ForeverFrom – Privacy Policy

Effective Date: **December 9th, 2025**

At ForeverFrom, we believe that a life worth living is a life worth remembering. Our mission is not only to preserve memories and legacies but also to protect the dignity, authenticity, and trust that comes with sharing your story. We understand that when you entrust us with your memories, your voice, and your personal data, you are giving us profound responsibility.

This Privacy Policy explains how we collect, use, share, and safeguard your information when you use our services, software, websites, applications, and platforms (collectively, the "Services"). It works in tandem with our Terms of Use, which outline the rules for accessing and using our Services.

By using ForeverFrom, you agree to this Privacy Policy. If you do not agree, you should not use our Services.

1. Information We Collect

We collect different types of information to provide and improve the Services:

(a) Information You Provide

(b) Memories and Stories: Voice recordings, text entries, photos, videos, reflections, and other personal content.

(c) Biometric Data (with explicit consent):

- Current Biometric Features: ForeverFrom collects biometric identifiers limited to the features you choose to use, which currently include voice-based biometric data (audio samples, voiceprints, unique voice characteristics, vocal patterns, prosody, acoustic features and derived voice models used to generate your personal voice clone).
- Future Biometric Features (Facial Recognition, etc.): ForeverFrom may expand to support additional biometric identifiers in the future — such as facial-recognition–based features, expression analysis, or similar modalities. These features will not be activated without providing you with an updated written notice and obtaining any additional consent required under applicable biometric privacy laws.

- Purpose of Collection: We use biometric identifiers solely for the features you explicitly enable — e.g., creating and maintaining your voice clone today, and any future biometric features only after you provide informed consent.
- Retention Schedule: We retain biometric identifiers for as long as your account exists and your biometric consent remains active. There is no automatic time-based expiration. When you delete your account or withdraw biometric consent, your biometric identifiers are permanently destroyed within 60 days, subject only to legal holds or backup retention cycles.
- Storage & Security: All personal data, including voice recordings and biometric data, is encrypted in transit and at rest using industry-standard encryption. Access is limited to authorized personnel and protected by strong access controls, including multi-factor authentication where applicable.
- Illinois BIPA Notice (for Illinois residents): We collect, use, and store biometric identifiers (voiceprints) as described in this Privacy Policy and our publicly available retention and destruction policy. You may review our retention schedule (above) and may withdraw consent and request deletion at any time by contacting privacy@foreverfrom.com.
- Texas CUBI Notice (for Texas residents): We retain your biometric identifiers (voiceprint) only for as long as your account exists or until you request deletion. They are permanently destroyed within 60 days of account deletion or your deletion request.
- Washington biometric identifiers law: When we enroll a biometric identifier for a commercial purpose, Washington law generally requires notice, consent, or a choice to prevent enrollment. We will provide clear notice of our purposes and obtain your consent before enrolling your biometric identifiers.

(d) Identity Data:

- Name.
- Email.
- Phone number.
- Birthdate.
- Verification details.

(e) Payment Data:

- Payment card details.
- Billing address.
- Subscription information (processed by third-party payment processors).

(f) Information We Collect Automatically:

- Device and usage data (IP address, browser type, operating system, mobile identifiers).
- Interaction data (pages visited, features used, session activity).
- Log and diagnostic data for performance and security.

(g) Information from Third Parties:

- Social media integrations (when you choose to connect).
- Legacy managers or family stewards (if designated).
- Advertising and analytics partners (as outlined below).
- Voice cloning technology providers: Hume AI (www.hume.ai) for voice services.
- AI processing service providers: OpenAI (www.openai.com) for memory processing and conversational AI features.

2. How We Use Your Information

We use your information to:

- Provide, maintain, and improve the Services.
- Generate, train, and maintain your digital twin.
- Ensure safety, security, and fraud prevention.
- Honor your consent settings and legacy wishes (including post-mortem plans).
- Process payments and manage subscriptions.
- Personalize your experience, including memory prompts and relevant features.
- Deliver advertising and sponsored content, consistent with this Policy.

