RESEMBLE AI, INC.

Data Processing Agreement

(DPA)

Last Updated	March 17, 2026
Processor	Resemble AI, Inc.
Applies To	All customers using Resemble AI Services
Governing Agreement	Resemble AI Terms of Service (https://www.resemble.ai/terms-of-service/) or applicable Enterprise Agreement

1. Introduction and Scope

This Data Processing Agreement ("DPA") forms part of the Resemble AI Terms of Service available at https://www.resemble.ai/terms-of-service/ or, where applicable, an executed Enterprise Agreement (the "Principal Agreement") between the customer entity using Resemble AI's Services ("Controller" or "Customer") and Resemble AI, Inc. ("Processor" or "Resemble AI"), collectively referred to as the "Parties."

This DPA applies to the processing of Personal Data by Resemble AI on behalf of the Customer in connection with the provision of voice AI services, including voice cloning, text-to-speech, deepfake detection, real-time voice agents, consent verification, and related platform services (the "Services").

This DPA is entered into to ensure compliance with applicable data protection legislation, including but not limited to:

(a) Regulation (EU) 2016/679 (General Data Protection Regulation, "GDPR");

(b) EU Standard Contractual Clauses for international data transfers pursuant to Article 46(2)(c) GDPR;

(c) Applicable national implementations of the GDPR in EU/EEA Member States and the United Kingdom; and

(d) Any other applicable data protection laws to the extent they apply to the processing of Personal Data under the Principal Agreement.

Where Resemble AI provides Services to the Customer, Resemble AI acts as a data processor on behalf of the Customer, who acts as the data controller. The details of the processing are set out in Annex 1 to this DPA.

Resemble AI maintains its information security program in alignment with SOC 2 Trust Services Criteria, ISO 27001, GDPR, and HIPAA standards, with audit engagements underway for formal certification.

2. Definitions

"Applicable Data Protection Law" means the GDPR, its national implementations, the UK GDPR, and any other data protection legislation applicable to the processing of Personal Data under this DPA.

"Controller" means the Customer, being the entity or individual that has agreed to the Principal Agreement and determines the purposes and means of the processing of Personal Data.

"Data Subject" means the identified or identifiable natural person to whom the Personal Data relates.

"Personal Data" means any information relating to a Data Subject that is processed by Resemble AI on behalf of the Customer in connection with the Services.

"Principal Agreement" means the Resemble AI Terms of Service (https://www.resemble.ai/terms-of-service/) or, where applicable, an executed Enterprise Agreement between the Customer and Resemble AI governing the Customer's use of the Services.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

“Processing” means any operation or set of operations performed on Personal Data, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, combination, restriction, erasure, or destruction.

“Processor” means Resemble AI, Inc., which processes Personal Data on behalf of the Controller.

“Special Category Data” means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person’s sex life or sexual orientation, as defined in Article 9 of the GDPR. For the purposes of this DPA, this includes voice biometric data (voice prints) and facial biometric data processed through Resemble AI’s deepfake detection services.

“SCCs” means the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Commission Implementing Decision (EU) 2021/914.

“Sub-Processor” means any third party engaged by Resemble AI to process Personal Data on behalf of the Controller in connection with the Services.

3. Processor Obligations

3.1 Resemble AI shall process Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country, unless required to do so by applicable law to which Resemble AI is subject. In such a case, Resemble AI shall inform the Controller of that legal requirement before processing, unless prohibited by law.

3.2 Resemble AI shall ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.3 Resemble AI shall implement and maintain the technical and organizational security measures set out in Annex 2, as appropriate to the risk presented by the processing, including as applicable measures referred to in Article 32(1) of the GDPR.

3.4 Resemble AI shall not engage another processor (Sub-Processor) without prior specific or general written authorization of the Controller, subject to Section 7 of this DPA.

3.5 Taking into account the nature of the processing, Resemble AI shall assist the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller’s obligation to respond to requests for exercising Data Subject rights under Chapter III of the GDPR.

