Navu Sensitive Data Management

Overview

Navu is committed to protecting the privacy and security of the personally identifiable information (PII) we collect on behalf of our customers. As a SaaS provider serving B2B companies, we collect visitor names and email addresses through our platform and ensure that this data is handled in accordance with strict privacy and data management practices.

This document outlines our policies regarding the deletion of customer data, both upon termination of service and upon request as well details about the third party processors in Navu's system that have access to PII.

Data Deletion Upon Termination of Service

When a customer terminates their use of Navu's services through cancellation of their subscription or through termination of a trial. Navu initiates a standard data deletion procedure designed to protect sensitive information while allowing a brief window for reactivation or retrieval.

Procedure Overview:

- **Deletion Timeline:** All customer data, including any PII collected through the customer's use of the platform, is scheduled for deletion within **30 days** following the effective date of service termination.
- **Scope of Deletion:** This includes all data associated with the customer's account, such as visitor logs, email addresses, names, analytics, and configuration data.
- **Data Retention Buffer:** The 30-day period serves as a buffer to allow the customer to reactivate their account or request data retrieval. After this period, data is permanently deleted and is unrecoverable.
- **Secure Deletion:** All deletions are performed using secure industry-standard practices to ensure complete removal of data from Navu's live system.
- **Monitoring:** Navu's admin dashboard lists all active sites and their current status. This dashboard is monitored and sites are deleted within 30 days after their service is terminated.

Data Deletion Upon Request

Navu recognizes that customers may, at times, request the deletion of their data prior to or independently of account termination. In accordance with data privacy best practices and compliance frameworks, we honor such requests promptly.

Policy Overview:

- **Request Process:** As documented in Navu's Privacy Policy, Customers may submit a data deletion request by email at contact@navu.co. Identity verification may be required to ensure data is not deleted without proper authorization.
- **Processing Timeline:** Data deletion requests are typically fulfilled within **7 business days** of receipt and verification.
- **Scope of Deletion:** Upon confirmation, Navu will delete all specified customer data from production systems, including PII collected from visitors.
- **Confirmation:** Upon successful completion of the deletion process, Navu will provide written confirmation to the customer.

Third-Party Data Processors

To support core functionality, ensure service reliability, and deliver intelligent insights to our customers, Navu relies on a curated set of third-party processors. These processors may handle or access personally identifiable information (PII) strictly for the purpose of fulfilling their designated roles within the Navu ecosystem. All processors are contractually obligated to adhere to industry-standard security practices and data protection regulations, including but not limited to GDPR and CCPA.

Third-Party Processor Overview:

Processor	Function	Access to PII	User Configurable
Amazon AWS	Email delivery, data backups & infrastructure	Yes	No
Stripe	Payment processing	Yes	No
Google	Oauth-based user authentication	Yes	Yes
IPData	Reverse IP lookup for visitor attribution	IP address only	Yes
OpenAI	LLM for AI-powered Retrieval-Augmented Generation (RAG) services	Potentially	Yes

Gemini	LLM for AI-powered Retrieval-Augmented Generation (RAG) services	Potentially	Yes
Claude	LLM for AI-powered analysis and report generation	Potentially	Yes
Slack	Internal system alerts and notifications	Yes	No
Helpscout	Customer support issue tracking	Potentially	No

Each processor is evaluated periodically for security and compliance. Sensitive data processed by these services is encrypted both in transit and at rest when applicable. Note that Navu's AI subprocessors do not use Navu collected information for their training purposes per their standard terms of service.

Customer-Configurable Integrations

In addition to core processors, Navu enables users to optionally connect their own systems via secure API key-based integrations. Access is controlled by the user's configured permissions and limited to the scope necessary for functionality.

Integration	Description	Access Control
HubSpot	CRM integration for syncing leads and engagement	User API key (scoped)
Salesforce	CRM integration for syncing contact data	User API key (scoped)
Slack	Sends event data to customer Slack channels	User API key (scoped)
Microsoft	Enables syncing with Outlook and Teams	User API key (scoped)
Zendesk	Customer support integration	User API key (scoped)

All user-configured integrations operate strictly within the permission bounds of the tokens or

credentials provided by the customer. Navu does not retain credentials beyond their active use and revocation is supported at any time by the user.