



FEALTHY LLC

Privacy Policy

Last updated: May 21, 2026

This Privacy Policy (the "Policy") describes how FEALTHY LLC (hereinafter "Fealthy," "we," or the "Company") collects, uses, protects, and discloses information (including personal data) about users (hereinafter "User," "you") of Fealthy services.

Fealthy is a personal finance management application that helps you track income and expenses, connect bank accounts for automatic transaction synchronization, receive AI-powered spending insights, and collaborate on shared budgets with family and friends.

Our services are available through:

- **Mobile application:** <https://fealthy.app> (<https://fealthy.app>)
- **Web application:** <https://web.fealthy.app> (<https://web.fealthy.app>)
- **Marketing website:** <https://fealthy.com.ua> (<https://fealthy.com.ua>)

(collectively, the "Services")

Key Principles

- **Transparency and Security.** We are committed to transparent and secure data processing. We comply with the Law of Ukraine "On Personal Data Protection" and apply GDPR-aligned practices as an additional assurance of data protection, given that our primary servers are located in the European Union.
- **Legal Bases for Processing.** We process personal data only with your consent or on other lawful bases, including when:
 - (a) processing is necessary to provide our Services (performance of a contract);

- (b) processing is necessary to comply with legal obligations (including tax or accounting requirements);
- (c) processing is in our legitimate interests, provided these do not override your rights and freedoms.
- **Special Categories of Data.** We do not process "special categories" of personal data (e.g., racial or ethnic origin, political opinions, religious or philosophical beliefs, health data, biometric data for identification purposes), unless expressly permitted by law and you have provided explicit consent.
- **AI Processing Transparency.** We use artificial intelligence to categorize your transactions and provide spending insights. You have the right to opt out of AI-based analysis at any time through your account settings.
- **Age Policy.** Fealthy is intended for users aged **14+** (Ukraine) or the applicable **13–16** EU threshold. Users below the threshold must have parental or guardian consent (full details in §8).
- **Acceptance of this Policy.** By using Fealthy's Services, you confirm that you have read this Policy and agree to the processing of data as described herein.

1. Definitions

1.1. Personal Data

Any information that directly or indirectly identifies a natural person (full name, contact details, technical device information, financial transaction data, etc.).

1.2. Processing

Any operation or set of operations performed on personal data (collection, storage, use, disclosure, deletion, etc.).

1.3. User / You

A natural person who has installed the App or uses the Website and has agreed to this Policy and the Terms of Service. Users under 14 (or the applicable EU age threshold — see §8) must have parental consent.

1.4. Application / App

The Fealthy mobile application for Android/iOS, as well as the web version at <https://web.fealthy.app> (<https://web.fealthy.app>).

1.5. Website

The informational and marketing site at <https://fealthy.com.ua> (<https://fealthy.com.ua>).

1.6. Bank Integration

The feature that allows read-only access to your bank account data through the Monobank API (support for additional Open Banking providers is planned as they become available in Ukraine). Fealthy cannot modify your bank data or initiate payments.

1.7. AI Processing

Automated analysis of your financial data to categorize transactions and provide spending insights and predictions.

1.8. Shared Budget

A feature allowing multiple users to collaborate on budget management, where each user controls the visibility of their own data.

1.9. Third-Party Services

Services or platforms of third parties (Google, Apple, Monobank, analytics providers, etc.) that Fealthy may use to provide the functionality of the Services.

2. Data We Collect

2.1. Registration and Authentication Data

- **Account credentials:**

Email address, password (processed and stored as a salted hash by our authentication provider Auth0 — see §4.5; Fealthy never sees your plaintext password), name or nickname.

- **Phone authentication:**

Phone number if you choose to register or authenticate via SMS/OTP.

- **Social login data:**

If you sign in with Google or Apple, we receive your name, email address, and unique identifier from that service. We do not receive your social account password.

- **QR code authentication:**

Session tokens for linking devices; no additional personal data is collected.

2.2. Financial Data (Read-Only Access)

- **Bank account data:**

If you connect a bank account (currently Monobank; additional Open Banking providers will be added as support is rolled out — see §12.3), we access your account balance, transaction history, income, and expenses. This access is strictly read-only — Fealthy cannot modify data, transfer funds, or make payments on your behalf.

- **Manual entries:**

Any income, expenses, or transactions you manually record in the app.

2.3. User-Generated Content

- **Profile photos:**

Avatar images you upload for your account.

