NOVELVOX

Product Privacy Policy

Applicable to NovelVox Products and Services

Last Updated: March 19, 2026

Version: 1.6

1. Introduction

This Product Privacy Policy ("Policy") describes how NovelVox and its affiliates ("NovelVox," "we," "us," or "our") handle data in connection with the NovelVox products and services ("Licensed Product") provided to our customers ("Clients") and used by their authorized end-users ("End-Users").

Scope: This Policy applies to data processed through the NovelVox Licensed Product across all deployment models: On-Premises, Private Cloud, and NovelVox Cloud. This Policy does not cover the NovelVox corporate website or marketing activities, which are governed by a separate website privacy policy.

Relationship to the EULA: This Policy supplements and should be read together with the NovelVox End User License Agreement (EULA) and, where applicable, the NovelVox Data Processing Agreement (DPA), which is available upon request. In the event of a conflict between this Policy and the EULA or DPA, the EULA and DPA shall prevail.

Our Role: NovelVox provides the Licensed Product as a service to Clients. The Client determines what data is processed through the Licensed Product and is the data controller (or equivalent under applicable law) for such data. NovelVox acts as a data processor on behalf of the Client. This Policy describes how NovelVox handles data in its capacity as a processor and service provider.

2. How the Licensed Product Works

Understanding how the Licensed Product processes data requires understanding its architecture. The Licensed Product operates primarily as a communication and integration layer that connects Client's End-Users with Client's backend systems.

2.1 Stateless Architecture

The Licensed Product processes data primarily on a transient, in-memory basis. The core request-response cycle operates as follows:

(a) A request is initiated from the Client's end-user interface (which may be a web browser, IVR system, IVA platform, AI engine, or other client-side application);

(b) The Licensed Product routes the End-User's request to the Client's designated System of Record (SOR) — such as a CRM, contact center platform, or other backend system;

(c) The Client's SOR processes the request and returns a response;

(d) The Licensed Product parses the response and delivers it to the originating end-user interface;

(e) Once the request-response cycle is complete, the data is purged from memory.

Key principle: NovelVox does not access, inspect, or analyze Client Data except as strictly necessary to route, parse, and relay requests and responses. Client Data flowing through the request-response cycle is processed transiently in memory and is purged upon completion of each cycle. Where required by the Client's requirements, certain operational and integration data may be stored persistently as described in Section 3.3 below.

2.2 Deployment Models

The data handling practices described in this Policy vary depending on the deployment model:

Deployment Model	Where Data Is Processed	Who Controls Infrastructure
On-Premises	On Client's own servers and infrastructure	Client is solely responsible for infrastructure, security, and data protection
Private Cloud	On a cloud instance dedicated to Client	Shared responsibility as defined in the SOW
NovelVox Cloud	On NovelVox's cloud infrastructure (AWS), with dedicated, isolated resources per Client	NovelVox manages cloud infrastructure; Client manages SOR and end-user access

The remainder of this Policy focuses primarily on the NovelVox Cloud deployment model, as this is where NovelVox has the most direct involvement in data processing. For On-Premises and Private Cloud deployments, the Client is primarily responsible for data handling, and this Policy applies only to the extent NovelVox accesses or processes data in the course of providing support or maintenance services.

3. What Data We Process

NovelVox processes two categories of data in connection with the Licensed Product:

3.1 Client Data (Transient)

Client Data is any data that flows through the Licensed Product during a request-response cycle between the end-user interface (web browser, IVR, IVA, AI engine, or other client-side system) and the Client's System of Record. This may include, depending on the Client's use case and SOR configuration:

(a) Customer names, email addresses, phone numbers, and account identifiers;

(b) Interaction history and case details;

(c) Any other data retrieved from or sent to the Client's SOR.

How we handle Client Data: Client Data flowing through the request-response cycle is processed only transiently and in memory. It is purged from memory upon completion of each request-response cycle. NovelVox does not control what Client Data flows through the product — this is determined entirely by the Client's SOR configuration and use case. Where required by the Client's requirements, certain data may also be stored persistently as described in Section 3.3.

