



Milesight LoRaWAN Gateway - Privacy & Data Protection Guideline

Document Information

Item	Detail
Product Family	Milesight LoRaWAN Gateways
Applicable Models	UG63, UG65, UG67, UG56, EG71, SG50
Document Version	1.1
Date	July 2026
Classification	Customer-Facing

1. Introduction

The General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) is the European Union's comprehensive data privacy framework. It governs how personal data is collected, processed, stored, and transferred.

This document describes how Milesight LoRaWAN gateways handle data within the GDPR and CCPA frameworks, clarifies the roles and responsibilities of each party in the data processing chain, and outlines the technical and organizational measures Milesight implements to protect data privacy. Section 12 addresses California Consumer Privacy Act (CCPA) requirements for deployments involving California residents.

1.1 Scope

This guideline 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 handling is addressed where relevant.

1.2 Target Audience

This document is intended for:

- **System integrators** deploying Milesight gateways in EU/EEA jurisdictions
- **End customers** (businesses, facility operators) who operate the gateways
- **Data Protection Officers (DPOs)** assessing compliance of IoT deployments

2. Regulatory Framework

Milesight gateways are subject to the following EU regulatory requirements:

Regulation	Scope	Compliance Status
------------	-------	-------------------

GDPR (EU) 2016/679	Personal data processing	Addressed in this document
CCPA (Cal. Civ. Code 1798.100 et seq.)	California consumer privacy rights	Addressed in Section 12 of this document
RED (EU) 2014/53/EU	Radio equipment essential requirements	Certified
RED Delegated Act (EU) 2022/30, Art. 3.3(e)	Cybersecurity & privacy protection for internet- connected radio equipment	EN 18031 compliant (certificates obtained)
CRA (EU) 2024/2847	Cyber Resilience Act for products with digital elements	Applicable; compliance roadmap in progress (deadline: Dec 2027)
Data Act (EU) 2023/2854	Product data accessibility for connected products	Self-assessment completed; see separate EU Data Act Disclosure document

2.1 RED Cybersecurity Compliance (EN 18031)

All Milesight LoRaWAN gateways have been assessed by **SGS-CSTC Standards Technical Services Co., Ltd.** (Guangzhou) and certified against the harmonised standards under the RED Delegated Act:

Model	EN 18031-1 (Network Security)	EN 18031-2 (Privacy Protection)	EU-Type Examination
UG65 / UG67	GZCS250800052101 (2025-08-13)	GZCS250800052102 (2025-08-13)	RED-3912 Issue 1 (2025-08-14)
UG56	GZCS250800052001 (2025-08-13)	GZCS250800052002 (2025-08-13)	RED-3911 Issue 1 (2025-08-14)
EG71	GZCS251000062701 (2025-12-19)	GZCS251000062702 (2025-12-19)	RED-4209 Issue 1 (2026-02-24, valid until 2031-02-24)

Notified Body: SGS Fimko OY (NB 0598)

All test results: **PASS** — the samples tested comply with the requirements of EN 18031-1:2024 and EN 18031-2:2024.

Note on DoC references: The UG65/UG67 and UG56 Declarations of Conformity currently reference EN 18031-1:2024 for both Article 3.3(d) and Article 3.3(e), as EN 18031-2 had not yet been formally harmonised when those DoCs were issued (August 2025). The EG71 DoC (issued February 2026) references EN 18031-1 for Art. 3.3(d) and EN 18031-2 for Art. 3.3(e). EN 18031-2:2024 testing has been completed for all models. As EN 18031-2 becomes formally harmonised under the RED-DA, the UG-series DoCs will be updated accordingly.

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

3. Roles Under GDPR

GDPR distinguishes three key roles in data processing. Understanding these roles is essential for determining each party's obligations.

