

MESURES DE SECURITE ORGANISATIONNELLES ET TECHNIQUES

(Article 32 du RGPD)

KEEPTRACE

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 souscrites aux offres de services proposées par KeepTRACE.

La société KeepTrace met tout en œuvre pour assurer la confidentialité, l'intégrité et la disponibilité des données.

PREAMBULE :

En tant que sous-traitant, KeepTrace a mis en œuvre 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 de KeepTrace.

KeepTrace a choisi le sous-traitant ultérieur IKOULA, pour le service d'hébergement afin de vous garantir un haut niveau de sécurité au niveau des données personnelles. Le service d'hébergement est composé de plusieurs DataCenters :

- Centre des données de Reims (51100 - REIMS) ;
- Centre des données de Telecity (92400 - COURBEVOIE) ;
- Centre de données de Eppes (02840 – EPPES)

Ce document est disponible, sur demande et sur notre site internet www.keeptrace.fr/documents/KEEPTRACE_MTO.pdf

- **Hébergement** des données personnelles de l'outil KeepTrace géré par notre sous-traitant ultérieur IKOULA
- **Support technique** : assistance et maintenance
- **Installation et mises à jour** de l'outil

Traitements réalisés en tant que sous-traitant



- KEEPTRACE 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.

Registre des traitements



- **Data sur les serveurs** : les durées de conservation sont définies par le client via l'outil KeepTrace
- **Data archivées** : les durées de conservation sont définies par le client via l'outil KeepTrace

Durée de conservation des données



- KEEPTRACE a fait le choix d'un hébergement des données uniquement dans l'Union Européenne
- Centre des données de Reims (51100 - REIMS)
- Centre des données de Telecity (92400 - COURBEVOIE)
- Centre de données de Eppes (02840 - EPPES)

Localisation des données personnelles hébergées



- La relation entre KEEPTRACE et IKOULA est encadrée par un **contrat d'hébergement**
- Un **avenant RGPD** a été rédigé pour être conforme aux exigences du RGPD en matière de sous-traitance
- En cas de **sous-traitants ultérieurs**, **IKOULA** s'engage à vérifier qu'ils soient conformes aux exigences du RGPD et à nous informer au préalable

Contrôle des sous-traitants



- **Au niveau des sites d'IKOULA** : contrôle d'accès, vidéosurveillance permanente, système de détection des incendies, système de détection d'intrusion par alarme, par chocs, accès par badge.
- **Au niveau des accès aux salles machines** : porte blindée, contrôle par badge, climatisation baies informatiques fermées par serrure à code, détection des incendies, système d'extinction à base de gaz

Contrôle des accès physiques aux données personnelles



- **Au niveau des DataCenters d'IKOULA** : Cloisonnement des réseaux (DMZ), filtrage des flux, redondance, authentification forte et attribution de droits d'accès, sondes, PCA, VPN, anti-virus, journalisation des événements
- **Au sein de KEEPTRACE** : Authentification forte, contrôle des accès par badge, vidéosurveillance, sécurité incendie, alarmes

Contrôle des accès informatiques aux données personnelles



- La connexion à l'outil KEEPTRACE est sécurisée via **https** (protocole TLS)
- Les échanges privés entre différents réseaux reliés entre eux par un réseau géré par un tiers sont **chiffrés** selon deux protocoles de tunneling : IPSEC (site à site et/ou client accès distant) et SSL (client accès distant)

Chiffrement des données à caractère personnel



- Une durée de rétention de 3 à 6 mois par IKOULA.
- Les événements sont ensuite externalisés et conservés durant un an.
- Les données de connexion sont également conservées et archivées pendant un an.
- IKOULA enregistre les tentatives de connexion pendant 1 mois sur le serveur et sauvegardées durant 1 an

Journalisation



- Sauvegardes stockées dans les datacenters IKOULA
- Sauvegardes **toutes les 24 heures conservées** sur disque pendant 7 jours.

Sauvegardes des données à caractère personnel



- **Au niveau d'IKOULA :**
Article 7 des conditions générales d'hébergement de données à caractère personnel dans le cadre du RGPD : le sous-traitant ultérieur doit adresser les demandes à KEEPTRACE.
- **Au sein de KEEPTRACE:**
Une procédure de gestion des demandes de droit des personnes concernées a été mise en place, un DPO est en charge de ces questions

Procédure de réponse aux droits des personnes concernées



- **Au niveau des DataCenters :**
Un Plan d'Assurance Sécurité (PAS) a été mis en place par IKOULA pour garantir la sécurité et l'intégrité des données
- **Au sein de KEEPTRACE :**
Une procédure de gestion des violations de données personnelles avec une sensibilisation du personnel ont été mis en place

Procédure de notification en cas de violation des données personnelles



- **Au niveau des DataCenters :**
Aucune procédure n'a été mise en place par IKOULA. Toutefois, ce dernier s'y engage dans les conditions générales d'hébergement.
- **Au sein de KEEPTRACE :**
Une procédure de gestion des demandes clients et une procédure en cas de contrôle CNIL (interne) avec sensibilisation du personnel ont été mis en place

Procédure d'aide du responsable de traitement en cas d'audit ou réclamation de l'autorité de contrôle



- **Au niveau des DataCenters :**
Les accès sont restreints aux membres autorisés d'IKOULA et aux membres habilités de KEEPTRACE
- **Au niveau de l'outil KEEPTRACE :**
Accès restreints au support technique

Gestion des comptes administrateurs



- **Au niveau des DataCenters :**
Dossier d'architecture complet
- **Au sein de KEEPTRACE :**
Utilisateurs Admin technique pour effectuer les mises à jour et/ou paramétrages avec un accès aux données personnelles des clients.

Protection des infrastructures informatiques



Le présent document relatif aux mesures de sécurité techniques et organisationnelles peut être amené à évoluer.

La dernière mise à jour a été effectuée le 17/06/2021