- **Receipt photos:**

Images of receipts captured using your device's camera for expense tracking.

- **Documents and files:**

Any documents you choose to upload and attach to transactions or budgets.

- **Notes and text:**

Comments, descriptions, and notes you add to transactions or budgets.

2.4. Voice Data

- **Voice commands:**

If you use voice features to create records or control the application, your voice is transmitted in real time to our third-party speech-to-text processors: **AssemblyAI** (primary, United States) and **OpenAI** (Whisper, fallback, United States). Fealthy does not store voice recordings on its own infrastructure. These processors may briefly retain audio to provide the service in accordance with their own privacy policies. The full list of third-party recipients and the categories of data each receives is set out in Section 4.7.

2.5. Biometric Data

- **Device biometrics (FaceID / TouchID):**

If you enable biometric authentication to unlock the app, this is processed entirely on your device by your operating system. **Fealthy never receives, transmits, or stores your biometric data** — we only receive a confirmation that authentication succeeded.

2.6. Technical Information

- **Device data:**

Device model, operating system version, unique device identifiers.

- **Log files:**

IP address, browser type, pages you visit, date and time of access, crash diagnostics and error reports.

2.7. Analytics and Interaction Data

- **Service usage:**

Session frequency and duration, features used, settings preferences, and AI categorization choices (collected only when AI features are enabled — see §10.3).

- **Shared budget participation:**

Group memberships, your visibility settings within groups.

- **Referral data:**

Pseudonymous referral tracking (we do not reveal your identity to referred users, but we may associate a referral with your account to credit rewards).

2.8. Payment & Subscription Data

- **Purchase receipts:**

Transaction identifiers, subscription status, validity period, and auto-renewal flags — from Apple App Store, Google Play, and Monobank Acquiring (see §4.11).

- **Billing email address:**

The email address associated with your account at the payment store (Apple ID / Google Account) when provided by the payment processor.

- **Payment-card details:**

Fealthy does not receive or store payment-card details. They are processed exclusively

by the relevant payment processor.

3. Purposes and Legal Bases of Processing

3.1. Providing and Improving the Services

We use your data to enable registration, account login, bank synchronization, income/expense tracking, AI-powered categorization, and all other app features.

Legal basis: Performance of a contract (providing the Services you requested).

3.2. Bank Data Synchronization

We retrieve your financial data from connected banks to display your transactions and provide analysis.

Legal basis: Performance of a contract; your explicit consent when connecting a bank account.

3.3. AI-Powered Analysis

We use artificial intelligence to automatically categorize transactions and provide spending insights, predictions, and recommendations.

Legal basis: Legitimate interest in improving user experience. You may opt out at any time in settings.

3.4. Communication

We may send you:

- Service notifications (security alerts, important updates, password resets)
- Marketing communications (newsletters, feature announcements, tips)

Legal basis: Legitimate interest for service notifications; your consent for marketing communications.

How we capture and revoke marketing consent: Consent for marketing communications is requested via a dedicated opt-in at sign-up or in account settings (the "Notifications / Marketing" section). You can revoke consent at any time by (a) toggling the setting in your account, or (b) clicking "Unsubscribe" in any marketing email. Revocation does not affect service notifications, which are sent on the contract-performance basis.

3.5. Analytics and Service Improvement

We analyze usage patterns (in anonymized/aggregated form where possible) to improve the Service, identify popular features, and fix issues.

Legal basis: Legitimate interest in improving and maintaining the Services.

3.6. Compliance with Legal Obligations

Where required, your data may be processed to comply with Ukrainian law (accounting, taxes, court requests, etc.) and with applicable European Union data-protection law for users located in the EU.

Legal basis: Legal obligation.

4. Disclosure and Transfer of Data

This section lists every category of third-party recipient that may process your data on our behalf to provide the Services. Data sharing with other members of shared budgets is described separately in Section 9.

4.1. Bank Integration Providers

When you connect a bank account, certain data is exchanged with:

- **Monobank** (via their official API)
- **Open Banking providers** (as we expand bank support)

These providers operate under their own privacy policies.

4.2. Cloud Infrastructure — Google LLC (Google Cloud Platform)

Your data is currently stored on **Google Cloud Platform** (Google LLC) servers located in **Warsaw, Poland** (European Union). Google Cloud complies with GDPR and maintains appropriate security certifications. We will update this Policy if the primary region changes.

