

NOTRE BOUSSOLE

Privacy Policy

Including Financial Data and Consumer Health Data Disclosures

Effective date: July 1, 2026

Version 1.0

Private by design. Shared by choice.

Privacy contact: security@notreboussole.app

Privacy at a glance

Key commitments

Notre Boussole does not sell personal information, does not share personal information for cross-context behavioral advertising, does not move money, and does not receive or store your online-banking username or password. You control whether financial accounts and sensitive relationship content are connected, processed by AI, or shared with your partner.

- Financial accounts are connected through Plaid only after you choose to connect them and complete Plaid Link.
- Connected financial data is used to provide account summaries, transactions, cash-flow tools, net-worth tracking, goals, commitments, and related features.
- Plaid access tokens are restricted to server-side systems and are encrypted separately from ordinary application data.
- Sensitive health, faith, intimacy, and relationship information is processed only for features you choose to use and, where required, with explicit consent.
- AI processing is optional. Financial and sensitive relationship data is not sent to an AI provider unless you intentionally use an AI-powered feature and the required consent is active.
- Privacy controls determine whether content is private, shared as a summary, or fully shared with your partner.
- You may request access, correction, export, deletion, or withdrawal of consent through the Service or by emailing security@notreboussole.app.

Contents

1. Scope and who we are
 2. Information we collect and its sources
 3. How we use information
 4. Legal bases for processing
 5. Financial account connections through Plaid
 6. Couple sharing and privacy controls
 7. AI-assisted features and profiling
 8. How we disclose information
 9. No sale or behavioral advertising sharing
 10. International data transfers
 11. Retention and deletion
 12. Security
 13. Your privacy rights and choices
 14. EEA and UK disclosures
 15. U.S. state privacy disclosures
 16. Children
 17. Changes to this policy
 18. Contact
- Appendix A. California Notice at Collection
- Appendix B. Consumer Health Data Privacy Notice

1. Scope and who we are

Notre Boussole ("Notre Boussole," "we," "us," or "our") provides a private digital workspace for couples to organize financial information, health and wellness information, faith and values, goals, traditions, memories, relationship discussions, and other shared or personal content. This Privacy Policy explains how we collect, use, disclose, retain, and protect personal information when you use our website, web application, and related services (collectively, the "Service").

Notre Boussole operates from Maine, United States and acts as the controller or business responsible for personal information processed through the Service, except where another party independently determines how it processes information, such as Plaid or your financial institution.

Privacy contact: security@notreboussole.app

This Policy applies to the Service and to information we process on our own behalf. It does not govern the independent privacy practices of your financial institution, Plaid, or third-party websites and services that you choose to use.

2. Information we collect and its sources

The information we collect depends on the features you use, the information you choose to provide, and the permissions you select.

2.1 Account and profile information

- Name, email address, authentication identifiers, profile image, language, locale, time zone, and account preferences.
- Couple membership, invitation status, partner identity, relationship dates, and privacy settings.

2.2 Relationship, journal, and shared-workspace content

- Goals, commitments, traditions, memories, notes, discussions, grievances, repair requests, check-ins, calendar entries, and other text you create.
- Photos, documents, audio, or other files you upload.
- Reactions, approvals, comments, and decisions made within shared features.

2.3 Sensitive and special-category information

Some optional features allow you to provide information that may be considered sensitive personal information or special-category data, including:

- Health, symptoms, medications, supplements, wellness, fertility, reproductive health, sleep, exercise, or disability-related information.
- Religious, spiritual, or faith beliefs and practices.
- Sexual or intimacy information and preferences.
- Emotional well-being, relationship conflict, and highly personal free-text content.
- Financial account, balance, transaction, debt, income, asset, and spending information.
- Inferences generated from sensitive content, such as themes, patterns, summaries, or suggested discussion topics.

You are not required to provide sensitive information unless it is necessary for a feature you choose to use. Where applicable law requires explicit consent, we request it separately and provide a way to withdraw it.

2.4 Financial information

You may enter financial information manually, import it from a file, or connect eligible financial accounts through Plaid. Depending on the feature and the accounts you select, we may receive or process:

- Financial institution name, account name, account type and subtype, masked account identifier, and connection status.
- Current and available balances and the date a balance was obtained.
- Transaction dates, amounts, merchant or payee names, descriptions, categories, and pending or posted status.
- Manually entered income, assets, liabilities, interest rates, payment dates, goals, commitments, and financial notes.
- Information about which partner owns an account and the visibility level selected for that account.

