GigWallet Data Retention and Disposal Policy

Document Title: Data Retention and Disposal Policy

Organization: DNR Corp (DBA GigWallet)

Version: 1.0

Effective Date: February 20, 2026

Next Review Date: February 20, 2027

Classification: Internal — Confidential

Approved By: Sagar Patel, Founder & CEO

---

1. Purpose

This policy defines how GigWallet collects, retains, and disposes of data to ensure compliance with applicable data privacy laws, minimize data exposure risk, and uphold consumer trust. This policy applies to all data processed by GigWallet, with particular emphasis on consumer financial data accessed through third-party integrations including Plaid.

---

2. Scope

This policy applies to:

- All consumer data collected, stored, or processed by GigWallet

- All systems and storage media used by GigWallet (on-device, backend servers, backups, logs)
- All personnel with access to GigWallet data
- All third-party services that process data on behalf of GigWallet

---

3. Data Inventory

3.1 Consumer Data Categories

Data Category	Description	Storage Location	Sensitivity
Account Information	Name, email, phone number	On-device (SwiftData), Backend DB	Sensitive (PII)
Authentication Credentials	Firebase UID, auth provider tokens	iOS Keychain, Backend DB	Highly Sensitive
Bank Connection Data	Plaid access tokens, Item IDs	Backend DB only	Highly Sensitive
Financial Transactions	Income, expenses, platform earnings	On-device (SwiftData), Backend DB	Highly Sensitive
Tax Information	Filing status, tax estimates, payments logged	On-device (SwiftData)	Highly Sensitive
Mileage Data	Trip distance, business/commute classification	On-device (SwiftData)	Sensitive
App Preferences	Notification settings, selected platforms, goals	On-device (SwiftData)	Internal

| **Application Logs** | API request logs, error logs | Backend server | Internal |
| **Authentication Logs** | Sign-in events, failed attempts | Backend server | Sensitive |

---

4. Retention Schedule

4.1 Consumer Data

Data Type	Retention Period	Justification
User account profile	Duration of active account + 30 days after deletion request	Service delivery; grace period for accidental deletion
Financial transactions (income, expenses)	Current tax year + 3 years	IRS recommends retaining tax records for 3 years from filing date (6 years if underreported income > 25%)
Tax estimates and payment records	Current tax year + 3 years	IRS record-keeping guidance
Mileage trip records	Current tax year + 3 years	IRS substantiation requirements for vehicle deductions
Plaid access tokens	Duration of active bank connection	Required for ongoing transaction sync; revoked upon disconnect
Plaid transaction data (raw)	90 days from sync date	Processed into app records; raw data not needed long-term
Exported reports (CSV, TXF, Schedule C)	Not retained by GigWallet	Generated on-device and delivered to user; GigWallet does not store copies

4.2 Operational Data

Data Type	Retention Period	Justification
Authentication logs	12 months	Security monitoring and incident investigation
API request/error logs	6 months	Troubleshooting and performance monitoring
Backend database backups	30 days (rolling)	Disaster recovery
Crash reports and diagnostics	6 months	Application stability monitoring

4.3 Data Not Retained

GigWallet does **not** retain:

- Passwords (delegated to Firebase Authentication)
- Bank account numbers or routing numbers (handled entirely by Plaid)
- Credit card numbers or payment instrument details
- Consumer data for users who have completed account deletion

---

5. Data Disposal Procedures

5.1 User-Initiated Account Deletion

When a user requests account deletion (via in-app Settings or by contacting support):

1. **Immediate Actions (within 24 hours):**
   - User session is terminated and authentication tokens are invalidated
   - Plaid access tokens are revoked via Plaid API (`/item/remove` endpoint)

- Bank connections are permanently severed

2. **Within 7 days:**
   - All on-device data is purged from SwiftData (occurs automatically when user deletes the app, or upon explicit account deletion within the app)
   - iOS Keychain entries associated with the account are deleted

3. **Within 30 days:**
   - User profile and all associated records are permanently deleted from the backend database
   - Backend database records include: user profile, transaction history, platform connections
   - Account enters a 30-day grace period before permanent deletion to allow recovery from accidental requests

4. **Within 60 days:**
   - User data is purged from all backup systems as backups rotate out on their 30-day rolling schedule