4.3. Analytics Services

We use the following analytics services to understand how our Services are used:

- **Google Analytics** (Google LLC) — website and app analytics
- **Firebase Analytics** (Google LLC) — mobile app analytics

These services may receive anonymized or pseudonymized usage data.

4.4. Social Login Providers

If you use social login:

- **Google** (Google LLC) — for "Sign in with Google"
- **Apple** (Apple Inc.) — for "Sign in with Apple"

These services only facilitate authentication; they do not receive your financial data.

4.5. Authentication & Identity Management — Auth0 (Okta, Inc., United States)

Auth0 processes your login credentials: email address, password hash, phone number (for SMS/passwordless flows), social-login identifiers, and authentication events. The tenant is hosted in the EU region.

4.6. AI Processing — OpenAI (OpenAI, L.L.C., United States)

Transaction descriptions, merchant information, and historical category labels are sent to **OpenAI** for automated categorization and spending insights. By default, OpenAI retains API requests for up to **30 days** for abuse monitoring; no Zero Data Retention agreement with OpenAI is currently in place. Used only when AI features are enabled (see §10.3).

4.7. Voice Transcription — AssemblyAI (United States), OpenAI Whisper (United States)

Audio captured by the voice-commands feature is transmitted to:

- **AssemblyAI, Inc.** — primary provider (United States)
- **OpenAI Whisper** — fallback provider (United States)

Active only when you invoke a voice command. Providers retain audio under their own privacy policies.

4.8. Transactional Email — Twilio SendGrid (United States)

SendGrid (a Twilio company) processes your email address and email body content for account verification, password reset, security alerts, and (with your consent) marketing communications.

4.9. Crash Reporting & Push Delivery — Google LLC (Firebase Crashlytics, Cloud Messaging)

Firebase Crashlytics processes crash diagnostics (device model, OS version, stack traces, anonymized user identifier). **Firebase Cloud Messaging** processes push device tokens and delivery status. Distinct from §4.3 (Firebase Analytics).

4.10. Observability & Logging — Grafana Labs, Inc. (Grafana Cloud — Loki / Tempo / Faro, EU)

Grafana Cloud processes application logs, traces, and frontend telemetry. May contain user identifiers, IP addresses, and operational metadata. Retention period: 30 days.

4.11. Payments & Subscriptions

Receipt validation and subscription state are shared with:

- **Apple Inc.** — App Store In-App Purchase
- **Google LLC** — Google Play Billing
(both via the `@capgo/native-purchases` SDK)
- **Monobank** (Monobank Acquiring API; branded "Mono Pay" in the checkout UI) — for direct payments

Card details are processed by the respective payment processors and are never transmitted to Fealthy or stored by us.

4.12. Support — Telegram FZ-LLC

When you contact Fealthy via the Telegram support bot, your Telegram identifier and message contents are processed by **Telegram**. Use of the support bot is optional.

4.13. Operational Vendors

- **logo.dev** — logo lookups by merchant domain (no user identifier is transmitted).
- **Slack Technologies, LLC** — internal error alerts (operational metadata only, no personal data).

4.14. Legal Requirements

We may disclose your data:

- Pursuant to a lawful request by Ukrainian courts or competent governmental authorities

- Where necessary to prevent violations, fraud, or threats to safety

4.15. Other Service Providers

We may share data with trusted service providers who assist our operations:

- Legal advisors and accountants
- Technical support providers

All such providers are bound by confidentiality agreements.

5. Data Storage and Security

5.1. Data Location

Your data is stored on Google Cloud Platform servers in **Warsaw, Poland** (European Union), ensuring GDPR-compliant infrastructure.

5.2. Retention Period

Data lives in several systems with different technical retention windows. The actual windows are:

5.2.1. Active accounts

Data is stored for as long as your account is active.

5.2.2. Account flagging

Within **1 hour** of receiving your deletion request, your account is flagged for deletion.

5.2.3. Active database

Once flagged, your account is deactivated and your personal data is no longer accessible through, or used by, the Services. Records are then erased from our active database as part of our deletion process; erasure is carried out on a periodic basis.

5.2.4. Database backups

Encrypted backups (point-in-time recovery + daily snapshots) retain copies of your data for up to **30 days**, after which they are automatically and irretrievably destroyed.

5.2.5. Application logs & telemetry

Retained for **30 days** (Google Cloud Logging, Grafana Cloud Loki, Firebase Crashlytics).

5.2.6. Uploaded files

Receipt photos, profile photos, and attachments stored in Google Cloud Storage are erased together with your account records (see §5.2.3).