3.6 Resemble AI shall assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of the processing and the information available to Resemble AI.

3.7 At the choice of the Controller, Resemble AI shall delete or return all Personal Data to the Controller after the end of the provision of Services, and delete existing copies unless applicable

law requires storage of the Personal Data. The specific retention and deletion schedules applicable to each processing activity are set out in Annex 1.

3.8 Resemble AI shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and this DPA, and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller, subject to Section 10 of this DPA.

3.9 Resemble AI shall immediately inform the Controller if, in Resemble AI's opinion, an instruction from the Controller infringes the GDPR or other applicable data protection provisions.

4. Controller Obligations

4.1 The Controller shall ensure that it has a valid legal basis for the processing of Personal Data as instructed to Resemble AI, including where applicable, obtaining explicit consent from Data Subjects for the processing of Special Category Data (voice biometric data, facial biometric data) as required by Article 9(2)(a) of the GDPR.

4.2 The Controller shall ensure that Data Subjects have been provided with appropriate privacy notices in compliance with Articles 13 and 14 of the GDPR, including information about the use of Resemble AI as a processor and the categories of processing performed.

4.3 The Controller shall ensure that its instructions to Resemble AI comply with Applicable Data Protection Law. The Controller acknowledges that Resemble AI's voice cloning services require explicit consent from the voice owner, and the Controller is responsible for ensuring such consent is lawfully obtained prior to submitting voice data for processing.

4.4 The Controller is responsible for ensuring that appropriate safeguards are in place for any automated decision-making processes that utilize Resemble AI's consent verification system, including the ability for Data Subjects to obtain human intervention, express their point of view, and contest the decision in accordance with Article 22 of the GDPR.

5. Special Category Data

5.1 The Parties acknowledge that the Services involve the processing of Special Category Data as defined in Article 9 of the GDPR, specifically:

(a) **Voice biometric data (voice prints):** Processed during voice cloning, text-to-speech, real-time voice agents, consent verification, and audio deepfake detection services.

(b) **Facial and visual biometric data:** Processed during image and video deepfake detection services and meeting deepfake detection services.

5.2 The Controller warrants that it has obtained explicit consent from Data Subjects for the processing of their biometric data as required by Article 9(2)(a) of the GDPR, or that another valid exemption under Article 9(2) applies.

5.3 Resemble AI shall apply enhanced security measures to Special Category Data, including encryption at rest (AES-256) and in transit (TLS 1.2+), strict role-based access controls, and data minimization practices as detailed in Annex 2.

6. Personal Data Breach Notification

6.1 Resemble AI shall notify the Controller without undue delay, and in any event within forty-eight (48) hours after becoming aware of a Personal Data Breach affecting the Controller's Personal Data.

6.2 Such notification shall, to the extent available, include:

(a) A description of the nature of the Personal Data Breach, including where possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

(b) The name and contact details of Resemble AI's data protection point of contact;

(c) A description of the likely consequences of the Personal Data Breach;

(d) A description of the measures taken or proposed to be taken by Resemble AI to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

6.3 Where it is not possible to provide all information at the same time, the information may be provided in phases without further undue delay.

6.4 Resemble AI shall cooperate with the Controller and take reasonable steps as directed by the Controller to assist in the investigation, mitigation, and remediation of each such Personal Data Breach.

6.5 Resemble AI's notification of or response to a Personal Data Breach shall not be construed as an acknowledgment by Resemble AI of any fault or liability with respect to the Personal Data Breach.

6.6 Upon becoming aware of a suspected Personal Data Breach, Resemble AI shall conduct a risk assessment to determine whether the incident constitutes a breach. A breach shall be presumed unless Resemble AI can demonstrate a low probability that Personal Data has been compromised, taking into account the nature and extent of the Personal Data involved, the identity of the unauthorized person who accessed the data, whether the data was actually acquired or viewed, and the extent to which the risk has been mitigated.

