

Pre-Contractual Information Art. 3 Data Act

AGILOX Services GmbH, as the provider of a connected product ("provider"), provides its customers with the following pre-contractual information within the meaning of Art. 3 of Regulation (EU) 2023/2854 ("Data Act"):

1. Identity and contact details of the provider

AGILOX Services GmbH
Gewerbepark 3
A-4671 Neukirchen bei Lambach
Austria
Email / Support: office@agilox.net

2. Description of the connected product

This statement applies to the provider's connected products:

- a. Autonomous Mobile Robots (AMR – automated guided vehicle systems)
- b. IPC Gateway Appliances (standalone gateway units that provide access to fleets)

3. Nature, scope and storage location of the data generated or collected

The connected product continuously generates data during operation. The connected product stores data locally on the device.

Depending on a setting selected by the customer, data are also transmitted to the AGILOX Data-Server. This is a prerequisite for using services via the AGILOX World platform.

a. Data types

- Vehicle status data, e.g. vehicle positions, battery level and temperatures.
- Further sensor data are generated, which are deleted after each programme cycle and are not stored permanently. Some current statuses are displayed on the HMI.
- Operating mode (Automatic, Manual, Maintenance).
- Diagnostic data such as error states (errors, problems, warnings).
- Order data, such as information on the start and destination of an order.
- Configuration parameters, e.g. Union configuration (name, ID) and vehicle configuration (name, type, model).

- System information, e.g. WLAN signal strength, operating time and CPU utilisation.
- The username may be visible in the log files.

b. Data formats

The data are made available in common formats such as JSON, TXT, CSV or binary format.

c. Data volume

Depending on usage, the average daily volume of data generated is expected to remain below 100 MB/day.

4. Options for customer access to the data

- **Human-machine interface:** The data listed in Section 3 are accessible via the human-machine interface (HMI).
- **Reports (log files)** are stored for 14 days and can be retrieved or exported via the HMI.
- Parts of the above-mentioned data can be queried via **API requests**.
- **Data request under the EU Data Act by contacting the provider** by email at *support@agilox.net*. When a request is received, the data are provided to and made available to the customer. If the customer has disabled data transmission in the HMI or by other technical measures, the data cannot be provided. The data are made available only to persons expressly authorised by the user.

Access to and use of the data are subject to the system's general terms of use. The data that may be accessed depend on the user's role. The provider makes the product data available in the form and quality in which they are generated by the connected product during normal operation. Technical specifications and authentication procedures are provided or linked before conclusion of the contract.

5. Restrictions and conditions governing data use

The provider explains the following before conclusion of the contract:

- The customer is entitled to use the data generated by the connected product and to request that they be made available to third parties designated by the customer (Art. 5 Data Act). If the customer requests that the data be made available to a designated third party, the provider is entitled to fair, reasonable and non-discriminatory (FRAND) remuneration. The customer may use the data for internal processes and optimisations, such as order processing with a fleet manager.

- For technical reasons, querying the data, including current status values, via the vehicle API more than once per second is not recommended.
- Data transmission to the server can be disabled in the HMI. In this case, the provider's provision of the data is correspondingly restricted.
- Data requests made by contacting the provider are processed without unnecessary delay; in exceptional cases, delays may occur for operational reasons.

6. Costs and charges

The raw data are made available to the customer free of charge via the options described in Section 4. Additional charges may be introduced in future for value-added and processing services (e.g. the AGILOX World platform or Analytics); the customer's access to its raw data remains free of charge.

In addition to raw data, processed data can also be requested via the AGILOX World platform. The applicable costs are specified in the offer or contract.

7. Use of data by the provider

The provider will use the data generated at the customer's site for operating, securing, improving and statistically evaluating the products and as a basis for billing for the products, and will comply with the limits of Art. 4(13) Data Act. Any independent processing of the data by third parties for the provider's own purposes beyond these purposes is not permitted without a separate agreement with the customer.

8. Disclosure to third parties / sub-processors

The provider is entitled at any time to use processing services—for example, cloud computing services (including IaaS, PaaS and SaaS services), hosting services or comparable solutions—for the purposes set out in Section 7. The same authorisation also applies to third-party service providers and sub-processors appointed by the provider.

Data are disclosed to third parties using appropriate up-to-date security measures. These include, in particular, authentication mechanisms to ensure the identity of the parties accessing the data and a role- and permission-based access control concept based on the least privilege principle, which permits access only to data explicitly assigned to connected products.

9. Data security

The provider will take appropriate technical and organisational measures to protect data

against unauthorised access, unauthorised use, unauthorised disclosure, loss, alteration or other impairment. This includes, in particular, risk-appropriate measures for access control, authentication, logging, encryption, integrity protection, vulnerability management and restoration of the affected systems. The hard drives of the connected products are encrypted. The HMI has role-based access control (RBAC) for authentication. For each swarm ([EN: Union](#)), an API key is generated; data are transmitted via SSL.

The provider has established a standard process and responsibilities for handling security incidents. If the provider identifies a security incident or has reasonable grounds to suspect one, it will, without undue delay, take appropriate measures to contain, investigate and remedy it and prevent further impacts. The provider is entitled temporarily to restrict, suspend or, where necessary, prohibit access to data, their use or their disclosure if and for as long as necessary to prevent, contain or remedy a security incident, or if access to, use of or further disclosure of the data concerned could undermine the security requirements of the connected product.

10. Changes during the term of the contract

The scope, format or frequency of data access may change where necessary to maintain or improve the product/service or to comply with legal requirements. The provider will make adjusted specifications available to the extent reasonably practicable.

11. Deletion of data

The customer may delete data generated locally on the device or request their deletion. Deletion may affect and/or prevent the provision of services by the provider and/or the functionality of the devices. The provider shall not be liable for the functionality of the devices and/or the provision of its services if the customer deletes the data without authorisation. The provider may refuse deletion if deletion impairs the functionality of the devices and/or the provision of its services.

Transmission of the data to the AGILOX Data-Server can be disabled at any time via the HMI.

12. Trade secrets

If the data made available contain trade secrets of the provider or third parties, they will be identified as such before being made available. Their disclosure may be made conditional upon the agreement of appropriate technical and organisational confidentiality measures.

13. Right to lodge a complaint

The customer is entitled to lodge a complaint with the competent supervisory authority about a suspected infringement of the provisions of the Data Act (Art. 37 Data Act).

14. Duration of use

The period during which the data are made available depends on the term of the relevant contract for the connected product. Termination of the contract does not affect the provider's use of data already held by the provider.