Data Retention Policy

How long we keep customer data, what triggers deletion, and the timeframes you can expect.

Last updated May 29, 2026

Scope

This policy describes how long Notion Scan retains customer data, the events that trigger deletion, and the timeframes within which deletion completes. It applies to all customer-associated data stored in our systems: workspace metadata, scan snapshots, derived analysis, encrypted Notion integration tokens, onboarding submissions, account records, and diagnostic scan logs.

Retention while engagement is active

For the duration of an active engagement, we retain:

- Workspace metadata and scan snapshots, for historical comparison and trend analysis.
- Encrypted Notion integration tokens, required to perform authorized scans.
- Onboarding submissions and consent records, required for customer setup, support, and audit history.
- Account records and authentication metadata for users authorized to access the Notion Scan platform.

"Account records" refers to the login accounts of people who sign in to the Notion Scan platform to view results: the Notion State team and any client users explicitly granted access. These are distinct from the members of your Notion workspace, who are captured only as metadata (user ID, display name, type) within scan snapshots and are governed by the scan snapshot timeframe below.

Deletion requests

We delete customer data upon confirmed customer request. Contract termination or integration revocation does not automatically delete stored data unless the customer requests deletion or the offboarding instructions include deletion.

Customers can request deletion via hello@notionscan.com. If a workspace administrator revokes the Notion integration, future API access stops immediately; revocation alone is not treated as a deletion request.

Deletion timeframes

Once a deletion request is confirmed:

- **Encrypted Notion integration token:** deleted within **7 business days**.
- **Scan snapshots and derived analysis:** deleted within **7 business days**.
- **Onboarding submissions and customer contact fields:** deleted or anonymized within **7 business days**.
- **Account records and authentication metadata:** deleted on customer or user request within **30 business days**, unless the user is associated with another active engagement.

Confirmation of deletion is sent to the customer's primary contact on request.

Logging

We generate two kinds of logs, handled differently:

- **Operational logs.** Standard server logs (request timestamps, route paths, response codes) used for security monitoring and debugging. These are generated and held by our hosting and infrastructure providers (Vercel, Railway, and Supabase) and expire according to each provider's own retention schedule. We do not maintain a separate copy. These logs do not contain request bodies, workspace content, database values, or personal data beyond standard request metadata.
- **Diagnostic scan logs.** Each scan produces a diagnostic log that records scan progress and errors. It does not contain workspace content or non-title database entry values. Scan logs are stored in private, access-controlled object storage and

are deleted when the associated scan is deleted; deleting a scan or its snapshot removes the corresponding log at the same time.

- **Onboarding abuse-prevention records.** The onboarding endpoint stores a rate-limit key derived from the source IP address, plus a request window and hit count. These records are used only for rate limiting and abuse prevention. They do not contain workspace content, database values, or integration tokens.

Backup retention

Our database provider (Supabase) maintains backups for our current production plan. After deletion from the live database, customer data may persist in encrypted backups for up to **7 days** before final purge. Backups are encrypted at rest and used only for disaster recovery; they are not queryable in the normal course of operations.

Legal and compliance exceptions

We may retain limited data beyond the deletion timeframes above when required by law, to enforce our terms of service, or to investigate fraud or security incidents. Any such retention is limited in scope and duration; we document the legal basis and review periodically.

Aggregated, anonymized data

We may retain aggregated metrics that do not identify a specific customer, workspace, or user. Examples: total scans per month, percentile distributions of database counts across all clients, model performance statistics.

Review

This retention schedule is reviewed annually, and on each material change to our product or infrastructure. The `Last updated` date at the top of this page reflects the most recent revision.

Contact

For deletion requests, retention questions, or to confirm a deletion has been completed: hello@notionscan.com.