6.7 All documentation related to a Personal Data Breach, including investigation logs, risk assessments, and notifications, shall be retained by Resemble AI for a minimum of six (6) years from the date of the breach.

6.8 Resemble AI may delay notification to the Controller if a law enforcement official determines that such notification would impede a criminal investigation or cause damage to national security. Any such delay shall be documented and notification shall be provided promptly once the law enforcement official confirms that the delay is no longer required.

7. Sub-Processors

7.1 The Controller acknowledges and authorizes Resemble AI's use of the Sub-Processors listed at https://trust.resemble.ai/subprocessors as of the date the Customer first accesses or uses the Services.

7.2 Resemble AI may update its Sub-Processors from time to time. Resemble AI will update the Sub-Processor list at https://trust.resemble.ai/subprocessors when engaging a new Sub-Processor. The Controller may subscribe to change notifications at that URL.

7.3 If the Controller has a material objection to a new Sub-Processor based on reasonable data protection grounds, the Controller may notify Resemble AI in writing within thirty (30) days of the Sub-Processor list being updated. If the Parties are unable to resolve the objection, the Controller's sole remedy shall be to terminate the affected Services in accordance with the Principal Agreement.

7.4 Where Resemble AI engages a Sub-Processor, Resemble AI shall:

(a) Impose on the Sub-Processor, by way of a written contract, data protection obligations no less protective than those set out in this DPA;

(b) Ensure the Sub-Processor provides sufficient guarantees to implement appropriate technical and organizational measures;

(c) Remain fully liable to the Controller for the performance of the Sub-Processor's obligations.

7.5 The current list of authorized Sub-Processors is maintained at https://trust.resemble.ai/subprocessors and is incorporated into this DPA by reference. Resemble AI maintains Data Processing Agreements with all Sub-Processors.

8. International Data Transfers

8.1 The Controller acknowledges that Resemble AI's infrastructure is primarily hosted in the United States (Google Cloud Platform us-east4, Render Oregon, Cerebrium US). Personal Data from the European Economic Area, United Kingdom, or Switzerland will be transferred to and processed in the United States.

8.2 To the extent that the processing of Personal Data involves a transfer of Personal Data to a country outside the EEA that has not received an adequacy decision from the European Commission, the Parties agree that such transfers shall be governed by the EU Standard Contractual Clauses (SCCs) as set out in Commission Implementing Decision (EU) 2021/914, which are incorporated by reference into this DPA.

8.3 For the purposes of the SCCs:

(a) Module Two (Controller to Processor) shall apply;

(b) Clause 7 (docking clause) shall apply, allowing additional parties to accede to the SCCs;

(c) Under Clause 9(a), Option 2 (general written authorization) shall apply, with a notice period of thirty (30) days as set out in Section 7.2;

(d) Under Clause 11, the optional language shall not apply;

(e) Under Clause 17, Option 1 shall apply, and the SCCs shall be governed by the law of Ireland;

(f) Under Clause 18(b), disputes shall be resolved before the courts of Ireland.

8.4 Where Sub-Processors participate in the EU-U.S. Data Privacy Framework (DPF) under an adequacy decision pursuant to Article 45 of the GDPR, such transfers may also rely on the DPF as an additional transfer mechanism.

8.5 Resemble AI shall ensure that all international transfers are subject to appropriate supplementary measures, including encryption in transit (TLS 1.2+), encryption at rest (AES-256), and access controls as described in Annex 2.

8.6 Resemble AI's Services are provided from its standard infrastructure as described in Section 8.1. Regional hosting options, including UK-based processing, may be available to enterprise customers under a separately negotiated Enterprise Agreement. Self-service customers acknowledge and accept that their data will be processed on Resemble AI's standard infrastructure.