Notre Boussole does not request or store your online-banking username, password, or one-time authentication code. We do not use Plaid Auth, Transfer, or payment-initiation products unless we provide a separate notice and obtain any required consent before enabling such a feature.

2.5 Device, usage, and security information

- IP address, browser type, device type, operating system, approximate location derived from IP address, language, and time zone.
- Login activity, session identifiers, feature usage, error events, security events, and audit records.
- Cookie or local-storage information used for authentication, security, preferences, and essential service operation.

2.6 Communications and support

We collect information you provide when you contact support, submit a privacy request, report a security issue, participate in product research, or otherwise communicate with us.

2.7 Sources of information

We collect information directly from you; from your partner when they invite you or add content to shared areas; from your device and use of the Service; from Plaid and the financial institutions you authorize; and from service providers that support authentication, hosting, security, communications, and optional AI features.

3. How we use information

- Provide, operate, maintain, personalize, and improve the Service.
- Create and manage accounts, couple workspaces, privacy settings, and invitations.
- Display financial accounts, balances, transactions, cash-flow summaries, net worth, goals, commitments, and other user-requested finance features.
- Process content through optional AI features such as rewriting, tone support, mediation, summarization, categorization, and guidance when you intentionally invoke those features.
- Apply the visibility and sharing choices selected by each user.
- Authenticate users, prevent fraud and abuse, investigate security events, maintain audit trails, and protect the Service and its users.
- Provide support, respond to requests, send service communications, and notify users about material product or policy changes.
- Comply with law, enforce our agreements, establish or defend legal claims, and protect rights, safety, and property.
- Create aggregated or de-identified information that does not reasonably identify an individual, and use it to understand and improve the Service.

We do not use connected financial data to determine credit eligibility, make lending decisions, initiate payments, or provide individualized investment, tax, legal, or lending advice.

4. Legal bases for processing

Where the GDPR or UK GDPR applies, we rely on the following legal bases. The basis depends on the specific processing activity.

Purpose	Typical information	Legal basis
Provide the Service and requested features	Account, couple, content, financial, and settings data	Performance of a contract or steps requested before entering a contract
Process sensitive relationship, health, faith, or intimacy information	Special-category and sensitive content	Explicit consent, together with the applicable Article 6 basis
Provide optional AI-assisted features	The content submitted to the selected AI feature and necessary context	Consent where required; otherwise contract for the user-requested feature
Security, fraud prevention, and service integrity	Device, authentication, logs, and limited account data	Legitimate interests and, where applicable, legal obligation
Legal compliance and claims	Information necessary for the legal purpose	Legal obligation and legitimate interests
Product analytics using aggregated or limited usage data	Usage and technical data	Legitimate interests, subject to user rights and applicable consent requirements

You may withdraw consent at any time through available Privacy settings or by contacting us. Withdrawal does not affect processing that occurred before withdrawal. Some features cannot function without the information or consent they require.

5. Financial account connections through Plaid

Read-only financial connectivity

Notre Boussole uses Plaid to allow you to connect financial accounts and retrieve user-permissioned account and transaction information. Notre Boussole does not move money and does not receive your bank login credentials.

5.1 Your authorization and Plaid Link

A financial account is connected only when you choose Connect a Bank, enter Plaid Link, select a financial institution and account, review the requested data, and authorize access. Plaid may present institution-specific authentication, consent, and data-transparency screens. You may decline or exit without connecting an account.

By completing the connection flow, you direct Plaid and the relevant financial institution to provide the selected financial information to Notre Boussole for the purposes described in this Policy and in the connection flow. Plaid independently processes information under its End User Privacy Policy.

Plaid End User Privacy Policy: <https://plaid.com/legal/#end-user-privacy-policy>

5.2 Data requested and purpose

We request only the Plaid products and data scopes needed for the finance features you choose to use. Our intended financial-management use case includes account details, balances, and transaction history necessary to provide:

- Account and institution identification using names, types, and masked identifiers.
- Balance and cash-availability summaries.
- Transaction history, categorization, recurring-item detection, and cash-flow summaries.
- Net-worth, debt, goal, and commitment tracking.
- Shared or private couple finance views according to the account owner's selected visibility setting.
- Connection health, synchronization, and error handling.