3.1 Role Definitions

Role	GDPR Reference	Definition
Data Controller	Art. 4(7)	Determines the purposes and means of personal data processing
Data Processor	Art. 4(8)	Processes personal data on behalf of the controller
Data Subject	Art. 4(1)	The identified or identifiable natural person whose data is processed

3.2 Milesight's Role

The gateway supports two deployment architectures:

Architecture A — Packet Forwarder (external NS):

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

Architecture B — Built-in NS (standalone):

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

Party	Typical Role	Rationale
Milesight (manufacturer)	Product provider	Milesight designs and manufactures the gateway hardware/software but does not operate it or determine data processing purposes after sale
Customer / Deployer	Data Controller	The entity that deploys the gateway determines what end devices connect, which operating mode is used, where data is forwarded, and how it is used
Network Server Operator	Data Processor (or joint Controller)	In Architecture A: the external NS provider. In Architecture B: the deployer themselves (NS runs on the gateway they control)
Application Owner	Data Controller	Determines how decoded sensor/device data is used

Key Point: Milesight, as the hardware manufacturer, does not process end-user data after the product is deployed. The gateway operates entirely under the customer's configuration and control, regardless of which architecture is used.

3.3 Why the Gateway Is Not a "Mere Conduit"

The gateway's data processing role varies by operating mode, but in neither case is it a passive network element:

- **In packet forwarder mode**, the gateway relays encrypted LoRaWAN frames to an external NS. It has access to RF metadata and DevEUI but does not decrypt application payloads. Its processing is limited to protocol-level forwarding.

- **In built-in NS mode**, the gateway performs full LoRaWAN protocol processing: it manages join procedures, holds both network and application session keys (NwkSKey and AppSKey), decrypts application payloads, decodes data via configured codecs, retains a packet history buffer, and makes decoded data available through its Web UI (Packets tab). This constitutes significant "processing" under GDPR Art. 4(2).
- **With Node-RED or Python applications**, the gateway can perform arbitrary user-defined data processing — including storage, transformation, visualization, and integration with external systems.

In all cases, the gateway acts as a **technical processing tool** operated by the Data Controller (the deployer). The deployer is responsible for determining the lawful basis, purpose, and retention policies for all processing performed by the gateway.

4. Data Processed by the Gateway

4.1 Data Categories

The gateway processes the following categories of data during normal operation:

A. LoRaWAN Protocol Data

Data Element	Description	Personal Data?	CCPA PI Category	Retention
DevEUI	Globally unique 64-bit end-	Potentially (can be linked to a person via	Identifiers	In device table until device is removed

	device identifier	device assignment)		
JoinEUI / AppEUI	Application-level identifier for OTAA join	No (identifies the application, not the person)	Not PI	In device table until device is removed
DevAddr	32-bit network address (assigned at join)	No (temporary, network-scoped)	Not PI	Session duration
NwkSKey	Network session key	No (cryptographic material)	Not PI	Session duration; stored in gateway LoRaWAN stack memory
AppSKey	Application session key	No (cryptographic material)	Not PI	Session duration; in built-in NS mode, held by gateway NS stack. In packet forwarder mode, not provisioned to the gateway
LoRa Payload	Application data from end devices	Depends on content	Depends on content (may include Internet/Network Activity)	Packet forwarder mode: transient, forwarded as-is (encrypted), not stored. Built-in NS mode: decrypted and optionally decoded; recent packets retained in rolling buffer (Packets tab) for troubleshooting; data also buffered if offline retransmission is enabled

RF Metadata	RSSI, SNR, timestamp, channel, gateway ID	No (technical measurements)	Not PI	Forwarded with uplink; may appear in local logs and Packets tab
-------------	---	-----------------------------	--------	---

B. Device Management Data

Data Element	Description	Personal Data?	CCPA PI Category	Retention
Device profile	Codec configuration, activation mode, data forwarding rules	No	Not PI	Until deleted by admin
Admin credentials	Web UI login (username, hashed password)	Yes (identifies the administrator)	Identifiers	Until changed or deleted
System logs	Operational events, errors, uplink/downlink counts	Potentially (may contain DevEUI, IP addresses)	Identifiers; Internet/Network Activity	Configurable retention; overwritten on rotation
Network configuration	IP address, DNS, NTP settings	Potentially (IP address may be personal data)	Identifiers; Internet/Network Activity	Until changed