3.2 Operational Metadata (Retained)

In the course of operating and supporting the Licensed Product, NovelVox collects and retains limited operational metadata. This metadata may incidentally contain personal data (such as identifiers in request headers). The categories of operational metadata are:

Category	Examples	Purpose
Request Headers	User-agent, content-type, timestamps, request identifiers, IP addresses	Performance monitoring, debugging, security
Authentication Tokens	Session tokens, log tokens in log files	Security monitoring, access auditing
Debug Payloads	Request and response payloads captured when debug mode is explicitly enabled	Diagnosing specific issues; time-limited and disabled upon resolution
Error Traces	Stack traces, error messages, diagnostic data from monitoring tools	Root cause analysis, error resolution, service improvement

Retention: Operational metadata is retained for no longer than ninety (90) days, unless a longer period is required for an ongoing incident investigation. Upon expiration of the retention period, metadata is permanently deleted or anonymized.

3.3 Persistent Operational Data (Where Applicable)

Where required by the Client's requirements, NovelVox may persistently store certain operational and integration data in a dedicated database on behalf of the Client. The type and scope of this data varies by Client and may include: customer interaction history, SOR ID mappings, user tokens, SOR scores, phonebook data, account-to-phone-number mappings, quick links, call resolution data, and call recording mappings.

Sensitive credentials (such as SOR usernames and passwords) are stored in encrypted format using AWS managed encryption services. This data is stored in a database that is, by default, dedicated and isolated per Client. It is used solely for the purpose of providing the Licensed Product functionality and is accessible only to authorized NovelVox personnel and the Client's Authorized Users. Upon termination of the Client's subscription, this data is deleted within thirty (30) days of the data export period, as described in Section 8.3.

4. How We Use Data

NovelVox uses data processed through the Licensed Product only for the following purposes:

4.1 Service Delivery

Routing, parsing, and relaying requests and responses between End-Users and Client's System of Record. This is the core function of the Licensed Product and involves only transient, in-memory processing.

4.2 Operational Support

Debugging, performance monitoring, root cause analysis (RCA), incident resolution, and ongoing service support. This involves the operational metadata described in Section 3.2.

4.3 Security

Detecting, preventing, and responding to security threats, unauthorized access, fraud, and other malicious activity.

4.4 Service Improvement

Improving and enhancing the quality and performance of the Licensed Product through anonymized, aggregated analytics. NovelVox does not use Client Data or identifiable personal data for this purpose.

What we do NOT do with data: NovelVox does not sell, rent, or share Client Data or End-User data with third parties for marketing, advertising, or any purpose unrelated to the provision of the Licensed Product. NovelVox does not use Client Data to build profiles of End-Users, train machine learning models, or for any purpose beyond what is described in this Policy and the EULA.

5. Who We Share Data With

NovelVox shares data only in the following limited circumstances:

5.1 Cloud Infrastructure Provider

For NovelVox Cloud deployments, Client Data transits through Amazon Web Services (AWS) infrastructure. AWS acts as a sub-processor. Each Client receives dedicated, isolated cloud resources (S3 bucket, CloudFront distribution, security controls). AWS processes data in the region specified in the Client's SOW.

5.2 NovelVox Personnel

NovelVox's engineering and support teams may access operational metadata for debugging, root cause analysis, and incident resolution. These teams may be located in any jurisdiction globally. Access is restricted to authorized personnel on a need-to-know basis, and all personnel are subject to confidentiality obligations.

5.3 Sub-processors

NovelVox may engage additional sub-processors in connection with the Licensed Product. Any sub-processor is bound by data protection obligations no less protective than those in the EULA. NovelVox maintains a list of sub-processors and notifies Clients of material changes in accordance with the EULA.

5.4 Legal Requirements

NovelVox may disclose data to the extent required by applicable law, regulation, legal process, or governmental request. Where legally permitted, NovelVox will notify the Client before making such disclosure.

No other sharing: NovelVox does not share Client Data or End-User personal data with any other third parties.

6. Data Security

NovelVox implements and maintains commercially reasonable security measures consistent with industry standards to protect data processed through the Licensed Product.

6.1 Encryption

(a) All data in transit between the end-user interface and NovelVox's cloud infrastructure, and between NovelVox's cloud infrastructure and Client's SOR, is encrypted using TLS 1.2 or AWS recommended encryption standards.

(b) Data at rest in Client's dedicated S3 bucket is encrypted using Amazon S3 managed keys (SSE-S3).

6.2 Tenant Isolation

Each Client's cloud environment is logically and physically isolated from other Clients. Each Client receives a dedicated S3 storage bucket, dedicated security controls, and a dedicated CloudFront distribution. Access controls ensure no Client can access another Client's resources or data.

