



Milesight LoRaWAN Gateway - EU Data Act Product Data Disclosure & Applicability Statement

Document Information

Item	Detail
Product Family	Milesight LoRaWAN Gateways
Applicable Models	UG63, UG65, UG67, UG56, EG71, SG50
Document Version	1.0
Date	July 2026
Classification	Customer-Facing
Regulatory Basis	Regulation (EU) 2023/2854 (Data Act), Article 3

1. Introduction

The EU Data Act (Regulation (EU) 2023/2854) establishes harmonised rules on fair access to data, switching of cloud services, and interoperability requirements for connected products in the European Union. It applies from 12 September 2025 across all EU/EEA Member States without the need for national transposition.

This document provides:

1. Pre-contractual transparency disclosures pursuant to Article 3(2) of the Data Act, describing the product data generated by Milesight LoRaWAN gateways and how users can access it.
2. A connected product applicability assessment for the gateway's two operating modes - Packet Forwarder mode and Built-in Network Server (NS) mode - addressing whether the Data Act's design obligations under Article 3(1) apply.
3. A self-declaration of data accessibility measures for the Built-in NS mode, where the gateway may constitute a connected product under the Data Act.

1.1 Relationship with Other Compliance Documents

This document complements the Milesight LoRaWAN Gateway - Privacy & Data Protection Guideline

(<https://resource.milesight.com/milesight/iot/document/milesight-lorawan-gateway-privacy-data-protection-guideline.pdf>), which addresses personal data protection under Regulation (EU) 2016/679. Where this document references data categories, storage, or security measures described in the GDPR Guideline, cross-references are provided.

The Data Act and GDPR are complementary instruments. The Data Act governs access to product data (which may or may not be personal data), while GDPR governs the processing of personal data. In the event of a conflict between the two, GDPR prevails (Data Act, Recital 88).

1.2 Scope

This statement applies to the following Milesight gateway products:

Model	Type	Environment
UG65	8-Channel LoRaWAN Gateway	Indoor
UG67	8-Channel LoRaWAN Gateway	Outdoor (IP67)
UG56	8-Channel LoRaWAN Gateway	Indoor
EG71	Building IoT Gateway (Multi-Protocol)	Indoor

Note: The EG71 supports additional building protocols (BACnet, Modbus, M-Bus, KNX) alongside LoRaWAN. Protocol-specific data is addressed where relevant.

2. Operating Modes

Milesight LoRaWAN gateways support two distinct operating modes. The applicability of the Data Act's connected product obligations differs between them.

Architecture A - Packet Forwarder Mode

In this mode, the gateway receives encrypted LoRaWAN frames from end devices and relays them to an external Network Server. The gateway does not decrypt application payloads, manage LoRaWAN session keys, or decode sensor data.

[End Device] --LoRa RF--> [Gateway] --UDP/TLS--> [External Network Server] --> [Application Server]

Architecture B - Built-in NS Mode

In this mode, the gateway performs full LoRaWAN protocol processing: it manages join procedures, holds network and application session keys, decrypts payloads, decodes data via configured codecs, and makes decoded data available through its Web UI and APIs.

[End Device] --LoRa RF--> [Gateway (built-in NS)] --MQTT/HTTP--> [Application / Node-RED / Python]

3. Article 3(2) Pre-Contractual Transparency Disclosure

Pursuant to Article 3(2) of Regulation (EU) 2023/2854, the following information is provided to the user before the conclusion of a contract for the purchase, lease, or rental of the connected product.

3.1 Product Data Types, Formats, and Estimated Volume

A. LoRaWAN Protocol Data

Data Element	Format	Generated Continuously	Estimated Volume
DevEUI	64-bit hex string (e.g., 24E124138C210001)	No - assigned at device registration	1 entry per end device
JoinEUI / AppEUI	64-bit hex string	No - assigned at device registration	1 entry per end device
DevAddr	32-bit hex string	Yes - assigned at each join procedure	1 entry per active session