C. EG71 Additional Data (Multi-Protocol)

The EG71 gateway supports additional building protocols. The following data is processed in addition to LoRaWAN data:

Protocol	Data Elements	Personal Data?	CCPA PI Category
----------	---------------	----------------	------------------

BACnet	Object identifiers, point values (temperature, occupancy, etc.)	Potentially (occupancy data may relate to individuals)	Internet/Network Activity; Inferences
Modbus	Register values (sensor readings, actuator states)	Depends on application	Depends on application
M-Bus	Meter readings (energy, water, heat consumption)	Potentially (consumption data may be linked to tenants)	Commercial Information; Internet/Network Activity
KNX	Group addresses, datapoint values (lighting, HVAC control)	Generally no	Not PI
I/O	Digital/analog input states, output control values	Depends on application	Depends on application

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

The gateway includes built-in runtimes for **Node-RED** and **Python**, enabling users to develop custom on-device applications:

Data Element	Description	Personal Data?	CCPA PI Category	Retention
Application logic	User-created Node-RED flows or Python scripts	No (code, not personal data)	Not PI	Until deleted by admin
Application data	Any data processed, stored, or generated by user applications	Entirely depends on user application design	Depends on application	Controlled by user application; erased on factory reset

Note: User-developed applications can access data received by the gateway (including decoded LoRaWAN payloads in built-in NS mode). Any personal data

processing performed by these applications is the responsibility of the Data Controller (the gateway deployer), not Milesight.

4.2 Default Behaviour vs. User-Enabled Features

To provide clarity on the gateway's data handling scope, the following distinguishes between **default behaviour** and **user-enabled capabilities**:

Capability	Default	User-Enabled
Decrypt application payloads (AppSKey)	✗ Not available in packet forwarder mode	✓ Available when built-in NS mode is activated
Decode payloads via codec	✗ Not active	✓ When codec is configured per device
Display decoded data (Packets tab)	Shows raw frames only	✓ Shows decoded values when codec + built-in NS are active
Store data locally (offline buffering)	✗ Disabled	✓ When buffering is enabled in forwarding settings
Run custom applications (Node-RED/Python)	✗ No applications running	✓ When user deploys flows or scripts
Auto-discover end devices	✗ Never (manual addition required)	N/A
Collect biometric / location / behavioural data	✗ No sensors for this	N/A (gateway has no cameras, microphones, or people-tracking capability)
Auto-Provisioning (device ID lookup)	Enabled - sends device serial to MDP routing server on boot; one-time, stops after Profile is retrieved	N/A (always active until Profile obtained)
MDP Development Platform (remote management)	Disabled	Transmits management metadata via MQTT; receives config via S3 URL

MDP Data Platform (sensor data forwarding)	Disabled	When data forwarding destination is configured to MDP; LoRaWAN payloads stored on MDP cloud (AWS)
---	----------	---

5. Data Flow

5.1 Data Path — Packet Forwarder Mode

```
End Device (sensor/actuator)
|
| LoRa RF (encrypted)
v
Milesight Gateway
|-- Receives frame, forwards as-is to external Network Server
|-- Does NOT decrypt application payload
|
| Semtech UDP / Basic Station (TLS)
v
External Network Server (customer-operated or third-party)
|
v
Application Server → End User Dashboard
```

5.1b Data Path — Built-in NS Mode

```
End Device (sensor/actuator)
|
| LoRa RF (encrypted)
v
Milesight Gateway (built-in NS)
|-- LoRaWAN stack: manages join, holds NwkSKey + AppSKey
|-- Decrypts network and application layers
|-- Codec: decodes payload to structured data
|-- Stores in packet history buffer (Packets tab)
```

```
|-- Offline buffer (if enabled): stores for retransmission
|-- Node-RED / Python: user apps can process, store, visualize
|
| MQTT / HTTP / HTTPS (customer-configured endpoint)
v
External Application / Cloud / Dashboard
```

