COMET Cloud is a unique platform which allows data acquisition, data storage and data analysis provided by COMET measurement instruments.

Protection of your personal data and your measured values is important for us. All data storage and processing inside COMET Cloud are done according to the highest safety and security standards and guidelines. We use only third-party IT infrastructure that meets such high standards.

This whitepaper contains all important information about COMET Cloud security and your data protection. This document describes COMET Cloud security for COMET IoT Sensors powered by Sigfox, WiFi Sensors, Web Sensors, IoT Wireless data loggers with built-in GSM modem or LTE modem.

If you have any question, feel free to ask us.

What does the data transfer chain look like?

IoT Sensors with output to the Sigfox network

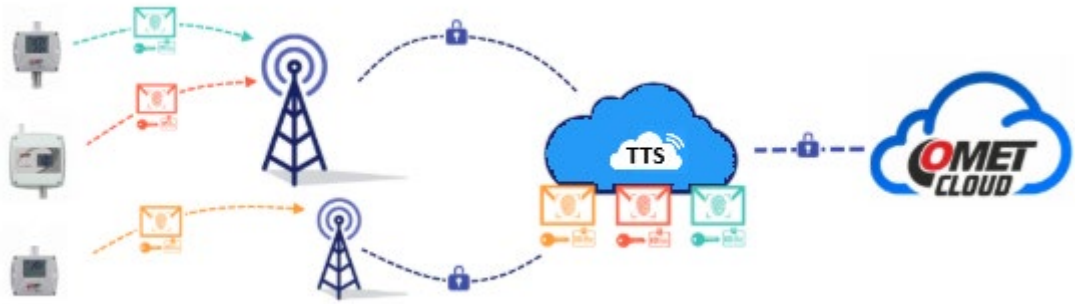
COMET IoT sensors send small data messages at selected intervals containing measurement values and status data of the sensor. These messages are received by Sigfox base stations (BTS). Infrastructure BTS can be used, or a local BTS installed by the end user. Data from BTS are securely transferred to the Sigfox Cloud infrastructure. In this infrastructure, the authenticity of the message is verified. When messages are successfully verified, they are transferred via a secure HTTPS connection to COMET Cloud. Incoming messages are decoded, processed, and stored in COMET Cloud.

The unlicensed 868 MHz band is used as the radio transfer channel. Communication is narrowband with frequency hopping. This allows data transfers to be highly resistant to interference. Due to the frequency hopping feature, it is technically very difficult for a potential attacker to capture a message.

Authenticity of messages is provided by signing of messages. Each IoT Sensor contains a unique secret key. This key is used for signing each transmitted message. The data message also contains a sequence number. This number provides protection against a “replay” type attack.

Due to signature authentication, the origin of the measured data is ensured. The signature prevents an attacker from sending malicious messages.

IoT Sensors with output to the LoRaWAN® network



COMET IoT sensors send small data messages containing measured values and device status data at defined intervals. These messages are received by LoRaWAN® gateways. Gateways can be operated directly by the user, or third-party infrastructure can be used. The gateway transmits the received radio data to the LoRaWAN® Network Server in The Things Stack (TTS) environment via a secure TLS connection. In the TTS environment, the authenticity and integrity of the message are verified. The message is then forwarded to the COMET Cloud via a secure channel for further management.

The unlicensed 868 MHz band is used for radio transmission. Communication is broadband (spread spectrum), which ensures high resistance to interference even in a demanding RF environment.

LoRaWAN® radio transmission uses unique cryptographic keys to encrypt transmitted data and authenticate messages. Furthermore, the transmission provides protection against a "replay attack". Thanks to the use of these mechanisms, IoT sensors ensure a high level of security even for the most demanding applications.

WiFi Sensors

COMET WiFi sensors send data into COMET Cloud at selected intervals via common 2.4 GHz WiFi infrastructure. WiFi sensors are equipped with their own non-volatile memory for samples which cannot be sent in case of WiFi or ISP connectivity outage.