LoRa Payload (uplink)	Binary (hex-encoded) or decoded JSON (when codec configured)	Yes - periodic uplink	~200 bytes per uplink per device; typical interval: 10 minutes (6 uplinks/hour)
LoRa Payload (downlink)	Binary (hex-encoded)	On demand - triggered by application or schedule	~50-242 bytes per downlink
RF Metadata (RSSI, SNR, timestamp, channel, gateway ID)	JSON fields	Yes - per uplink event	~100 bytes per uplink

A.2 Network Management Traffic

The gateway generates additional network management traffic during normal operation:

Traffic Type	Protocol	Frequency	Estimated Volume
NTP time synchronization	NTP (UDP)	Every 15 minutes (4/hour)	~48 bytes/packet, ~1.1 KB/hour
ICMP connectivity check	ICMP	Configurable, every 5 minutes (12/hour)	~64 bytes/packet, ~4.5 KB/hour
MQTT keepalive	MQTT PINGREQ/PINGRESP	Not configurable (typical: every 60 seconds)	~2 bytes/packet, ~7.2 KB/hour
MQTT uplink forwarding	MQTT PUBLISH	Per device uplink	Payload (~200 bytes) + MQTT overhead (~30 bytes topic/header), ~230 bytes/message
MQTT downlink	MQTT PUBLISH (subscribe)	On demand	Payload + ~30 bytes overhead

Estimated total network traffic per gateway (8 devices):

Timeframe	Uplink Data (8 devices)	Management Traffic (NTP + ICMP + MQTT keepalive)	Total
Per hour	~18.4 KB	~12.8 KB	~31.2 KB
Per day	~442 KB	~307.2 KB	~749.2 KB
Per month	~13.3 MB	~9 MB	~22.3 MB
Per year	~159 MB	~108 MB	~267 MB

Note: Volumes are estimates based on typical deployment parameters (200 bytes/uplink, 10-minute interval, 8 end devices). Actual volumes depend on the number of connected end devices, reporting frequency, payload size, and MQTT configuration.

B. Device Management Data

Data Element	Format	Generated Continuously	Estimated Volume
Device profiles (codec, activation mode, forwarding rules)	JSON configuration	No - created/modified by admin	~1-5 KB per device profile
Admin credentials	Hashed (bcrypt); not exported	No - set at configuration	Not applicable (not retrievable)
System logs	Plain text / syslog format	Yes - operational events, errors, uplink/downlink counts	Configurable retention; ring buffer (typical: 1-10 MB)
Network configuration (IP, DNS, NTP, firewall rules)	JSON / configuration file	No - set at configuration	~1-10 KB

C. EG71 Additional Data (Multi-Protocol)

Protocol	Data Elements	Format	Generated Continuously
BACnet	Object identifiers, point values (temperature, occupancy, etc.)	JSON	Yes - per polling interval
Modbus	Register values (sensor readings, actuator states)	JSON	Yes - per polling interval
M-Bus	Meter readings (energy, water, heat consumption)	JSON	Yes - per polling interval
KNX	Group addresses, datapoint values	JSON	Yes - per event
I/O	Digital/analog input states, output control values	JSON	Yes - per polling/event

D. User Application Data (Node-RED / Python)

Data Element	Format	Generated Continuously
Application logic (flows, scripts)	JSON (Node-RED) / Python source	No - deployed by user
Application data	User-defined (any format)	Depends entirely on user application design

3.2 Data Storage and Retention

Data Type	Storage Location	Encryption	Retention
Device configuration	Internal flash / Docker volume	Filesystem-level	Until deleted by admin
System logs	Internal flash (ring buffer)	No	Configurable; overwritten on rotation
LoRaWAN session keys	LoRaWAN stack memory	In-memory only	Session duration; not persisted to disk

Firmware images	Internal flash	Signed (integrity verified)	Current + optional backup
Packet history (Packets tab)	Internal flash (rolling buffer)	No	Rolling buffer; size configurable; overwritten
Offline data buffer	Internal flash	No	Auto-retransmitted when connectivity restored; admin-controlled enable/disable
Node-RED flows and data	Internal flash / Docker volume	No	Until deleted by admin
Python application data	Internal flash / Docker volume	No	Until deleted by admin

3.3 Data Access, Retrieval, and Deletion

Users (gateway administrators) can access, retrieve, and delete product data through the following mechanisms:

