NOVELVOX

Data Processing Agreement (DPA)

Supplement to the NovelVox End User License Agreement (EULA)

Last Updated: March 19, 2026

Version: 1.8

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is entered into between NovelVox ("Processor") and the Client identified in the applicable Purchase Order or Statement of Work ("Controller") and supplements the NovelVox End User License Agreement ("EULA" or "Agreement").

This DPA applies where and to the extent that the Processor processes Personal Data, if any, that is subject to Applicable Data Protection Law on behalf of the Controller in the course of providing the Licensed Product under the Agreement. Capitalized terms not defined in this DPA shall have the meanings given to them in the Agreement.

1. Definitions

"Applicable Data Protection Law" means all laws and regulations relating to data protection, privacy, and the processing of Personal Data that apply to the processing of Personal Data under this DPA, including but not limited to: (a) the EU General Data Protection Regulation 2016/679 ("GDPR"); (b) the UK Data Protection Act 2018 and UK GDPR; (c) the California Consumer Privacy Act ("CCPA") as amended by the California Privacy Rights Act ("CPRA"); (d) India's Digital Personal Data Protection Act, 2023 ("DPDPA"); and (e) any other applicable national, state, or regional data protection legislation, in each case as amended or replaced from time to time.

"Controller" means the Client, as the entity that determines the purposes and means of the processing of Personal Data.

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

"Personal Data" means any information relating to a Data Subject that is processed by the Processor on behalf of the Controller in connection with the Licensed Product, as further described in Annex 1.

"Personal Data Breach" means any 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 by the Processor.

"Processor" means NovelVox, as the entity that processes Personal Data on behalf of the Controller.

"Sub-processor" means any third party engaged by the Processor to process Personal Data on behalf of the Controller in connection with the Licensed Product.

2. Scope and Purpose of Processing

The Processor shall process Personal Data solely for the purpose of providing the Licensed Product to the Controller as described in the Agreement, and in accordance with the Controller's documented instructions. The details of the processing are set forth in Annex 1 to this DPA.

The Processor shall not process Personal Data for any purpose other than as set out in this DPA and the Agreement, unless required to do so by applicable law, in which case the Processor shall inform the Controller of that legal requirement before processing (unless prohibited by law from doing so).

3. Nature of Processing

As described in the Agreement, the Processor processes Personal Data primarily on a transient, in-memory basis for the purpose of routing, parsing, and relaying requests and responses between the Controller's end-user interfaces (including web browsers, IVR systems, IVA platforms, AI engines, or other client-side applications) and the Controller's System of Record (SOR). The Processor may also persistently store certain operational and integration data ("Persistent Operational Data") in a dedicated database where required by the Controller's requirements, as described in Section 6.3(d) of the Agreement. Such data may incidentally contain Personal Data. Operational metadata and logs as described in Section 6.3(c) of the Agreement may also incidentally contain Personal Data (such as identifiers in request headers or error traces).

Cross-Border Access to Operational Metadata: In the course of debugging, root cause analysis (RCA), incident resolution, and ongoing service support, NovelVox's back-office engineering and support teams (which may be located in any jurisdiction globally) may access and transfer operational metadata and logs from Client's AWS region to NovelVox's back-office locations. Such transfers are limited to operational metadata as described in Section 6.3(c) of the Agreement and are subject to the international data transfer safeguards set forth in Section 10 below.

4. Controller Obligations

The Controller shall: (a) ensure that it has a valid legal basis for the processing of Personal Data under Applicable Data Protection Law, including obtaining any necessary consents from Data Subjects; (b) ensure that its instructions to the Processor comply with Applicable Data Protection Law; (c) be solely responsible for the accuracy, quality, and legality of Personal Data provided to or made accessible through the Licensed Product; and (d) provide the Processor with all information and cooperation reasonably necessary for the Processor to fulfil its obligations under this DPA.

5. Processor Obligations

The Processor shall: (a) process Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data, unless required by applicable law (in which case the Processor shall inform the Controller in advance, unless prohibited by law); (b) ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; (c) implement and maintain appropriate technical and organizational security measures as described in Section 7 below; (d) comply with the conditions for engaging Sub-processors set out in Section

6 below; (e) taking into account the nature of the processing, assist the Controller by appropriate technical and organizational measures for the fulfilment of the Controller's obligation to respond to Data Subject requests; (f) assist the Controller in ensuring compliance with its obligations regarding security, breach notification, data protection impact assessments, and prior consultations with supervisory authorities, taking into account the nature of processing and the information available to the Processor; (g) at the Controller's choice, delete or return all Personal Data to the Controller after the end of the provision of the Licensed Product, and delete existing copies unless applicable law requires storage of the Personal Data; and (h) make available to the Controller all information necessary to demonstrate compliance with this DPA and the Processor's obligations under Applicable Data Protection Law.