5.2.7. Third-party processors

Providers listed in Section 4 retain copies in their own systems for the windows defined by their privacy policies (e.g., OpenAI — up to 30 days by default; Auth0 — plan-dependent; AssemblyAI — per their policy).

5.2.8. Legal retention

Records required by Ukrainian tax, accounting, or anti-money-laundering law are retained for the statutory period (typically **3 years** from end of fiscal year) regardless of any deletion request.

5.3. Security Measures

We implement appropriate organizational and technical measures to protect your data:

- **Encryption:** Data encrypted in transit (TLS/SSL) and at rest
- **Access controls:** Strict access policies for employees and systems
- **Security monitoring:** Continuous monitoring for unauthorized access attempts
- **Password hashing:** Passwords are processed and stored as salted hashes by Auth0 (see §4.5)
- **Responsible vulnerability disclosure:** Security researchers may report vulnerabilities to security@fealthy.com.ua. We respond to security reports as quickly as possible.

5.4. Biometric Security

Biometric data (FaceID/TouchID) is processed entirely on your device and **never transmitted to or stored on our servers**.

5.5. Voice Processing Security

Fealthy does not store voice recordings on its own servers. Audio is transmitted in real time to third-party speech-to-text processors (see §4.7); those processors may briefly retain

audio to deliver the service in accordance with their own privacy policies.

6. Your Rights

Under the Law of Ukraine "On Personal Data Protection," you have the following rights:

6.1. Access

You have the right to know whether we process your personal data and to receive information about such processing.

6.2. Rectification and Update

You can correct or update your personal data (name, email, profile information) in your account settings at any time.

6.3. Erasure

You can delete your account and all associated data through the app settings. Upon deletion:

- Your account is flagged for deletion within 1 hour and immediately deactivated
- Bank connections are immediately severed
- Shared budget memberships are terminated
- Your data is then erased across our systems within the windows described in §5.2

6.4. Restriction of Processing

In certain cases, you may request that we restrict processing of your data (e.g., while we verify its accuracy).

6.5. Objection to Processing

You can object to processing based on our legitimate interests (e.g., marketing communications). We will cease such processing unless we have compelling legitimate grounds.

6.6. AI Opt-Out

You have the right to opt out of AI-based transaction categorization and spending insights. This can be done in your account settings. Opting out will not affect your access to other features. Opting out also stops collection of AI-related telemetry (categorization choices, model interactions); previously collected AI-derived data is retained per §5.2 unless you separately request its deletion.

6.7. Withdraw Consent

Where processing is based on consent (e.g., marketing emails, bank connections), you may withdraw consent at any time without affecting the lawfulness of prior processing.

6.8. Right to Data Portability

You may request a machine-readable export of your personal data by contacting hello@fealthy.ua. We will provide the export within **30 days** of identity verification. Self-serve export is on our roadmap.

6.9. Right to Lodge a Complaint

You may lodge a complaint with the **Ukrainian Parliament Commissioner for Human Rights** (the Ombudsperson, the supervisory authority for personal-data protection in Ukraine — ombudsman.gov.ua (<https://ombudsman.gov.ua>)). Users in the European Union may also lodge a complaint with the Data Protection Authority (DPA) of their country of residence.

6.10. Right to Be Informed of a Breach

If a personal-data breach is likely to result in a high risk to your rights and freedoms, we will notify you and the relevant supervisory authority without undue delay (and in any event within **72 hours** where required by law).

To exercise your rights, contact:

hello@fealthy.ua

. We may request additional information to verify your identity.

7. Cookies and Similar Technologies

7.1. Cookies

We use cookies (small text files stored on your device) to improve website and app performance, analyze traffic, and remember your preferences.

7.2. Types of Cookies

- **Session cookies:** Deleted when you close your browser
- **Persistent cookies:** Stored on your device for a defined period
- **Third-party cookies:** Placed by analytics services (Google Analytics, Firebase)

7.3. Essential vs Non-essential Cookies

We categorize cookies into two groups:

- **Essential:** required for the Services to operate (login session, security tokens, preferences). Set regardless of your consent on the contract-performance basis.
- **Non-essential:** analytics cookies (Google Analytics, Firebase Analytics) that help us understand usage patterns and fix issues.

