

Soniox GDPR & Data Protection Overview

Overview

Soniox provides a real-time and asynchronous speech-to-text, text-to-speech, and speech intelligence platform that transcribes and translates spoken audio and generates speech from text across 60+ languages with low latency and high accuracy.

Soniox is committed to protecting personal data and complying with the EU General Data Protection Regulation (GDPR) and other applicable data protection laws. Soniox implements technical and organizational measures designed to safeguard personal data processed through the Soniox platform.

This document provides an overview of Soniox's data protection practices and how they support customers in meeting their GDPR obligations.

Roles and Responsibilities

Under GDPR, Soniox generally acts as a data processor, while the customer acts as the data controller.

- Customer (Data Controller) determines the purposes and means of processing personal data.
- Soniox (Data Processor) processes data on behalf of the customer to provide speech-to-text, text-to-speech, and speech intelligence services.

Soniox processes customer data only in accordance with the customer's instructions and the applicable Data Processing Agreement (DPA).

Categories of Data Processed

Depending on how customers use the Soniox platform, the following types of data may be processed:

- Audio submitted for transcription or translation
- Text submitted for speech generation
- Transcripts generated from submitted audio
- Audio generated from submitted text
- Metadata associated with API requests
- Account and service usage information

Customers control the data they submit to the Soniox platform and are responsible for ensuring they have a lawful basis for processing personal data.

Data Processing Principles

Soniox processes data according to core data protection principles including:

- Purpose limitation: data is processed only to provide the requested services
- Data minimization: only data necessary for service delivery is processed
- Integrity and confidentiality: data is protected using appropriate security measures
- Transparency: customers maintain visibility and control over their data usage

Data Security

Soniox maintains a comprehensive information security program designed to protect customer data.

Security measures include:

- Encryption in transit using TLS
- Access controls based on least privilege
- Authentication and authorization controls
- Logging and monitoring of system activity
- Secure software development practices

Infrastructure is hosted with leading cloud providers including AWS, Google Cloud, and Oracle Cloud Infrastructure, which maintain robust physical and environmental security controls.

Data Retention

Soniox services process audio and text to generate transcripts, generated audio, and related outputs based on customer requests.

Key principles of Soniox data handling include:

- Audio is processed transiently during transcription and translation.
- Text is processed transiently during speech generation.
- Soniox does not store audio or text by default.
- Transcripts, generated audio, and other derived outputs may be stored depending on customer configuration.
- Customers control the retention and management of their data.

International Data Transfers

Soniox may process data using infrastructure located in multiple regions, including the United States, European Union, and Japan, depending on the deployment selected by the customer.

Where personal data is transferred outside the European Economic Area (EEA), Soniox implements appropriate safeguards, including Standard Contractual Clauses (SCCs) where applicable.

Customers may choose regional deployments to support their data residency requirements.

Subprocessors

Soniox may use trusted third-party service providers to support delivery of the platform (for example, cloud infrastructure providers).

All subprocessors are subject to contractual data protection obligations.

A current list of Soniox subprocessors is available through the Soniox Console.

Data Subject Rights

Under GDPR, individuals have rights regarding their personal data, including:

- Right of access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to object to processing

As a data processor, Soniox assists customers in responding to data subject requests in accordance with the Data Processing Agreement.

Data Processing Agreement (DPA)

Soniox offers a Data Processing Agreement (DPA) that governs the processing of personal data under GDPR.

The DPA defines:

- Data protection obligations
- Security measures
- Subprocessor management
- International data transfer mechanisms

Customers can review and execute the DPA through the Soniox Console.

Security Program

Soniox maintains a comprehensive security and privacy program aligned with recognized industry standards.

The Soniox security program includes independent certifications such as:

- SOC 2 Type II
- ISO/IEC 27001

Additional compliance documentation is available through the Soniox Console.

Contact

For privacy or data protection inquiries, please contact:

Soniox Security & Privacy Team
security@soniox.com