9. Data Subject Rights

9.1 Resemble AI shall, taking into account the nature of the processing, assist the Controller by appropriate technical and organizational measures for the fulfilment of the Controller's obligations to respond to requests from Data Subjects exercising their rights under Chapter III of the GDPR, including rights of access, rectification, erasure, restriction, data portability, and objection.

9.2 If Resemble AI receives a request from a Data Subject directly, Resemble AI shall promptly forward the request to the Controller and shall not respond to the Data Subject unless instructed by the Controller or required by applicable law.

9.3 Resemble AI supports the following data subject right fulfillment capabilities through its platform:

(a) **Right to erasure:** Voice models and all associated training audio can be permanently deleted. Deletion is irreversible and includes removal from all infrastructure providers (GCP, Render, Cerebrium).

(b) **Right to access / portability:** Customer data, voice model metadata, and processing records can be exported in machine-readable formats through the API and platform.

(c) **Right to restriction:** Processing of specific voice models or data can be suspended upon Controller instruction.

10. Audit Rights

10.1 Resemble AI shall make available to the Controller all information reasonably necessary to demonstrate compliance with this DPA and shall allow for and contribute to audits, including inspections, conducted by the Controller or an independent auditor appointed by the Controller.

10.2 The Controller shall provide at least thirty (30) days' prior written notice of any audit request. Audits shall be conducted during normal business hours, shall not unreasonably disrupt Resemble AI's operations, and shall be subject to reasonable confidentiality obligations.

10.3 The Controller shall bear its own costs in connection with any audit. If the Controller requests an audit more than once in any twelve (12) month period, Resemble AI may charge the Controller for the reasonable costs of any additional audits.

10.4 Resemble AI may satisfy audit requests by providing the Controller with:

(a) A copy of Resemble AI's most recent SOC 2 Type II report or ISO 27001 certificate, where available;

(b) Responses to reasonable written information requests or security questionnaires;

(c) Results of penetration testing or vulnerability assessments conducted by qualified third parties, subject to confidentiality restrictions.

10.5 If the Controller reasonably determines that the information provided under Section 10.4 is insufficient to verify compliance, the Controller may conduct or commission an on-site audit subject to the conditions set out in Sections 10.2 and 10.3.

11. Data Return and Deletion

11.1 Upon termination or expiration of the Principal Agreement, Resemble AI retains the Controller's Personal Data in an archived state for the sole purpose of enabling the Controller to access and retrieve their data should they return to the platform. This retention is provided as a convenience to the Controller and Resemble AI does not actively process archived data for any other purpose.

11.2 The Controller may request deletion of all Personal Data at any time, including after termination of the Principal Agreement, by contacting Resemble AI at support@resemble.ai. Upon receiving such a request, Resemble AI shall:

(a) Delete all Personal Data and certify such deletion in writing to the Controller; or

(b) Return all Personal Data to the Controller in a commonly used, machine-readable format, and subsequently delete all copies.

11.3 Resemble AI shall complete the return or deletion within thirty (30) days of the Controller's request, unless applicable law requires further retention.

11.4 Specific retention schedules by processing activity are set out in Annex 1. Where the Controller has not requested deletion, voice models and associated data remain in archived storage and are available for retrieval upon the Controller's reactivation of Services.

11.5 Resemble AI shall ensure that Sub-Processors delete or return Personal Data in accordance with this Section 11 upon receiving a deletion request from the Controller.

12. Security Program and Certifications

12.1 Resemble AI maintains an information security program and is actively pursuing certification and compliance across the following frameworks:

(a) **SOC 2 Type II:** Resemble AI's governance, risk management, and technical controls are designed in alignment with SOC 2 Trust Services Criteria for security, availability, and confidentiality. SOC 2 Type II audit engagement is underway.

(b) **ISO 27001:** Resemble AI's information security management practices are aligned with ISO 27001 requirements, including risk assessment methodology, management review, and continuous improvement. ISO 27001 certification is in progress.

