The world's leading businesses trust Hubtype to safeguard their customer communications at the enterprise level

Through our dedication to information security, rigorous testing, and strict adherence to global privacy standards, our partners gain the confidence they need to serve customers on messaging at scale.
We are ISO27001 certified as of July 4th, 2023.

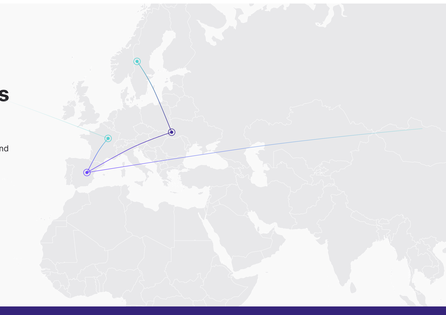
By partnering with Hubtype - a GDPR-compliant service provider - our clients save time, limit their exposure to data breaches, and avoid regulatory penalties.

Our commitment to information security is global

All Hubtype products align with European, Canadian, and US privacy standards. We're ISO27001 certified and conduct an annual security audit that covers GDPR requirements and general security, privacy, and data practices.

Official ISO27001 Certification Links

> English Version
> Spanish Version



What is the purpose of GDPR?

The General Data Protection Regulation (GDPR) has enhanced the privacy laws of European consumers to give them more control over their digital personal data. The EU regulation has created a framework of privacy rules that apply uniformly across the EU and can be legally enforced in every member state.

GDPR requires companies to deliver improved security standards, breach notification requirements, and gives more rights to consumers to access their data. Consumers have the right to 'data portability', which allows them to obtain a copy of their data, and have the 'right to be forgotten', which allows consumers to have their data deleted.

How Hubtype meets GDPR obligations

As a third-party service that communicates and stores personal data on behalf of your company, Hubtype is considered a "data processor." Data processors must be GDPR compliant.

Below is a simplified version of Article 28 of the GDPR, which outlines the obligations of data processors. We've also summarized how Hubtype meets these standards.

To remain GDPR compliant, data processors must	How Hubtype meets these GDPR obligations
Only act on your behalf as the controller's documented instructions.	Huptype will only process personal data in order to provide the services in accordance with our contractual agreement.
Impose confidentiality obligations on all personnel who process the relevant data.	Privacy by Design is a core part of our software development process. Everyone with access to personal data, from the engineering team to the CEO, is trained on Privacy by Design, and is under appropriate obligations of confidentiality.
Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the personal data that it processes.	Among other measures, Hubtype encrypts all customer data, both in transit and at rest. Our servers are encrypted via HTTPS and Transport Layer Security (TLS) industry best-practices.
Abide by the rules regarding appointment of sub-processors.	We hold our third-party service providers to the highest standards. We sign with them a DPA (Data Processing Agreement), where we impose the same data protection obligations as set out in our contract with you. In case of data transfers to third countries, we use EU Standard Contractual Clauses/ Model Clauses with all third parties who process personal data.
Implement technical and organizational measures to assist the controller in complying with the rights of data subjects.	Our platform includes features that help our customers easily respond to an individual's request for access, correction, erasure, restriction, and portability.
Assist the controller in obtaining approval from DPAs (Data Processing Agreements) where required.	We clearly outline our commitments in our Privacy Policy, Privacy Statement for Service Data, and our Data Processing Agreement (DPA). This makes it easy to understand the ways we both follow industry best practices and exceed the minimum for legal compliance.
At the controller's election, either return or destroy the personal data at the end of the relationship (except as required by EU or Member State law).	Our platform makes it easy for you, as the controller, to delete collected data at any time, not just at the end of the relationship.
Provide you with all information necessary to demonstrate compliance with the GDPR.	This report is available upon request and subject to NDA.

We help you be GDPR compliant

Because your bots have to be GDPR compliant too, we give you the necessary tools to comply with; allowing your customers to either delete their data whenever they want or to not store it at all.

Penetration tests

We regularly conduct penetration tests to ensure enterprise-level security. These tests are authorized security attacks, generally performed by an external company, used to expose vulnerabilities.

Confidentiality agreements

All contractors, consultants and new hires are required to sign non-disclosure and confidentiality agreements. These prohibit the disclosure of information such as client lists, technical structures, and more.

Incident response plan

In the case that a data breach has been discovered, Hubtype's incident response plan is compliant with Article 33 of the GDPR. Within 72 hours, all necessary parties will receive information pertaining to the nature of the personal data breach. This includes, where possible, the categories and the approximate number of data subjects concerned and the categories and the approximate number of personal data records concerned.

If a data breach is detected, Hubtype's incident response plan is compliant with Article 33 of the GDPR. To summarize, within 72 hours all necessary parties will be notified about the extent and nature of the data breach.