7.4. Analytics Technologies

We use Google Analytics and Firebase Analytics to collect pseudonymized usage statistics, including:

- Pages/screens visited
- Session duration
- Feature usage patterns
- Crash reports

7.5. Consent and Cookie Management

Current state: A dedicated consent banner for non-essential cookies is not yet in place. We are actively working to add it, after which non-essential (analytics) cookies will be set only once you have given explicit opt-in consent. We treat the absence of this banner as a known compliance gap that we are remediating — we do not rely on your continued use of the Services as consent to non-essential cookies.

In the meantime, you can opt out of non-essential cookies at any time via:

- Your browser settings (block or delete cookies)
- Your device settings (for mobile advertising identifiers)
- [Google Analytics Opt-Out](https://tools.google.com/dlpage/gaoptout) (<https://tools.google.com/dlpage/gaoptout>)
- Firebase Analytics settings linked to your account

Disabling essential cookies may render parts of the Services inoperable.

8. Children's Policy

8.1. Age Requirements

Fealthy is intended for users aged **14 and older** (per Ukrainian law). For EU users, national age thresholds apply (13–16 years; see §8.4). Users below the applicable threshold in their country of residence must have **parental or guardian consent** before using the Services.

Fealthy does not currently operate an automated age-verification or parental-consent system. We rely on the representation that any required parental or guardian consent has been obtained, and we act on any parental or guardian notice as described in §8.2. We are evaluating dedicated age-assurance measures.

Age ratings set by the Apple App Store and Google Play may differ — please check the relevant store listing before downloading.

8.2. Parental Consent

If you are a parent or guardian and believe your child below the applicable age threshold has provided personal data without your consent, please contact us at hello@fealthy.ua so we can delete such information.

8.3. Parental Controls

Parents/guardians may contact us to:

- Access their child's data
- Request correction of their child's data
- Request deletion of their child's account

8.4. Users in the European Union

The age of consent for data processing in the EU varies by member state between **13 and 16**. Users below the applicable threshold in their country of residence must obtain parental consent under their local law before using the Services. Fealthy is primarily targeted at the Ukrainian market, where the 14-year threshold applies under Ukrainian law.

9. Shared Budgets and Social Features

9.1. Shared Budgets

Fealthy allows you to create and participate in shared budgets with family members or friends. When using this feature:

- **You control visibility:** You decide what data (transactions, categories, amounts) is visible to other group members
- **Custom sharing:** Each item can have individual visibility settings
- **Group membership:** Other members can see that you are part of the group

9.2. Data Visible to Other Members

Depending on your visibility settings, other group members may see:

- Shared transactions and amounts you choose to share
- Shared category totals
- Your name/nickname as a group member

They **cannot** see:

- Data you have not explicitly shared
- Your bank account details or credentials
- Your personal transactions outside the shared budget

9.3. Leaving Groups

You can leave any shared budget at any time. When you leave:

- Your future data will no longer be visible to group members.

- Your existing contributions to the shared budget ledger (transactions, categories, comments) that you previously shared with the group may remain visible to other members because the ledger is jointly held.
- You may contact us to request removal of your contributions from the shared ledger — we will review such requests balancing them against other members' rights to the continuity of their copy of the ledger (see §6.3).
- When you fully delete your account (§6.3), your individual group memberships are terminated; the handling of your prior contributions is as described above.

9.4. Pseudonymous Referrals

The people you refer cannot see your personal details unless you choose to share them. Internally, we link a referral to your account solely to credit rewards (see §2.7).

10. AI and Automated Processing

10.1. What AI Does

Fealthy uses artificial intelligence to:

- **Automatically categorize transactions** (e.g., groceries, transport, entertainment)
- **Provide spending insights** (patterns, trends, unusual activity)
- **Generate predictions** (upcoming expenses, savings opportunities)

10.2. How AI Works

Our AI analyzes:

- Transaction descriptions and amounts
- Merchant information (when available)
- Your historical spending patterns

AI processing is performed by **OpenAI** (see §4.6).

10.3. Opting Out of AI

You can disable AI features at any time in your account settings. When opted out:

- Transactions will not be automatically categorized

- You will not receive AI-generated insights or predictions
- You can still manually categorize transactions
- Collection of AI-related telemetry (categorization choices, model interactions) stops; previously collected AI-derived data is retained per §5.2 unless you separately request its deletion

10.4. Automated Decision-Making

We do not use AI to make decisions that produce legal or otherwise significant effects on you — AI features are informational and advisory only. If we introduce automated decisions that materially affect you in the future, we will notify you in advance, and you will have the right (under GDPR Article 22 and equivalent provisions of Ukrainian law) to: (a) obtain human intervention, (b) express your point of view, and (c) contest the decision.

