Informative Notice on Product Data Access and Sharing

(Pursuant to Regulation (EU) 2023/2854 – EU Data Act)

Product and Manufacturer Identification

Product Name: *Inxpect SRE 200 Series & Inxpect SRE 100 Series*
Manufacturer: *Inxpect S.p.A*
Contact: *Via Serpente, 91 25131 Brescia Tel: +39 030 578 5105*
Email: hello@inxpect.com, Web: www.inxpect.com

Purpose of this notice

This notice informs you, as the user of the product, about your rights under the EU Data Act (Regulation (EU) 2023/2854) concerning access to data generated through your use of the product.

Please note: The manufacturer of this product, Inxpect S.p.A, does not collect, store, or control any of the data generated by the product.
All data generated are stored locally on the device and remain under your control as the user.

System description

Quick description of the system

The 100 and 200 Series systems are designed to detect the presence of persons ensuring safety functions. Each system is composed of a control unit and a combination of up to six sensors based on RADAR technology connected via CAN bus.
The Radar sensor shall detect the presence of a target inside a safe detection field and communicate with the CAN interface that is considered an internal interface of the system only for sensor connection.
The control unit shall process incoming messages from the sensors and safely convert them to a suitable output interface.

System configuration parameters

The system configuration consists of all the parameters that can be set by the operator and that can safely affect the behavior of the system, in particular: detection field definitions, input/output functionality, network and fieldbus settings, etc.
The system configuration is performed by an external PC-based engineering tool (configuration Software) that needs to communicate with the control units using one of the suitable channels: USB or Ethernet communication channels.
The configuration parameters are permanently stored on the control unit device, protected by a multi-user authentication mechanism and only users with proper privileges, listed below, can access the device:

- **Observer**, that has minimum privileges. He can just read the system configuration without making any changes;

- **Expert**, that can read the system configuration, launch the real-time validation and download the logs without making any changes;
- **Safety Engineer,** that can configure the system performing changes of the monitored areas, number of sensors and all the parameters linked to the detection capability of the system;
- **Administrator**, that has maximum privileges level and can configure the system, the parameters related to communication interfaces and manage the other users (resetting passwords, enabling/disabling the account)

An additional access level, called **Service,** can be created and enabled by the Administrator in order to allow service operations by the Inxpect Technical Support. In this case, access is limited to performing support operations and is terminated once they are completed. No data, generated by the system, are downloaded and saved by Inxpect.

In addition, the C20xB control unit models provide an SD card interface for backup/restore of the system configuration.

The system configuration is permanently stored into the external flash of the control unit.

The sensors do not permanently store the configuration. At every power up or new configuration, the control unit sends the parameters to the connected sensors that apply the configuration into the processing.

Which data are generated

Generated data

The system may generate the following categories of data during operation:

- sensor readings (presence and position of the target in the detection fields)
- Status and diagnostic data – diagnostic events, safety and security events, error logs

These data are not transmitted to the manufacturer or to any external server by default.

They are stored locally within the device and can only be accessed via a physical or digital interface (e.g., USB/Ethernet, configuration software, internal logs).

The control unit provides the capability to log events that can be downloaded, at a later time, via the engineering tool. In addition to diagnostic events and detection field events, security events are recorded into the external flash of the control unit, in particular: login, failed login attempts, factory reset event.

The event log recorded by the system can be downloaded following the instruction in the user manual, accessible through Inxpect Tools area.

User Rights under the EU Data Act

Even though Inxpect S.p.A does not hold your data, you have the following rights:

- Access the data stored on your device in a structured, commonly used, machine-readable format
- Port the data to third parties of your choice
- Authorize third parties to retrieve data directly from the device, where technically possible
- Control when and how your data are shared or deleted

How to access or share your data

Since the data are stored on the device itself, you can access or export them by:

- Using the Configuration Software (Inxpect Safety App or Inxpect Safety Studio)
- Following the instructions in the user manual, accessible through Inxpect Tools area

- Consulting the Technical Support who can assist with data extraction

If you choose to allow a third party to access your data, ensure they comply with EU Data Act obligations regarding fair, transparent, and secure use.

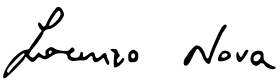
Manufacturer's Role and Limitations

- Inxpect S.p.A has no access to your data and does not process, analyze, or share them in any way.
- We cannot retrieve, store, or manage your data on your behalf.
- Our responsibility is to ensure the product enables easy, secure, and transparent access to the data by you and any third party you authorize.

Legal Disclaimer

This informative notice is provided pursuant to Article 3(2) of Regulation (EU) 2023/2854 (EU Data Act). It is intended to clarify the roles and responsibilities regarding data access and sharing for products that store data locally and where the manufacturer is not the data holder.

Name and role: Lorenzo Nava, CPO

Firma / Signature: 

Data / Date: 25/08/2025