WiFi sensors support state-of-the-art WLAN security standards for WiFi connectivity. In addition to the usual standards such as WEP and WPA/WPA2, WiFi sensors support the latest standards WPA3, WPA2 PMF (protected management frames) and WPA2-EAP. All data communication between WiFi sensors and COMET Cloud is encrypted and transferred via HTTPS protocol. Each communication between WiFi sensor and COMET Cloud is verified by mutual authentication.

Due to the use of well-proven security standards, WiFi sensors provide a high level of protection against a potential attacker. This applies both to the protection of data content and to protection against sending malicious data to COMET Cloud.

Web Sensors (t-line, p-line, h-line)

COMET Web sensors send data into COMET Cloud via Ethernet infrastructure. Measured values are sent via the SOAP protocol transported over HTTP.
The authenticity of data transmission is ensured via a unique entry point for each Web Sensor. This entry point is generated in the COMET Cloud web interface and needs to be inserted into each Web Sensor separately. The authenticity of messages from Web Sensors is ensured when the unique entry point is kept secret.

COMET Cloud is equipped with an automatic incoming data integrity protection system. Data flow from the device is suspended if unusual activity is detected, such as a shorter sending interval than is allowed.

IoT Wireless data loggers with built-in GSM modem or LTE modem

IoT Wireless data loggers with built-in GSM modem or LTE modem use HTTP communication for data transfers via GSM or LTE connection. IoT wireless data loggers are equipped with their own non-volatile memory where samples are stored in case of the GSM or LTE network outage. This memory can be used for optimising data transfers in conjunction with saving energy from the internal battery.

Protection of data content is provided by GSM or LTE network. Incoming messages into COMET Cloud are checked for integrity before processing.

Which data are stored in COMET Cloud?

Apart from measured values from devices, email addresses are stored in COMET Cloud. These addresses are used for purposes of sending alarm notifications from devices or Cloud service information. These emails are not used for marketing purposes of any kind. When mobile application for messaging is used, COMET Cloud stores unique identification for each Android or iOS device. COMET Cloud does not store other personal data. Stored data differs according to device model:

IoT Sensors with output to the Sigfox and LoRaWAN® network

- Measured values
- Device state and alarm states
- Device configuration
- Localisation data

Localisation of Sigfox devices is based on triangulation from BTS. Accuracy of localisation depends on the number of BTS in range and accuracy is not better than street or town district range. The

purpose of localisation data is to display device positions on a map. The position on the map may be modified by end-user if needed.

WiFi Sensors

- Measured values
- Device state and alarm states
- Local IP address

Local IP address of device is transferred from device. The purpose of this IP address is to allow opening the device webpage from COMET Cloud. No other network infrastructure related information is transferred into COMET Cloud from WiFi sensors. External IP addresses of data connections from successfully authenticated WiFi sensors are not logged.

Web Sensors (t-line, p-line, h-line)

- Measured values
- Device state and alarm states

No other data than stated above are provided by Web Sensors. External IP addresses of data connections from successfully authenticated messages are not logged.

IoT Wireless data loggers with built-in GSM modem or LTE modem

- Measured values
- Device state and alarm states

All collected data from IoT Wireless data loggers are stated above. External IP addresses of data connections from successfully authenticated messages are not logged. Localization data from GSM network are not collected.
Data communication between COMET Cloud and web browser may be logged for servicing purposes in order to ensure the operation of the system. This communication is not used to monitor the behaviour of end-users.

Where are my data stored?

COMET Cloud uses the infrastructure of Microsoft Azure Cloud services for data storage and processing. Data centres located in the EU are used for COMET Cloud. The data centres used are certified according to the ISO/IEC 27001:2022 standard.

Are my data safe?

COMET Cloud is designed as a high-availability service. Multiple server clusters are used for the operation of COMET Cloud including offsite backup. The status of COMET Cloud services is continually monitored by an automated system and authorized employees of COMET System s.r.o. Any deviation in service availability is addressed immediately.

When newly arrived measured values are saved, older measured values are not overwritten. Measured values are stored together with timestamps and alarm states. This allows all values to be displayed as a time progression.