We do not use sensitive information (memories, biometric data, health data) for advertising purposes, unless you provide explicit, separate, opt-in consent.

Sensitive Data & Optional Advertising Features. ForeverFrom will never use your biometric data, memory content, voice recordings, emotional inferences, health-related information, or any other sensitive personal data for advertising, personalization, or cross-context behavioral targeting, unless you provide explicit, separate, opt-in consent. If ForeverFrom introduces optional advertising or personalization features in the future, we will present a clear consent screen

describing the categories of data involved, the purpose, and your right to refuse or withdraw consent at any time.

2A. Biometric Data – Specific Uses and Protections

Permitted Uses of Biometric Data. We use biometric data exclusively for the following purposes:

- Creating and maintaining your personalized voice clone.
- Improving voice synthesis quality and naturalness.
- Ensuring security and preventing unauthorized access to your account.
- Training and refining AI models (only with your explicit consent, and using de-identified/anonymized data).
- Complying with legal obligations and responding to valid legal process.

Prohibited Uses. We will never:

- Sell, rent, lease, or trade your biometric data.
- Use biometric data for advertising purposes without your explicit, separate, opt-in consent.
- Share biometric data with third parties except as required for service delivery or legal compliance.
- Disclose biometric data in violation of applicable biometric privacy laws.
- Profit from your biometric data in any manner.

Illinois Residents: We do not and will never profit from the sale, lease, or trade of your biometric identifiers or biometric information.

Third-Party Processors. We use third-party AI service providers to deliver our Services:

Hume AI (Voice Technology). We use Hume AI (www.hume.ai) as our voice cloning technology provider. Hume AI processes voice data to provide voice synthesis services and operates under their standard terms of service and privacy policy. Hume AI's role:

- Provides the underlying voice synthesis technology.
- Processes your audio samples to create voice models.
- Implements technical safeguards including consent attestation, pattern detection, and rate limiting.
- Operates under their terms of service and privacy policy.

ForeverFrom remains primarily responsible for your biometric data and will be your point of contact for all privacy requests.

OpenAI (Memory Processing and Conversational AI). We use OpenAI (www.openai.com) for memory intelligence and conversational AI features. OpenAI operates under their API Terms of Service. When you create or interact with memories, OpenAI processes your memory content for:

- Metadata extraction: Identifying people, places, emotions, events, and time periods from your memories.
- Memory organization: Intelligently splitting multi-part memory inputs into distinct memories.
- Conversational AI: Generating responses, follow-up questions, and interactions with your digital twin.
- Natural language understanding: Processing your queries and generating contextual responses.

What OpenAI does:

- Processes memory content via their API infrastructure.
- Operates under their API Terms of Service.
- Current API Data Usage Policy states that API inputs are not used to train their models.
- However, data does pass through OpenAI's infrastructure and is subject to their security practices and data retention policies.
- ForeverFrom cannot control or guarantee OpenAI's future data practices and will notify you of material changes to their policies that affect your data.

What ForeverFrom Does:

- Selects and contracts with reputable AI service providers.
- Selects service providers with strong data protection commitments.
- Enforces strict usage policies against unauthorized use.
- Provides user verification and consent mechanisms.
- Responds to and investigates reported policy violations and takes enforcement action where appropriate.
- Maintains reporting mechanisms (privacy@foreverfrom.com, abuse@foreverfrom.com).
- Ensures compliance with biometric privacy laws and data protection regulations.

Forever From

Important Disclosures

Platform and Third-Party Services. ForeverFrom acts as a platform that coordinates multiple AI services. While we enforce strong policies and respond to reports of misuse:

- Voice processing technical safeguards are provided by Hume AI.
- Memory processing AI capabilities are provided by OpenAI.
- We do not control these third parties' underlying technical infrastructure.
- Each provider operates under their own terms, security practices, and limitations.
- ForeverFrom remains primarily responsible and is your point of contact for privacy matters.