5.2 Local Data Storage

Data Type	Storage Location	Encryption	Access Control
Device configuration	Internal flash / Docker volume	Filesystem-level	Admin authentication required
System logs	Internal flash (ring buffer)	No	Admin authentication required
LoRaWAN session keys	LoRaWAN stack memory	In-memory (persisted for ABP devices)	Visible in Web UI device detail; editable in ABP mode; admin authentication required
Firmware images	Internal flash	Signed (integrity verified)	System-level only
Packet history (Packets tab)	Internal flash (rolling buffer)	No	Admin authentication required
Offline data buffer	Internal flash	No	Auto-retransmitted; admin-controlled enable/disable
Decoded payload cache	Internal flash	No	Admin authentication required (Web UI dashboard)
Node-RED flows & data	Internal flash / Docker volume	No	Admin authentication required (Node-RED editor)
Python application data	Internal flash / Docker volume	No	Admin authentication required

5.3 Data Forwarding Destinations

The gateway forwards data **only** to destinations explicitly configured by the administrator:

- **MQTT broker** — configurable broker address, port, TLS, credentials
- **HTTP/HTTPS endpoint** — configurable URL, headers, authentication
- **AWS IoT / Azure IoT Hub** — via built-in cloud connectors (if applicable)
- **LoRaWAN Network Server** — Semtech packet forwarder protocol (UDP) or Basic Station (TLS)

The gateway transmits only its device identifier (serial number) to the MDP routing server on boot for Auto-Provisioning purposes. This is a one-time lookup that stops once a Profile is retrieved. No other data is sent to Milesight unless the administrator explicitly enables the MDP Development Platform or configures MDP as a data forwarding destination.

- **Auto-Provisioning** (enabled by default): on boot, the gateway sends its serial number to the MDP routing server and retrieves a Profile and platform URL via AWS S3. This is a one-time operation. Once the Profile is obtained, the gateway does not re-fetch it on subsequent boots.
- **MDP Development Platform** (disabled by default): when enabled, the gateway connects to the MDP cloud via HTTPS, exchanges TLS certificates, and communicates via MQTT. Configuration updates are delivered via AWS S3 pre-signed URLs. The gateway transmits management metadata (serial number, firmware version, status metrics) and supports optional SSH-based remote access.

6. Security Measures

Milesight implements the following technical and organizational measures in compliance with GDPR Art. 32 and EN 18031:

6.1 Technical Measures

Measure	Implementation
Transport encryption	TLS 1.2/1.3 for MQTT, HTTPS, and cloud connections
Web UI protection	HTTPS with certificate validation; session timeout
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; MIC integrity check
Network isolation	Configurable firewall rules; VLAN support (model-dependent)
Secure boot	Bootloader integrity verification (model-dependent)
Log integrity	Tamper-evident log rotation; syslog forwarding to external collector

6.2 Organizational Measures

Measure	Description
ISO 27001	Information security management system certified
Privacy by Design	Data minimization and privacy safeguards integrated into product development
Vulnerability management	Regular security assessments and firmware patch releases

Access discipline	Strict role-based access control for Milesight internal systems
Supply chain security	Component sourcing verification and firmware build integrity

7. Data Subject Rights

Under GDPR Chapter III (Art. 12–23), data subjects have the following rights. Since Milesight does not operate deployed gateways, these rights must be facilitated by the **Data Controller** (the gateway deployer/operator):

Right	GDPR Reference	How the Gateway Supports It
Right of access	Art. 15	Admin can export device configuration and logs via Web UI
Right to rectification	Art. 16	Admin can modify device profiles and configuration
Right to erasure	Art. 17	Admin can delete device entries, clear packet history, clear logs, delete Node-RED/Python app data, and factory-reset the gateway
Right to data portability	Art. 20	Device list can be exported as CSV; device catalog can be exported as JSON; full gateway backup uses AES-encrypted format for secure restore
Right to restriction	Art. 18	Admin can disable specific devices or disable data forwarding
Right to object	Art. 21	Admin can remove specific end devices from the gateway

