

Biometric Data Privacy

Effective Date: May 30, 2026

Avtar Biometric Information Privacy Notice and Consent

1. Introduction

Avtar is an independent platform for creating a personalized AI assistant ("Avtar Personal AI Assistant") using images and voice.

This Biometric Privacy Notice and Consent describes how Avtar Group Inc. ("Avtar," "our," "we," "us") collects, uses, discloses, secures, retains and otherwise processes biometric information, including through third-party service providers acting on our behalf, when you use our services, including our retention schedule and guidelines for destroying biometric information. This Notice is intended to satisfy applicable United States biometric privacy and data protection laws, including but not limited to the Illinois Biometric Information Privacy Act (BIPA), the Texas Capture or Use of Biometric Identifier Act (CUBI), the Washington Biometric Identifiers Law, and similar state laws.

Please read this Biometric Information Privacy Notice and Consent carefully and ensure that you understand it.

By uploading an image, video or audio to the Avtar App, you consent to our collection, use, disclosure, retention and other processing of your biometric information as described in this Notice, including processing conducted by our service providers.

2. What is Biometric Information?

When we refer to "biometric information," we mean information generated by measurements of your physical, behavioral, or biological characteristics that are used to identify you. Information like eye, hand, or face scans, fingerprints, or voiceprints may be considered biometric information if they are being used to identify you by technical means. As used in this Notice, "biometric information" includes "biometric identifier," which means a voiceprint, or scan of face geometry derived from images, video or audio.

3. What Biometric Information Do We Collect and how is it processed?

To create your Avatar Personal AI Assistant, we need to scan and analyze images, video and/or audio that you upload. As a result of this processing, Avatar and our service providers acting on our behalf may collect, generate, process, and store biometric identifiers and biometric information such as face and voice geometry as a result. We use your photo and voice information to provide and improve our products and services (including to train our AI models that power our services).

Biometric processing may be performed by a service provider whose name, location, and specific role are as follows:

- Service face provider name: LemonSlice
- Service provider location(s): 2108 North Street, Suite N, Sacramento, CA 95816
- Description of biometric processing performed: Facial Structure Analysis, it scans your features to understand how your face is shaped and how it moves. Lip Sync and expression synthesis, uses neural models to sync mouth movements with either a text script or a voice recording.
- Service voice provider name: Cartesia AI, Inc.
- Service provider location(s): 1766 18th Street, Suite 1200 San Francisco, CA 94107
- Description of biometric processing performed: Instant Voice Cloning -
- Cartesia Sonic model architecture is used to provide high-fidelity, real-time voice cloning. To create a digital voice persona, the system performs an acoustic feature extraction on a brief audio sample (typically 5–15 seconds) provided by the user to analyze unique vocal markers such as pitch, resonance, and tempo. These characteristics are then processed via vectorization, a method that converts biometric vocal traits into a Voice Vector (or mathematical embedding). This vector serves as a non-human-readable digital blueprint, allowing the AI to synthesize entirely new speech that mirrors the user's vocal identity without storing or "playing back" the original raw audio recordings.

Such service providers are authorized to process biometric information solely to provide services to Avatar and are contractually required to protect the information, keep it confidential, and not use it for its own independent purposes.

Avatar uses biometric information to provide, maintain, and improve its products and services, including generating Avatar Personal AI Assistants, improving system performance, training and refining AI models (to the extent permitted by law), verifying user identity, detecting and preventing fraud, and complying with legal obligations.

4. How Do We Disclose Biometric Information?

We only disclose biometric information as described in this Biometric Information Privacy Notice. We do not sell, lease, trade or otherwise disclose your biometric information for profit. However, we may disclose your biometric information to limited service providers and other vendors who help us provide our products and services.

5. Security and Retention

We store, transmit, and protect your biometric information using a reasonable standard of care that is at least as protective as the way we store, transmit, and protect other confidential information. Notwithstanding any security measures that we take, it is important to remember that the transmission of data via the Internet may not be completely secure, and we cannot guarantee that the collection, transmission and storage of data will always be secure.

We retain your biometric information as long as necessary to fulfill the purposes described in Notice, or until the earlier of:

- The initial purpose for collecting or obtaining biometric information has been satisfied; or
- **Active Accounts:** To provide and improve our services, we retain your facial data, interaction history, and generated outputs for as long as your account remains active.
- **Account Deletion:** If you delete your account, we purge your personal and biometric data from our active systems. While this process is typically immediate, please allow up to 30 days for data to be fully removed from all backups and security archives.
- **System Logs:** For security and troubleshooting, we store technical logs for a maximum of 30 days, after which they are automatically and permanently deleted.

Unless a shorter retention period is required by applicable law, biometric information will be permanently destroyed at the end of the applicable retention period or upon a verified request for deletion, using commercially reasonable methods designed to prevent reconstruction or retrieval.

6. Your Rights and Consent

You have the right to receive information about Avtar's biometric data practices, to request deletion of your biometric information, and to withdraw your consent, subject to applicable law. Withdrawal of consent may impact your ability to use certain Avtar services.

For any questions regarding your biometric information, or to withdraw your consent, please contact us by email at info@Avtargroup.ai. Otherwise, for more information about how we process personal information, as well as your rights and choices regarding our data practices, please review our [Privacy Policy](#).