We do not access financial accounts or data categories that you did not select or consent to through Plaid Link or a later consent update flow.

5.3 Credentials and tokens

Plaid, your financial institution, or an institution-hosted OAuth page handles the authentication used to connect your account. Notre Boussole does not receive or store your financial-institution username, password, security answer, or one-time authentication code.

After a successful connection, Plaid provides Notre Boussole with a server-side access token. We restrict that token to server-side systems, encrypt it separately from ordinary application records, and do not expose it to the browser, your partner, or other users. Plaid API credentials and encryption keys are maintained outside user-accessible application tables.

5.4 Disconnecting and deleting financial data

You may disconnect a financial institution through the Service when the feature is available or request disconnection by contacting us. After disconnection, we stop requesting new data and delete or render unusable the associated access token. You may choose whether previously imported account and transaction records are retained in Notre Boussole for historical use or deleted, subject to limited legal, security, and backup exceptions.

You may also manage eligible Plaid-powered connections through Plaid Portal. Disconnecting from Notre Boussole does not close or alter your account at the financial institution.

5.5 No payment or credit activity

Notre Boussole's finance features are informational and organizational. We do not initiate transfers, debit accounts, make payments, hold funds, provide credit, or make credit, insurance, employment, housing, or other eligibility decisions based on connected financial data.

6. Couple sharing and privacy controls

Notre Boussole is designed for both personal and shared use. The visibility of information depends on the feature and the choices you make. The Service may offer settings such as private, shared summary, and shared full access.

- Private content is intended to be visible only to its author, subject to necessary access by authorized service personnel for security, support, or legal reasons.
- Shared-summary financial accounts may display limited account and aggregate information to a partner without displaying transaction-level details.
- Shared-full accounts and content are visible to both partners as described in the interface.
- Content entered in a shared area should be treated as visible to the other partner.
- Changing a privacy setting may change what the partner can see. We provide confirmation where a change materially expands sharing.

Each person must use their own account. Do not share login credentials. If a couple disconnects or one person leaves a shared workspace, we may retain shared records for the remaining user while deleting or restricting access to the departing user's private records, consistent with ownership, user choices, and applicable law.

7. AI-assisted features and profiling

7.1 Optional AI processing

Some features use an AI provider to perform user-requested functions, such as rewriting text, checking tone, summarizing a discussion, categorizing content, identifying possible themes, or generating partner-guidance suggestions. We send only the content and limited context reasonably necessary for the selected feature.

AI processing of sensitive relationship, health, faith, intimacy, or financial content occurs only when you intentionally use the AI feature and any required AI-processing consent is active. You can withdraw consent, after which new content will not be sent for optional AI processing unless you consent again.

AI output may be inaccurate, incomplete, or inappropriate. It is not professional medical, mental-health, financial, tax, legal, or relationship advice and should not be treated as a substitute for a qualified professional.

7.2 Profiling and inferences

The Service may derive structured categories, summaries, patterns, or suggested topics from information you provide. These inferences are used to provide the features you request, not to make decisions that produce legal or similarly significant effects. Notre Boussole does not make solely automated decisions about credit, employment, housing, insurance, legal rights, or access to essential services.

8. How we disclose information

We disclose information only as reasonably necessary for the purposes described below.

8.1 Your partner and people you direct us to share with

We disclose information to your partner according to the visibility controls and shared features you select. We may also disclose information when you direct us to export or share it.

8.2 Service providers

We use service providers that process information on our behalf under contractual restrictions appropriate to their role. Key providers may include:

Provider	Purpose	Information involved
Supabase	Authentication, database, and access-controlled file storage	Account, content, finance, settings, and security records
Vercel	Application hosting, delivery, and operational infrastructure	Technical requests, limited application data, and logs
Plaid	User-permissioned financial account connectivity	Connection, account, balance, transaction, device, and consent data processed by Plaid
OpenAI or Anthropic	Optional AI-assisted features selected by the user	Content and limited context submitted to the selected AI feature

The specific provider used may change as our infrastructure evolves. We require providers to process information only for authorized purposes and to maintain appropriate safeguards. Plaid and financial institutions may also act as independent controllers for portions of their processing.

8.3 Legal, safety, and business events

We may disclose information when reasonably necessary to comply with law or legal process; respond to lawful government requests; protect users, the public, or the Service; investigate fraud, abuse, or security incidents; enforce agreements; or establish, exercise, or defend legal claims. If ownership or control of the Service changes through a merger, acquisition, financing, reorganization, or sale, information may be transferred subject to this Policy and applicable law.

