EU Data Information Notice	Information Notice Category	Date updated	Version
Mercury Wireless Fire Alarm System Integration Unit	Connected Product	06/08/2026	01

Manufacturer/Distributor
Biosite – ASSA ABLOY Global Solutions

Introduction

This Information Notice explains what data is generated by the Mercury Wireless Fire Alarm System Integration Unit ("**the Product**") in line with the requirements under Article 3(2) of the EU Data Act.

Product description

This module enables authorized users to receive SMS notifications generated by the fire alarm system, including alarm, fault, and other configured events.

Scope of Data Processing

Generated Data

Data type	Format	Estimated volume	Generation	Data retention
Configuration data; recipient name, recipient telephone number, user-defined notification settings.	JSON	>1 kb per record	Occasional – requires manual input to user	Indefinite – requires manual removal / deletion

Data type	Format	Estimated volume	Generation	Data retention
Event and communication logs, including; Date and time of transmission, message sent status and system event that triggered the notification	Plain text	>1 kb per event	Occasional – data is only logged in the event of a transmission	Temporary – log flushed every two hours

Connectivity and data storage

Connectivity features	Data storage	Data holder
N/A	On device	N/A

Data access and user capabilities

Direct access to data	Indirect access to data	Erasure of data
Data stored on the module can only be accessed by establishing a local physical connection to the device using approved service procedures. Data is not available through a remote interface, cloud service, web portal, or mobile application. Access requires: • Physical access to the equipment; • Appropriate service tools and connection method;	The system owner or operator may authorize suitably qualified service providers to access data directly from the device using local access methods. The manufacturer does not remotely collect, access, or share operational data from the module during normal operation.	The system owner or operator may authorize suitably qualified service providers to access data directly from the device using local access methods for deletion.

Direct access to data	Indirect access to data	Erasure of data
• Authorised access rights under the site owner's security procedures.		

Contact information

Should you have any questions regarding the data generated by the Product, do not hesitate to contact us at dataact.biosite@assaabloy.com.