fois le traitement terminé, la Société détruit toute copie des données du Client en sa possession.

3.3. Exploitation

- ***Installation***

Le Client autorise la Société dans le cadre de son suivi à avoir accès et à stocker toute information utile pour la bonne réalisation de l'installation et du suivi qui en découle. Pour ces besoins, le Client doit fournir au minimum :

- Des codes utilisateurs et mots de passe systèmes avec les privilèges suffisants selon les préconisations techniques fournies par les éditeurs de solutions ;
- Des codes utilisateurs, mots de passe logiciels et moteurs de bases de données nécessaires pour l'installation et le paramétrage des solutions ;
- La liste des personnes autorisées à accéder aux applications installées et leurs permissions pour le paramétrage des droits nécessaires.

Le Client doit s'assurer que son infrastructure respecte les préconisations techniques, fournies par la Société, nécessaires à l'installation des applications.

Le Client doit informer la Société de toute particularité ou imprévu sur son infrastructure avant la date prévue de son installation. Pour des raisons de sécurité et des performances optimales, nous préconisons que :

- Un serveur non contrôleur de domaine et dédié à la gestion des bases de données des applications de gestion soit mis à disposition de la Société ;
- Les systèmes d'exploitation soient installés avec des versions professionnelles, et soient mis à jour avant l'installation de nos applications ;
- Les postes clients soient intégrés dans un domaine réseau ;
- Le protocole TCP/IP soit installé sur tous les équipements réseaux participant à l'accès à nos applications ;
- Les configurations des postes clients et serveurs soient adaptées en fonction du nombre d'utilisateurs souhaité ;

- Toutes les sécurités informatiques nécessaires soient mises en place, et maintenues à jour en terme d'antivirus, firewall, routeurs… ;
- Les versions d'Office installées soient compatibles avec la version d'application de gestion.

➢ ***Mesures de sécurité au sein des Solutions de Gestion***

La Société informe et préconise des mesures de sécurité techniques et organisationnelles possibles selon la version de solution acquise par le Client. Nous recommandons fortement de suivre ces préconisations. Dans le cas contraire, sa conformité au RGPD ne peut être garantie. Le Client assumera cette responsabilité auprès de l'autorité de contrôle (Article 24 du règlement UE 2016/679) en tant que Responsable du traitement.

Nous préconisons entre autres :

- Un code utilisateur par application par utilisateur nommé ;

  Le RGPD impose la traçabilité et l'imputabilité des accès aux Données à Caractère Personnel, la Société déconseille vivement d'utiliser des comptes génériques.

- L'affectation d'un mot de passe, non vide, différent du code utilisateur, complexe avec au moins une majuscule, une minuscule, un chiffre, un caractère spécial sur minimum 8 caractères ;
- Le renouvellement des mots de passe tous les 90 jours ;
- La limitation des droits par utilisateur aux fonctions uniques dont il a besoin dans l'application.

  Le RGPD impose de garantir la confidentialité des Données à Caractère Personnel.

➢ ***Sauvegardes et restaurations***

Le Client reste toujours responsable de la sauvegarde de ces données. Il doit s'assurer de leurs bons déroulements. Nous préconisons :

- Une sauvegarde à minima journalière des bases de données ou toute durée inférieure si le Client juge qu'en cas de restauration, la perte de données éventuelle ne peut être inférieure à cette durée ;
- Le déclenchement et la vérification d'une sauvegarde avant tout traitement irréversible ;
- L'ajustement de la durée de conservation des sauvegardes en fonction du besoin de remontées d'historiques du Client selon l'application ;
- Le stockage centralisé et la sauvegarde incrémentielle des répertoires d'installation, de stockage des mises en page de document ou paramétrages personnalisés ;
- Une vérification régulière du bon déroulement des sauvegardes ;
- Des tests réguliers de restauration sur un stockage hors production, ne pouvant pas influer sur le bon fonctionnement des applications en place ;

Dans le cas où le Client souhaite une prestation de restauration de données, concernant les applications dont la Société a la charge, il doit fournir la sauvegarde appropriée à la Société afin de permettre la réalisation de cette intervention.

- ***Support***

Lorsque des documents contenant des Données à Caractère Personnel sont transmis par le Client au service Support de la Société, le Client doit faire tout son possible pour anonymiser ces informations.

A l'issue des traitements, la Société détruira tout document contenant les Données à Caractère Personnel du Client de manière à les rendre inexploitables.

- ***Mises à jour des applications fournies par la Société***

La Société se tient à disposition pour indiquer les dernières versions disponibles des applications qu'elle déploie. La Société se tient également disponible pour mettre à jour ces applications.

Il est bien sûr primordial que le Client s'assure que les versions dont il disponible sont bien compatibles avec le RGPD, règlement UE 2016/679.