COMET Cloud is unique platform which allows data acquisition, storing data and analysing data provided by the 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 highest safety and security standards and guidelines. We use 3rd party IT infrastructure which meets such high standards only.

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.

How looks data transfer chain?

IoT Sensors with output to the Sigfox network

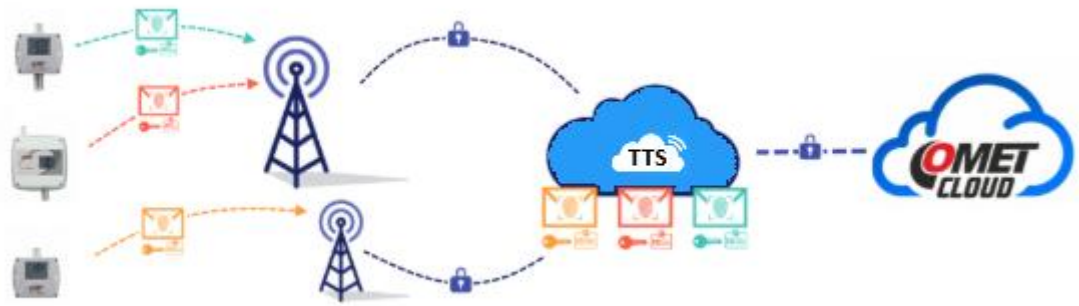
COMET IoT Sensor sensors send at selected interval small data messages containing measurement values and status data of sensor. These messages are received by Sigfox base stations (BTS). It can used infrastructure BTS or local BTS installed by end user. Data from BTS are securely transferred into Sigfox Cloud infrastructure. At this infrastructure is authenticity of message verified. When messages are successfully verified then are transferred via secure HTTPs connection into COMET Cloud. Incoming messages are at COMET Cloud decoded, processed, and stored.

As radio transfer channel is used unlicensed band 868 MHz. Communication is narrowband with frequency hopping. This allows to be data transfers highly resistant to interferences. Due to frequency hopping feature is technically very hard to capture message by potential attacker.

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

Due to authentication against signature is ensured origin of measured data. Signature prevents to send malicious messages by the attacker.

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 is 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 interval via common 2.4 GHz WiFi infrastructure. WiFi sensors are equipped by 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 like a WEP and WPA/WPA2 WiFi sensors supports 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.

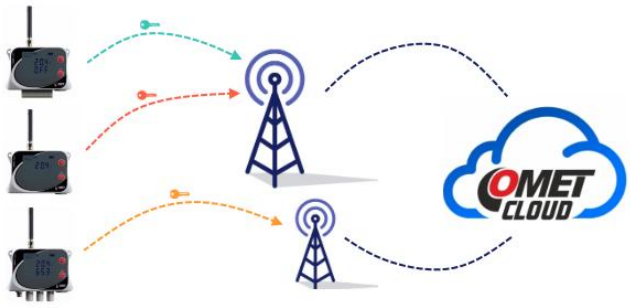
Due to using well proven security standards, WiFi sensors provide high level of protection against potential attacker. Regardless protection of data content or protection against sending malicious data into COMET Cloud.

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

COMET Web sensors send data into COMET Cloud via Ethernet infrastructure. Measured values are sent via SOAP protocol transported by HTTP transfers. Authenticity of data transmission is done via unique entry point for each Web Sensor. This entry point is generated at COMET Cloud web interface and needs to be inserted to each Web Sensor separately. Authenticity of messages from Web sensors is secured when unique entry point is kept at secret.

COMET Cloud is equipped by automatic incoming data integrity protection system. Data flow from device is suspended in case of unusual activity is detected like 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 uses for data transfers HTTP communication via GSM or LTE connection. IoT wireless data loggers are equipped by the 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 internal battery.

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

Which data are stored in COMET Cloud?

Apart measured values from devices are e-mail addresses stored at the COMET Cloud. These addresses are used for purposes of sending alarms warnings 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 counts of BTS in range and accuracy is not better than street or town district range. Purpose of localisation data is showing device positions at map. Position at map may to be rewritten 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. Purpose of this IP address is allowing to open 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 to be logged from servicing purpose order to ensure the operation of the system. This communication is not used to monitoring behaviours of end-users.

Where are my data stored?

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

Are my data safe?

COMET Cloud is designed as high availability service. For operation of COMET Cloud is used multiple server clusters including offsite back-up. Status of COMET Cloud services is continually monitored by automated system and authorized employees of COMET System s.r.o. Any deviation of the services availability is addressed immediately.

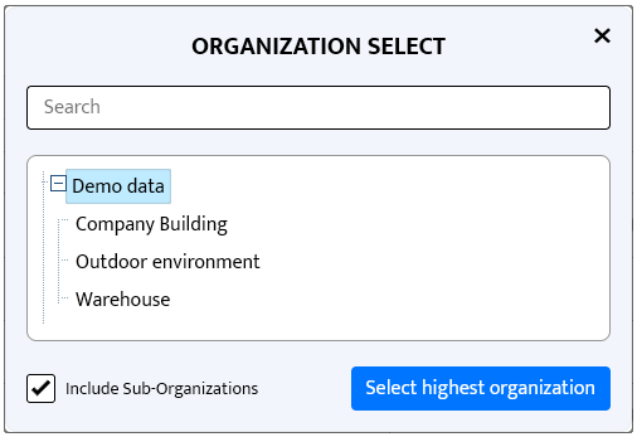
When newly arrived measured values are saved, older measured values are not overwritten. Measured values are stored together with timestamps and alarm states. This allows to show all values as time progression.
COMET Cloud is provided as service paid by annual subscription. Newly purchased IoT Sensors powered by Sigfox are shipped with one year subscription. Other models are shipped with three months free subscription. Subscription for each device can be prolonged by purchasing credits. When subscription of device expire, incoming data from device are suspended.

Privacy protection of data transfers between COMET Cloud and internet browser is secured the HTTPs connection. COMET Cloud uses trusted certificate issued by DigiCert Inc.

Who has access to my stored data?

Access to data have person which were approved by owner of device. Access to data have stuff of COMET System s.r.o. which provides technical support for proper function of COMET Cloud. COMET System s.r.o. does not provide access to end-user's data to 3rd party.

COMET Cloud devices and user accounts are sorted by tree structure. User can view devices at same and lower branches of organisation structure. Number of user accounts for each organisation is not limited.



COMET Cloud have integrated extensive system of access rules. This allows to limit actions possible by each user. Levels of user rights:

- Administrator
- Device administrator
- Alarm administrator
- User
- Guest administrator (for demo purpose)
- Guest
- View by measured places

What is a related data protection legislation?

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

Which certificates are there?

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

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

How safely use devices at own network infrastructure?

WiFi sensors and Web Sensors use end-users network infrastructure for data transfers into COMET Cloud. For securing data transfers from devices into Cloud are following measures recommended. It is recommended to enable device security at final deployment to protect devices from unauthorised access. Please follow IT security advices from instruction manual for WiFi sensors.

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

For customers which cannot use 3rd party Cloud service from the security reasons or users which want to execute data acquisition system at own server infrastructure is here COMET Database solution. 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.