Data Retention and Disposal Policy

NopeSub · Operated by Ole Christian Nygjelten, sole proprietor (Norway)
Document version: 1.0 · Effective date: 2026-06-01 · Last reviewed: 2026-06-01 · Next review: 2026-12-01

1. Purpose

This policy defines how NopeSub collects, retains, reviews, and securely disposes of consumer and operational data. It governs all data NopeSub receives from the Plaid API, the NopeSub iOS application, the NopeSub website at nopesub.com, and supporting back-office systems. The policy ensures compliance with the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act / California Privacy Rights Act (CCPA / CPRA), the US Gramm-Leach-Bliley Act (GLBA) Safeguards Rule, and Plaid's End User Data Handling requirements.

2. Scope

This policy applies to:

- All consumer data retrieved from the Plaid API (Transactions, Recurring Transactions, Transactions Refresh).
- All consumer account data (email, password hash, display name, device identifiers).
- Payment metadata processed via Stripe and Apple In-App Purchase.
- Call recordings and call metadata generated via Twilio for the NopeSub Path C cancellation flow.
- Operational logs (server access logs, application audit logs, error/crash telemetry).
- Business records (tax records, accounting, correspondence).

3. Data classification

Class	Examples	Encryption
Highly sensitive (financial)	Plaid transaction data, account masked identifiers, recurring subscription detection output	AES-256 at rest, TLS 1.2+ in transit
Sensitive (PII)	Email, password hash, display name, IP address, device ID	AES-256 at rest, TLS 1.2+ in transit
Operational	Server logs, crash reports, anonymized analytics	AES-256 at rest, TLS 1.2+ in transit
Business	Tax records, invoices, customer correspondence	AES-256 at rest, TLS 1.2+ in transit

4. Retention schedule

Each data category is retained for the minimum period required to deliver the Service and meet legal obligations, then disposed of per Section 6.

Data category	Retention period	Legal/operational basis
Plaid transaction data (raw transactions, recurring subscription detection output)	**30 days** from retrieval, then automatic purge	Operational minimum for subscription-detection processing; GDPR Art. 5(1)(e) data minimization
Plaid access tokens (Item tokens)	Lifetime of the user's account; deleted within 7 days of account deletion or Plaid Item disconnect	Operational requirement to refresh transaction data on user request
Account data (email, password hash, display name)	Lifetime of the active account; 30 days after account deletion	Operational requirement; deletion grace period for recovery
Cancellation records (which subscription was cancelled, when, via which path, outcome)	**24 months** from cancellation date	Evidence retention for disputes with subscription providers; consumer protection
Payment records (Stripe/Apple receipts, refunds, chargebacks)	**7 years** from transaction date	Norwegian Bookkeeping Act § 13; GLBA record-keeping requirements
Twilio call recordings (Path C cancellation calls)	**90 days** from call date, then automatic purge	Operational requirement for dispute resolution; minimum two-party-consent statutory hold
Twilio call metadata (call duration, called number, outcome flag)	24 months (matches cancellation record retention)	Audit trail for cancellation outcomes
Server access logs, application audit logs	**30 days**	Security and incident-response requirement; GLBA Safeguards Rule § 314.4(b)
Crash reports, anonymized analytics	13 months	Engineering debugging window; GDPR-compliant analytics retention
Customer support correspondence	24 months from last contact	Operational requirement for context on repeat inquiries
Marketing email subscription state		CAN-SPAM compliance for unsubscribe enforcement

	Until user unsubscribes; suppression list retained indefinitely	

5. End-user data rights

End users may exercise the following rights at any time, regardless of the retention schedule:

- **Right of access:** Users may request a copy of all data NopeSub holds about them by emailing christian@nopesub.com or via in-app Settings → Privacy → Export my data. Responded to within 30 days (GDPR) or 45 days (CCPA).
- **Right of erasure:** Users may delete their account and all associated data via in-app Settings → Account → Delete account, or by emailing christian@nopesub.com. Deletion is executed within 7 business days of request, subject only to records NopeSub is legally required to retain (e.g. 7-year tax records, which are isolated to the accounting system and otherwise inaccessible).
- **Right to rectification:** Users may correct inaccurate data in-app or by request.
- **Right to portability:** Data export is provided in machine-readable JSON.
- **Right to restrict or object:** Users may pause data processing at any time without account deletion.
- **Plaid Item disconnect:** Users may disconnect a Plaid Item via in-app Settings → Connected accounts → Disconnect, which triggers immediate purge of all transaction data associated with that Item, regardless of the 30-day operational retention window.

