Security and Privacy Policy

I. What data does RFiD Discovery collect?

As part of the use of the RFID Discovery platform, we are required to collect various data including:

- Personal data
- Non-personal data

All this data is stored on our servers, hosted in the European Union at OVH.

1. Use of personal data

"Personal data" is information that identifies you as an individual or relates to an identifiable individual.
We may collect and generate personal data through the RFiD Discovery application, for example, when creating users or alert notifications.
We collect the following types of personal data:

Name
E-mail address
Password
Phone number

We need to collect personal information to provide the services that are relevant to you. You may choose not to provide us with certain requested information. However, this will mean that we may not be able to provide you with some of our services.
If you disclose personal information about other people, you acknowledge that you are authorised to do so and that you authorise us to use that information in accordance with this privacy policy.

2. How do we use the personal information we collect about you?

The personal information we collect from you helps us personalise your experience and our communications with you and helps us continually improve your experience of our services.

We use the personal information collected above for the following purposes:

- To ensure the functionality of our services and fulfill your requests, including:
    - Opening and accessing your account in a personal and secure way.
    - Responding to your questions and requests for example when you contact us via one of our contact forms or online chat.
    - Processing your order or other transactions, including warranty and product registration, and providing you with dedicated customer service.
    - Sending you administrative information, such as changes to our terms and conditions.
    - Ensuring the proper functioning of the subscribed services, in particular the sending of emails and/or SMS alerts
    - Sending you advertising or marketing emails, text messages, and letters with information about our services, new products, and other company news.

We engage in this activity with your consent granted when you place your order which respects our general conditions of sale.

3. Use of non-personal data

The use of non-personal data allows optimal functioning of the platform. To do this, we collect different types of data, including:

- The plans of the buildings in which the solution is installed.
- The department structure of your organisation.
- The list of your equipment, as well as its associated geolocation.

This data is provided by you as the customer which we import on to the RFID Discovery platform. They are only used to ensure the proper functioning of the services subscribed, including the geolocation of the equipment.

II. Recommendations to improve the security of your data.

In this section, you will find some tips to improve the security of your data, personal or not, when using the RFiD Discovery platform.

- **Gateway on dedicated VLAN**
    - The gateways are used to communicate information from the geolocation network to our servers, and therefore request access outside of your establishment. Put them on a separate network from the rest of the infrastructure IT enables total sealing in the event of an attack.

- **Avoid having a personal username**
  - We recommend that you do not enter your name in the "username" field and enter your title instead. For example, "Head of the biomedical department".

- **Password standard**
  - Use passwords that are long, complex, and difficult to guess. Most cyber attacks are often to the result of passwords that are too simple or reused. At the slightest doubt, or even regularly as prevention, change them.

- **Mailing list security info (IT department)**
  - Provide us with the contact details of a person responsible for IT security at your organisation so that we can exchange urgent information about your cybersecurity.

- **Up-to-date browsers**
  - This corrects security vulnerabilities that could be used by hackers to break into your devices, steal your personal information or passwords, or even destroy your data or spy on you.

- **Use plans with the necessary information only**
  - We recommend that you give us access to simplified hospital maps used only for geolocation. They must not contain safety features such as emergency exits or electricity meters.

- **Use antivirus software**
  - Antivirus software protects against the majority of known malware and viruses. Regularly check that the antivirus software on your equipment is up to date and perform thorough scans regularly to verify that you have not been infected.

- **Beware of unexpected messages.**
  - In case of receipt of an unexpected or alarming message by messaging, SMS, or chat, always ask the sender for confirmation. It could be a phishing attack to trick you into revealing confidential information (passwords, identity or banking information) or sending a virus contained in an attachment that you are encouraged to open.