ANNEXE 2 :

Aperçu des mesures de sécurité

La présente annexe comprend un aperçu des mesures de sécurité prises par le Sous-traitant pour protéger au maximum les Données à caractère personnel qu'il traite.

Le Sous-traitant s'efforce notamment de prendre toutes les mesures techniques et organisationnelles appropriées et raisonnables afin de veiller à ce que les Données à caractère personnel qui lui sont confiées ne fassent pas l'objet d'une perte ou d'un traitement illicite et ne soient notamment pas accessibles à des personnes non autorisées.

Pour déterminer les mesures de sécurité appropriées, une pondération est effectuée sur base des risques du traitement en tenant compte notamment des critères suivants :

- Type de Données à caractère personnel qui sont traitées (sensibles ou non sensibles) ;
- Nombre de Personnes concernées dont les données sont traitées ;
- Finalité du traitement des Données à caractère personnel ;
- …

Aperçu des mesures de sécurité techniques :

- Utilisation d'un antivirus ;
- Installation d'un pare-feu ;
- Application d'une politique concernant les mots de passe (c.-à-d. codes login uniques et mots de passe personnels adaptés régulièrement) ;
- Sauvegardes sécurisées systématiques à titre de protection contre les pertes de données ;
- Protection de l'accès physique aux Données à caractère personnel pour les personnes qui ne doivent pas y avoir accès du fait de leurs tâches ;
- Pas d'utilisation de disques durs non sécurisés ;
- Recours à des techniques de cryptage pour l'enregistrement des données à caractère personnel ;
- Sécurisation physique de l'accès aux locaux où des Données à caractère personnel sont traitées et enregistrées *(p. ex. au moyen de badges ou de codes de sécurité)* ;
- …

Aperçu des mesures organisationnelles :

- Politique générale d'information du personnel sur la protection de la vie privée ;
- Organisation de séances périodiques de formation et de conscientisation pour le personnel au sujet de la gestion des Données à caractère personnel ;
- Mise en place de procédures internes concernant l'entrée en service et la sortie de service de collaborateurs qui gèrent des Données à caractère personnel ;
- Établissement de clauses de confidentialité avec les collaborateurs qui gèrent des Données à caractère personnel ;
- Mise en place d'une politique et de directives internes concernant la gestion confidentielle de Données à caractère personnel ;
- Mise en place de procédures internes en cas d'incidents (Fuite de données…) ;
- Application d'un enregistrement personnel et de systèmes d'identification pour le contrôle d'accès aux bâtiments pour que les personnes non autorisées n'aient pas accès aux locaux de l'entreprise ;

- Désignation d'un responsable de la sécurité informatique ;
- Planification et exécution, à intervalles réguliers, d'audits et de contrôles de sécurité internes ;
- Utilisation d'une politique de rangement du bureau (*clean desk*) afin de protéger au maximum les données confidentielles des regards de personnes non autorisées ;
- Utilisation de déchiqueteuses à papier ou d'autres moyens pour détruire les éventuelles données confidentielles ;
- Application d'une procédure spécifique pour la suppression des Données à caractère personnel qui se trouvent sur les supports de stockage et équipements mis au rebut (p. ex. ordinateurs portables et smartphones) et sur les appareils qui sont restitués par les collaborateurs qui quittent l'entreprise ;
- ...