6. Secure disposal

6.1 Automated disposal

Transaction data, call recordings, and server logs are subject to automated time-based deletion via scheduled jobs running daily. Job execution is monitored and logged.

- Database records: deleted via parameterized SQL `DELETE` statements, followed by table-level `VACUUM` on PostgreSQL to remove from physical storage.
- Object storage (call recordings, exports): deleted via cloud provider API; provider's data-disposal guarantee applies (Cloudflare R2, AWS S3 standard erasure).
- Log files: rotated and deleted via systemd journal retention policy + logrotate.

6.2 On-request disposal

User-initiated deletion (account deletion, Plaid Item disconnect, transaction-history purge) executes the same disposal pathway as automated disposal, on demand. Confirmation is sent to the user upon completion.

6.3 Hardware and media disposal

NopeSub does not maintain on-premises servers. Production data lives only on cloud-provider managed services. On contract termination with any cloud provider, NopeSub will (a) export and re-locate any required data per the retention schedule and (b) request cryptographic erasure and written destruction confirmation from the provider.

6.4 Backup disposal

Encrypted database backups are retained for 30 days, then automatically purged. Backups inherit the same encryption (AES-256) and access controls as production data. Backup disposal is verified monthly.

7. Encryption

- **At rest:** All consumer data is encrypted with AES-256 at the storage layer. Sensitive fields (Plaid access tokens, PII) are additionally encrypted at the column level via PostgreSQL pgcrypto or equivalent application-layer encryption.
- **In transit:** TLS 1.2 minimum (TLS 1.3 preferred) for all data transmission, enforced at the edge (Cloudflare) and at the origin (Caddy reverse proxy). Plaid API, Stripe API, Twilio API, and RevenueCat API connections all require TLS 1.2+ by contract.
- **Key management:** Encryption keys are stored separately from data, accessed only by the production application via secrets-management with chmod 600 file permissions. Keys are rotated on suspected compromise.

8. Access controls

- Principle of least privilege. Only the founder (Ole Christian Nygjelten) holds production access.
- Multi-factor authentication enforced on all administrative interfaces (Google Workspace, Plaid Dashboard, Stripe Dashboard, RevenueCat Dashboard, Cloudflare Dashboard, production VPS via SSH keys).
- Audit logging of all production system access is captured and retained for 30 days.
- No third-party advertising trackers or fingerprinting libraries are deployed.
- Bank credentials never touch NopeSub systems; they are handled entirely by Plaid Link.

9. Policy review

This policy is reviewed at minimum every 6 months and on any of the following triggers: (a) material change to the data processing landscape, (b) onboarding of a new sub-processor, (c) change in applicable law, (d) any data security incident. Review is performed by the Information Security Lead (currently the founder). Outcomes are recorded in the policy version history below.

10. Incident response and breach notification

In the event of a data breach affecting consumer data, NopeSub will:

- Notify affected users within 72 hours of confirmed discovery (GDPR Art. 33-34).
- Notify Plaid via the security disclosure channel within 24 hours of confirmed discovery, per Plaid Production Terms.
- Notify the Norwegian Data Protection Authority (Datatilsynet) within 72 hours where statutorily required.
- Investigate, contain, document, and remediate per a written incident-response runbook.

11. Sub-processors

Current sub-processors with access to consumer data, each contractually bound to equivalent or stronger data-protection standards:

- Plaid Inc. (USA) — Transactions retrieval.
- Stripe, Inc. (USA, Ireland) — Web payment processing.
- Apple Inc. (USA) — iOS In-App Purchase.
- RevenueCat, Inc. (USA) — iOS subscription state.
- Twilio Inc. (USA) — Voice and SMS for Path C cancellation flow.
- OpenAI, L.L.C. (USA) — AI voice assistant during cancellation calls (no transaction data shared; only call audio and per-cancellation script context).
- Google LLC (USA) — Operational email (Google Workspace).
- Cloudflare, Inc. (USA) — DNS, CDN, edge TLS termination, DDoS protection.

An up-to-date sub-processor list is maintained at **nopesub.com/privacy**.

12. Compliance attestation

NopeSub attests that this policy is operative as of the effective date above and will be applied consistently to all consumer data retrieved from the Plaid API. NopeSub will remediate any gaps identified during Plaid's Production Security Diligence within reasonable timeframes proposed by Plaid.

13. Version history

Version	Date	Change	Reviewer
1.0	2026-06-01	Initial policy authored for Plaid Production Security Diligence.	Ole Christian Nygjelten

Approved by: Ole Christian Nygjelten, Founder & Information Security Lead

Organization: NopeSub (sole proprietorship)

Effective date: 2026-06-01

Contact: christian@nopesub.com