

POLICY STATEMENT TO USERS ON DATA GENERATED BY CONNECTED PRODUCTS AND RELATED SERVICES

pursuant to EU Regulation 2023/2854 (Data Act)

1. Premise

This policy statement is provided in accordance with Regulation (EU) 2023/2854¹ (the “Data Act”) and describes the data generated by the connected products² and the related services³ offered by CAME S.p.A., the rights and obligations of the end users⁴ and the Data Holder⁵, and the data access and sharing mechanisms.

Please refer to article 2 of Regulation (EU) 2023/2854 for the definitions used in this document or for other definitions relating to the Data Act.

2. Data Holder

Came S.p.A. (Tax Code/VAT No. 4835400260), with registered office in Dosson di Casier (TV), Viale delle Industrie 89/A.

E-mail: support.cameconnect@came.com - Phone: +39 0422 1569511

¹ Law designed to improve the data economy of the EU and promote a competitive data market, making the data (especially industrial data) more accessible and usable, encouraging data-based innovation and increasing their availability. To that end, the Data Act ensures fairness in the allocation of value from data among actors in the data economy, clarifying who can use the data, what data and under what terms. For more information: [Explanation of the Data Act | Shape the digital future of Europe](#)

² **Connected product:** an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user. **Product data** means data generated by the use of a connected product that the manufacturer designed to be retrievable, via an electronic communications service, physical connection or on-device access, by a user, data holder or a third party, including, where relevant, the manufacturer.

³ **Related service:** a digital service, other than an electronic communications service, including software, which is connected with the product at the time of the purchase, rent or lease in such a way that its absence would prevent the connected product from performing one or more of its functions, or which is subsequently connected to the product by the manufacturer or a third party to add to, update or adapt the functions of the connected product. **Related service data** means data representing the digitisation of user actions or of events related to the connected product, recorded intentionally by the user or generated as a by-product of the user's action during the provision of a related service by the provider.

⁴ **User:** a natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services.

⁵ **Data Holder:** a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service.

3. Connected products and related services involved

This policy statement applies to the following connected products and related services of the Data Holder:

AREA	CONNECTED PRODUCTS	RELATED SERVICES (APPS/CLOUD)	TYPE OF DATA PROCESSED
TEMPERATURE CONTROL	Thermostats that use Wi-Fi and Bluetooth technology: - TH/550 WH WI-FI - TH/700 WI-FI - TH/750 WI-FI - TH/ONE - TH/ONE B	Apps: "THermo" and "THermo Wi-Fi" "CAMEConnect" Cloud	Physical/environmental measurements such as: - internal ambient temperature - internal ambient humidity - historic internal and external temperature metrics - historic humidity metrics. Usage data such as: - information on the usage made (e.g. turning on/off relay and boiler) - connecting/disconnecting the device from the Cloud - selected operating mode (manual/automatic/holiday/boost/off) - season set - programmes set - status/activation of alarms at certain temperature levels - temperature set (if manual) - temperature adjustment algorithm - device firmware version - pairing matter QR code - geolocation: the system can reveal the position of the user through the application installed on their smartphone. Diagnostic data like information on the status of the device (for example if the device is online/offline, when the thermostat loses connection with CAMEConnect).
ACCESS CONTROL / AUTOMATION	MTMAC video intercom module (entry panel)	"CAME Access" app "CAMEConnect" Cloud	Access events that include: - date/time - ID of user requesting access (telephone no. is included if a call is made to the video intercom entry panel and the number is not associated with any other registered user) - access status: carried out with success/error, giving the reason (e.g. wrong pin, unauthorised badge ID) - access point (indication of the physical device used for access)

