Omilia
Conversational Intelligence

Voice Biometric Data Policy

Public retention and destruction policy for voice biometric identifiers

Purpose of This Policy

Omilia's Voice Biometric Authentication functionality, where enabled by a customer, processes elements of an individual's voice to create a derived biometric template (a "voiceprint") used for speaker identification, verification, authentication, fraud prevention, and related security purposes. This policy sets out, in publicly available form, Omilia's approach to the collection, retention, and destruction of voice biometric identifiers, consistent with the requirements of biometric privacy laws including the Illinois Biometric Information Privacy Act (BIPA) and comparable state and international laws.

What We Collect

- Voice biometric templates (voiceprints), being unique mathematical representations derived from an individual's vocal characteristics such as pitch, tone, cadence, and spectral features.
- Enrollment and verification voice samples used to generate and match voiceprints.
- Related authentication metadata, including liveness detection outputs, voice activity detection signals, and speaker segmentation data.

Voice biometric data is only collected and processed where Omilia's customer has expressly enabled Voice Biometric Authentication for its deployment of the Omilia Cloud Platform (OCP).

Purpose of Processing

Omilia processes voice biometric data solely to support speaker enrollment, verification, re-enrollment, liveness detection, and fraud prevention functionality authorized by the customer that has enabled this feature. Omilia does not use voice biometric data for any purpose unrelated to providing this functionality, and does not sell, license, or otherwise disclose voice biometric identifiers for commercial purposes unrelated to the Services.

Who Is Responsible for Consent

Omilia acts as a data processor with respect to voice biometric data processed on behalf of its customers. Omilia's customer, as data controller, is responsible for determining the lawful basis for collecting and processing voice biometric data for its own use case, providing any required notices to individuals, and obtaining any required consents or authorizations under applicable law prior to enabling this functionality.

Retention and Destruction

Voice biometric data is retained only for as long as necessary to fulfil the authorized purpose described above, and in any event Omilia will not retain voice biometric identifiers or voiceprints for longer than the earlier of: (a) the point at which the initial purpose for collecting the data has been satisfied, or (b) three (3) years from the individual's last interaction with the relevant OCP deployment, unless a longer retention period is required by applicable law.

Specific retention periods for a given deployment may be configured within these limits under the terms of the governing customer agreement and its associated Data Processing Addendum (DPA). Upon expiry of the applicable retention period, voice biometric identifiers are securely deleted or rendered irrecoverable in accordance with Omilia's standard data destruction procedures.

Security Safeguards

Voice biometric data is protected using the technical and organizational measures Omilia applies to Customer Personal Data generally, including encryption in transit and at rest, role-based access controls, and access logging. Further detail on these measures is available to customers under the applicable DPA.

Further Information

This policy is a public summary. The complete contractual terms governing Omilia's processing of voice biometric data, including deployment-specific retention configuration and the allocation of responsibilities between Omilia and its customers, are set out in Omilia's Data Processing Addendum (DPA), available to customers and prospects under NDA via the Trust Center.

For questions about this policy, contact corporate-grc@omilia.com.