Sécurité des données confidentielles

I. Quelles sont les données collectées par RFID Discovery ?

Dans le cadre de l'utilisation de la plateforme RFID Discovery, nous sommes amenés à collecter différentes données dont :

- Des données personnelles
- Des données non personnelles

Toutes ces données sont stockées sur nos serveurs, hébergées dans l'Union Européenne chez OVH.

1. Utilisation des données personnelles

Les « données personnelles » sont des informations permettant de vous identifier en tant qu'individu ou se rapportant à un individu identifiable.
Nous pouvons collecter et générer des données personnelles via l'application RFiD Discovery, par exemple, lors de la création d'utilisateurs ou de notifications d'alertes.
Nous collectons les types de données personnelles suivantes :

Nom
Adresse électronique
Mot de passe
Numéro de téléphone

Nous avons besoin de collecter des informations personnelles afin de fournir les services qui vous correspondent. Vous pouvez choisir de ne pas nous fournir certaines informations demandées, cependant, il est possible que vous ne puissiez pas bénéficier de certains de nos services ou que nous ne puissions pas vous fournir ces services.
Si vous nous divulguez des informations personnelles concernant d'autres personnes, vous reconnaissez avoir l'autorisation de le faire et vous nous permettez d'utiliser ces informations conformément à cette politique de confidentialité.

2. Comment utilisons-nous les informations personnelles que nous collectons sur vous ?

Les informations personnelles que nous collectons auprès de vous nous aident à personnaliser votre expérience et nos communications avec vous et nous aident également à améliorer continuellement votre expérience avec nos services.
Nous utilisons les informations personnelles collectées ci-dessus pour les objectifs suivants :

- Assurer la fonctionnalité de nos services et s'acquitter de vos demandes, notamment :
    - Ouvrir et accéder à votre compte de manière personnelle et sécurisé.

- Répondre à vos questions et à vos demandes par exemple lorsque vous nous contactez via un de nos formulaires de contact ou chat en ligne.
- Traiter votre commande ou autres transactions, y compris la garantie et l'enregistrement de produit, les réclamations ou demandes, et vous offrir un service client dédié.
- Vous envoyer des informations administratives, telles que les changements de nos conditions générales et politiques.
- Assurer le bon fonctionnement des services souscrits, notamment l'envoi des alertes mails et/ou SMS

- Vous proposer nos newsletters et/ou d'autres documents marketing, et faciliter le partage social.
  - Vous envoyer des courriels publicitaires ou marketing, des SMS, et courriers avec des informations sur nos services, de nouveaux produits et d'autres nouvelles de notre entreprise.
  - Faciliter le partage sur les réseaux sociaux de la fonctionnalité que vous choisissez d'utiliser.

Nous nous engageons dans cette activité avec votre consentement accordé lors de votre commande qui respecte nos conditions générales de vente.

3. Utilisation des données non personnelles

L'utilisation des données non personnelles permet un fonctionnement optimal de la plateforme. Pour cela, nous collectons différents types de données, notamment :

- Les plans des bâtiments dans laquelle la solution est installée.
- La structure des services de votre organisation.
- La liste de votre matériel, ainsi que sa géolocalisation associée.

Ces données sont fournies par le client, que nous importons telles quelles sur la plateforme RFID Discovery. Elles ne sont utilisées que pour garantir le bon fonctionnement des services souscrits, notamment la géolocalisation du matériel.

II. Recommandations pour améliorer la sécurité de vos données.

Dans cette partie, vous trouverez quelques conseils pour améliorer la sécurité de vos données, personnelles ou non, lors de votre utilisation des solutions RFiD Discovery.

- **Gateway sur VLAN dédié**
  - Les gateways servent à communiquer les informations du réseau de géolocalisation vers nos serveurs, et demandent donc un accès vers l'extérieur de votre établissement . Les mettre sur un réseau séparé du reste de l'infrastructure IT permet une étanchéité totale en cas d'attaque.

- **Evitez d'avoir un nom d'utilisateur personnel.**
  - Nous vous recommandons de ne pas indiquer votre nom dans le champ « nom d'utilisateur » et d'inscrire votre titre. Par exemple « Responsable du service biomédical »

- **Norme des mots de passe.**
  - Utilisez des mots de passe suffisamment longs, complexes et différents. La majorité des attaques est souvent due à des mots de passe trop simples ou réutilisés. Au moindre doute, ou même régulièrement en prévention, changez-les. Une bonne pratique serait d'utiliser un gestionnaire de mots de passe en ligne.

- **Mailing liste sécurité info (service IT)**
  - Nous communiquer le contact d'une personne responsable de la sécurité dans votre établissement afin que nous puissions échanger des informations urgentes sur votre cybersécurité.

- **Navigateurs à jour.**
  - Vous corrigez ainsi les failles de sécurité qui pourraient être utilisées par des pirates pour s'introduire dans vos appareils, pour y dérober vos informations personnelles ou vos mots de passe, voire pour détruire vos données ou encore vous espionner.

- **Utilisez des plans avec les informations nécessaires uniquement.**
  - Nous vous recommandons de nous donner accès à des plans de l'hôpital simplifiés servant seulement à la géolocalisation. Ils ne doivent pas contenir d'éléments de sécurité comme les issus de secours ou les compteurs électriques.

- **Utilisez un antivirus.**
  - Les antivirus permettent de se protéger d'une grande majorité d'attaques et de virus connus. Il existe de nombreuses solutions gratuites ou payantes selon vos usages et le niveau de protection ou de services recherchés. Vérifiez régulièrement que les antivirus de vos équipements sont bien à jour et faites des analyses (scans) approfondies pour vérifier que vous n'avez pas été infecté.

- **Méfiez-vous des messages inattendus.**
  - En cas de réception d'un message inattendu ou alarmiste par messagerie, SMS ou chat, demandez toujours confirmation à l'émetteur par un autre moyen s'il vous semble connu et légitime. Il peut en effet s'agir d'une attaque par hameçonnage (phishing) visant à vous piéger pour vous dérober des informations confidentielles (mots de passe, informations d'identité ou bancaires), de l'envoi d'un virus contenu dans une pièce-jointe qu'on vous incite à ouvrir, ou d'un lien qui vous attirerait sur un site malveillant.