6. Sub-processors

6.1 Authorized Sub-processors

The Controller acknowledges and agrees that the Processor may engage Sub-processors to process Personal Data on behalf of the Controller. As of the Effective Date, the Processor's authorized Sub-processors are:

Sub-processor	Purpose	Location	Data Processed
Amazon Web Services (AWS)	Cloud infrastructure hosting, compute, storage, CDN	As specified in SOW	All data transiting through the Licensed Product; configuration data in S3

6.2 Notification of Changes

The Processor shall maintain an up-to-date list of Sub-processors on its website or make such list available upon request. The Processor shall notify the Controller of any new or replacement Sub-processor by email or website update at least ten (10) days prior to the new Sub-processor commencing processing of Personal Data. The Controller's continued use of the Licensed Product after such notice period shall constitute acceptance of the new Sub-processor.

6.3 Objection Right

If the Controller has a reasonable, data-protection-related objection to a new Sub-processor, the Controller shall notify the Processor in writing within ten (10) days of receiving notice. The Parties shall work together in good faith to find a mutually acceptable resolution. If no resolution can be reached within thirty (30) days of the objection, either Party may terminate the affected service by providing thirty (30) days' written notice, without prejudice to any fees incurred prior to the effective date of termination.

6.4 Sub-processor Obligations

The Processor shall: (a) impose on each Sub-processor, by way of a written contract, data protection obligations no less protective than those set out in this DPA; (b) remain fully liable to the Controller for the performance of the Sub-processor's obligations; and (c) conduct appropriate due diligence on each Sub-processor prior to engagement.

7. Security Measures

The Processor shall implement and maintain appropriate technical and organizational measures to protect Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, or damage. Such measures shall include, at a minimum:

(a) Encryption of Personal Data in transit using TLS 1.2 or AWS recommended encryption standards;

(b) Encryption of data at rest in S3 buckets using Amazon S3 managed keys (SSE-S3);

(c) Logical and physical isolation of each Controller's cloud environment from other clients;

(d) Access controls ensuring that only authorized personnel can access systems that process Personal Data;

(e) Periodic security testing consistent with industry practice;

(f) Logging and monitoring of access to systems processing Personal Data;

(g) Employee confidentiality obligations and data protection training;

(h) Incident response procedures for detecting, reporting, and responding to Personal Data Breaches.

The Processor shall regularly review and update its security measures to ensure continued effectiveness, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risks to Data Subjects.

8. Personal Data Breach Notification

The Processor shall notify the Controller without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Personal Data Breach. Such notification shall include: (a) a description of the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects and Personal Data records concerned; (b) the name and contact details of the Processor's contact point from whom more information may be obtained; (c) a description of the likely consequences of the Personal Data Breach; and (d) a description of the measures taken or proposed to be taken to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

The Processor shall cooperate with the Controller and take commercially reasonable steps to assist in the investigation, mitigation, and remediation of each Personal Data Breach. The Processor shall not inform any third party of a Personal Data Breach without first consulting with and obtaining the consent of the Controller, unless notification is required by applicable law.

9. Data Subject Rights

The Processor 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 obligation to respond to requests from Data Subjects exercising their rights under Applicable Data Protection Law (including rights of access, rectification, erasure, restriction, portability, and objection).

Given the transient nature of the Processor's data processing (as described in Section 3), the Processor's ability to assist with Data Subject requests may be limited. Where the Processor does not hold or cannot identify the relevant Personal Data, the Processor shall inform the Controller promptly and cooperate to the extent reasonably possible.

If the Processor receives a request directly from a Data Subject, the Processor shall promptly redirect the Data Subject to the Controller and shall notify the Controller of the request, unless prohibited by applicable law.

10. International Data Transfers

10.1 General Restriction

The Processor shall not transfer Personal Data (including Client Data payloads) to a country outside of the country or region specified in the SOW unless: (a) such transfer is necessary for the provision of the Licensed Product (e.g., where the Controller's SOR is located in a different jurisdiction); (b) appropriate safeguards are in place as required by Applicable Data Protection Law; and (c) the Controller has provided prior written consent.

10.2 Operational Metadata Transfers

The Controller acknowledges and agrees that NovelVox's back-office engineering and support teams, which may be located in any jurisdiction globally, may access and transfer operational metadata and logs (as described in Section 6.3(c) of the Agreement) from Client's AWS region for the purposes of debugging, root cause analysis, incident resolution, and service support.

Such operational metadata transfers shall be subject to the following safeguards:

(a) Transfers are limited to operational metadata (request headers, log tokens, debug-mode payloads, error traces) and do not include bulk Client Data payloads under normal operating conditions;

(b) Access is restricted to authorized NovelVox personnel on a need-to-know basis and subject to confidentiality obligations no less protective than those in the Agreement;

(c) Transferred metadata is subject to the same retention limits as set forth in Section 6.3(c) of the Agreement (not exceeding ninety (90) days);

(d) NovelVox shall maintain appropriate technical and organizational measures to protect transferred metadata in transit and at rest at the receiving location;

(e) NovelVox shall maintain a record of back-office locations from which operational metadata may be accessed, and shall make such record available to the Controller upon reasonable request.