(c) **GDPR:** Resemble AI maintains full GDPR compliance documentation including Data Protection Impact Assessments, Data Transfer Agreements, and Records of Processing Activities for all processing operations.

(d) **HIPAA:** Resemble AI is pursuing compliance with the Health Insurance Portability and Accountability Act (HIPAA), including implementation of administrative, physical, and technical safeguards for Protected Health Information. Customers requiring HIPAA compliance should contact Resemble AI to execute a Business Associate Agreement (BAA) under a separately negotiated Enterprise Agreement.

12.2 Resemble AI shall maintain its security program throughout the term of this DPA and shall not materially reduce the overall level of security without prior written notice to the Controller.

12.3 Upon request, Resemble AI shall provide the Controller with evidence of its security certifications and compliance documentation as they become available, including SOC 2 Type II reports and ISO 27001 certificates, subject to reasonable confidentiality obligations.

13. Liability

13.1 Each Party's liability under this DPA shall be subject to the exclusions and limitations of liability set out in the Principal Agreement, unless otherwise required by Applicable Data Protection Law.

13.2 Nothing in this DPA shall limit either Party's liability to Data Subjects or to supervisory authorities under Applicable Data Protection Law.

14. Term and Termination

14.1 This DPA shall come into effect on the date the Customer first accesses or uses the Services and shall continue in force for as long as Resemble AI processes Personal Data on behalf of the Controller under the Principal Agreement.

14.2 Upon termination or expiration of the Principal Agreement, this DPA shall automatically terminate, subject to the obligations in Section 11 (Data Return and Deletion) which shall survive termination.

14.3 Sections 6 (Personal Data Breach Notification), 10 (Audit Rights), 11 (Data Return and Deletion), 12 (Security Program), and 13 (Liability) shall survive the termination of this DPA.

15. General Provisions

15.1 In the event of a conflict between this DPA and the Principal Agreement, this DPA shall prevail with respect to the processing of Personal Data.

15.2 This DPA, together with its Annexes and the SCCs incorporated by reference, constitutes the entire agreement between the Parties with respect to the subject matter hereof.

15.3 Resemble AI may update this DPA from time to time to reflect changes in applicable law, regulatory guidance, or its processing practices. Resemble AI will provide reasonable advance notice of material changes by posting the updated DPA on its website. Continued use of the Services after such notice constitutes acceptance of the updated DPA. Enterprise customers with executed agreements may negotiate amendments in writing.

15.4 This DPA shall be governed by and construed in accordance with the laws of the State of Delaware, United States, except to the extent overridden by Applicable Data Protection Law. Where an Enterprise Agreement specifies different governing law, that governing law shall apply to this DPA.

15.5 If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions shall remain in full force and effect.

Acceptance

By using Resemble AI's Services, the Customer agrees to be bound by the terms of this Data Processing Agreement. This DPA is effective as of the date the Customer first accesses or uses the Services under the Principal Agreement.

Enterprise customers with individually negotiated agreements may execute this DPA by countersignature as an addendum to their Enterprise Agreement. For questions regarding this DPA, please contact Resemble AI at support@resemble.ai.

Annex 1: Details of Processing

This Annex describes the processing activities carried out by Resemble AI on behalf of the Controller.

A. Subject Matter and Duration

Resemble AI processes Personal Data for the purpose of providing AI services to the Controller, including voice cloning, text-to-speech synthesis, deepfake detection, real-time voice agents, and consent verification. The duration of processing corresponds to the term of the Principal Agreement.