Mechanism	Access Method	Capabilities
Web UI	HTTPS browser interface	View device list, packet history, system status, logs; export configuration; delete devices; clear logs; factory reset
REST API	HTTPS JSON API	Programmatic access to all device data, packet history, system configuration; CRUD operations
MQTT/HTTP forwarding	Configurable endpoints	Real-time data forwarding to user-specified brokers/endpoints (JSON payload)
Node-RED editor	HTTPS browser interface	Visual flow editor; access to application data; import/export flows
Factory reset	Physical button / Web UI / MDP remote	Erases all locally stored data: device configurations, session keys, packet history, logs, applications, credentials

Data export formats: JSON (machine-readable), plain text (logs), configuration files (import/export).

3.4 Data Holder Identity

Party	Role Under Data Act	Rationale
Milesight (manufacturer)	Product manufacturer	Designs and manufactures the gateway; does not operate it or determine data processing purposes after sale
Customer / Deployer	Data holder	Deploys the gateway, configures data flows, determines which end devices connect, and controls all data access
Network Server Operator	Third-party data recipient (Packet Forwarder mode)	Receives relayed LoRaWAN frames from the gateway

Key point: After deployment, Milesight does not have access to the gateway's product data. The customer (deployer) is the sole data holder and controls all data access, forwarding, and retention.

3.5 Milesight Development Platform (MDP)

The Milesight Development Platform (MDP) is an optional cloud-based remote management and IoT data service. It consists of two components: Auto-Provisioning (enabled by default) and the Milesight Development Platform (disabled by default).

Auto-Provisioning (enabled by default)

On each boot, the gateway attempts to contact an MDP routing server to retrieve configuration profile.

Behaviour	Detail
Trigger	On every boot; also when the feature is manually disabled and re-enabled via the Web UI, or after a factory reset
On success (Profile found)	The gateway downloads the profile via an AWS S3 pre-signed URL. Subsequent boots will NOT re-fetch the profile
On failure (no network)	The gateway continues with local configuration; retries on next boot or next manual enable

On empty response (no config on MDP)	The gateway continues with local configuration; retries on next boot or next manual enable
Delivery mechanism	MDP creates an AWS S3 bucket containing the profile file; the gateway receives a URL and downloads it

Data transmitted during Auto-Provisioning:

Data Element	Direction	Purpose
Gateway serial number / device identifier	Gateway to MDP routing server	Device identification for profile lookup
Profile file (configuration template)	MDP (S3) to Gateway	Initial device configuration
Platform URL	MDP (S3) to Gateway	Address of the MDP platform for subsequent connection

Key point: Auto-Provisioning is a one-time provisioning step. Once the profile is successfully retrieved, it is not fetched again on subsequent boots. The gateway operates with the provisioned configuration until the next factory reset or manual re-enable.

Milesight Development Platform (disabled by default)

When the Milesight Development Platform is enabled (either via the provisioned profile or manually by the gateway administrator), the gateway establishes a persistent connection to the MDP cloud for ongoing remote management.

Step	Mechanism
1. Connect to platform URL	HTTPS connection to the URL obtained via Auto-Provisioning or manual configuration
2. Certificate exchange	The gateway obtains TLS certificates via an encrypted channel for mutual authentication
3. MQTT communication	All subsequent communication uses MQTT over the authenticated TLS channel
4. Configuration delivery	MDP creates an AWS S3 bucket with the configuration file; sends the URL to the gateway via MQTT; the gateway downloads and applies it

Data transmitted to MDP cloud (Gateway to Cloud):

Data Element	Format	Purpose
Gateway serial number	String	Device identification
Firmware version	String	Version tracking
Status metrics (uptime, CPU, memory, connectivity)	JSON via MQTT	Remote monitoring and health checks
Network interface status	JSON via MQTT	Remote diagnostics

Data received from MDP cloud (Cloud to Gateway):

Data Element	Mechanism	Purpose
Configuration updates	S3 URL via MQTT, gateway downloads	Remote configuration management
Firmware update packages	S3 URL via MQTT, gateway downloads	Over-the-air firmware updates
SSH remote access commands	Encrypted MQTT tunnel	Optional remote technical support

Refer to the MDP Privacy Policy (<https://www.milesight.com/legal/development-platform/privacy-policy>) for details on data center locations, international transfers, and retention periods.

