## Mesures techniques et organisationnelles

Compte tenu de l'état de l'art, des coûts de mise en œuvre et de la nature, de la portée, des circonstances et des finalités du traitement, ainsi que de la probabilité et de la gravité variables du risque pour les droits et libertés des personnes physiques, le Prestataire, en sa qualité de sous-traitant des données, met en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque, y compris, mais sans s'y limiter, les éléments suivants :

**1. Pseudonymisation**

La pseudonymisation désigne le traitement des Données du Client visant à faire en sorte que les données personnelles ne puissent plus être attribuées à une personne concernée spécifique sans utiliser d'informations supplémentaires, à condition que ces informations supplémentaires soient conservées séparément et fassent l'objet de mesures techniques et organisationnelles visant à garantir que les données personnelles ne sont pas attribuées à une personne physique identifiée ou identifiable.

**2. Confidentialité**

**2.1 Contrôle d'accès physique**

Le Prestataire prend les mesures appropriées pour réduire le risque que des personnes non autorisées aient accès aux systèmes de traitement des données avec lesquels les Données du Client sont traitées et utilisées. Les mesures de contrôle d'accès peuvent inclure, par exemple, des systèmes de contrôle d'accès automatiques, l'utilisation de cartes à puce et de transpondeurs, le contrôle d'accès par des services de portier et des systèmes d'alarme. Les serveurs, les systèmes de télécommunications, les technologies de réseau et les équipements similaires peuvent être protégés, par exemple, par des armoires de serveurs verrouillables. Il est également judicieux de contrôler l'accès par le biais de mesures organisationnelles (par exemple, des directives de service stipulant que les locaux de service doivent être fermés à clé en cas d'absence des employés).

**Mesures techniques :**

● Système de contrôle d'accès automatique.

● Cartes à puce / systèmes de transpondeurs.

● Système de verrouillage manuel

● Portes avec boutons extérieurs.

**Mesures organisationnelles :**

● Contrôle des clés (remise de clés, etc.).

● Accompagnement des visiteurs par des employés.

● Sélection minutieuse du personnel de nettoyage.

**2.2 Contrôle d'accès au système**

Le Prestataire prend les mesures appropriées pour éviter que les systèmes de traitement des données (ordinateurs) ne soient utilisés par des personnes non autorisées.

À cette fin, le Prestataire doit prendre les précautions suivantes :

**Mesures techniques :**

● Connexion avec nom d'utilisateur + mot de passe.

● Connexion partielle avec les données biométriques.

● Cryptage des smartphones

● Cryptage des ordinateurs portables / tablettes.

● Gestion des ordinateurs portables

● Utilisation d'un logiciel anti-virus pour les serveurs.

● Déploiement de logiciels anti-virus pour les Clients.

● Verrouillage automatique du bureau.

**Mesures organisationnelles :**

● Gérer les autorisations des utilisateurs

● Créer des profils d'utilisateurs

● Politique relative à l'utilisation d'un appareil personnel.

● Politique relative aux appareils mobiles

● Politique générale en matière de protection et / ou de sécurité des données.

**2.3 Contrôle d'accès aux données**

Le Prestataire prend les mesures appropriées pour que les personnes autorisées à utiliser les systèmes de traitement des données ne puissent accéder qu'aux données personnelles soumises à leur autorisation d'accès et que les Données du Client ne puissent être lues, copiées, modifiées ou supprimées sans autorisation pendant le traitement, l'utilisation et après le stockage. A cet effet, le Prestataire prend les précautions suivantes :

**Mesures techniques :**

● Effacement physique des supports de données sur les ordinateurs portables avant leur réutilisation.

● Journalisation de l'accès aux documents importants, notamment lors de la saisie, de la modification et de la suppression de données.

● Destruction de fichiers (niveau 3 minimum, coupe transversale).

**Mesures organisationnelles :**

● Création d'un concept d'autorisation

● Gestion des droits par l'administrateur système.

● Réduction du nombre d'administrateurs.

● Zone fermée pour les documents sensibles.

