NOTRE BOUSSOLE

Data Retention and Secure Disposal Policy

Plaid Production Submission

Effective date: July 1, 2026 | Version 1.0

Organization: Notre Boussole | Application: notreboussole.app

Policy owner

Privacy & Security Lead

Production control standard

This policy defines mandatory controls for Notre Boussole. Plaid production access must not be enabled until the Plaid-specific controls in this policy are implemented and verified.

Confidentiality: Internal policy; may be provided to Plaid and other authorized reviewers.

Document control

Policy title	Data Retention and Secure Disposal Policy
Effective date	July 1, 2026
Version	1.0
Policy owner	Privacy & Security Lead
Review cycle	At least annually and whenever a material data practice, provider, or Plaid product changes
Contact	security@notreboussole.app
Related notice	https://notreboussole.app/privacy

1. Purpose

This policy establishes how Notre Boussole identifies, retains, archives, deletes, and securely disposes of personal data. It covers consumer information, sensitive relationship and health-related content, and financial data obtained through Plaid or supplied directly by users.

The policy is designed to ensure that personal data is kept only for a defined business, security, legal, or user-requested purpose; is protected throughout its lifecycle; and is deleted or de-identified when that purpose ends.

2. Scope

This policy applies to all Notre Boussole production and support environments, employees and contractors with authorized access, and service providers processing data on Notre Boussole's behalf. It includes:

- Account, profile, authentication, and couple-workspace data.
- Relationship content, goals, memories, health, faith, intimacy, and other sensitive free-text or uploaded content.
- Manual financial data, CSV imports, and normalized data obtained through Plaid.
- Plaid access tokens, Item and account identifiers, consent and connection metadata, and webhook records.
- Application, security, audit, support, billing, and deletion records.
- Copies held in primary databases, object storage, temporary processing locations, logs, and backups.

3. Core retention principles

Purpose limitation: Data is retained only for the disclosed service, security, legal, or user-requested purpose.

Data minimization: Notre Boussole does not retain raw financial credentials, unnecessary raw provider responses, or full account and routing numbers for the Financial Compass use case.

Defined limits: Each data category has a documented retention period or a documented event that ends retention.

User control: Users can disconnect financial institutions and request deletion through available in-app controls or by contacting security@notreboussole.app.

Secure deletion: Deletion includes the production database, object storage, temporary files, provider access, and downstream processors where applicable.

Restricted exceptions: Legal holds and security exceptions are narrow, documented, access-restricted, and reviewed.

Verifiability: Deletion and retention jobs are logged and periodically tested without placing sensitive content into operational logs.

4. Roles and responsibilities

Privacy & Security Lead: Owns this policy, approves exceptions, reviews the retention schedule, coordinates privacy requests, and verifies that external notices match actual practice.

Engineering: Implements lifecycle fields, deletion workflows, token revocation, purge jobs, logging controls, and backup-aware deletion procedures.

Support and Operations: Verifies request identity, avoids collecting unnecessary sensitive data, and escalates deletion or legal-hold requests.

Authorized administrators: Access retained data only when needed for approved support, security, or legal functions and may not bypass retention controls.

Service providers: Must be contractually limited to processing for Notre Boussole and must support deletion or return of data when instructed, subject to documented backup cycles and legal obligations.

5. Data lifecycle states

Trigger	Required action	Target completion
Active	Data is available for the user-facing service and protected by authentication, authorization, and least-privilege access controls.	For the period in the retention schedule
Soft-deleted	Data is no longer displayed or used for ordinary service functions and is queued for permanent deletion.	Normally no more than 30 days
Permanently deleted	Records and objects are removed from active production systems and cannot be restored through normal application functions.	At the end of the deletion window
Backup-only	Deleted data may remain temporarily in encrypted provider backups until normal rotation. It is not used or selectively restored.	No more than the configured backup cycle
Legal hold	Deletion is paused only for specifically identified data required for a legal, fraud, security, or dispute purpose.	Until the documented hold is released
De-identified	Data is transformed so it cannot reasonably be linked to a person or couple and is protected against re-identification.	May be retained longer or indefinitely

6. Retention schedule

The periods below are maximum operational defaults unless a shorter period is required by a user request, consent withdrawal, product configuration, contract, or law. Data subject to a documented legal hold is governed by Section 11.