MDP Default State and Control

Setting	Description	Default
Auto-Provisioning	One-time Profile/URL fetch on boot	Enabled
Milesight Development Platform	Persistent MQTT connection for remote management	Disabled
SSH remote access	Remote tunnel for technical support	Disabled

Key points:

- Auto-Provisioning is enabled by default but is a one-time operation; it only transmits the device identifier and receives a Profile/URL
- The Milesight Development Platform is disabled by default and requires explicit enablement (via provisioned Profile or manual configuration)
- All configuration delivery uses AWS S3 pre-signed URLs; no configuration data is transmitted directly over the MQTT channel
- The gateway administrator can disable the Milesight Development Platform at any time via the Web UI (Platform page)
- When the Milesight Development Platform is enabled, Milesight acts as a data processor (processing data on behalf of the gateway deployer)
- The gateway deployer (data controller) should execute a Data Processing Agreement (DPA) with Milesight when using the Milesight Development Platform

3.6 Third-Party Data Sharing

No data is transmitted to Milesight or any third party by default. Data forwarding destinations are configured exclusively by the gateway administrator.

Scenario	Data Shared	Recipient	Opt-In Required
Default operation	None	N/A	N/A - no external data transmission
Packet Forwarder mode	Encrypted LoRaWAN frames + RF metadata	User-configured external Network Server	Yes - admin configures NS address
MQTT/HTTP forwarding	Decoded payloads or raw frames (user-configured)	User-configured broker/endpoint	Yes - admin configures destination
Milesight Development Platform (MDP)	Management metadata (serial, firmware, status) and/or sensor data (if configured)	MDP cloud (AWS-hosted)	Yes - explicit admin configuration required
AWS IoT / Azure IoT Hub	User-configured payloads	Cloud provider (user account)	Yes - admin configures cloud connector
MDP Auto-Provisioning	Device identifier (serial); receives Profile + URL	MDP routing server / AWS S3	No - enabled by default; one-time per device

MDP Development Platform	Gateway metadata (serial, firmware, status) via MQTT; receives config via S3 URL	Milesight MDP cloud (AWS- hosted)	Yes - explicit enable (via Profile or manual)
--------------------------------	---	---	---

Complaints: Users have the right to lodge a complaint with the competent national authority regarding the Data Act obligations. Contact information for the relevant authority in each EU Member State is available from the European Commission.

4. Packet Forwarder Mode - Connected Product Exemption Analysis

4.1 Applicable Legal Framework

Article 2(5) of the Data Act defines a "connected product" as:

"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."

However, Article 2(5) also contains an exclusion:

"The definition does not cover items whose primary function is to store, process or transmit data on behalf of any party other than the user."

The European Commission's Data Act FAQ further clarifies this exclusion, explicitly listing servers and routers as examples of products that fall outside the connected product definition.

4.2 Assessment

In Packet Forwarder mode, the Milesight gateway:

- Receives encrypted LoRaWAN RF frames from end devices
- Extracts RF metadata (RSSI, SNR, timestamp) for protocol-level forwarding
- Relays frames as-is (without decryption or decoding) to an external Network Server
- Does not access, decrypt, or decode application-layer payloads
- Does not manage LoRaWAN session keys (NwkSKey, AppSKey)
- Does not store application data beyond transient protocol buffers

The gateway's primary function in this mode is to relay data on behalf of the LoRaWAN Network Server operator - a party other than the gateway user (deployer). This is functionally analogous to a network router, which the EC FAQ explicitly excludes from the connected product definition.

4.3 Conclusion

Based on this self-assessment, Milesight considers that the gateway, when operated exclusively in Packet Forwarder mode, does not constitute a "connected product" within the meaning of Article 2(5) of the Data Act, because its primary function is to transmit data on behalf of a party other than the user (the external Network Server operator).

Accordingly, the design obligations under Article 3(1) of the Data Act do not apply to the gateway in this operating mode.