International Data Transfer. Your data may be transmitted to and processed by:

- OpenAI's infrastructure (primarily US-based).
- Hume AI's infrastructure.
- Our own cloud infrastructure (AWS).

We ensure appropriate safeguards are in place for international data transfers by selecting service providers with strong data protection commitments and contractual data processing provisions.

Your Rights Regarding Biometric Data. You have the right to:

- Withdraw consent for biometric data collection and use at any time.
- Request deletion of your biometric data (with a 60-day destruction guarantee).
- Receive information about how your biometric data is stored and used.
- File a complaint with relevant data protection authorities.
- Receive notification of any biometric data breach without undue delay and within timeframes required by applicable law.

State-Specific Biometric Rights:

- Illinois (BIPA): Written consent required; private right of action for violations; liquidated damages available; we do not profit from your biometric data.
- Texas (CUBI): We retain your biometric identifiers (voiceprint) only for as long as your account exists or until you request deletion. They are

permanently destroyed within 60 days of account deletion or your deletion request.
- Washington (biometric identifiers law): Consent required; notice of data collection purposes required.
- California (CPRA): Enhanced protections for sensitive personal information including biometric data.

To exercise these rights, contact us at privacy@foreverfrom.com.

3. Advertising & Personalization

The Services may include advertising, promotions, and sponsored content. We may use non-sensitive data (device information, interactions, account settings) to personalize ads:

- Personalized Ads. Ads may be tailored to your activity and preferences.
- Sensitive Data Exclusion. Your memories, biometric data, and health-related data will never be used for advertising, unless you provide explicit, separate, opt-in consent.
- Third-Party Ads. Third-party advertisers are solely responsible for their content. ForeverFrom does not endorse or guarantee their products or services.

ForeverFrom may introduce optional advertising or personalization programs in the future. Participation in these programs will always be voluntary, and ForeverFrom will never use sensitive personal information for advertising without your express opt-in.

4. Legal Bases for Processing

Where applicable we rely on the following legal bases:

- Consent (for biometric data, memories, voice recordings, and post-mortem usage).
- Contract (to provide the Services you subscribe to).
- Legitimate Interests (improving and securing the Services, personalization).
- Legal Obligations (complying with data protection, fraud, or financial laws).

Specific Consent for Biometric Data. For biometric identifiers and biometric information (as defined under applicable state biometric privacy laws), we rely exclusively on your explicit, informed, written consent obtained through a separate consent mechanism during account setup or voice cloning feature activation. This consent is voluntary, and you may withdraw it at any time, though withdrawal may limit your ability to use certain Services features.

5. Sharing of Information

We may share information with:

- Service Providers: Hosting, payment, analytics, security, and verification providers.
- AI Service Providers: Hume AI for voice cloning technology; OpenAI for memory processing.
- Advertising Partners: To deliver personalized or contextual ads (excluding sensitive categories and always with your explicit, separate, opt-in consent).
- Legacy Stewards / Family Managers: When authorized by you.
- Legal & Regulatory Authorities: If required by law, subpoena, or government request.
- Corporate Transactions: In mergers, acquisitions, or asset transfers, with notice provided.
- We do not sell your personal information.

6. Data Security

We implement strong safeguards, including:

- Encryption of data in transit and at rest using industry-standard encryption.
- Access strictly limited to authorized personnel and protected by multi-factor authentication.
- Account verification mechanisms.

No system is 100% secure, but ForeverFrom is built on a Security by Design foundation.

6A. Biometric Data Breach Notification

In the event of a data breach involving your biometric data, we will:

- Notify you directly via email without undue delay and within timeframes required by applicable law after determining that a breach occurred.
- Provide information about the nature of the breach, types of data involved, and steps we are taking to mitigate harm.
- Notify relevant regulatory authorities as required by law.
- Offer identity theft protection or credit monitoring services if warranted by the nature of the breach.

