

botario & Data Protection:

Secure AI-Powered Conversations, Built for Trust.

botario empowers enterprises to deliver intelligent, automated customer interactions through AI-driven Voice and Chatbots. As a platform operating in complex data environments, we put **data protection and compliance at the core** of our architecture—whether you run botario in the cloud, hybrid, or fully on-premises.

Data Storage & Retention

Chat and voice data are stored on botario's German-hosted platform for 30 days by default, then automatically deleted. Each chat has a session ID, and audio is temporarily cached for transcription. Custom retention periods and manual deletions are available on request.



Encryption & Data Transmission

Data is encrypted in transit using **TLS/HTTPS**, ensuring secure communication between botario and external systems. While stored on the platform, data is also encrypted at rest. For processing by Large Language Models (LLMs), data must be decrypted beforehand, as LLMs cannot operate on encrypted inputs. This decryption only happens during model interaction, not during transmission or storage.

Third-Party Services & Responsibilities

botario supports both open-source LLMs hosted in certified German data centers and LLM/TTS services via Azure. All data is encrypted during transmission, and processing follows strict GDPR-compliant safeguards. Customers using their own Azure instances are responsible for the necessary data processing agreements. In this case, botario does not connect to these services unless explicitly configured by the customer.

LLM Integration & Data Flows



botario supports multiple AI deployment models, giving customers full flexibility in how they integrate language models while maintaining full visibility and control over their data.

Three Common Scenarios:

- 01 botario-hosted open-source LLMs run on EU servers (Germany)**, fully managed by botario. All data stays in the EU, with no third-country transfer—ideal for customers seeking full control without external vendors.
- 02 Customers can connect their own Azure OpenAI instance via secure API.** While data stays in EU data centers, the U.S. ownership of Microsoft qualifies it as a third-country transfer. Customers must manage the DPA with Microsoft.
- 03 botario and the LLM can be deployed entirely on-premises, keeping all data within the customer's infrastructure.** botario only accesses data if explicitly granted, offering maximum control for regulated industries.

Let's Talk Data Protection

Need to tailor botario to your compliance environment?
Our team is ready to help.

www.nffon.com