9. No sale or behavioral advertising sharing

We do not sell personal information for money or other valuable consideration. We do not share personal information for cross-context behavioral advertising and do not use sensitive personal information to target advertising. We do not disclose Plaid-derived financial data to marketers, data brokers, or unrelated third parties.

If our practices change, we will update this Policy and provide any legally required opt-out controls before engaging in the new practice.

10. International data transfers

Notre Boussole and some service providers operate in the United States and other countries. Information may therefore be processed outside the country where you live. Where required, we use legally recognized safeguards for restricted transfers, such as adequacy decisions, data-protection agreements, Standard Contractual Clauses, and the UK International Data Transfer Addendum or other approved mechanisms. You may contact us for information about the safeguards applicable to your data.

11. Retention and deletion

We retain personal information only for as long as reasonably necessary for the purpose for which it was collected, to provide the Service, honor user choices, maintain security and auditability, resolve disputes, enforce agreements, and satisfy legal obligations. The following describes our general criteria:

Category	General retention criteria
Account and profile information	While the account is active and for a limited period after closure to complete deletion, security, and legal processes.
Relationship content, photos, and uploaded files	Until you delete the content, the account is closed, or the content is no longer needed for the feature, subject to shared-record and legal exceptions.
Plaid access tokens	While the financial connection is active; deleted or rendered unusable promptly after disconnection, subject to operational completion and legal requirements.
Imported financial accounts and transactions	While retained by the user for finance history; deleted when requested or at account closure, subject to user choices, shared records, security, legal, and backup exceptions.
Security, audit, and access logs	For a period proportionate to security, fraud-prevention, troubleshooting, and legal needs.
Consent and privacy-request records	For the period reasonably necessary to demonstrate consent, honor requests, and comply with law.
Backups	Deleted information may remain in encrypted backups until those backups are overwritten under our backup cycle; it is not restored to active use except for disaster recovery or legal necessity.

Our standard target is to remove user-deleted information from active systems within 30 days. Encrypted backup copies may persist for up to 90 days or the applicable backup cycle. We may retain limited information longer where reasonably necessary for security, fraud prevention, legal compliance, dispute resolution, or to protect the rights of another user.

12. Security

We maintain administrative, technical, and organizational safeguards designed to protect personal information. Measures include, as appropriate:

- Encryption in transit and encryption at rest provided by our infrastructure providers.
- Database row-level security and couple-scoped authorization controls.
- Least-privilege access and separation of privileged service credentials from browser code.
- Server-side storage and separate encryption of Plaid access tokens, with encryption keys held outside ordinary application tables.
- Access-controlled storage for uploaded files and photos.
- Audit logging, vulnerability patching, dependency review, monitoring, backup protection, and incident-response procedures.
- Restrictions on personnel and contractors, limiting access to those with an authorized business need.

No system can guarantee absolute security. You are responsible for protecting your password, device, and account access and for notifying us promptly if you suspect unauthorized access.

13. Your privacy rights and choices

Depending on where you live and subject to applicable exceptions, you may have the right to:

- Know whether we process your personal information and obtain access to it.
- Receive information about the categories, sources, purposes, and recipients of personal information.
- Correct inaccurate personal information.
- Delete personal information.
- Obtain a portable copy of information you provided, where technically feasible.
- Withdraw consent or limit optional processing, including sensitive-data and AI processing.
- Object to or restrict certain processing.
- Opt out of sale, cross-context behavioral advertising sharing, or qualifying profiling. We do not currently engage in those activities.
- Appeal a denial of a qualifying U.S. state privacy request.
- Use an authorized agent where permitted by law.
- Exercise rights without unlawful discrimination or retaliation.

You can use in-product privacy controls where available or email security@notreboussole.app. We may verify your identity and authority before completing a request. For shared couple records, we may need to balance your request with the rights of your partner and distinguish private records from jointly created records. We will respond within the time required by applicable law.

14. EEA and UK disclosures

If you are located in the European Economic Area or United Kingdom, you may have rights to access, rectification, erasure, restriction, objection, data portability, withdrawal of consent, and complaint to a supervisory authority. You may object at any time to direct marketing; Notre Boussole does not currently use personal information for direct marketing profiling.