Data category	Active retention	Deletion / archive rule	Operational notes
Account, profile, and authentication data	While the account is active	30-day account-deletion window, then permanent purge	A minimal deletion receipt may be retained as described below.
Couple workspace content, goals, memories, and relationship records	While the account and relevant shared workspace are active	30 days after deletion request or workspace termination	Deletion must respect ownership and must not allow one partner to silently erase the other partner's independently owned private data.
Sensitive health, faith, intimacy, and free-text content	Only while needed for enabled features and valid consent	Delete after feature deletion, consent-based deletion request, or account purge	No secondary use after consent withdrawal. A minimal consent record may remain.
Photos, documents, and attachments	While active and user-selected	30 days after deletion request; temporary derivatives deleted with source	Access-controlled object storage; purge thumbnails and generated variants.
Manual financial accounts, balances, debts, goals, and transactions	While the Finance feature or account is active	30 days after user deletion or account deletion	Shared financial records follow ownership and couple-sharing rules.
Normalized Plaid financial data	While the user maintains the connection or affirmatively retains imported history	Delete within 30 days after disconnect unless the user expressly chooses to keep a historical copy; delete on account purge	Includes account metadata, balances, transactions, liabilities, and investments only for activated Plaid products.
Plaid access tokens	Only while the Item is connected	Revoke and delete immediately on confirmed disconnect or account deletion; automated retries completed within 24 hours	Server-only; encrypted; never returned to client code or written to application logs.
Plaid Item/account identifiers and connection metadata	While connected and for short-term troubleshooting	Delete or irreversibly pseudonymize within 30 days after disconnect	A non-sensitive event receipt may be retained for audit and billing reconciliation.

Data category	Active retention	Deletion / archive rule	Operational notes
Raw Plaid API responses	Transient processing only	Not retained after normalization; queued payloads expire within 24 hours	Do not place raw payloads in logs or analytics.
Raw CSV and financial file uploads	Temporary import processing	Delete immediately after successful or failed processing; maximum 24 hours	Retain only normalized records and import counts, not the source file.
AI prompts and outputs	Only when the user initiates an AI feature and consents	Application copies follow the underlying content retention; transient payloads follow processor contract	No Plaid access tokens or bank credentials may be sent to AI providers.
Consent and privacy preference records	While active	Minimal consent event record retained for up to 6 years after withdrawal or account closure	Retain only what is needed to show the consent state, date, notice version, and action.
Security and authentication logs	Rolling security window	90 days, unless linked to an active incident	Do not log message bodies, financial payloads, tokens, or full identifiers.
Application/runtime logs	Short operational window	30 days maximum	Production logging must be structured and privacy-filtered. Provider plan may retain less.
Finance and privacy audit events	While active	24 months after the event	Append-only event metadata; no raw tokens, credentials, or transaction descriptions.

Data category	Active retention	Deletion / archive rule	Operational notes
Support communications	While ticket is active	24 months after closure	Delete or redact unnecessary attachments and sensitive content earlier.
Billing, tax, and accounting records	For active billing and statutory needs	Up to 7 years after the transaction or account closure	Payment-card details are handled by the payment provider and are not stored by Notre Boussole.
Deletion request records	During request handling	Minimal receipt retained for up to 6 years	May include request date, verification result, scope, completion date, and systems affected; not deleted content.
Backups	Rolling disaster-recovery cycle	Maximum 30 days unless a documented provider configuration requires less	Deleted data is not restored for ordinary use. If a backup is restored, deletion queues must be replayed.
Irreversibly de-identified analytics	As needed for service reliability and aggregate insights	May be retained indefinitely	Must not be reasonably linkable to a person, account, household, or couple and may not be re-identified.

7. Plaid-specific retention and disposal controls

Read-only financial connectivity

Notre Boussole uses Plaid to retrieve only the financial data needed for user-authorized Financial Compass features. Notre Boussole does not use Plaid to move money and does not store online-banking usernames, passwords, or multifactor-authentication codes.

7.1 Data collection and minimization

- Only Plaid products and account types required for the disclosed use case may be requested in Link.
- The application stores normalized fields needed to display accounts, balances, transactions, liabilities, investments, categorization, goals, and cash-flow insights when those products are enabled.
- Full account and routing numbers are not collected or retained for the read-only Financial Compass use case. Only masked identifiers may be displayed.
- Raw Plaid responses are processed server-side and are not retained after normalization except for short-lived, encrypted retry queues with a maximum lifetime of 24 hours.
- Plaid-derived data may not be sold, used for cross-context behavioral advertising, or used for a purpose the user did not authorize.

