Annexe : Mesures techniques et organisationnelles
Version Janvier 2020

Les dispositions suivantes de la présente Annexe définissent les mesures techniques et organisationnelles actuelles de KEYRUS. KEYRUS peut les modifier à tout moment sans préavis, tant qu'elles conservent un niveau de sécurité comparable.

1.1 Contrôle des accès physiques. Seules les personnes autorisées sont en mesure d'accéder physiquement aux bâtiments, locaux ou pièces où sont situés les systèmes de traitement de données qui traitent et/ou utilisent les données à caractère personnel.

Mesures :

- KEYRUS assure la protection de ses biens et ses installations en recourant aux moyens adaptés, conformément à la Politique de sécurité du Système d'information (PSSI) de KEYRUS.
- En fonction de la classification de la sécurité, certaines zones précises et leurs environs peuvent être protégés par des mesures supplémentaires, notamment par des profils d'accès spécifiques, la vidéo-surveillance ou un système d'alarme en cas d'intrusion.

1.2 Contrôle des accès au système. Seules les personnes autorisées peuvent utiliser les systèmes de traitement des données utilisés pour fournir les services définis dans le Contrat au CLIENT.

Mesures :

- Différents niveaux d'autorisation sont utilisés en ce qui concerne l'accès aux systèmes sensibles, notamment le stockage et le traitement des données à caractère personnel. Les autorisations sont octroyées conformément à la PSSI de KEYRUS.
- L'ensemble du personnel accède au système KEYRUS par le biais d'un identifiant et mot de passe propres.
- KEYRUS a mis en place des procédures afin que les modifications d'autorisation demandées soient uniquement effectuées en conformité avec la PSSI de KEYRUS. Lorsqu'un salarié quitte la société, ses droits d'accès sont révoqués.
- La politique établie par Keyrus en matière de mots de passe (i) interdit leur partage, (ii) impose les mesures à prendre pour constituer son mot de passe, (iii) les mesures à prendre en cas de divulgation de celui-ci, (iv) exige que les mots de passe soient modifiés périodiquement et (v) que les mots de passe par défaut soient modifiés. Tous les mots de passe sont stockés sous forme chiffrée. Dans le cas des mots de passe de domaine, le système impose un changement tous les 90 jours et le choix de mots de passe complexes. Chaque session utilisateur est programmée pour se verrouiller au bout de 10 minutes et l'écran de veille est protégé par mot de passe.
- Un logiciel antivirus actualisé est utilisé aux points d'accès au réseau de la société, notamment pour les comptes de messagerie électronique ainsi que sur la totalité des serveurs de fichiers et des postes de travail.
- Les mises à jour de sécurité régulières et périodiques sont assurées par la gestion des correctifs de sécurité. Un système d'authentification protège l'accès à distance à l'intégralité du réseau interne de KEYRUS et à son infrastructure.

1.3 Contrôle des accès aux données. L'accès aux données à caractère personnel se limite aux personnes habilitées. Les données à caractère personnel ne pourront pas être consultées, copiées, modifiées ou supprimées sans autorisation dans le cadre de leur traitement.

Mesures :

- Dans le cadre de la PSSI de KEYRUS, les données à caractère personnel doivent faire l'objet d'un niveau de protection égal à celui des informations « confidentielles », selon la norme de classification des informations de KEYRUS.
- L'ensemble des données CLIENT sont protégées conformément à la PSSI de KEYRUS. des concepts d'autorisation sont employés afin de documenter les processus d'autorisation et les rôles affectés par compte (identifiant d'utilisateur).
- Les Utilisateurs ne peuvent pas installer, désactiver ou désinstaller les logiciels de leur poste de travail (à l'exception des personnes possédant les droits administrateur).
- KEYRUS a mis en place une procédure de suppression et destruction des données à caractère personnel et des supports de données lorsqu'ils ne sont plus requis.

1.4 Contrôle des saisies de données. Toute saisie, modification ou suppression de données à caractère personnel pourra être examinée et établie rétrospectivement, ainsi que la personne ayant effectué lesdites actions.

Mesures :
- Keyrus octroie un accès aux données à caractère personnel uniquement au personnel autorisé, selon les besoins pour accomplir ses obligations.
- Un système de journalisation des saisies, modifications, suppressions et blocages de données à caractère personnel par KEYRUS ou ses sous-traitants ultérieurs, le cas échéant, a été établi par Keyrus.

1.5 Contrôle des transmissions de données. Les données à caractère personnel ne doivent pas être consultées, copiées, modifiées ou supprimées sans autorisation, pendant leur transfert, sauf dispositions contraires applicables.

Mesures :
- Toutes les données sensibles doivent être protégées de manière sécurisée si elles doivent être transportées physiquement ou électroniquement, conformément à la PSSI de Keyrus.
- Le CLIENT assume dans tous les cas la responsabilité d'un quelconque transfert de données dès lors qu'il sort du cadre des systèmes contrôlés par KEYRUS.

1.6 Contrôle de la disponibilité. Les données à caractère personnel sont protégées contre les risques de perte et les destructions accidentelles ou non autorisées, en conformité avec la PSSI de Keyrus.

Mesures :
- KEYRUS emploie des procédures de sauvegarde régulières afin de sécuriser les Systèmes d'information et garantir la protection et la pérennité des Informations, conformément à la PSSI de Keyrus.
- Des systèmes d'alimentation sans coupure (par exemple générateurs) sont utilisés par KEYRUS afin de garantir une alimentation continue.
- KEYRUS a établi un plan de continuité d'activités.
- Des tests sont régulièrement effectués sur les procédures et systèmes d'urgence.

1.7 Contrôle de la séparation des données. Les données à caractère personnel recueillies à des fins différentes peuvent être traitées de manière séparée.

Mesures :
- Le CLIENT (et ses responsables du traitement approuvés) accède uniquement à ses propres données, grâce à une authentification sécurisée et à des autorisations.
- En cas d'incident de maintenance émanant du CLIENT, des données à caractère personnel sont requises pour la gestion dudit incident de maintenance, les données sont affectées audit message afin de le traiter. Il est impossible d'y accéder afin de traiter un autre message. Lesdites données sont stockées dans des systèmes d'aide dédiés.

1.8 Contrôle de l'intégrité des données. Les données à caractère personnel demeurent intègres dans le cadre des activités de traitement.

Mesures :
KEYRUS a mis en œuvre une politique sur plusieurs niveaux visant à assurer une protection contre les modifications non autorisées.
KEYRUS utilise entre autres les éléments suivants pour mettre en œuvre la protection visée aux articles relatifs aux contrôles et aux mesures décrits précédemment :
- Pare-feu
- Logiciel antivirus
- Sauvegarde et récupération
- Audits externes réguliers pour démontrer la mise en œuvre des mesures de sécurité

1.9 Contrôle des tâches. Le contrôle des tâches permet de garantir que les données à caractère personnel traitées pour le compte du CLIENT le sont conformément aux instructions de ce dernier.

Mesures :
- Des contrôles et procédures sont utilisés par KEYRUS pour veiller au respect des contrats conclus entre KEYRUS et ses clients, sous-traitants ultérieurs ou autres prestataires de services.
- Une obligation de confidentialité des données est imposée aux employés et sous-traitants ultérieurs contractuels ou autres prestataires de services.
  Les clients KEYRUS ont à tout moment le contrôle de leurs connexions de maintenance à distance, en ce qui concerne le Support KEYRUS. Les employés de KEYRUS peuvent uniquement accéder au système d'information du CLIENT si celui-ci en est informé et y consente.