7.1 Factory Reset

All Milesight gateways support a factory reset that erases **all** locally stored data, including:

- Device configurations and LoRaWAN session keys
- Packet history and offline data buffer
- Node-RED flows and Python applications (with their data)
- System logs and admin credentials

This can be initiated via:

- Physical reset button on the device
 - Web UI administration panel
 - Remote management platform (MDP, if enrolled)
-

8. Customer Responsibilities

As the Data Controller, the gateway deployer/operator is responsible for:

1. **Lawful basis** — Establishing and documenting a lawful basis for processing (Art. 6), such as legitimate interest or consent
2. **Transparency** — Providing data subjects with the information required by Art. 13–14 (what data is processed, why, where it goes, retention periods)
3. **Data Processing Agreements** — Executing DPAs with any third-party processors (network server providers, cloud hosting providers, MDP platform if used as a data forwarding destination, etc.) per Art. 28
4. **Data Protection Impact Assessment (DPIA)** — Conducting a DPIA (Art. 35) if the deployment involves high-risk processing (e.g., large-scale monitoring)
5. **Security configuration** — Properly configuring the gateway's security settings (strong passwords, TLS, firewall rules, firmware updates)
6. **Incident response** — Establishing procedures for detecting and reporting personal data breaches (Art. 33–34)
7. **Data retention** — Configuring appropriate log retention periods and data forwarding rules

9. International Data Transfers

Milesight gateways do not transfer data internationally by default. Data forwarding destinations are entirely configured by the customer.

If the customer configures the gateway to forward data to a destination outside the EU/EEA, the customer is responsible for ensuring appropriate safeguards are in place (Art. 44–49), such as:

- EU Standard Contractual Clauses (SCCs)
- Adequacy decisions
- Binding Corporate Rules

Note: If using the optional Milesight Development Platform (MDP), data is processed on AWS cloud infrastructure which operates 4 global data centers. Depending on the selected region, data may be stored outside the EU/EEA. When MDP is configured as a data forwarding destination, this includes LoRaWAN sensor application data. Refer to the MDP Privacy Policy (<https://www.milesight.com/legal/development-platform/privacy-policy>) for details on data center locations, international transfers, and applicable safeguards. The customer (Data Controller) is responsible for ensuring appropriate transfer mechanisms are in place when using MDP.

10. Certifications & Compliance

Certification	Standard	Scope	Report Reference
CE Marking	RED 2014/53/EU	Radio equipment compliance	EU-Type Examination: RED-3911, RED-3912, RED-4209

EN 18031-1:2024	RED-DA Cybersecurity	Network security	See Section 2.1 for per-model report numbers
EN 18031-2:2024	RED-DA Privacy	Personal data protection safeguards	See Section 2.1 for per-model report numbers
ISO 27001	Information security management	Organizational	—
ISO 9001	Quality management	Organizational	—

Notified Body: SGS Fimko OY (NB 0598)

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

Test reports and DoC are available upon request from your Milesight sales representative.

13. Privacy Policy & Contact

Milesight Privacy Policy

For information about how Milesight processes personal data in its capacity as a company (website, customer relationships, cloud services), please refer to:

<https://www.milesight.com/legal/policy>

Milesight Trust Center

For an overview of Milesight's security certifications and compliance framework:

<https://www.milesight.com/company/trust-center>

Data Protection Contact

For GDPR-related inquiries regarding Milesight products:

Email: iot.support@milesight.com

Address: Building C09, Software Park Phase III, Xiamen 361024, Fujian, China

This document is provided for informational purposes and does not constitute legal advice. Customers deploying gateways in the EU/EEA should consult with qualified legal counsel to ensure full compliance with applicable data protection laws.

