CLARIPROD

Plug-and-play **smart manufacturing**

Data Security

At Clariprod, we take security seriously. We are aware that your data is valuable and we are committed to keeping it secure. That is why we work with leading global technology partners to store and process your data and we why we have built our solution using some of the most widely used communication protocols and operating platforms.

1. Our solution central piece of hardware is a data acquisition controller based on the Android operating system. This Clariprod Controller is connected to your company's WIFI network. The WIFI connection can be protected in WPA2 mode. The WPA2 key, is an alphanumeric code protecting access to the WIFI network. Without this password, you cannot access the Wi-Fi network. This type of security key includes all the mandatory elements of the 802.11 standard certified by the WiFi Alliance. Our solution is therefore as secure as an Android mobile phone connecting to your WIFI network. If you do not let mobile phones connect to your company network and would like to separate the Clariprod Controllers from your main company network, we recommend setting up a WIFI network independent of that of the company, such as a "Guest" network. This can easily be done on most network equipment and at a low cost.

2. The Clariprod Controller connects to a secure Application Programming Interface (API) via HTTPS on our servers hosted by Amazon Web Services (AWS) and OVHCLoud (OVH), two world leaders in cloud information technology. Only a controller with a known MAC address (Unique Physical Address of the Controller) associated with the Clariprod database can interact with the API. This association is made manually by our database managers at each customer account opening to limit security breaches. An unidentified device will therefore not be able to exchange data with the Clariprod servers or gain access to your data.

3. This data is stored on AWS and OVH servers in a redundant architecture. That is, database services and systems have duplicates in both physical equipment and data, to ensure continued operation and access to data in the event that one of the components proves to be defective. Customers can rest assured that they will always have access to their data and that their data will always be backed up.