Politique de sécurité

OBJECTIF

Cette politique de sécurité détaille comment et dans quelle mesure ARKHEUS assure la sécurité, ce qui signifie le contrôle et l'accès, des données qu'il collecte, stocke, traite, et plus généralement de tout le système d'information de ARKHEUS.
En ce qui concerne le règlement général de l'UE sur la protection des données (UE 2016/679), ce document vise à garantir que ARKHEUS couvre toutes les exigences de sécurité des données.

1 RÔLES ET RESPONSABILITÉS

1.1 Au sein d'ARKHEUS

Paul DIOWO agit en tant que responsable de la sécurité de ARKHEUS. Il peut être contacté à pdiowo@arkheus.fr.
Ses responsabilités comprennent:
● le contrôle et la maintenance de toutes les ressources informationnelles de ARKHEUS
● gestion de l'équipe de développement pour superviser toutes les modifications apportées le code source
● gestion de l'équipe sysadmin pour superviser toutes les décisions d'infrastructure

Conformément au règlement général sur la protection des données de l'UE, ARKHEUS a nommé un délégué à la protection des données (DPO) qui peut être contacté sur dpo@arkheus.fr.
Les responsabilités du DPO comprennent:
● Éduquer l'entreprise et les employés sur la conformité RGPD et ses exigences;
● Former le personnel impliqué dans le traitement des données;
● Réalisation d'audits pour garantir la conformité et résoudre les problèmes potentiels proactivement;
● Servir de point de contact entre l'entreprise et les Autorités de contrôle;
● Tenir à jour des enregistrements complets de toutes les activités de traitement des données menées par l'entreprise, y compris la finalité de tout traitement activités, qui doivent être rendues publiques sur demande.

1.2 Externalisation

la société Dutiko assure le service de conseil et d'infogérance d'infrastructure d'Arkheus. Son rôle est de gérer les serveurs hébergés dans les centres de données scaleway. Ils installent les machines et supervisent le matériel.
Scaleway est notre centre de données. Son rôle est de fournir un espace pour héberger nos serveurs. Ils contrôlent l'accès physique à nos machines.
La société Quality Unit est le fournisseur en marque blanche de la plateforme technologique CASANEO.

2 ACCÈS ET STOCKAGE

2.1 Installations commerciales

L'accès à l'emplacement de l'entreprise est contrôlé par un système de badge / clé. Installations: la surveillance est surveillée par des caméras.

2.2 Stockage

● Les données sont hébergées par la société d'externalisation informatique Scaleway dans ses centres de données.
Pour plus d'information sur les systèmes de sécurités les données hébergées par Scaleway: https://www.scaleway.com/en/pdf/PSSI.pdf

2.3 Applications

● Notre application garantit que les données fournies par notre partenaire ne peuvent être vues que par notre partenaire ou nos employés (afin de suivre nos engagements).
● Nous avons une authentification par login / mot de passe sur notre interface CASANEO, pour les collaborateurs, clients et fournisseurs de ARKHEUS.
● La règle de complexité du mot de passe est de 8 caractères minimum.

2.4 Journaux et accès aux journaux

● La quantité d'informations enregistrées est trop importante pour être détaillée. ARKHEUS enregistre tout type d'informations sur les actions sur l'interface, sur le serveur web…
● Les journaux sont stockés dans des bases de données et / ou des fichiers. Leur durée de stockage dépend du type de journal (journaux d'accès, journaux d'actions ...), il peut varier de l'infini à un quelques jours.
● Les partenaires commerciaux de ARKHEUS peuvent accéder aux journaux sur demande à son directeur technique. La demande sera acceptée ou non selon sa légitimité.

2.5 Sécurité de l'appareil

Tous les employés de ARKHEUS utilisent un appareil protégé par antivirus et mises à jour.
La connexion aux ordinateurs personnels est protégée par un mot de passe qui doit respecter un critère de longueur minimale.

3 AUDIT

Si le contrat de prestation le prévoit, les partenaires commerciaux de ARKHEUS sont invités à auditer les procédures de ARKHEUS avec les limitations nécessaires pour assurer la confidentialité de nos clients et fournisseurs.

4 DONNÉES

4.1 Données personnelles

● Toutes les données personnelles et catégories de données collectées, stockées et traitées par ARKHEUS pour le compte de son client sont conservées dans un registre des traitements disponible sur demande. Ce registre détaille tous les objectifs et les informations légales de base de chaque activité de traitement.
● ARKHEUS n'utilise aucune donnée personnelle à d'autres fins que celles décrites dans le registre du traitement.

4.2 Accessibilité des données

● La plupart des données personnelles traitées par ARKHEUS ne sont pas accessibles par les employés de la société, seule une partie peut l'être. Dans ce cas, il peut être accessible de n'importe où dans le monde en connexion via un VPN à la plate-forme de CASANEO de ARKHEUS.
● ARKHEUS ne transfère aucune donnée personnelle à un partenaire tiers sans aucun acceptation du responsable du traitement.
● ARKHEUS ne transfère pas de données en dehors de l'UE. Si, dans un cas exceptionnel, il doivent le faire, ARKHEUS ne procéderait pas sans l'acceptation préalable des titulaires des données.
● L'accès limité, le cryptage et la suppression régulière des données sont les principales mesures pour assurer la sécurité des données.

4.3 Documentation juridique

ARKHEUS a une politique de confidentialité publique disponible sur demande.
Toute la documentation juridique liant ARKHEUS et ses partenaires commerciaux est également disponible sur demande.

4.4 Droits des utilisateurs

Les données peuvent être transférées, supprimées ou modifiées sur demande à M. Paul Diowo via pdiowo@arkheus.fr.
Pour la suppression et la modification, l'opération sera traitée avec des limitations que nous conservons suffisamment de données pour nos obligations légales (comme les données de facturation).

5 MESURE ORGANISATIONNELLE

5.1 Transfert de données

Le transfert de données entre ARKHEUS et ses clients (ou leurs représentants) se fait conformément aux règles prévues dans contrat de prestation.

5.2 Accès des employés

Chaque identifiant d'utilisateur est lié à un individu.
Les mots de passe des ordinateurs personnels ne peuvent être réinitialisés ou modifiés que par des employés habilités pour une procédure donnée.

5.3 Confidentialité

La sécurité et la confidentialité avec lesquelles les employés de ARKHEUS doivent traiter les données personnelles est décrites et mis en évidence dans la charte informatique de ARKHEUS.
En outre, une session de formation sur le RGPD menée par DPO SPRING chez ARKHEUS a été mise en place pour mettre en avant l'importance de la confidentialité.

5.4 Formation et sensibilisation des employés

ARKHEUS dispose de son propre outil de formation interne pour fournir l'information idoine et organiser des sessions de formation sur la sécurité des données, les bonnes pratiques de confidentialité et procédures internes.
ARKHEUS a sensibilisé ses employés à travers des modules de formation sur l'importance de la confidentialité dans nos activités et en particulier du respect du RGPD.

5.5 Autres politiques

ARKHEUS a mis en place des accords avec tous les sous-traitants et des tiers pour garantir que les opérations sont traitées avec le même niveau de sécurité qu'offre ARKHEUS. Toute la documentation légale liant ARKHEUS et ses partenaires commerciaux est également disponible sur demande.

6 SURVEILLANCE ET SIGNALEMENT DES INCIDENTS

Une surveillance externe est effectuée pour suivre la disponibilité des services clés. Les alertes sont envoyées à Paul DIOWO et par e-mail aux employés en service.