**2.4 Contrôle de la séparation**

Le Prestataire prend les mesures appropriées pour que les Données du Client collectées à des fins différentes puissent être traitées séparément. À cette fin, le Prestataire prend les précautions suivantes :

**Mesures techniques :**

● Stockage séparé sur des systèmes ou des supports de données distincts.

● Division des Clients par un logiciel

**Mesures organisationnelles :**

● Création d'un concept d'autorisation

● Détermination des droits sur les bases de données.

**3. Intégrité**

**3.1 Contrôle de la transmission**

Le Prestataire prend des mesures raisonnables pour réduire le risque que les Données du Client puissent être lues, copiées, modifiées ou supprimées sans autorisation pendant la transmission électronique ou pendant leur transport ou leur stockage sur des supports de données. A cette fin, le Prestataire prend les précautions suivantes :

**Mesures techniques :**

● Cryptage des courriers électroniques

● Consignation des accès et récupération de documents et données importants

● Mise à disposition *via* desconnexions cryptées telles que sftp, https

● Utilisation des procédures de signature

**Mesures organisationnelles :**

● Possibilité de créer un aperçu des opérations régulières de récupération et de transmission.

**3.2 Contrôle de l'entrée des données**

Le Prestataire prend les mesures appropriées pour qu'il soit possible de vérifier et de déterminer rétrospectivement si et par qui les Données du Client ont été introduites dans les systèmes de traitement des données, modifiées ou supprimées. A cette fin, le Prestataire prend les précautions suivantes :

**Mesures techniques :**

● Possibilité de journalisation technique de la saisie, de la modification et de la suppression des données personnelles.

**Mesures organisationnelles :**

● Traçabilité de l'entrée, de la modification et de la suppression des données personnelles grâce aux noms d'utilisateurs individuels.

● Conservation des formulaires à partir desquels les données personnelles ont été transférées vers des traitements automatisés.

● Attribution des droits de saisie, de modification et de suppression des données personnelles sur la base d'un concept d'autorisation.

**4. Disponibilité et résilience**

**4.1 Contrôle de la disponibilité**

Le Prestataire prend des mesures raisonnables pour garantir que les Données du Client sont protégées contre la destruction ou la perte accidentelle. A cette fin, le Prestataire prend les précautions suivantes :

**Mesures techniques :**

● Systèmes de détection d'incendie et de fumée.

● Sélection attentive du fournisseur de services d'hébergement.

**Mesures organisationnelles :**

● Contrôle régulier du fournisseur de services d'hébergement.

**5. Procédures d'examen, d'évaluation et de contrôle réguliers.**

Le Prestataire met en œuvre des procédures d'examen, d'évaluation et de contrôle réguliers de l'efficacité des mesures techniques et organisationnelles visant à garantir la sécurité du traitement.

**5.1 Gestion de la protection des données**

**Mesures techniques :**

● Documentation centrale de toutes les procédures, réglementations et directives sur la protection des données avec accès pour les employés selon les besoins/autorisations.

● Un examen de l'efficacité des mesures techniques de protection est effectué régulièrement.

**Mesures organisationnelles :**

● Employés formés à la confidentialité.

● Sensibilisation des employés par le biais de la formation.

Le Prestataire respecte les obligations d'information conformément aux art. 13 et 14 du RGPD.

Un processus formel de traitement des demandes d'information des personnes concernées est en place.

**5.2 Gestion de la réponse aux incidents**

Assistance en cas de violation de la sécurité.

**Mesures techniques :**

● Utilisation de filtres anti-spam et mise à jour régulière.

● Utilisation d'un scanner de virus et mise à jour régulière.

**Mesures organisationnelles :**

● Documentation des incidents de sécurité et des violations de données.

● Réglementation des responsabilités en matière de suivi des incidents de sécurité et des violations de données.

**5.3 Paramètres par défaut respectueux de la vie privée (article 25, paragraphe 2, du GDPR) ; *Privacy by design / Privacy by default.***

**Mesures techniques :**

● Il n'est pas collecté plus de données personnelles que ce qui est nécessaire pour la finalité respective.