6.3 Access Controls

Access to systems that process data is restricted to authorized NovelVox personnel on a need-to-know basis. All personnel with access are subject to confidentiality obligations and data protection training.

6.4 Security Testing and Monitoring

NovelVox performs periodic security testing consistent with industry practice, maintains logging and monitoring of security events, and conducts regular security patching of infrastructure and application components.

6.5 Incident Response

NovelVox maintains incident response procedures for detecting, reporting, and responding to security breaches. In the event of a confirmed security breach affecting Client Data, NovelVox will notify the Client without undue delay and in any event within seventy-two (72) hours of becoming aware of the breach, as detailed in Section 6 of the EULA.

7. International Data Transfers

7.1 Client Data

Client Data processed through the NovelVox Cloud remains within the AWS region specified in the Client's SOW. NovelVox does not transfer Client Data to a different region without the Client's prior written consent, except where necessary for disaster recovery.

7.2 Operational Metadata

Operational metadata and logs may be accessed by NovelVox engineering and support teams located in any jurisdiction globally for the purposes of debugging, root cause analysis, and incident resolution. Such access is subject to the safeguards described in the EULA, including need-to-know access restrictions, confidentiality obligations, retention limits, and appropriate technical and organizational measures.

7.3 Transfer Safeguards

Where transfers of 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 jurisdiction that has not been deemed to provide an adequate level of data protection, NovelVox ensures appropriate transfer mechanisms are in place, which may include the

European Commission's Standard Contractual Clauses (SCCs), the UK International Data Transfer Agreement or Addendum, or other approved mechanisms.

8. Data Retention

8.1 Client Data

Client Data flowing through the request-response cycle is not retained by NovelVox. It is processed transiently in memory and purged upon completion of each request-response cycle. Where Persistent Operational Data is stored (as described in Section 3.3), such data is retained for the duration of the Client's subscription and deleted in accordance with Section 8.3.

8.2 Operational Metadata

Operational metadata (as described in Section 3.2) is retained for no longer than ninety (90) days, unless a longer period is required for an ongoing incident investigation. Debug-mode payloads are retained only for the duration of the specific debugging session and are deleted promptly upon resolution of the issue.

8.3 Upon Termination

Upon termination of a Client's subscription: (a) the Client has thirty (30) days to export any configuration data, Persistent Operational Data, and artifacts from their dedicated S3 bucket and database; (b) NovelVox permanently deletes all Client-specific configuration data, Persistent Operational Data, access credentials, and cloud resource allocations; (c) NovelVox provides written confirmation of deletion upon request.

9. End-User Rights

End-Users of the Licensed Product may have rights under applicable data protection laws, including rights of access, rectification, erasure, restriction, portability, and objection.

How to exercise rights: Because NovelVox processes data on behalf of the Client (as a data processor), End-Users should direct any data rights requests to the Client (who is the data controller). NovelVox will assist the Client in responding to such requests to the extent required by the EULA.

Limitations: Due to the primarily transient nature of NovelVox's data processing, NovelVox's ability to identify, access, or modify specific End-User data is limited. Transient Client Data is not stored by NovelVox, and operational metadata may not contain sufficient information to identify specific individuals. Where Persistent Operational Data is stored, NovelVox will assist the Client in responding to data rights requests to the extent the relevant data can be identified. Where NovelVox receives a data rights request directly from an End-User, NovelVox will promptly redirect the End-User to the Client.

10. Sensitive and Special Category Data

NovelVox does not control what data flows through the Licensed Product — this is determined by the Client's SOR and use case. However, Clients operating in regulated industries (such as healthcare, financial services, or government) should be aware of the following:

(a) Clients should not transmit sensitive or special category personal data (as defined under applicable data protection law) through the Licensed Product unless they have obtained all necessary consents and legal bases and have notified NovelVox in writing.

(b) The Licensed Product's architecture means that sensitive data transiting through the request-response cycle is processed only in memory and is not persistently stored. However, where Persistent Operational Data is stored (Section 3.3), it may contain sensitive information depending on the Client's configuration. Operational metadata captured during processing may also incidentally contain fragments of sensitive data (for example, in error traces).

(c) Clients are solely responsible for ensuring that their use of the Licensed Product complies with applicable industry-specific regulations (such as HIPAA, PCI-DSS, or equivalent).