7. Consent & Control

- Granular Consent. You choose what to share (stories, values, health, public visibility).
- Dynamic Consent. You may adjust or revoke permissions at any time.
- Post-Mortem Controls. You may set legacy instructions (memorialize, archive, or delete your twin).
- Family Rights. Legacy managers may have access consistent with your wishes.
- Biometric Consent. Separate, explicit consent required for voice cloning and biometric data collection.

8. Children's Privacy

ForeverFrom is intended for adults who are at least 18 years old (or the age of majority in their jurisdiction, if higher). Individuals under this age are not permitted to create an account or use the Services.

We do not knowingly allow anyone under 18 to use the Services.

We also do not knowingly collect personal information from children under 13. If we become aware that we have collected personal information from a child under 13, we will delete it as required under the U.S. Children’s Online Privacy Protection Act (COPPA).

9. International Data Transfers

If you are outside the U.S., your information may be transferred to and processed in the U.S. or other jurisdictions (including by Hume AI and OpenAI operating as our service providers). These providers operate under their own terms of service and privacy policies, and we select providers with strong data protection commitments.

For users in the European Economic Area (EEA), UK, or Switzerland:

- Where required, we rely on Standard Contractual Clauses (SCCs) or other valid safeguards, or will do so before transferring personal data.
- We select service providers with strong data protection commitments.
- You have the right to request copies of appropriate safeguards.

10. Data Retention

We retain data only as long as necessary:

- To provide the Services and fulfill your instructions.
- To comply with legal obligations.
- To support post-mortem legacy settings (if chosen).

Biometric Data Retention. ForeverFrom maintains a public Biometric Data Retention & Destruction Policy, and all biometric identifiers and biometric information (including voiceprints and derived voice models) follow that policy.

We retain biometric data for:

- The duration of your active account while consent remains active.
- Until you explicitly revoke consent and request deletion, or delete your account.

There is no automatic time-based expiration. Biometric data is permanently destroyed within sixty (60) days of deletion request or account termination, subject to backup retention cycles (typically within 90 days). Deletion is permanent and irreversible.

Users may request deletion at any time by contacting privacy@foreverfrom.com, subject to legal and backup obligations.

11. Your Rights

Depending on where you live, you may have rights to:

- Access, correct, or delete your data.
- Withdraw consent (especially for biometric and sensitive data).
- Port your data to another service.
- Opt-out of targeted advertising or "sales" of personal information.
- File a complaint with your data protection authority.

Additional Rights for Biometric Data:

- Right to receive written notice before collection of biometric data.
- Right to know the specific purpose and length of retention.
- Right to consent before any disclosure to third parties.
- Right to destruction of biometric data when you request deletion, withdraw consent, or delete your account.
- Right to sue for damages if your biometric data is mishandled (in jurisdictions with private right of action, such as Illinois).

California Residents – Sensitive Personal Information. Under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), biometric information is classified as "sensitive personal information." You have the right to:

- Limit use and disclosure of sensitive personal information.
- Opt-out of "sale" or "sharing" (we do not sell or share biometric data).
- Request deletion of sensitive personal information.
- Receive notice of automated decision-making using sensitive data.

How to Exercise Rights:

Email: privacy@foreverfrom.com or support@foreverfrom.com

Subject line: "Biometric Data Rights Request" or "California Privacy Rights".

Include: Your name, email, account details, and specific request.

If you believe your biometric voice data has been used without authorization, you may submit a report to abuse@foreverfrom.com.

We will respond within 45 days (or as required by applicable law) and will not discriminate against you for exercising your rights.

12. Changes to this Policy

We may update this Privacy Policy as our Services evolve. For material changes, we will provide notice via email or in-product alerts. Continued use after updates means acceptance.

