DATA ACT COMPLIANCE DECLARATION

EU Regulation (EU) 2023/2854 – Data Act

1. Product Identification

Product Name	ALPENLUFT SMART Smoke Detector Interlinked
Model / SKU	ISA-10000
ASIN	B0GGSRCFTY
Product Type	Wireless Interlinked Smoke Detector (RF 868 MHz)
Manufacturer	MAJUMU GmbH

2. Device Description

The ISA-10000 is a wireless smoke alarm operating on RF 868 MHz technology, designed for residential fire detection. The device is capable of interlinking with other compatible smoke alarms via radio frequency communication to enable synchronized alarm triggering.

The device may be used in conjunction with the ALPENLUFT Connect mobile application and a manufacturer-operated cloud service for notification and monitoring purposes.

3. Categories of Data Generated

The device generates and processes the following categories of data:

- Alarm events (smoke detection alerts)
- Device status information (normal, fault, test)
- Battery status (including low battery warnings)
- Device identifiers (e.g. serial number, device ID)
- Interlink communication signals between devices

When used with the mobile application and cloud service, additional data may be processed, including:

- User account data (e.g. email address)
- Device binding information
- Event logs stored in the cloud
- Network-related data (e.g. IP address)

4. Data Access by the User

Users have access to data generated by the device through the following means:

- Mobile application interface (real-time status and event notifications)
- Historical event records available within the application
- Data access requests submitted to the manufacturer

Data is provided in a structured, commonly used, and machine-readable format where applicable.

5. Data Sharing and Third-Party Access

Data generated by the device is not shared with third parties for commercial purposes.

However, data may be processed by third-party service providers strictly where necessary for the provision of the service, including:

- Cloud infrastructure providers
- IT and system maintenance service providers

Such processing is carried out under appropriate contractual and data protection safeguards.

6. Manufacturer Access to Data

The manufacturer does not routinely access user-specific data.

Access may occur under limited circumstances, including:

- Technical support requests initiated by the user
- System maintenance and troubleshooting
- Compliance with legal obligations

All access is subject to appropriate technical and organizational safeguards.

7. Personal Data Considerations

The device itself does not directly collect personal data.

However, personal data may be processed in connection with the mobile application and cloud service, in particular:

- User account information
- Network identifiers

Such processing is carried out in accordance with applicable data protection laws, including the General Data Protection Regulation (GDPR).

8. Data Security

Appropriate technical and organizational measures are implemented to protect data, including:

- Secure communication protocols
- Access control mechanisms
- Data minimization principles

9. Effective Date

This declaration is valid as of: April 2026

10. Authorized Representative

Name:	Maurice Müller
Position:	CEO
Company	MAJUMU GmbH
Signature:	