10.3 Transfer Mechanisms

Where transfers of Personal Data (including operational metadata that may incidentally contain Personal Data) are made from the European Economic Area (EEA), the United Kingdom, or Switzerland to a country that has not been deemed to provide an adequate level of data protection, the Parties shall ensure that appropriate transfer mechanisms are in place, which may include: (i) the European Commission's Standard Contractual Clauses (SCCs) as applicable; (ii) the UK International Data Transfer Agreement or Addendum; or (iii) any other transfer mechanism approved under Applicable Data Protection Law. The applicable transfer mechanism shall be specified in the SOW or executed separately between the Parties.

11. Audit Rights

The Processor shall satisfy the Controller's audit requirements by providing, upon reasonable request and subject to reasonable confidentiality obligations:

(a) Security documentation describing the Processor's technical and organizational measures;

(b) Responses to a reasonable data protection and security questionnaire provided by the Controller;

(c) A summary of the Processor's most recent SOC 2 Type II report or equivalent independent third-party audit report, where available.

Such documentation shall be provided no more than once per twelve (12) month period, unless a Personal Data Breach has occurred or a supervisory authority requires additional information.

On-Site Audits: On-site audits of the Processor's facilities or systems shall only be permitted where expressly required by Applicable Data Protection Law or by order of a competent supervisory authority. Any such on-site audit shall be conducted at the Controller's sole expense, upon at least thirty (30) days' prior written notice, during normal business hours, and in a manner that does not unreasonably disrupt the Processor's operations. The Controller shall ensure that any auditor is bound by appropriate confidentiality obligations.

12. Data Retention and Deletion

Given that the Processor processes Personal Data primarily on a transient basis (as described in Section 3), transient Personal Data is not retained beyond the duration of each request-response cycle under normal operating conditions. Where Persistent Operational Data is stored as described in Section 6.3(d) of the Agreement, such data is retained for the duration of the Subscription Term and deleted within thirty (30) days of termination unless the Controller requests an export.

With respect to operational metadata and logs that may incidentally contain Personal Data (as described in Section 6.3(c) of the Agreement): (a) such data shall be retained for no longer than ninety (90) days unless a longer period is required for an ongoing incident investigation; and (b) upon expiration of the retention period, such data shall be permanently deleted or anonymized.

Upon termination of the Licensed Product, the Processor shall delete all Personal Data (including any incidental Personal Data in logs) in accordance with the termination provisions of the Agreement. The Processor shall certify such deletion in writing upon the Controller's request.

13. Liability

Each Party's liability under this DPA shall be subject to the limitations of liability set forth in the Agreement. Nothing in this DPA shall limit either Party's liability with respect to any rights of Data Subjects under Applicable Data Protection Law.

14. Term and Survival

This DPA shall remain in effect for the duration of the Agreement and the Processor's processing of Personal Data on behalf of the Controller. The obligations of the Processor under this DPA shall survive the termination or expiration of the Agreement to the extent and for the duration necessary for the Processor to complete the deletion of Personal Data in accordance with Section 12.

15. Relationship to the Agreement and Effectiveness

This DPA is incorporated into and forms part of the EULA and becomes effective upon execution of the applicable Purchase Order or the Client's use of the Licensed Product, whichever occurs first. No separate signature or execution of this DPA is required for it to take effect.

In the event of a conflict between this DPA and the Agreement, this DPA shall prevail with respect to the processing of Personal Data. All other terms of the Agreement remain in full force and effect.

ANNEX 1

Details of Processing

Element	Description
Subject Matter of Processing	Processing of Personal Data as necessary to provide the Licensed Product under the Agreement, including routing, parsing, and relaying requests and responses between the Controller's end-user interfaces (including web browsers, IVR, IVA, AI engines, or other client-side systems) and the Controller's System of Record (SOR).
Duration of Processing	For the term of the Agreement, plus any period required for data deletion in accordance with Section 12.
Nature of Processing	Primarily transient, in-memory processing for the purpose of request routing and response parsing. Persistent storage of operational and integration data (such as interaction history, SOR mappings, user tokens, and related records) in a dedicated database where required by the Controller's configuration. Incidental capture of operational metadata in logs.
Purpose of Processing	To provide the Licensed Product, including: (a) routing end-user requests to the Controller's SOR; (b) parsing and relaying SOR responses to end-users; (c) operational monitoring, debugging, root cause analysis, and error resolution (which may involve cross-border access to operational metadata by NovelVox back-office teams as described in Section 10.2); and (d) service improvement through anonymized, aggregated analytics.
Categories of Data Subjects	End-users of the Controller (e.g., the Controller's employees, agents, customers, or other individuals who interact with the Licensed Product). The specific categories depend on the Controller's use case and SOR configuration.
Types of Personal Data	As determined by the Controller's SOR and use case, which may include but is not limited to: names, email addresses, phone numbers, account identifiers, customer records, interaction history, IP addresses, session identifiers, call metadata, and system-generated identifiers. The Processor does not control the types of Personal Data transmitted through the Licensed Product.
Sensitive / Special Category Data	The Controller shall not transmit sensitive or special category Personal Data (as defined under Applicable Data Protection Law) through the Licensed Product unless: (a) the Controller has obtained all necessary consents and legal bases; (b) the Controller has notified the Processor in writing; and (c) additional safeguards have been agreed upon in writing between the Parties.

End of NovelVox Data Processing Agreement v1.8