11. Children's Data

The Licensed Product is a business-to-business service provided to enterprise Clients. It is not directed at or intended for use by children under the age of 16 (or the applicable age of consent in the relevant jurisdiction). NovelVox does not knowingly process personal data of children through the Licensed Product. If NovelVox becomes aware that children's personal data is being processed through the Licensed Product, NovelVox will notify the Client promptly so that the Client can take appropriate action.

12. Cookies and Tracking Technologies

Where the Licensed Product is accessed via a web browser, it may use cookies or similar technologies strictly for the purpose of session management, authentication, and security. The Licensed Product does not use cookies or tracking technologies for advertising, analytics, or profiling purposes. Any cookies used are functional/essential cookies required for the service to operate.

Where the Licensed Product is accessed via non-browser interfaces (such as IVR, IVA, AI engines, or other automated systems), cookies are not applicable. Authentication and session management for such interfaces are handled through API tokens, session identifiers, or other mechanisms as specified in the Documentation.

The Client is responsible for informing its End-Users about the use of cookies or similar technologies in accordance with applicable law.

13. AI and Automation Use

The Licensed Product may be used by the Client in conjunction with automated systems, scripts, bots, or artificial intelligence agents. NovelVox does not control or determine the actions executed by such systems and processes data solely as required to transmit requests and responses between connected systems.

NovelVox makes no representations or warranties regarding the accuracy, reliability, or appropriateness of outputs generated by any automated system or AI agent that interacts with

the Licensed Product. The Client is solely responsible for: (a) the configuration, deployment, and governance of any automated systems or AI agents that interact with the Licensed Product; (b) ensuring that any such systems comply with applicable laws and regulations; and (c) any decisions made or actions taken based on outputs generated through such automated interactions.

14. Legal Basis for Processing (EEA/UK)

Where the GDPR or UK GDPR applies, NovelVox processes personal data on the following legal bases:

Processing Activity	Legal Basis	Details
Service delivery (transient processing of Client Data)	Performance of contract	Processing is necessary to perform the EULA and provide the Licensed Product to the Client
Operational metadata collection and retention	Legitimate interest	Necessary for debugging, security, and maintaining the service; balanced against minimal privacy impact given the technical nature of the data
Security monitoring and incident response	Legitimate interest / legal obligation	Necessary to protect the security of the Licensed Product and to comply with applicable security and breach notification laws
Service improvement (anonymized, aggregated)	Legitimate interest	Anonymized data is not personal data; where aggregation occurs prior to anonymization, legitimate interest applies

Note: The Client, as data controller, is responsible for establishing its own legal basis for processing personal data through the Licensed Product, including obtaining any necessary consents from End-Users.

15. Client's Privacy Obligations

As described in the EULA, the Client (as data controller) is responsible for:

(a) Determining the legal basis for processing personal data through the Licensed Product;

(b) Providing appropriate privacy notices to End-Users regarding the processing of their personal data;

(c) Obtaining any necessary consents from End-Users;

(d) Ensuring that personal data transmitted through the Licensed Product is accurate, lawful, and collected in accordance with applicable law;

(e) Responding to data subject rights requests from End-Users;

(f) Notifying End-Users and relevant supervisory authorities of data breaches to the extent required by applicable law (NovelVox will notify the Client of breaches as described in Section 6.5);

(g) Ensuring that any sensitive or special category data transmitted through the Licensed Product is handled in accordance with Section 10 of this Policy and the EULA.

16. Changes to This Policy

NovelVox may update this Policy from time to time to reflect changes in our practices, technology, legal requirements, or other factors. When we make material changes, we will notify Clients through reasonable means, which may include email notification, notice through the Licensed Product, or posting an updated version on our website. The "Last Updated" date at the top of this Policy indicates when it was last revised.

Continued use of the Licensed Product after the effective date of any changes constitutes acceptance of the updated Policy. If a Client does not agree with the changes, the Client may terminate the applicable subscription in accordance with the EULA.

17. Contact Information

For questions about this Policy or NovelVox's data handling practices, please contact:

Email: privacy@novelvox.com

NovelVox NA INC

760 Old Roswell Road, Suite 392, Roswell, GA 30076, USA

NovelVox Softwares India Pvt. Ltd.

609-610, 6th Floor, SSR Corporate Park, Faridabad 121003, Haryana, India

For data protection inquiries specifically related to GDPR or UK GDPR, please contact our designated data protection contact at the email address above.

End of NovelVox Product Privacy Policy v1.6