Where we rely on legitimate interests, those interests generally include operating and securing the Service, preventing abuse, improving reliability, and protecting users. We balance those interests against your rights and expectations. Where special-category information is processed based on explicit consent, you may withdraw that consent at any time.

Notre Boussole does not make decisions based solely on automated processing that produce legal effects or similarly significant effects. You may contact your local data-protection authority or the UK Information Commissioner's Office, as applicable. We encourage you to contact us first so we can address your concern.

15. U.S. state privacy disclosures

15.1 California

California residents may have rights to know, access, correct, delete, and obtain information about our collection and disclosure practices; to limit certain uses of sensitive personal information; to opt out of sale or sharing; and to receive equal service and pricing when exercising privacy rights. We do not sell personal information or share it for cross-context behavioral advertising. Appendix A provides our Notice at Collection.

15.2 Consumer health data

Some optional features may process information that qualifies as consumer health data under laws such as the Washington My Health My Data Act or similar state laws. Appendix B describes our consumer health data practices, sources, purposes, disclosures, and rights. We do not sell consumer health data and do not use geofences around healthcare facilities to identify or track individuals seeking health services.

15.3 Other state rights

Residents of other U.S. states may have similar rights, including access, correction, deletion, portability, opt-out, and appeal rights. Submit a request through the Service or at security@notreboussole.app. If we deny an appeal, we will provide information about additional complaint options where required.

16. Children

The Service is intended for adults and is not directed to children under 18. We do not knowingly collect personal information from children under 13. If you believe a child has provided personal information without appropriate authorization, contact us so we can investigate and delete it as required.

17. Changes to this policy

We may update this Policy to reflect changes in the Service, our practices, or legal requirements. We will post the updated version with a new effective date and provide additional notice when a change is material or when law requires consent.

18. Contact

Controller: Notre Boussole

Location: Maine, United States

Privacy and security email: security@notreboussole.app

Privacy requests may also be submitted through the Privacy area of the Service when available. Please include enough information for us to identify your account and understand the request, but do not email bank credentials, full account numbers, medical records, or other unnecessary sensitive information.

Appendix A - California Notice at Collection

This Notice at Collection applies to California consumers and supplements the Privacy Policy. It describes the categories of personal information we may collect, the purposes for collection and use, whether the category is sold or shared for cross-context behavioral advertising, and our retention criteria. We do not sell or share any category listed below for cross-context behavioral advertising.

Category collected	Examples	Purposes	Retention criteria / sold or shared
Identifiers	Name, email, account ID, IP address, profile and authentication identifiers	Create and secure accounts; provide support; operate the Service	Account life plus limited security/legal period. Sold/shared: No.
Customer records and profile information	Profile, locale, preferences, couple membership, support communications	Personalize and provide the Service; manage couple workspace	Until deleted, account closure, or no longer needed. Sold/shared: No.
Commercial and subscription information	Subscription status, plan, transaction record from payment provider	Manage subscriptions, billing, and records	As needed for account, tax, accounting, disputes, and law. Sold/shared: No.
Internet or electronic activity	Browser, device, login, usage, session, error, and security logs	Authentication, security, fraud prevention, troubleshooting, and improvement	Proportionate to security and operational need. Sold/shared: No.
Geolocation	Approximate location derived from IP address	Security, localization, fraud prevention, and service delivery	Limited to operational and security need. Sold/shared: No.
Audio, visual, or similar information	Profile photos, memories, uploaded images, audio, or files	Provide user-selected memory, profile, and shared-workspace features	Until deleted, account closure, or no longer needed. Sold/shared: No.
Professional or employment-related information	Employer or occupation if voluntarily entered in goals, profile, or financial records	Provide requested organizational and financial features	Until deleted or no longer needed. Sold/shared: No.
Sensitive personal information	Account credentials for Notre Boussole, precise content concerning health, faith, sex life or intimacy, financial account and transaction information, and private communications	Provide requested sensitive features; security; user-selected AI features; legal compliance	Until deleted, consent withdrawn where applicable, account closure, or no longer needed; subject to legal/security exceptions. Sold/shared: No.
Financial information	Institution, account type, masked identifier, balances, transactions, debts, income, assets, and goals	Cash flow, net worth, financial planning, goals, and couple sharing controls	While connected or retained by the user; deleted upon request subject to exceptions. Sold/shared: No.
Inferences	Themes, categories, summaries, patterns, and suggested topics derived from submitted content	Provide requested insights, organization, and optional AI-assisted features	Until deleted, feature disabled, consent withdrawn where applicable, or no longer needed. Sold/shared: No.

