Privacy Policy — Friendly IT Solutions

Last update: 16 September, 2025

At **Friendly IT Solutions** ("**Friendly**," "**we**," "**us**," "**our**"), we respect your privacy and are committed to protecting your personal data. This Privacy Policy explains how we collect, use, disclose, and protect your information when you use our products and services, including our **card program** and related applications (the "**Services**").

By accessing or using the Services, you acknowledge that you have read and agree to this Privacy Policy.

1. What personal data do we collect?

1.1. Overview

We collect personal data in accordance with applicable laws (e.g., AML/CTF, data protection). We obtain data:

a. directly from you;
b. from your use of the Services;
c. from third parties (e.g., identity verification vendors, issuing/processing partners);

1.2. Data stored on our servers

We **only** store on our servers the following personal data you provide or confirm to us:

a. Full name;
b. Date of birth;
c. Mobile phone number;
d. Email address;
e. Gender;
f. Residential address;

We do **not** store biometric templates, identity document images/video, card PAN/CVV, or full transaction histories on our servers.

1.3. Data processed by our KYC provider (Sumsub)

For identity verification and liveness/anti-fraud checks we use **Sumsub** as our processor. Depending on your verification flow and local legal requirements, Sumsub may collect and process on our behalf:

a. Images/scans of identity documents and proof-of-address;
b. Selfie/liveness video frames, face embeddings, and other **biometric** identifiers strictly for identity verification;
c. Verification results, risk flags, and audit logs required by AML/CTF law.

These data are **stored by Sumsub** under their security and retention policies. Friendly does not store biometric templates or document images/videos on its servers.

Where required by law, we will obtain your **explicit consent** for biometric processing. In other jurisdictions, processing may rely on **legal obligations** under AML/CTF rules and legitimate interests in fraud prevention.

1.4. Card program and payments data (via partners)

To issue and operate payment cards, our **issuing bank / BIN sponsor / card processor** (collectively, “card program partners”) process data such as:

- Card lifecycle data (card identifier, token, masked PAN/last-4, status);
- Transaction metadata (date/time, amount, currency, merchant name/MCC, country, auth/clearing status);
- Fraud/risk signals, disputes/chargebacks.

Friendly may **view** or **temporarily cache** limited metadata via API to display it to you, but we do **not** store PAN/CVV and do not maintain your full transaction history on our servers. Card data are stored and secured by our card program partners.

1.5. Technical/usage data

We may collect technical information (IP address, device type/ID, OS, app version, locale, interaction logs) to secure and improve the Services.

1.6. Children

We do not knowingly collect data from individuals under **18**. Do not use the Services or submit data if you are under 18.

2. How do we collect personal data?

We collect data when you:

a. register or interact with the Services;
b. undergo KYC/identity verification (processed by Sumsub);
c. request a card or use card features (processed by card program partners);
d. contact support.

We may update our records using information from authorized third parties, ensuring they comply with data protection laws and have informed you appropriately.

3. Purposes and legal bases

We process personal data for:

Purpose	Legal basis
Provide and operate the Services (including onboarding, account profile, app features)	Contract performance
Card issuance and servicing with our card program partners	Contract performance

Identity verification (KYC), sanctions/PEP screening, AML/CTF compliance	Legal obligation; substantial public interest where applicable; explicit consent for biometrics where required
Fraud prevention, risk scoring, abuse/threat detection, security monitoring	Legitimate interests
Support and service communications (notices, updates, security alerts)	Contract performance / Legitimate interests
Improve user experience, functionality, and safety	Legitimate interests
Direct marketing and personalized offers (if applicable)	Consent (where required) / Legitimate interests (where permitted)

We do **not** make decisions **solely** by automated means that produce legal or similarly significant effects without human review. Automated tools (including AI-assisted checks) may assist fraud/KYC reviews, subject to human oversight.

4. How do we protect your personal data?

We apply technical and organizational measures including encryption in transit and at rest (where applicable), network and application firewalls, access controls, logging/monitoring, and vendor due diligence. While no method is 100% secure, we maintain a program to prevent, detect, and respond to incidents, and we contractually require processors to protect data appropriately.

5. How long do we keep your data?

We retain personal data **only as necessary** for the purposes above and to meet legal obligations. For AML/CTF, identity verification records are typically retained for **up to 5 years** after the end of your relationship (or longer if required by law).

a. **On Friendly servers**: only the fields listed in §1.2, retained per contract/legal requirement;
b. **Biometrics/ID documents**: retained by **Sumsub** under AML/CTF retention rules;
c. **Card/transactions**: retained by **card program partners** per scheme/banking laws.

6. Who is the data controller? Who are the processors?

Data Controller: Friendly IT Solutions Limited (Hong Kong)

Registered office: Unit 1603, 16/F, The L. Plaza, 367–375 Queen's Road Central, Sheung Wan, Hong Kong

Contact: **info@friendlypay.io**

We use vetted **processors** to provide parts of the Services, including:

a. **Sumsub** (identity verification, biometrics and KYC processing);
b. **Issuing bank / BIN sponsor / card processor** (card issuance, transactions, fraud, disputes);
c. Communications providers (SMS/e-mail), hosting/cloud, analytics, and support tooling.

Each processor acts under our instructions and appropriate data protection terms.

7. Sharing and disclosures

We may share personal data with:

a. **Service providers/processors** acting on our behalf (see above), limited to what's necessary;
b. **Card program partners** (issuer, processor, BIN sponsor, card network/scheme) to issue and operate your card;
c. **Auditors, advisors, and consultants** (including security and compliance audits);
d. **Law enforcement/regulators/courts** where required by law;
e. **Other users or third parties** at your request or with your authorization.

We implement contractual safeguards (including **Standard Contractual Clauses**/UK **IDTA** or other approved mechanisms) for international transfers and require recipients to maintain adequate security.

8. Your rights

Your rights may include: information, access, rectification, erasure, restriction, objection (including to direct marketing), data portability, and complaint to a supervisory authority. These may vary by jurisdiction and can be limited by AML/CTF or other legal obligations.

a. Biometrics/KYC handled by Sumsub: submit requests to us and we will coordinate with Sumsub;

9. Cross-border data transfers

We and our processors may transfer data internationally (including outside your country of residence) to operate the Services, comply with law, and perform the card program and KYC. Where required, we rely on approved transfer tools (e.g., **SCCs**, **IDTA**, or adequacy decisions).

10. Updates

Wallet may change this Privacy Policy from time to time at its sole discretion. By continuing to use our services, you agree to be bound by these updates and changes to the Privacy Policy.