5.2 Bank Connection Disconnection

When a user disconnects a bank account:
- Plaid access token for that connection is revoked immediately via Plaid API
- The Plaid Item record is deleted from the backend database
- Previously synced transactions remain in the user's records (as they are the user's financial data)
- No further transaction syncs occur for the disconnected account

5.3 Subscription Cancellation

When a user cancels their premium subscription:
- The user retains access to their data (downgraded to free tier)
- No data is deleted upon subscription cancellation
- Data is only deleted upon account deletion request

5.4 Automated Data Disposal

Process	Frequency	Action
Raw Plaid transaction cleanup	Weekly	Raw transaction data older than 90 days is purged from backend
Log rotation	Daily	Logs exceeding retention period are permanently deleted
Backup rotation	Daily	Backups older than 30 days are permanently deleted
Inactive account review	Quarterly	Accounts inactive for 24+ months are flagged; users are notified via email before deletion

5.5 Disposal Methods

Storage Type	Disposal Method
Backend database records	Permanent deletion via SQL DELETE with verification
iOS on-device data (SwiftData)	SwiftData model deletion; iOS file system handles secure erasure
iOS Keychain entries	Keychain item deletion via Security framework

| Log files | Secure file deletion from server |

| Backup files | Secure deletion upon rotation |

| Plaid tokens | API revocation via Plaid `/item/remove` endpoint |

---

6. Data Handling Prohibitions

GigWallet strictly prohibits:

- **Selling or renting** consumer financial data to any third party
- **Sharing** consumer data with third parties for marketing or advertising purposes
- **Retaining** Plaid access tokens after a user disconnects a bank connection or deletes their account
- **Storing** bank account numbers, routing numbers, or payment card numbers
- **Retaining** consumer data beyond the defined retention periods without legitimate business justification
- **Transferring** consumer financial data to jurisdictions without adequate data protection unless required for service delivery

---

7. Consumer Rights

7.1 Right to Deletion

Users may request deletion of their account and all associated data at any time through:

- In-app account deletion (Settings)
- Email request to support@gigwallet.app

7.2 Right to Data Portability

Users may export their financial data at any time in the following formats:

- CSV (spreadsheet format)
- TXF (tax software import format for TurboTax, H&R Block, TaxAct)
- Schedule C Summary (text report for tax preparers)

7.3 Right to Access

Users may request a copy of all personal data held by GigWallet by contacting support@gigwallet.app. Requests are fulfilled within 30 days.

7.4 Right to Correction

Users may update their personal information at any time through the in-app Settings profile section.

---

8. Third-Party Data Processors

Vendor	Data Processed	Vendor Retention Policy	Our Controls
Plaid	Bank account tokens, transaction data	Per Plaid's privacy policy; tokens revocable via API	Tokens revoked on disconnect/deletion
Firebase (Google)	Authentication data (UID, email, auth provider)	Per Google Cloud data retention policies	Account deleted via Firebase Admin SDK on user deletion

| **Apple (App Store)** | Subscription/purchase records | Per Apple's privacy policy | No consumer financial data shared with Apple |

GigWallet ensures that all third-party processors maintain security standards consistent with this policy through vendor assessment and contractual obligations.

---

9. Compliance

9.1 Applicable Laws and Regulations

This policy is designed to comply with:

- **California Consumer Privacy Act (CCPA)** — Right to deletion, right to know, right to opt-out of sale
- **IRS Record Retention Guidelines** — 3-year minimum for tax records
- **Plaid Developer Policy** — Data handling and retention requirements for Plaid API consumers
- **Apple App Store Guidelines** — Privacy and data handling requirements

9.2 Regulatory Updates

This policy is reviewed when relevant privacy laws or regulations are updated to ensure ongoing compliance.

---

10. Policy Review and Enforcement

10.1 Review Schedule

This policy is reviewed and updated:

- At least annually
- When new data categories are introduced
- When new third-party integrations are added
- When applicable laws or regulations change
- Following any data breach or security incident

10.2 Enforcement

Violations of this policy may result in disciplinary action. Any suspected violation should be reported immediately to leadership.

10.3 Policy Exceptions

Exceptions to retention periods require written approval from the Founder & CEO and must include:

- Business justification
- Risk assessment
- Defined expiration date for the exception

---

11. Contact Information

For data deletion requests, data access requests, or questions about this policy:

Support: support@gigwallet.app

Security: security@gigwallet.app

This document is the property of DNR Corp. Unauthorized distribution is prohibited.

Last reviewed: February 20, 2026 | Next review: February 20, 2027