Information on SERVICE BUTTON CLOUD (the "related service") pursuant to Article 3(3) of the Data Act

Product data that the provider is expected to receive:

Type of Product Data	Estimated Scope of the Product Data	Frequency of Product Data Collection
Device telemetry data (e.g., sensor	Approx. 5–20 KB per transmission (JSON format)	Every 1–15 minutes (configurable), or event-based
Device identifiers (device ID, firmware version, hardware model)	< 2 KB per transmission	Upon device registration and firmware updates
Operational status logs and alerts	2–10 KB per event	Event-driven (only when triggered)
Connectivity metadata (IP address, signal strength, timestamp)	1–5 KB per transmission	With each device communication session

- Related service data that the provider is expected to generate:

Type of related service data	Data format	Estimated scope of the data	Frequency of collection
System events (device communication, errors)	JSON	0.5–1 KB per event	Event-based
Usage data (dashboard or API interactions)	JSON	0.5–1 KB per event	Event-based

Related service data is generated in the course of providing the GIOT platform, including access logs, system events, and usage data (e.g., dashboard or API interactions). This data is processed solely for service provision, security, and system performance purposes.

Additional Clarifications

- Data volumes are estimates and may vary depending on device configuration and customer setup.
- Collection frequency may be configurable depending on the service plan.

• Modalities regarding the storage and duration of the aforementioned data by the provider:

Gimasi Deutschland GmbH
Lindwurmstr 97a, 80337 München
DE319590118
+49 89 20002118-0
support@gimasi.de

- The following technical means are available to the customer with regard to the aforementioned data.:
  - Access to the data:
    1. **Web-Based Dashboard (Service Button Cloud Portal):**
       Authenticated users can securely log in to the IoT Cloud web platform via browser to view device data, telemetry, historical records, and account-related information.
    2. **Role-Based Access Control (RBAC):**
       Access is restricted based on user roles and permissions to ensure data visibility is limited to authorized users only.
    3. **Secure Communication:**
       All data access occurs over encrypted HTTPS (TLS) connections.
    4. **Real-Time & Historical View:**
       Data can be displayed in real time and through historical charts, logs, and reports within the platform.
  - **Data retrieval**

1. **Access to the data directly from the product:**
   data can be requested via email to support@gimasi.de

- Deletion of data:

1. **Account Deletion Request:**
   Customers may request deletion of their account and associated personal data through the platform or by contacting support.
2. **Device Removal:**
   Devices can be removed from the account via the IoT **Cloud** dashboard. Upon removal, data processing related to the device ceases.
3. **GDPR Data Erasure Mechanism:**
   IoT Cloud supports formal data erasure requests in accordance with GDPR Article 17 (“Right to be Forgotten”). Upon verified request:
   a. Personal data is deleted from active systems.
   b. Data is removed from backups according to the defined retention cycle.
   c. A confirmation of deletion is provided
4. **Data Retention Policy:**
   Data is retained only for the period necessary to provide the service or to meet legal obligations.

- For the aforementioned technical means

The following terms of use apply:

- Access to **Service Button Cloud** is restricted to registered and authenticated users.
- Users are responsible for maintaining the confidentiality of login credentials and device authentication keys.
- Devices (e.g., Service Button) must be properly configured and authorized before transmitting data via MQTT.

Gimasi Deutschland GmbH
Lindwurmstr 97a, 80337 München
DE319590118
+49 89 20002118-0
support@gimasi.de

- API access is subject to authentication, authorization, and reasonable rate limits.
- The service may only be used in compliance with applicable laws and the contractual agreement between the parties.

The following service quality applies:

- Target system availability of 99% monthly uptime, excluding scheduled maintenance.
- Telemetry transmission frequency depends on device configuration (interval-based or event-based).
- MQTT communication supports configurable Quality of Service (QoS) levels (0, 1, or 2).
- Scheduled maintenance, where possible, is communicated in advance.

The provider does not expect to use readily available data for its own independent commercial purposes.
The data is used solely for the following purposes:

- Provision and operation of the **Service Button Cloud** platform;
- Processing and visualization of telemetry data from connected devices;
- Ensuring connectivity, system security, and performance monitoring;
- Troubleshooting, diagnostics, and service improvement (in aggregated or anonymized form where applicable);
- Compliance with legal obligations.

The provider does not intend to allow one or more third parties to use readily available data for independent purposes.
Access may be granted only to contracted data processors (e.g., cloud infrastructure providers) acting under binding data processing agreements, or to third parties explicitly designated by the user.

Precise identity of the potential data holder:
Gimasi Deutschland GmbH
Lindwurmstrasse 97a, 80337 München
DE319590118
+49 89 20002118-0
support@gimasi.de

Where applicable, contracted cloud hosting providers act as data processors.

Communication methods that allow the provider to be contacted quickly and communicated with efficiently:

- Email support: support@gimasi.de
- Telephone support +49 89 20002118-0

The user can request that the data be shared with a third party as follows:

- By generating and providing API credentials to the designated third party;
- By exporting data in standard formats (e.g., CSV or JSON);
- By enabling MQTT forwarding or webhook integrations where supported.

The user can stop data sharing as follows:

- By revoking API credentials;
- By disabling integrations within the platform;
- By removing third-party access permissions;
- By submitting a request to **Service Button Cloud** support.

The user has the right to lodge a complaint with the competent authority referred to in Article 37 of the Data Act regarding a breach of any of the provisions of Chapter II of the Data Act.

The data accessible via the connected product or generated during the provision of the related service does not contain trade secrets of the provider.
Proprietary algorithms, firmware logic, and internal platform architecture are not disclosed and remain protected as trade secrets.

Trade secret owner:
Gimasi Deutschland GmbH

The following applies to the contract between the user and the provider:

- **Duration:**
  The contract is valid for the agreed subscription period and renews automatically unless terminated in accordance with the contractual terms.
- **Modalities for early termination of the contract:**
  Either party may terminate the contract with 14 days' written notice, unless otherwise agreed. Immediate termination is possible in case of material breach of contract. Upon termination, access to the service is disabled and data is handled in accordance with the applicable retention and deletion policy.

Gimasi Deutschland GmbH
Lindwurmstr 97a, 80337 München
DE319590118
+49 89 20002118-0
support@gimasi.de