Data Handling & GDPR Compliance

Overview

FiredUp is committed to GDPR compliance and transparent data handling practices. This document details what data we collect, how we process it, retention periods, and user rights procedures.

Data Collection

Data Collected from Tink

When a user connects their bank account, we receive the following data from Tink:

Data Type	Fields	Purpose
Account Information	IBAN, account name, account type, balance	Display connected accounts
Transactions	Date, amount, description, merchant name	Import for budgeting
Categories	Tink PFM category	Auto-categorization
Balances	Current balance, available balance	Dashboard display

Data We Do NOT Collect

Data Type	Why Not
Bank credentials	Handled by Tink Link directly
PINs / Security codes	Never accessed
Credit card CVV	Never accessed
Biometric data	Bank handles this

Data Processing

How We Use Bank Data

Purpose	Legal Basis (GDPR)
Display in app	Contract (Art. 6(1)(b))
Auto-categorization	Contract (Art. 6(1)(b))
Budget calculations	Contract (Art. 6(1)(b))
Reports generation	Contract (Art. 6(1)(b))

Processing Flow

```
 1. User connects bank → Consent captured (GDPR Art. 6(1)(a))
2. Tink fetches data → Passed to FiredUp via API
3. FiredUp stores raw data → BankTransaction table
4. User reviews transactions → Converts to expenses/incomes
5. Original raw data retained → Until disconnection + 30 days
6. Processed data retained → Until user deletes
```

Data Retention Periods

Retention Schedule

Data Type	Retention Period	Trigger for Deletion
User account data	Until account deletion	User request or deletion
Manual financial data	Until account deletion	User request or manual deletion
Raw bank data	Until bank disconnection + 30 days	Disconnection or account deletion
Processed transactions	Until manual deletion	User action or account deletion

Data Type	Retention Period	Trigger for Deletion
Access tokens	~1 hour (auto-expires)	Expiration
Refresh tokens	~90 days or until revocation	Expiration or disconnection
Audit logs	12 months	Automatic rotation
Analytics data	24 months from last activity	Inactivity

Retention Rationale

Data Type	Rationale
Raw bank data (30 days after disconnect)	Allow user to reconnect without losing history, audit trail
Processed transactions (indefinite)	User’s budget history, intentionally created data
Audit logs (12 months)	Security compliance, incident investigation

---

Data Deletion Procedures

User-Initiated Deletion

Option 1: Disconnect Single Bank (In-App)

Path: Settings → Bank Connections → Disconnect

What happens: - Connection status set to inactive - No new data fetched - Raw bank data queued for deletion (30 days) - Processed expenses/incomes **remain**

Option 2: Tink Consumer Revocation

URL: https://tink.com/consumer/revocation

What happens: - Tink revokes consent - FiredUp receives webhook (if configured) - Connection marked as inactive - Same deletion process as Option 1

Option 3: Full Account Deletion

Path: Settings → Delete Account (or email request)

What happens: - User account deleted - All connections deleted - All raw bank data deleted - All processed transactions deleted - Analytics data anonymized - Audit logs retained (12 months, anonymized user_id)

Option 4: GDPR Erasure Request (Art. 17)

Contact: privacy@firedup.app

What happens: - All data deleted within 30 days - Confirmation sent to user - Audit log entry created (anonymized)

Deletion Timeline

```
Day 0:  Request received / action taken
Day 1:  User data marked for deletion
Day 7:  Access tokens invalidated (if not already)
Day 30: Raw bank data permanently deleted
Day 30: Confirmation sent to user
```

Data Subject Rights (GDPR)

Right of Access (Art. 15)

Request method: Email to privacy@firedup.app **Response time:** 30 days **Format:** JSON or PDF export

Data provided: - User profile information - All financial data (manual + imported) - Bank connection status - Processing activities log

Right to Rectification (Art. 16)

Method: In-app editing or email request **Scope:** User-entered data only (not bank source data)

Right to Erasure (Art. 17)

Method: In-app or email request **Scope:** All user data **Timeline:** 30 days

Right to Data Portability (Art. 20)

Method: Settings → Export Data (or email request) **Format:** CSV or JSON **Included:** All transactions, accounts, categories

Right to Restriction (Art. 18)

Method: Email request **Effect:** Data retained but not processed

Right to Object (Art. 21)

Method: Email request **Scope:** Marketing (if any), analytics **Note:** Cannot object to core service processing

Right to Withdraw Consent (Art. 7)

Method: Disconnect bank in-app or Tink revocation portal **Effect:** No further data collection **Note:** Previously collected data retained per schedule

---

Third-Party Data Sharing

Data Processors

Processor	Purpose	Location	DPA
Tink AB	Bank data aggregation	Sweden (EU)	Yes
Vercel Inc.	Frontend hosting	USA (EU-US DPF)	Yes
PostHog Inc.	Product analytics	USA/EU	Yes
Google LLC	Authentication	USA (EU-US DPF)	Yes

Data Transfer Safeguards

For transfers outside EU/EEA: - EU-US Data Privacy Framework (certified recipients) - Standard Contractual Clauses (SCCs) - Data minimization (only necessary data transferred)

No Data Selling

FiredUp **does not** sell user data to third parties. Data is only shared with processors necessary to provide the service.

Consent Management

Initial Consent (Account Creation)

When user creates account: - Accept Terms of Service - Accept Privacy Policy - Consent to necessary data processing

Bank Connection Consent

When user connects bank: 1. **In-App Notice:** Explains what data will be accessed 2. **Tink Link:** User authenticates with bank 3. **Bank Consent Screen:** User grants consent to bank 4. **Recorded:** Timestamp and consent scope stored

Consent Records

Field	Stored
`user_id`	Yes
`consent_type`	Yes (account, banking)
`timestamp`	Yes
`scope`	Yes (data types)
`version`	Yes (policy version)
`ip_address`	Yes (for fraud prevention)

Privacy Policy Reference

Our public Privacy Policy covers: - Administrator identification (Section 1) - Data collected (Section 2) - Processing purposes (Section 3) - Legal basis (Section 4) - Tink integration details (Section 5) - Data sharing (Section 6) - Retention periods (Section 7) - User rights (Section 8) - Consent withdrawal (Section 9) - Security measures (Section 10) - Cookies (Section 11) - Policy changes (Section 12) - Complaints to PUODO (Section 13) - Contact information (Section 14)

URL: https://firedup.app/privacy

Compliance Checklist

Requirement	Status	Evidence
Privacy Policy published	✅	https://firedup.app/privacy
Terms of Service published	✅	https://firedup.app/terms
Data retention defined	✅	DATA_RETENTION constants
Deletion procedures	✅	In-app + email
Data export available	✅	Settings → Export
Consent recorded	✅	TinkConnection.created_at
DPAs with processors	✅	On file
PUODO notification	✅	Processing registry
Data minimization	✅	Only necessary scopes
Purpose limitation	✅	Budgeting only

Contact for Data Requests

Data Protection Contact: - Email: privacy@firedup.app - Response time: 30 days (as per GDPR)

Supervisory Authority: - Prezes Urzędu Ochrony Danych Osobowych (PUODO) - ul. Stawki 2, 00-193 Warszawa - https://uodo.gov.pl

---

Document Revision

Version	Date	Changes
1.0	February 2026	Initial version