13. Contact Us

If you have questions, concerns, or requests regarding this Privacy Policy, contact us at:

ForeverFrom Inc.

support@foreverfrom.com

privacy@foreverfrom.com

abuse@foreverfrom.com (for unauthorized voice cloning reports)

legal@foreverfrom.com

14. Your California Privacy Rights (CCPA/CPRA)

If you are a California resident, you have the following rights under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA):

- Right to Know: You may request that we disclose the categories and specific pieces of personal information we have collected about you.
- Right to Delete: You may request that we delete personal information we have collected, subject to legal exceptions.
- Right to Correct: You may request that we correct inaccurate personal information.
- Right to Opt-Out of "Sale" or "Sharing": ForeverFrom does not sell or share your personal information for cross-context behavioral advertising. You may still contact us at privacy@foreverfrom.com with "Do Not Sell or Share" in the subject line if you wish to exercise this right.
- Right to Limit Use of Sensitive Personal Information: You may request that we limit the use and disclosure of sensitive personal information (including biometric data) to what is necessary to provide the Services.

- Right to Non-Discrimination: You will not be discriminated against for exercising your privacy rights.
- How to Submit Requests: You may exercise these rights by emailing privacy@foreverfrom.com or via your account settings (where available). We will verify your request and respond within 45 days.
- Retention: We retain personal information only as long as necessary to provide the Services, comply with law, fulfill your settings, or maintain security. Biometric retention follows our Biometric Data Retention & Destruction Policy: we retain biometric data for the duration of your active account until you request deletion, withdraw consent, or delete your account. There is no automatic time-based expiration.

Cookies & Similar Technologies. We use cookies and similar technologies to operate and improve the Services. You can control cookies via your browser settings.

AI & Voice Cloning Safety. You may only clone your own voice. Impersonation or deepfakes violate our Terms and result in immediate account termination. AI outputs may contain errors and are not professional advice.

Biometric Data & Voice Cloning – Information and Consent Notice. This notice serves as the written disclosure and consent required under the Illinois Biometric Information Privacy Act (BIPA), Texas Capture or Use of Biometric Identifier Act (CUBI), Washington biometric laws, and similar statutes.

By enabling the "Speak in your voice" feature and clicking "I Agree", you provide explicit written consent for ForeverFrom to collect, store, and use your biometric identifiers and biometric information as described below:

(a) What biometric data we collect

When you choose to create a personal voice clone, we collect and process:

- Voiceprints (unique acoustic features of your voice).
- Audio samples you record for this purpose.

(b) Specific and only purpose

We do not use your biometric data for advertising, surveillance, sale, or unrelated behavioral tracking. We use your voiceprint only for the purposes described in this Privacy Policy — including creating and maintaining your voice clone, improving synthesis quality, ensuring security, complying with legal obligations, and enabling playback of a private synthetic voice that sounds like you so your memories can be spoken in your own voice. We do not use your biometric data for commercial identity-verification services or for any purpose unrelated to the features you have chosen to enable.

(c) We never monetize or share your biometric data

ForeverFrom will never sell, lease, trade, or otherwise profit from your voiceprint or voice model. Your biometric data is shared only with our service providers (such as Hume AI and our cloud hosting providers) and with authorities where required by law, solely to deliver the Services and comply with legal obligations.

(d) Retention and destruction schedule

Your voiceprint and derived voice model are retained for the duration of your active account until you request deletion, withdraw consent, or delete your account. There is no automatic time-based expiration. When you delete your account or withdraw consent, your voiceprint and voice model are permanently destroyed within sixty (60) days, subject to backup retention cycles (typically within 90 days) and legal obligations.

(e) Your rights

You may withdraw consent and request immediate deletion of your voiceprint and voice clone at any time by:

- Disabling voice cloning in your account settings, or
- Emailing privacy@foreverfrom.com with the subject “Revoke Biometric Consent” or “Biometric Data Deletion Request”.

(f) Own-voice-only rule

Forever From

You may only submit recordings of your own voice. Submitting anyone else's voice violates our Terms of Use and will result in immediate account termination.

Illinois Residents: ForeverFrom does not and will never profit from the sale, lease, or trade of your biometric identifiers or biometric information.