7.2 Token and secret handling

- Plaid access tokens and secrets are server-side only and are never exposed to the browser, mobile client, analytics tools, support interfaces, or production logs.
- Access tokens are encrypted using authenticated encryption. The encryption key is stored separately from the database in the production secret-management environment.
- Access is limited to the minimum production service role required for Plaid synchronization and revocation.
- A compromised token is rotated or invalidated, affected sessions are investigated, and the event is handled under the incident-response process.
- The application retains the access token needed to call /item/remove for as long as the Item is active, then deletes the token after revocation is confirmed or after documented retry exhaustion.

7.3 Disconnect, revocation, and permission withdrawal

When a user disconnects an institution, deletes the connected account, revokes permission through an institution or Plaid control, or deletes their Notre Boussole account, Notre Boussole must:

- Stop scheduled synchronization and reject new sync work for the connection.
- Call Plaid /item/remove when an active Item can be removed.
- Delete the encrypted access token and sensitive connection secrets immediately after successful revocation, or retry for up to 24 hours while the token remains inaccessible to users and ordinary application processes.
- Delete pending raw webhook or response payloads associated with the Item.
- Delete normalized Plaid data within 30 days unless the user affirmatively elects to retain a historical copy as ordinary Finance data.
- Record a minimal, non-sensitive audit event showing that disconnection and deletion actions occurred.

7.4 Consent expiration and reconnection

Where an institution or Plaid connection requires renewed consent, Notre Boussole must suspend unavailable data access, present a reconnect or update flow, and avoid retaining a token for an inactive connection longer than necessary. Reconnection does not revive data previously deleted under this policy.

8. User deletion and account-closure procedure

Deletion requests may be initiated through available in-app controls or by contacting security@notreboussole.app. Notre Boussole must use a process proportionate to the sensitivity of the requested data and must not require more information than necessary to verify the requester.

Trigger	Required action	Target completion
Finance account deletion	Show a deletion preview, remove the selected data from active views, queue permanent purge, and preserve only permitted audit metadata.	Active removal promptly; purge within 30 days
Plaid disconnect	Stop sync, call /item/remove, delete the encrypted token, clear pending payloads, and apply the user's choice to retain or delete normalized history.	Token revocation/deletion immediately; retries within 24 hours
Account deletion	Disable access, begin the 30-day deletion window, delete private data, resolve ownership of shared records, instruct processors, and complete purge.	Complete within 30 days after the cooling-off window begins
Consent withdrawal	Stop the consent-dependent processing and prevent new data from entering that workflow. Delete associated data when requested or required.	Processing stops promptly
Provider or institution revocation notice	Suspend access, delete pending data, and remove associated Plaid data unless a valid user instruction supports retention as historical data.	Promptly; maximum 30 days for normalized data

9. Secure disposal methods

Disposal must be appropriate to the storage medium and data type. Approved methods include:

- Database hard deletion or cryptographic deletion from active tables after the soft-delete period.
- Deletion of objects, thumbnails, and generated derivatives from access-controlled storage.
- Revocation of provider access followed by deletion of encrypted access tokens and connection secrets.
- Immediate removal of temporary uploads, retry payloads, and import work files after processing.
- Expiration through documented backup rotation; no selective use of deleted records from backups.
- Secure media destruction or provider-certified sanitization when physical storage media are retired.
- Irreversible de-identification when aggregate information is retained beyond the identifiable-data period.

10. Backups and disaster recovery

Production backups are encrypted and retained only for the configured disaster-recovery cycle, which must not exceed 30 days under this policy. Backups are not queried for product analytics, support, or individual record recovery.

Because deletion from immutable or rolling backups may not be immediate, deleted data may remain until the relevant backup expires. If a backup is restored, Notre Boussole must reapply completed deletion requests and purge queues before the restored environment returns to ordinary production use.

Backup access is limited to authorized administrators and service-provider personnel who require access for disaster recovery. Restoration events are documented and reviewed.