			- module used (number pad; telephone no. if call-based access; badge ID; remote control ID) Call events (when the entry panel contacts a remote party to request action on the access point) including: - ID of the party reached by the entry panel call - response by the party (response/no response) - action taken by the contacted party (e.g. access point activation) Generic device data (not associated with access control), for example: - general status of the device settings - update - gateway configurations - configuration backups.
	RBE PLUS receiver system (wall-mounted control panel): - 806RV-0060 (RBE PLUS 24) - 800RV-0070 (RBE PLUS 230)	“CAME Access” app “CAMEConnect” Cloud	Access events that include: - User ID (e.g. <u>name and surname</u> of the user that activated the automation if activated through CAMEConnect Web; <u>alias user</u>, if access is via a badge, number pad or remote control; <u>QUICK&EASY ACCESS system</u> to manage temporary accesses activated for the user) - indication of the device that originated the access command (e.g. web platform; remote control; number pad; keycard RFID code) - access status (granted/not granted) - access point activation (indicate which automation was activated following the input through RBE PLUS). Generic device data (not associated with access control), for example: - device update - command invoked and carried out - gateway configurations - configuration backups.

4. Access, use and availability of the data

The data generated by the connected products and the related services used by the user will be processed by the Data Holder to:

- ensure the **proper operation** of said products and services

- ensure adequate **technical support** for any malfunctions
- collect any data that could be useful to **continuously improve** the devices and applications produced.

In accordance with Regulation (EU) 2023/2854, the user has the right to access the data generated by use of the connected products held and related services used.

The data will be made available in a clear and simple way, without additional costs for the User, with the option to export them in a structured, commonly used and machine-readable, interoperable, standardised format (CSV format) using the tools made available by the Data Holder.

4.1. Temperature Control Data

They can be extracted immediately by the user using the “Download” function on the CAMEConnect web platform on the individual device management page.

The temperature control devices can generate data continuously. The estimated volume of data will depend on the variability of the metric collected linked to the change in temperature variations.

The retention policy applied to the device data is currently three years.

4.2 Access control/automation data

Downloads of the log files linked to the automation may currently be carried out in two ways according to whether the data are recent or older:

→ **data from the most recent two months (sixty days):** the user can use the immediate “Download” function on the CAMEConnect web platform on the individual device management page.

→ **data older than two months:** the user must send an extraction request to the Data Holder at the address noted in paragraph 3. This is necessary since data older than two months are stored by the Data Holder in its storage cloud in a destructured format and therefore have to be retrieved. Once the requested data have been retrieved, along with the pertinent metadata needed to interpret and use the data, they will be sent by the Data Holder to the user in the shortest time possible by email, sharing the applicable link to download the requested data.

For data relating to generic events (e.g. use of an access point), reference to the section “Events” should be made for the download in the CAMEConnect web platform.

The current download systems of the system logs linked to MTMAC and RBE PLUS devices allow a maximum of 10,000 log event/access lines to be downloaded. More than one download will have to be carried out to extract more events.

The retention policy applied to the generic event data is currently 60 days.

5. Obligations of the Parties

In order to share the connected product and related service data, the Data Holder will have to check to ensure that the natural or legal person requesting access to the data is actually the user entitled to access said data, asking for additional information for identification, provided that it is limited and necessary for that purpose.

The Data Holder shall not store information, especially register data, on the access by the user to the requested data apart from what is necessary to properly carry out the user’s request for access and for the security and maintenance of the data infrastructure.

Data containing trade secrets shall be stored and disclosed only on condition that prior to sharing, the Data Holder and the user take all the measures needed to protect confidentiality, especially with respect to third parties (for example by adopting standard contractual clauses, confidentiality agreements, strict access protocols, etc.).

If there is no agreement to that effect, the Data Holder shall be authorised to block and, if necessary, stop sharing the data identified as trade secrets, notifying the user of its decision.

In any case the user may not:

→ use the data obtained to develop a connected product that competes with the connected product from where the data came or share the data with a third party that has this intention

→ use the data to obtain information on the economic situation, resources or production methods of the Manufacturer/Data Holder

→ take advantage of any data protection shortcomings in the technical infrastructure of the Data Holder in order to obtain access to them.

6. Sharing data with third parties

At the user's request, the Data Holder will make the connected products and the related services data promptly available to third parties without delay and in an easy, secure way and free of charge for the user, in a complete, structured, commonly used and machine-readable format.

