Biometric Data Retention and Destruction Policy

Version 2026-11-14-draft - published 2026-11-14

This policy explains how [CLIENTOR LEGAL ENTITY] (EzTechTonic), doing business as Clientor.ai and C2R ("we", "us"), collects, keeps and destroys voice recordings and the voice models made from them, which some laws treat as biometric identifiers or biometric information. It is our publicly available retention schedule and destruction guidelines, and it forms part of our Privacy Policy (clientor.ai/legal/privacy).

1. What this policy covers

"Voice Data" means (a) a recording of a person's voice made so that we can create a voice copy, and (b) the voice model derived from it that lets our voice engine speak in a similar voice. We collect Voice Data in the "Use my voice" step of the c2r.ai demo and in Voice Studio in the C2R.ai (Clientor) platform (Business plan and above). We do not collect fingerprints, face geometry, retina or iris scans, or any other biometric data.

2. Consent before collection

We collect Voice Data only after the person whose voice it is has been told in writing what we collect, why and for how long, and has given explicit written consent: an unchecked consent box, followed by a script whose first sentence is a spoken consent. Only a person's own voice may be cloned; no one may record, upload or clone another person's voice. In the platform, the customer must make sure that each person whose voice is cloned in its workspace gives that consent personally (Terms of Service and Acceptable Use Policy).

3. How Voice Data is used

Voice Data is used only to play the demo in the person's voice (sample clips and, on request, one demo call to the number the person entered) and to let the customer's AI agents speak in that voice. It is never used to identify or verify anyone, to infer characteristics about anyone, for marketing, or to train general-purpose AI models. Calls made in a cloned voice are still AI calls and carry the AI disclosure.

4. Who receives Voice Data

We never sell, lease, trade or otherwise profit from Voice Data. We disclose it only to our voice-engine subprocessor (clientor.ai/legal/subprocessors), under a written contract that limits its use to providing the service to us and requires deletion when we delete; when a law, subpoena or court order requires it; or with the person's consent.

5. Retention schedule

We keep Voice Data only until the purpose for collecting it is satisfied, and in any case no longer than 3 years after the person's last interaction with us:

- Demo recording, demo voice copy and demo clips: deleted within 24 hours of recording, unless the visitor signs up and keeps the demo agent.

- Voice kept from a demo: moves to the new workspace's Voice Studio and follows the platform rule below.

- Platform voices (Voice Studio): until the customer deletes the voice, the person withdraws consent, or the account is closed; and in any case no later than 3 years after the voice was last used or the person last interacted with us, whichever comes first.

- Backups: roll off within 35 days after deletion from production systems.

- Consent records (wording, version, time, IP address, browser; they contain no Voice Data): kept as our Privacy Policy describes for consent records, to prove consent.

6. Destruction

When a retention period ends, a voice is deleted in Voice Studio, consent is withdrawn or an account is closed, we delete the recording and the voice model from our storage and ask our voice engine to delete its copy, promptly and in any case within 30 days. Automated jobs carry out the 24-hour demo deletion. Deletion is logged by identifier only.

7. Security

We store, transmit and protect Voice Data with at least the same care as our other confidential and sensitive information: encryption in transit, recordings kept outside our databases in storage encrypted by the storage provider, and access limited to the systems and staff that need it.

8. Your choices

You can delete a platform voice at any time in Voice Studio, or ask us to delete any Voice Data, including a demo voice, by emailing [PRIVACY EMAIL] or using clientor.ai/legal/data-deletion. Declining or withdrawing consent never affects the rest of the demo or the platform; agents can use a standard voice instead.

9. Laws and changes

This policy is designed to meet the Illinois Biometric Information Privacy Act (740 ILCS 14), the Texas Capture or Use of Biometric Identifier Act (Tex. Bus. & Com. Code § 503.001), Washington's biometric identifier law (RCW 19.375) and similar laws. We will post any change here with a new version. Questions: [PRIVACY EMAIL].