11. Legal holds and permitted exceptions

Notre Boussole may retain a narrowly defined subset of data beyond the standard period when required to comply with law, preserve evidence for an active dispute, investigate fraud or a security incident, enforce agreements, or protect users. An exception must:

- Identify the affected records and the reason for retention.
- Restrict the retained data from ordinary product use and secondary processing.
- Limit access to authorized personnel.
- Be reviewed at least every 90 days.
- End with prompt deletion when the reason no longer applies.

A general desire to retain data for possible future use is not an approved exception.

12. Service providers and downstream deletion

Notre Boussole maintains a current inventory of processors that may receive personal data, including hosting, database, storage, email, payment, error-monitoring, AI, and financial-data providers. Before production use, each provider must be reviewed for security, retention, deletion support, data-location considerations, and appropriate contractual terms.

When Notre Boussole receives a valid deletion request, it must instruct relevant processors to delete or return the data, subject only to documented legal obligations and normal backup rotation. Provider-specific retention that exceeds this policy requires a written exception and an update to the Privacy Policy where material.

13. Monitoring, evidence, and assurance

- Automated purge and token-revocation jobs must emit non-sensitive success and failure events.
- Failed deletion jobs must be retried and escalated; failures may not remain unresolved without an owner and due date.
- At least quarterly, Engineering or the Privacy & Security Lead must sample deletion events across database, storage, tokens, and imports.
- At least annually, the organization must compare this policy, the Privacy Policy, actual database schemas, storage buckets, logs, processors, and Plaid products.
- Material control failures must be evaluated under the incident-response process and corrected promptly.
- Evidence of review may include job metrics, test results, configuration screenshots, processor attestations, and change records, but must not include unnecessary personal content.

14. Policy exceptions and enforcement

Exceptions require written approval from the Privacy & Security Lead, a documented reason, compensating controls, an expiration date, and a remediation owner. Permanent or open-ended exceptions are not permitted.

Accessing or retaining personal data contrary to this policy may result in removal of access, contract remedies, disciplinary action, and escalation under applicable incident or legal processes.

15. Review and change management

This policy is reviewed at least annually and before or promptly after any material change involving:

- A new Plaid product, use case, or financial-data field.
- A new processor or hosting environment.
- A change to account deletion, consent, couple-sharing, or AI processing.
- A material legal or regulatory development.
- A security incident or failed deletion control.

Changes must be reflected in the public Privacy Policy and user notices before new processing begins where required.

16. Contact

Questions, deletion requests, and security or privacy concerns may be sent to:

security@notreboussole.app

Privacy Policy: https://notreboussole.app/privacy

Appendix A - Operational deletion checklist

Trigger	Required action	Target completion
Verify scope	Confirm requester, account, couple context, connected institutions, files, financial records, AI records, and processors affected.	Before deletion starts

Trigger	Required action	Target completion
Protect shared data	Determine ownership and sharing state so one partner cannot delete the other partner's independently owned private data.	Before destructive action
Stop processing	Disable syncs, scheduled jobs, notifications, and consent-dependent processing for the targeted data.	Promptly
Revoke Plaid access	Call /item/remove, delete the token and secret record, and clear queued provider payloads.	Immediate; retry window up to 24 hours
Delete active data	Hard-delete or queue database records, storage objects, derivatives, imports, and related search/index copies.	Within 30 days
Notify processors	Send deletion instructions to processors that hold the data and record completion or applicable backup limitation.	Without undue delay
Preserve minimal receipt	Retain only request metadata necessary to demonstrate completion and prevent accidental re-creation.	Up to 6 years
Verify completion	Check job results, token absence, record counts, storage keys, and processor confirmations without logging deleted content.	At completion
Handle backups	Allow deleted data to expire through the configured cycle and replay deletion queues after any restore.	Maximum 30-day cycle

Appendix B - Control references

This policy is informed by the following control and regulatory sources. These references do not replace the requirements of applicable law or Notre Boussole's contracts:

- Plaid Launch Checklist
- Plaid API - Items and /item/remove
- Plaid Developer Policy
- Plaid API Security Guidance
- EU General Data Protection Regulation, Article 5
- FTC - Protecting Personal Information: A Guide for Business

Implementation gate

Before Plaid production access is enabled, Notre Boussole must verify that the application, database policies, token store, deletion jobs, support procedures, and public Privacy Policy actually match this document.