The data will be made available to the third-party recipient⁶ in accordance with the provisions of article 8 ("*Conditions under which data holders make data available to data recipients*") and article 9 ("*Compensation for making data available*") of the Data Act.

The obligation to make the data available to a data recipient does not require the disclosure of trade secrets by the Data Holder.

Trade secrets shall be disclosed to third parties only to the extent to which disclosure is strictly necessary to pursue the purposes agreed between the user and the third party subject to the adoption between the Data Holder and the third party of all the measures needed to protect the confidentiality of the shared data such as the adoption of standard contractual clauses, confidentiality agreements, strict access protocols, etc.

If there is no agreement or the third party does not implement the agreed measures or compromises the confidentiality of the trade secrets, the Data Holder shall be authorised to block, or if necessary, stop sharing the data identified as trade secrets. In this case, the Data Holder will notify the third party of its decision in writing.

The data will only be used for the purposes specified and will not be shared without the agreement of the user, unless said sharing is indispensable in accordance with the laws of the Union or domestic laws that apply or if there is an exceptional need to use the data.

The Data Holder may also be asked to make the data available to a public sector body, the European Commission, the European Central Bank or a Union body if the body involved shows, through a reasoned request, the exceptional need⁷ to use the data held by the Data Holder.

7. Data protection and confidentiality

The Data Holder shall adopt technical and organisational measures that can guarantee the confidentiality, completeness and availability of the data generated by the connected products and related services used by the user, ensuring compliance with Regulation (EU) 2023/2854 and the laws on privacy to the extent applicable.

⁶ **Data recipient:** means a natural or legal person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a connected product or related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation adopted in accordance with Union law.

⁷ The exceptional need to use the data shall be limited in time and scope and will exclusively be considered to exist in the cases listed under letters a) and b) of article 15 of Regulation (EU) 2023/2854:

a) where the data requested are necessary to respond to a public emergency and the public sector body is unable to obtain such data by alternative means in a timely and effective manner under equivalent conditions

b) in circumstances not covered by point (a) and only insofar as non-personal data is concerned, where:

i) a public sector body has identified specific data, the lack of which prevents it from fulfilling a specific task carried out in the public interest, that has been explicitly provided for by law, such as the production of official statistics or the mitigation of or recovery from a public emergency

ii) the public sector body has exhausted all other means at its disposal to obtain such data, including purchase of data on the market by offering market rates, or by relying on existing obligations to make data available or the adoption of new legislative measures which could guarantee the timely availability of the data.

The data generated by the connected products and related services shall be collected, processed and stored on a secure cloud infrastructure located in the European Union available to the Data Holder through a cloud provider. The data will not be used by the cloud provider for its own purposes.

The data will be stored for the time necessary to ensure the functioning of the connected products and related services, subject to any legal obligations that may require longer storage times.

8. Rights of the user

- **Right of access** to the data generated by use of the connected product or related service and to obtain a copy, free of charge, in a comprehensive, structured, commonly used and machine-readable format.
- **Right to data sharing** with third parties, including the providers of after-sales services or data intermediaries for any lawful purpose.
- **Right to the confidentiality** of any personal data processed: the data must be collected, accessed and used in accordance with Regulation (EU) 2016/679 (GDPR). In the case of conflict between the Data Act and Union law on the protection of personal data, the GDPR shall prevail.
- **Right to portability**, i.e. to request the transfer of one's data (personal and non-personal) to another service provider, facilitating the transfer between the various suppliers.
- **Right to use the data** for any lawful purpose provided for under the Data Act.
- **Right to lodge a complaint** according to the provisions of article 39 of Regulation (EU) 2023/2854 if one considers that the rights under the Data Act have been infringed.

This policy statement is subject to amendment in accordance with any regulatory updates or changes in the Data Holder's corporate processes. The users will be informed of any amendments through the web platform of CAMEConnect (e.g. by pop-up notifications).

Last updated: 26/06/2025