

Data Privacy And Security

- [Data Privacy & Security | Developer Documentation](#)

Data Privacy & Security | Developer Documentation

Data Privacy & Security

Updated: Mar 31, 2026

This page describes how Meta provides Cloud API as a standalone service for businesses to message users at scale via WhatsApp. Meta also offers additional optional services that businesses can choose to use with Cloud API. For example, a business can leverage Meta's AI capabilities to converse with customers via Cloud API. When a business chooses to use these services, different terms could apply. Please consult the applicable documentation for additional details on how Meta processes data for these services.

Message Flows

When a user sends a message to a business that uses Cloud API, the message travels encrypted via WhatsApp between the user and Cloud API. Once the message is received by Cloud API, Cloud API decrypts the message and forwards it to the business. When a business uses Cloud API to send a message to a user, the reverse applies. Upon receiving a message from a business, Cloud API will encrypt the message using the Signal protocol before sending it to the user via WhatsApp. Per the Signal protocol, the user and Cloud API, acting on behalf of the business, negotiate encryption keys and establish a secure communication channel.

WhatsApp acts as the transport channel. WhatsApp protects users by detecting unusual messaging patterns (like a business trying to message all users) and collecting spam reports from users. Cloud API, operated by Meta, acts as the intermediary between WhatsApp and businesses using Cloud API. In other words, those businesses have designated Cloud API to operate on their behalf.

To the extent any data protection or privacy law applicable to you recognizes the concepts of "data processor" or "service provider" as defined within those laws, Meta, in providing Cloud API service, acts as a data processor/service provider on behalf of the business. Cloud API will only use the messages it processes on behalf of and at the instruction of the business, unless otherwise directed. Cloud API will not automatically use WhatsApp messages to inform the ads that a person sees.

For further detail on message flows and encryption, see the [WhatsApp Encryption Overview technical whitepaper](#).

Stored and Collected Data

All data collected, stored, and accessed by Cloud API is controlled and monitored to ensure proper usage and to maintain a high level of privacy.

Business Data. Information about the businesses, including their business phone numbers, business address, etc. is maintained by Meta and the Meta Business Suite or Business Manager product, and is subject to the terms of service provided by Meta.

Message Data. Messages have a maximum retention period of 30 days in order to provide the base features and functionality of the Cloud API service; for example, retransmissions.

User Data. Identifiers are used as sources or destinations of individual messages; as such they are deleted within 30 days of the last status update (sent, delivered, read) of a message, unless otherwise directed.

For a more detailed resource on Cloud API's storage and processing of data, see the [Meta Business Messaging Compliance Center](#), which includes Cloud API's certifications and compliance documentation.

FAQs

Does Meta use the WhatsApp messages that are shared with it by a business for advertising?

Cloud API will not automatically use WhatsApp messages to inform the ads that a person sees. However, as is always the case, businesses can use messages they receive for their own marketing purposes, which may include advertising on Facebook or other channels, like email or TV.

Where are the servers for Cloud API?

Cloud API processes messages on servers in [Meta data centers](#). If a business opts to use Cloud API Local Storage, message data is stored in data centers located in another [designated country](#).

Is the Cloud API end-to-end encrypted? What is the encryption model?

See [Cloud API Overview, Encryption](#).

What happens to message data at rest? How long is it stored?

Cloud API messages at rest are encrypted. Messages have a maximum retention period of 30 days in order to provide the base features and functionality of the Cloud API service; for example, retransmissions.

Does Meta have access to encryption keys?

In order to send and receive messages through Cloud API, Cloud API manages the encryption/decryption keys on behalf of the business. For more detail, see the [WhatsApp Encryption Overview technical whitepaper](#).

What is the security model? Which certifications does the Cloud API have?

We have obtained SOC 2 Type II and ISO 27001 reports. Please visit our [Meta Business Messaging Compliance Center](#) to learn more.

How does Cloud API comply with regional data protection laws (such as GDPR, LGPD, and PDPB)?

Meta takes data protection and people's privacy very seriously and we comply with applicable legal, industry, and regulatory requirements governing data protection, as well as industry best practices. Cloud API customers must meet their own obligations under data protection laws, such as the General Data Protection Regulation (GDPR). Please visit our [Meta Business Messaging Compliance Center](#) to learn more.

What does Meta and WhatsApp do to make sure the transfer of data from the E.U. and/or the UK to the US is compliant?

Meta and WhatsApp rely on appropriate GDPR-compliant transfer mechanisms when it transfers data from the E.U. and/or the UK to the US.

See the following legal terms for additional information:

For all customers, see the [Meta Hosting Terms for Cloud API](#). For customers in the European Region, see the [WhatsApp Business Data Transfer Addendum](#). For customers in the UK, see the [WhatsApp Business UK Data Transfer Addendum](#).

See the applicable [WhatsApp Business Data Processing Terms](#) or [Meta Hosting Terms for Cloud API](#) for an applicable list of sub-processors.

We will ensure that our businesses and partners can continue to enjoy business solutions while keeping their data safe and secure.