11. Voice Commands

11.1. How Voice Works

Fealthy supports voice commands for creating records and controlling the application. When you use this feature:

- Your device's microphone captures your voice
- Voice is converted to text in real-time
- The text command is processed

11.2. Voice Data Handling

Audio captured by the microphone is transmitted to third-party speech-to-text providers:

- **AssemblyAI** — primary provider (United States)
- **OpenAI Whisper** — fallback provider (United States)

Fealthy does not store voice recordings on its own infrastructure. These providers may briefly retain audio to deliver the service in accordance with their own privacy policies. For details on the categories of data each third-party processor receives, see Section 4.7.

11.3. Microphone Permission

You control microphone access through your device settings. Voice features will not work without this permission, but all other app features remain available.

12. Bank Integration

12.1. Read-Only Access

When you connect a bank account, Fealthy receives **read-only access** to:

- Account balance
- Transaction history
- Income and expense data

We cannot and will not:

- Initiate transfers or payments
- Modify any bank data
- Access your banking credentials (login/password)

12.2. Current Bank Support

Currently supported:

- **Monobank** (via official API)

12.3. Future Bank Support

We plan to expand bank support through Open Banking APIs as they become available in Ukraine.

12.4. Bank Data Security

- **No bank passwords:** We never receive or store your bank login or password. Connection is established via scoped API tokens issued by the bank itself (currently Monobank).
- **Read-only:** These tokens grant read-only access — transferring funds or modifying account data is not possible.

- **Disconnection:** You can revoke a token at any time by disconnecting the bank in settings (see §12.5).

12.5. Disconnecting a Bank

To disconnect a bank account:

1. Go to Settings > Connected Accounts
2. Select the bank you wish to disconnect
3. Confirm disconnection

Upon disconnection:

- We immediately stop receiving new data from that bank
- Previously synced transaction data remains in your account (you can delete it separately)

13. International Data Transfers

13.1. Server Location

Your data is processed and stored on servers located in **Warsaw, Poland** (European Union), operated by Google Cloud Platform.

13.2. Legal Framework

Data transfers are conducted in compliance with:

- The Law of Ukraine "On Personal Data Protection"
- GDPR requirements (as our primary servers are in the EU)
- Google Cloud's data protection commitments

13.3. Transfers to Processors Outside the EEA

Several third-party processors listed in §4 (e.g., OpenAI, AssemblyAI, SendGrid, Apple, Google, Telegram, Slack) are based in the United States or other non-EEA jurisdictions. For transfers of personal data from the EEA / Ukraine to the US, we rely on one or more of the following legal instruments:

- The European Commission's **Standard Contractual Clauses (SCCs)**, incorporated into our contracts with these processors
- The processor's certification under the **EU-US Data Privacy Framework**, where applicable
- Other instruments permitted under GDPR Article 46

13.4. Safeguards

We ensure appropriate safeguards for any data transfers, including contractual protections with our service providers.

14. Changes to this Policy

14.1. Policy Updates

We may update this Policy to reflect:

- Changes in our data processing practices
- New features or services
- Changes in applicable law

Material changes — changes that affect your rights, the categories of personal data we process, or the categories of recipients with whom we share data — take effect **30 days** after we notify you via the channels in §14.2. Non-material changes (clarifications, typo fixes, formatting) take effect immediately on publication.

14.2. Notice of Changes

For material changes, we will notify you through the channels below, in order of reliability:

- **Prominent notice on our website** — the primary channel; deemed to have been given to all users.
- **Email notification** — secondary channel, sent on a best-effort basis (not delivered if your email is unverified, or if you have unsubscribed from non-transactional messages).
- **Push notification in the app** — secondary channel, sent on a best-effort basis (not delivered if push notifications are disabled on your device or the token is invalid).

14.3. Continued Use

Your continued use of the Services after policy changes constitutes acceptance of the updated Policy.

15. Contact Us

If you have questions, complaints, or suggestions regarding data protection and privacy:

- **Responsible person:** Rostyslav Anatoliiovych Pidburachynskyi, Director, FEALTHY LLC
- **Email:** hello@fealthy.ua

We will respond to your data-protection inquiry within **30 days**; we may request additional information to verify your identity.

This Privacy Policy is governed by the laws of Ukraine. It is published in Ukrainian and English; in the event of any discrepancy between the versions, the Ukrainian version prevails.