Sicherheit und Datenschutzerklärung

I. Welche Daten werden von RFID Discovery erfasst?

Im Rahmen der Nutzung der RFID-Discovery-Platform sind wir verpflichtet, verschiedene Daten zu erheben, darunter:

- Personenbezogene Daten
- Nicht personenbezogene Daten

Alle diese Daten werden auf unseren Servern gespeichert, die in der Europäischen Union bei OVH gehostet werden.

1. Verwendung personenbezogener Daten

"Personenbezogene Daten" sind Informationen, die Einzelpersonen identifizieren oder sich auf eine identifizierbare Person beziehen.
Wir können personenbezogene Daten über die RFiD-Discovery-Anwendung erheben und generieren, z. B. beim Erstellen von Benutzern oder bei Warnmeldungen.
Wir erheben die folgenden Arten von personenbezogenen Daten:

Name
E-Mail-Adresse
Passwort
Telefonnummer

Personenbezogene Daten werden gesammelt, um die für Sie relevanten Dienstleistungen erbringen zu können. Sie können sich dafür entscheiden, uns bestimmte angeforderte Informationen nicht zur Verfügung zu stellen. Es kann jedoch sein, dass Sie dann einige unserer Dienstleistungen nicht in Anspruch nehmen können oder wir Ihnen einige Dienstleistungen nicht anbieten können.
Wenn Sie personenbezogene Daten über andere Personen offenlegen, erkennen Sie an, dass Sie dazu berechtigt sind, und Sie ermächtigen uns, diese Informationen in Übereinstimmung mit dieser Datenschutzrichtlinie zu verwenden.

2. Wie verwenden wir die personenbezogenen Daten, die wir über Sie sammeln?

Die personenbezogenen Daten, die wir von Ihnen sammeln, helfen uns, unsere Kommunikation mit Ihnen zu personalisieren und Ihre Erfahrungen mit unseren Diensten kontinuierlich zu verbessern.

Wir verwenden die oben genannten personenbezogenen Daten für folgenden Zwecke:

- Zur Sicherstellung der Funktionalität unserer Dienste sowie Ihre Anfragen zu erfüllen, inklusive:
    - Benutzerkonto Einrichtung sowie sicherer Zugriff auf dieses
    - Um auf Ihre Fragen und Wünsche zu antworten, z. B. wenn Sie uns über eines unserer Kontaktformulare oder einen Online-Chat kontaktieren.
    - Bearbeitung Ihrer Bestellung oder anderer Transaktionen, einschließlich Garantie- und Produktregistrierung, Reklamationen oder Anfragen, und Bereitstellung des Kundendienstes.
    - Zusendung administrativer Informationen, wie z. B. Änderungen unserer Allgemeinen Geschäftsbedingungen.
    - Gewährleistung des ordnungsgemäßen Funktionierens in Anspruch genommener Dienste, insbesondere des Versands von E-Mail- und/oder SMS-Benachrichtigungen
- ~~Um Ihnen unsere Newsletter und/oder andere Marketingmaterialien zur Verfügung zu stellen und das Teilen in sozialen Netzwerken zu erleichtern.~~
    - Zusendung von Werbe- oder Marketing-E-Mails, Textnachrichten und/oder Briefe mit Informationen über unsere Dienstleistungen, neue Produkte und andere Unternehmensnachrichten.
    - Um es Ihnen zu erleichtern die Funktionen, die Sie benutzen, in sozialen Netzwerken zu teilen.

Wir führen diese Aktivität mit Ihrer Zustimmung durch, die Sie während Ihrer Bestellung erteilt haben und die unsere allgemeinen Verkaufsbedingungen berücksichtigen.

3. Verwendung nicht personenbezogener Daten

Die Verwendung nicht personenbezogener Daten ermöglicht ein optimales Funktionieren der Plattform. Zu diesem Zweck erheben wir verschiedene Arten von Daten, darunter:

- Die Pläne der Gebäude, in denen die Lösung installiert ist.
- Die Abteilungsstruktur Ihrer Organisation.
- Die Liste Ihrer Geräte sowie die zugehörige Geolokalisierung.