12. CCPA Compliance

The California Consumer Privacy Act (CCPA, Cal. Civ. Code 1798.100 et seq.), as amended by the California Privacy Rights Act (CPRA), grants California residents specific rights regarding their personal information. This section describes how the Milesight LoRaWAN gateway relates to CCPA requirements.

12.1 Applicability

CCPA applies to for-profit businesses that (a) have gross annual revenue exceeding \$25 million, (b) buy, sell, or share personal information of 100,000 or more consumers/households, or (c) derive 50% or more of annual revenue from selling personal information.

Milesight, as the gateway hardware manufacturer, does not determine the purposes or means of data processing after the product is sold. The entity that deploys and operates the gateway (the Data Controller / deployer) is typically the "business" under CCPA. Milesight's obligations are limited to designing products that enable CCPA-compliant operation.

12.2 CCPA Consumer Rights and Gateway Support

The following table maps CCPA consumer rights to the gateway's technical capabilities. As with GDPR (Section 7), these capabilities are operated by the Data Controller (the deployer), not by Milesight directly.

CCPA Right	CCPA Reference	How the Gateway Supports It

Right to Know	1798.100, 1798.110	Admin can export device configuration, logs, and decoded payload history via Web UI. Data categories and sources are documented in Section 4.
Right to Delete	1798.105	Admin can delete device entries, clear packet history, clear logs, delete Node-RED/Python application data, and perform a full factory reset (Section 7.1).
Right to Opt-Out of Sale	1798.120	Not applicable. Milesight does not sell personal information collected by or through the gateway.
Right to Non-Discrimination	1798.125	Not applicable at the gateway level. The deployer is responsible for ensuring non-discriminatory service.
Right to Correct	1798.106 (CPRA)	Admin can modify device profiles and configuration data.
Right to Limit Use of Sensitive PI	1798.121 (CPRA)	The gateway does not collect sensitive personal information categories (SSN, financial data, precise geolocation, biometrics) by default. Any sensitive PI processing is determined by the deployer's end-device configuration.

12.3 CCPA Data Categories (12-Month Disclosure)

CCPA requires businesses to disclose the categories of personal information collected in the preceding 12 months. The CCPA PI Category column in Section 4.1 maps each gateway data element to the corresponding CCPA category:

- **Identifiers:** DevEUI (when linked to a person), admin usernames, IP addresses
- **Internet/Network Activity:** system logs, network configuration, BACnet/Modbus/M-Bus sensor data
- **Inferences:** occupancy patterns derived from BACnet sensor data
- **Commercial Information:** M-Bus meter readings (when linked to tenants)
- **Not PI:** cryptographic keys, RF metadata, device configuration, application code

12.4 No Sale of Personal Information

Milesight does not sell personal information collected by or through its LoRaWAN gateways. The gateway forwards data only to destinations explicitly configured by the administrator (Section 5.3). No data is transmitted to Milesight unless the administrator explicitly enables the Milesight Development Platform (MDP) or configures MDP as a data forwarding destination.

Accordingly, no "Do Not Sell My Personal Information" link or opt-out mechanism is required at the gateway level.

12.5 Differences from GDPR

While GDPR and CCPA share similar privacy principles, the following differences are relevant to gateway deployments:

- **Legal basis:** GDPR requires a lawful basis before processing (Art. 6); CCPA allows processing by default but grants opt-out rights.
- **Consent model:** GDPR defaults to opt-in; CCPA defaults to opt-out.
- **Sale concept:** CCPA has specific "sale of PI" provisions; GDPR has no equivalent.
- **International transfers:** GDPR restricts cross-border transfers (Art. 44-49); CCPA has no equivalent provision.
- **Scope:** GDPR applies to any processing of EU residents' data; CCPA applies only to businesses meeting specific thresholds.
- The gateway's technical capabilities (Section 7) support both frameworks. The deployer is responsible for determining which obligations apply and configuring the gateway accordingly.