Disclaimer: This assessment represents Milesight's interpretation of the Data Act based on the available regulatory guidance as of the date of this document. It has not been confirmed by a regulatory authority or notified body. The final determination of whether a product constitutes a "connected product" under the Data Act may be subject to interpretation by national competent authorities or the European Commission. Milesight will update this assessment as regulatory guidance evolves.

5. Built-in NS Mode - Data Act Self-Declaration

5.1 Applicability

In Built-in NS mode, the gateway performs full LoRaWAN protocol processing, including decryption of application payloads, codec-based data decoding, and local data storage and display. In this mode, the gateway's primary function extends beyond data relay to include data generation, processing, and presentation - activities that are not performed on behalf of a third party, but for the benefit of the gateway deployer. Milesight acknowledges that the gateway, when operated in Built-in NS mode, may constitute a "connected product" within the meaning of Article 2(5) of the Data Act. The following self-declaration addresses the applicable obligations.

5.2 Product Data Scope - "Designed to Be Retrievable"

The following table identifies which data categories are designed to be retrievable in Built-in NS mode:

Data Category	Designed to Be Retrievable	Retrieval Mechanism

Device list (DevEUI, JoinEUI, DevAddr, device names)	Yes	Web UI, REST API
Decoded sensor data (via codec)	Yes	Web UI (Packets tab), REST API, MQTT/HTTP forwarding
LoRaWAN RF frames (raw binary)	Yes	Web UI (Packets tab), forwarding
LoRaWAN session keys (NwkSKey, AppSKey)	Yes	Web UI (device detail); editable in ABP mode
RF metadata (RSSI, SNR, timestamp, channel)	Yes	Web UI, REST API, forwarding
Device profiles and configuration	Yes	Web UI, REST API, configuration export
System information (firmware version, uptime, network config)	Yes	Web UI, REST API
System logs	Yes	Web UI (log viewer), syslog forwarding
Node-RED flows and application data	Yes	Node-RED editor, flow import/export
Admin credentials (hashed passwords)	No	Not displayed in Web UI; included in encrypted backup file only

5.3 Data Accessibility Measures

Pursuant to Article 3(1), the gateway is designed and manufactured with the following measures to ensure product data is accessible by default, easily, securely, free of charge, in a comprehensive, structured, commonly used, and machine-readable format:

Requirement (Article 3(1))	Implementation
Accessible by default	Product data is available through the Web UI and REST API immediately upon gateway deployment - no additional software or licensing required

Easily	Web UI provides a graphical interface; REST API provides programmatic access with standard HTTP methods
Securely	All access is protected by HTTPS (TLS 1.2/1.3); admin authentication required; role-based access control (Admin / Viewer)
Free of charge	No licensing fees, subscription, or per-request charges for data access
Comprehensive	All data designed to be retrievable (Section 5.2) is accessible through documented interfaces
Structured	Data is returned in structured JSON format with typed fields
Commonly used	JSON is the standard data interchange format for IoT and web applications
Machine-readable	JSON payloads can be parsed by any standard programming language or integration platform

5.4 Additional Technical and Organizational Measures

Measure	Description
Transport encryption	TLS 1.2/1.3 for all Web UI, API, MQTT, and HTTPS connections
Authentication	Username/password with bcrypt hashing; configurable password complexity
Role-based access	Admin and Viewer roles with differentiated permissions
Firmware integrity	Digitally signed firmware updates; automatic signature verification
LoRaWAN security	AES-128 encryption at network and application layers

Factory reset	Erases all locally stored data (device configs, session keys, packet history, logs, applications, credentials)
Data export	Device configuration export in standard JSON format
ISO 27001	Information security management system certified
Privacy by Design	Data minimisation integrated into product development

5.5 User Rights Under Article 4

For Milesight gateways in Built-in NS mode:

User Right	How It Is Supported
Access product data	Web UI (dashboard, Packets tab, device list) and REST API provide real-time access to all retrievable data
Export / port data	Device list export (CSV); device libraries export (JSON); MQTT/HTTP/BACnet/Modbus forwarding to user-specified endpoints; log export; full gateway backup (encrypted format for restore)
Delete data	Per-device deletion via Web UI/API; packet history clearing; log clearing; factory reset (full erasure)
Restrict processing	Admin can disable specific end devices or disable data forwarding rules