B. Nature and Purpose of Processing

The following processing activities are performed:

Processing Activity	Purpose	Retention
Voice Cloning & Model Training	Create custom AI voice models from audio samples provided by the Controller	Retained for archival retrieval; deleted within 30 days of Controller's deletion request
Text-to-Speech Inference	Convert text to speech using custom or pre-built voice models	Input text and generated audio retained for archival retrieval; deleted within 30 days of Controller's deletion request
Deepfake Detection (Audio)	Analyze audio files to detect AI-generated synthetic speech	Input data and analysis results retained for archival retrieval; deleted within 30 days of Controller's deletion request. When Privacy Mode is enabled, input data is discarded after processing and only results are returned
Deepfake Detection (Image/Video)	Analyze images and video for AI-generated or manipulated content	Input data and analysis results retained for archival retrieval; deleted within 30 days of Controller's deletion request. When Privacy Mode is enabled, input data is discarded after processing and only results are returned
Meeting Deepfake Detection	Real-time monitoring of meeting audio/video for deepfake content	Non-flagged data discarded immediately; flagged recordings retained per Controller instruction
Real-Time Voice Agents	Live two-way AI voice conversations via WebRTC	Transient stream processing; conversation data not persistently stored by default
Consent Verification	Automated validation of voice clone consent authenticity	Consent recordings retained for the duration of the associated voice model
Platform & Account Management	User authentication, API key management, usage tracking, billing	Retained for duration of account plus 1 year after termination; deleted within 30 days of Controller's deletion request

System and Application Logs	API usage logs, access logs, and security audit trails	12 months, then automatically rotated and securely deleted
Backup Data	System and database backups containing Controller Personal Data	90-day rolling retention; encrypted backups deleted after lifecycle expiry

C. Categories of Data Subjects

- End users of the Controller's applications that utilize Resemble AI Services
- Voice owners who provide audio samples for voice cloning
- Individuals whose audio, image, or video content is submitted for deepfake detection analysis
- Participants in meetings monitored by Meeting Deepfake Detection
- Controller's authorized users of the Resemble AI platform

D. Categories of Personal Data

- Voice recordings and audio samples
- Voice biometric data (voice prints) – Special Category Data under Article 9
- Facial and visual biometric data (for image/video deepfake detection) – Special Category Data under Article 9
- Text input for speech synthesis
- Account information (name, email address, organization)
- API usage metadata and logs
- IP addresses and technical identifiers
- Meeting audio and video streams (for Meeting Deepfake Detection)
- Consent recordings

Annex 2: Technical and Organizational Security Measures

Resemble AI implements the following technical and organizational measures to protect Personal Data processed on behalf of the Controller. These measures are aligned with SOC 2 Trust Services Criteria and ISO 27001 Annex A controls.

Measure	Description
Encryption in Transit	All data in transit is encrypted using TLS 1.2 or higher across all infrastructure providers and internal service communications.
Encryption at Rest	All data at rest is encrypted using AES-256 across Google Cloud Platform, Render, and Cerebrium storage systems, including databases and object storage.
Access Control	Role-based access controls (RBAC) are enforced across all systems. Production data access is restricted to authorized engineering personnel. API authentication is required for all product endpoints.
Network Security	Cloudflare Web Application Firewall (WAF) and DDoS protection are deployed on all public-facing services. GCP firewall rules restrict inbound traffic to necessary ports and protocols. Database access is limited to application servers via private networking.
Application Monitoring	New Relic provides application performance monitoring. Sentry provides real-time error tracking and alerting. GCP audit logs record infrastructure activity.
Incident Response	Documented incident response procedures including severity classification, breach notification within 48 hours, root cause analysis, and post-incident review.
Personnel Security	Background checks conducted for all new hires. Annual GDPR and information security awareness training. Confidentiality obligations in employment agreements.
Data Minimization	Processing limited to what is necessary for the stated purpose. Non-flagged deepfake detection inputs are discarded after analysis. Transient processing for TTS inference and real-time voice agents.
Secure Development	Secure development practices including code review, automated testing, and deployment pipelines with separation of staging and production environments.
Backup and Recovery	Regular database backups with defined retention schedules. GCP Cloud Storage provides built-in data redundancy.
Vendor Management	Data Processing Agreements executed with all Sub-Processors. Sub-Processors assessed and risk-tiered. Annual vendor compliance reviews.