Sources and disclosures

We collect personal information from you, your partner, your device and use of the Service, Plaid and financial institutions you authorize, and service providers. We disclose information to your partner according to your settings; to service providers described in Section 8; and as required for legal, safety, security, or business-transfer purposes.

California rights

California residents may submit requests to know, access, correct, delete, or limit qualifying uses of sensitive personal information, and may use an authorized agent. We do not sell or share personal information for cross-context behavioral advertising, so no sale/sharing opt-out is necessary for our current practices. Submit requests through the Service or at security@notreboussole.app.

Appendix B - Consumer Health Data Privacy Notice

Effective date: July 1, 2026

This Consumer Health Data Privacy Notice supplements the Notre Boussole Privacy Policy and applies where consumer health data laws, including the Washington My Health My Data Act and similar laws, apply. "Consumer health data" means personal information that identifies or can reasonably be linked to a consumer and identifies past, present, or future physical or mental health status, health care, or related inferences.

B.1 Consumer health data we may collect

- Health conditions, symptoms, medications, supplements, treatment information, allergies, pain, disability, or wellness information that you choose to record.
- Reproductive, fertility, menstrual, sexual-health, and intimacy-related information.
- Mental or emotional well-being, stress, mood, relationship conflict, or counseling-related information.
- Exercise, sleep, nutrition, habit, and wellness-goal information.
- Faith or spiritual practices where they relate to health, well-being, or care preferences.
- Inferences generated from the information above, such as categories, patterns, summaries, or suggested topics.

B.2 Sources

We collect consumer health data directly from you; from your partner when you choose to participate in a shared health or relationship feature; and from service providers only as necessary to perform a feature you requested. We do not collect consumer health data from data brokers.

B.3 Why we collect and use it

- Provide the health, wellness, relationship, goal, reminder, journal, and shared-workspace features you choose to use.
- Display information back to you and, only according to your selected visibility controls, to your partner.
- Provide optional AI-assisted rewriting, summarization, organization, or guidance when you intentionally invoke the feature and required consent is active.
- Maintain security, prevent abuse, provide support, and comply with law.
- Create de-identified or aggregated information that cannot reasonably be linked to you.

B.4 How we disclose consumer health data

We may disclose consumer health data:

- To your partner only according to your express sharing choices and the feature's visibility controls.
- To Supabase and Vercel as infrastructure providers necessary to host, secure, store, and deliver the Service.
- To OpenAI or Anthropic only when you intentionally use an AI-assisted feature involving that data and required consent is active.
- To legal authorities or others when required by law or reasonably necessary to protect rights, safety, and security.
- In connection with a business transaction, subject to applicable consumer health data requirements.

We do not sell consumer health data. We do not use consumer health data for targeted advertising. We do not use geofences around healthcare facilities or other locations to identify, track, or collect information about people seeking health services.

B.5 Consent

Where required, we obtain consent before collecting or sharing consumer health data for the stated purpose. A request to sell consumer health data would require a separate valid authorization; Notre Boussole does not sell consumer health data. You may withdraw consent through the Service or by contacting us. Withdrawal stops future consent-based processing but does not affect processing completed before withdrawal.

B.6 Your consumer health data rights

Subject to applicable law, you may request to:

- Confirm whether we collect, share, or sell your consumer health data.
- Access the consumer health data we hold about you, including a list of third parties and affiliates with whom it was shared when required by law.
- Withdraw consent for collection or sharing.
- Delete consumer health data, including data maintained by processors as required by law.
- Appeal a denial of your request where an appeal right applies.

Submit a request through the Service or email security@notreboussole.app. We may verify your identity and authority. We will not discriminate against you for exercising a right. If an appeal is denied, we will provide information about contacting the appropriate regulator where required.

B.7 Deletion and retention

Consumer health data is retained only while needed for the feature you selected, while your account is active, or as otherwise described in Section 11. When deletion is requested, we remove the data from active systems and instruct relevant processors to delete it as required. Backup copies may remain until overwritten under the backup cycle and will not be restored to active use except for disaster recovery, security, or legal necessity.

B.8 Contact

Email: security@notreboussole.app

Controller: Notre Boussole, Maine, United States

End of Privacy Policy