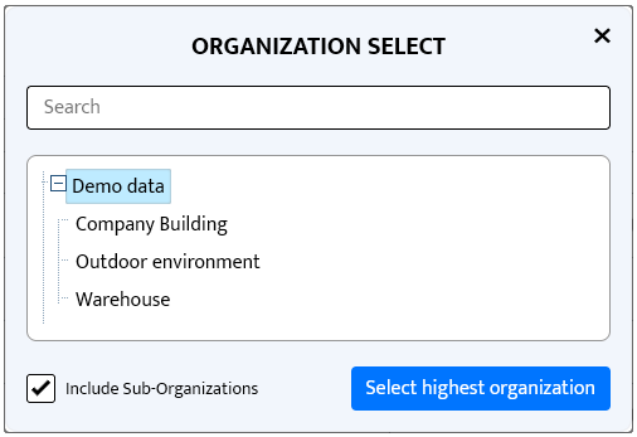
COMET Cloud is provided as a service paid by an annual subscription. Newly purchased IoT Sensors powered by Sigfox are shipped with a one-year subscription. Other models are shipped with a three-month free subscription. Subscription for each device can be prolonged by purchasing credits. When the subscription of a device expires, incoming data from the device are suspended.

Privacy protection of data transfers between COMET Cloud and an internet browser is secured through an HTTPS connection. COMET Cloud uses a trusted certificate issued by DigiCert Inc.

Who has access to my stored data?

Access to data is granted to persons approved by the device owner. Access to data is granted to staff of COMET System s.r.o. who provide technical support for proper function of COMET Cloud. COMET System s.r.o. does not provide access to end-user data to third parties.

COMET Cloud devices and user accounts are organized in a tree structure. A user can view devices in the same or lower branches of the organizational structure. The number of user accounts for each organisation is not limited.



COMET Cloud uses a role-based access control model (Role-Based Access Control – RBAC).

This model enables:

- defining different levels of permissions,
- restricting access to selected devices or organizational units,
- controlling which actions a user may perform (e.g., device configuration, alarm management, user management, or data viewing).

Roles and their associated permissions are defined within the COMET Cloud system. The account owner with administrative privileges determines the assignment of individual roles to specific subordinate users.

The system is designed to ensure that each user has access only to the functions and devices necessary for their work (principle of least privilege).

The scope of roles may be updated as part of system development and always reflects the current version of the service.

What related data protection legislation applies?

End-user data are protected by the data protection law of the Czech Republic. This data protection law is harmonised with EU law.

Which certificates are there?

Data centres are certified according to the ISO/IEC 27001:2022 standard.

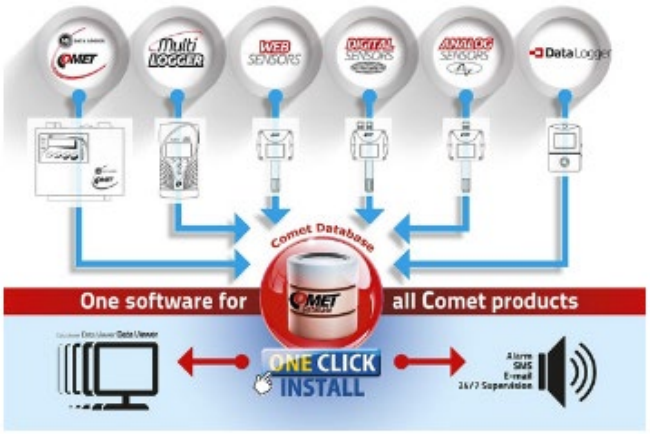
Internal processes at COMET System s.r.o. are certified according to quality management system ISO 9001:2015.

How can devices be safely used within your own network infrastructure?

WiFi sensors and Web Sensors use the end-user's network infrastructure for data transfers into COMET Cloud. The following measures are recommended to secure data transfers from devices to the cloud.
It is recommended to enable device security at final deployment to protect devices from unauthorised access. Please follow IT security advice in the instruction manual for WiFi sensors.

I cannot use 3rd party Cloud services. What option do I have?

For customers who cannot use third-party Cloud services for security reasons or users who want to operate the data acquisition system on their own server infrastructure, the COMET Database solution is available. COMET Database is a solution using Microsoft SQL database server as data storage and Viewer software installed at client stations.



COMET Database solution allows to capture data from multiple types of COMET devices, including Web Sensors, WiFi sensors and IoT Wireless data loggers.