6. Relationship with GDPR

The EU Data Act and GDPR are complementary regulatory instruments:

Dimension	GDPR (EU) 2016/679	Data Act (EU) 2023/2854
Protected interest	Personal data privacy	Fair access to product data
Beneficiary	Data subjects (natural persons)	Users (natural or legal persons)

Key obligation for manufacturers	Privacy by design (Art. 25)	Data accessibility by design (Art. 3(1))
Data scope	Personal data (any information relating to an identified/identifiable natural person)	Product data (data generated by the use of a connected product, designed to be retrievable)

Overlap: Some product data may also constitute personal data (e.g., DevEUI linked to an identifiable individual, admin login credentials, IP addresses). In such cases, both regulations apply simultaneously.

Conflict resolution: Where obligations under the Data Act conflict with GDPR, GDPR prevails (Data Act, Recital 88 and Article 1(3)).

For a comprehensive description of how Milesight gateways handle personal data under GDPR - including roles, data categories, security measures, data subject rights, and international transfers - please refer to the Milesight LoRaWAN Gateway - Privacy & Data Protection Guideline

(<https://resource.milesight.com/milesight/iot/document/milesight-lorawan-gateway-privacy-data-protection-guideline.pdf>).

7. Standards and Certification Status

7.1 Current Status

As of the date of this document, no harmonised standards have been published under the Data Act that would provide a presumption of conformity for connected product obligations (Article 33).

The European Commission issued Standardisation Request M/614 to CEN, CENELEC, and ETSI on 7 July 2025. This mandate will produce:

- 4 European Standards (EN) - two of which are intended for citation in the Official Journal of the EU (OJEU) to provide a presumption of conformity
- 3 Technical Specifications (TS)

These deliverables are being developed by CEN/CENELEC Joint Technical Committee 25 (JTC 25) and ETSI TC DATA. Completion is expected in the 2027-2028 timeframe.

7.2 Milesight's Commitment

Milesight is monitoring the M/614 standardisation process and will:

1. Assess the gateway's compliance against the published harmonised standards once they become available
2. Update this self-declaration to reference applicable standards and any conformity assessment results
3. Implement any required design or documentation changes in subsequent firmware releases

7.3 Existing Certifications

While no Data Act-specific standards exist yet, Milesight gateways hold the following certifications relevant to data protection and cybersecurity:

Certification	Standard	Relevance to Data Act
CE Marking	RED 2014/53/EU	Radio equipment compliance
EN 18031-1:2024	RED-DA Cybersecurity (Network Security)	Technical measures for data access security
EN 18031-2:2024	RED-DA Privacy (Personal Data Protection)	Privacy safeguards overlapping with Data Act data protection
ISO 27001	Information Security Management	Organizational security framework
ISO 9001	Quality Management	Product development and documentation quality

Notified Body: SGS Fimko OY (NB 0598)

Testing Laboratory: SGS-CSTC Standards Technical Services Co., Ltd., Guangzhou Branch

Test reports and Declaration of Conformity (DoC) are available upon request from your Milesight sales representative.

8. Contact and References

Milesight Privacy and Data Protection

- Privacy Policy: <https://www.milesight.com/legal/policy>
- Trust Center: <https://www.milesight.com/company/trust-center>

Data Act Compliance Inquiries

- Email: iot.support@milesight.com
- Address: Building C09, Software Park Phase III, Xiamen 361024, Fujian, China

Related Documents

- Milesight LoRaWAN Gateway - Privacy & Data Protection Guideline (<https://resource.milesight.com/milesight/iot/document/milesight-lorawan-gateway-privacy-data-protection-guideline.pdf>)
- Milesight LoRaWAN Gateway - Datasheets and User Manuals (available from your sales representative)

This document is provided for informational purposes and represents Milesight's self-assessment of the applicability of Regulation (EU) 2023/2854 (Data Act) to its LoRaWAN gateway products. It does not constitute legal advice. The assessment of whether a product constitutes a "connected product" under the Data Act is subject to interpretation by competent regulatory authorities. Customers deploying gateways in the EU/EEA should consult with qualified legal counsel to ensure full compliance with all applicable regulations.