Diese Daten werden vom Ihnen zur Verfügung gestellt, und werden in Folge von uns in die RFID Discovery-Platform importiert. Sie werden lediglich dazu verwendet, das ordnungsgemäße Funktionieren der zur Verfügung gestellten Dienste zu gewährleisten, einschließlich der Geolokalisierung der Geräte.

II. Empfehlungen zur Verbesserung der Sicherheit Ihrer Daten.

In diesem Teil finden Sie einige Tipps, um die Sicherheit Ihrer personenbezogenen und unpersönlichen Daten bei der Verwendung von RFiD Discovery-Lösungen zu verbessern.

- **Gateway im zugeordneten VLAN**
  - Gateways werden verwendet, um Informationen aus dem Geolokalisierungsnetz an unsere Server zu übermitteln und somit den Zugriff außerhalb Ihrer Einrichtung zu beantragen. Sie sollten in einem vom Rest der IT-Infrastruktur getrennten Netzwerk untergebracht sein, was eine vollständige Abschottung im Falle eines Angriffs ermöglicht.

- **Vermeiden Sie persönliche Benutzernamen**
  - Wir empfehlen Ihnen, Ihren Namen nicht in das Feld "Benutzername" einzutragen, sondern Ihren Titel einzugeben, zum Beispiel "Leiter der biomedizinischen Abteilung".

- **Passwort-Standard**
  - Verwenden Sie Passwörter, die lang, komplex und unterschiedlich genug sind. Die meisten Angriffe sind auf Passwörter zurückzuführen, die zu einfach sind oder häufig wiederverwendet werden. Ändern Sie Ihre Passwörter im im Verdachtsfall der unautorisierten Weitergabe oder zur Vorbeugung sogar regelmäßig zur. Die Verwendung eines Online-Passwort-Managers ist zu empfehlen.

- **Sicherheitsinformationen zur Mailingliste (IT-Abteilung)**
  - Geben Sie uns gerne den Kontakt zu einer Person, die für die Sicherheit in Ihrer Einrichtung verantwortlich ist, damit wir im Bedarfsfall dringende Informationen über Ihre Cybersicherheit austauschen können.

- **Aktuelle Browser**
  - Um Sicherheitslücken zu vermeiden verwenden Sie bitte durchgehend die jeweils aktuellste Version Ihres Browsers, da Sicherheitslücken veralteter Versionsstände von Hackern ausgenutzt werden könnten. Hierdurch kann das Risiko des Eindringens in Ihre Geräte und der resultierende Diebstahl oder die Änderung Ihrer persönlichen Daten oder Passwörter verringert werden.

- **Verwenden Sie nur Pläne, die die erforderlichen Informationen enthalten**
  - Wir empfehlen Ihnen, lediglich vereinfachten Krankenhausplänen zukommen zu lassen, welche nur für die Geolokalisierung verwendet werden. Diese sollten keine Sicherheitseinrichtungen wie Notausgänge oder Stromzähler enthalten.

- **Verwenden Sie ein Virenschutzprogramm**
  - Antivirenprogramme schützen vor einer großen Mehrheit der bekannten Angriffe und Viren. Es gibt viele kostenlose oder kostenpflichtige Lösungen, abhängig von Ihren Verwendungszwecken und dem gewünschten Schutzniveau oder den gewünschten Diensten. Überprüfen Sie regelmäßig, ob die Antivirensoftware auf Ihren Geräten auf dem neuesten Stand ist, und führen Sie gründliche und regelmäßige Scans durch, um sicherzustellen, dass Sie nicht infiziert wurden.

- **Vorsicht bei unerwarteten Nachrichten**
  - Wenn Sie eine unerwartete oder alarmierende Nachricht per Email, SMS oder Chat erhalten, bitten wir Sie den Absender immer um eine Bestätigung auf andere Weise. Es könnte sich um einen Phishing-Angriff handeln, der Sie dazu verleitet, vertrauliche Informationen (Passwörter, Identitäts- oder Bankdaten) preiszugeben oder einen Anhang zu öffnen, indem ein Virus gesendet wird.