PRIVACY POLICY

PILOT INNOVATION SP. Z O.O.

This Privacy Policy applies to users of:

- the website **www.paypilot.org**
- the PayPilot mobile application

(hereinafter collectively referred to as the “Platform”).

This Privacy Policy (the “Policy”) explains how we collect, use, process, store, and disclose personal data obtained:

- directly from users,
- automatically through use of the Platform,
- via cookies and similar technologies,
- or in connection with the provision of our services.

This Policy constitutes an integral part of the Terms of Service.

Data Controller

The controller of personal data processed in connection with the use of the Platform is:

Pilot Innovation sp. z o.o.
KRS: 0001137957
Registered office: al. Stanów Zjednoczonych 32/8, 04-036 Warsaw, Poland
(hereinafter referred to as the “Company”, “PayPilot”, “we”, “us” or “our”).

The Platform is owned and operated by PayPilot.

The Platform is intended for individuals who are at least 18 years of age. Persons under the age of 18 are not permitted to use the Platform.

Scope and Purpose of Data Processing

We provide services enabling the exchange of cryptocurrencies into fiat currencies and other digital asset-related services as described in our Terms of Service.

In connection with the provision of our services, we collect and process personal data strictly to the extent necessary for the following purposes:

- providing access to and operating the Platform;
- performing identity verification (KYC) and complying with AML/CFT obligations;
- processing transactions;
- maintaining security and preventing fraud;
- responding to user inquiries;
- improving the functionality and performance of the Platform;
- complying with legal and regulatory obligations.

The Platform enables users to contact the Company and provide identification details, contact information, and the content of their messages.

We also collect data related to user activity on the Platform, including but not limited to:

- time spent on the Platform,

- number of pages viewed,
- search queries,
- date and source of visit,
- technical device and connection information.

Personal data is processed exclusively for the purposes defined in this Policy and in accordance with applicable data protection laws.

We share personal data with third parties only where it is necessary for the provision of our services, compliance with legal obligations, or based on another valid legal basis under applicable law (including user consent where required).

Contact Details

If you have any questions regarding this Privacy Policy or the processing of your personal data, you may contact us at:

Email: support@paypilot.org
Postal address:
Pilot Innovation sp. z o.o.
al. Stanów Zjednoczonych 32/8
04-036 Warsaw, Poland

Categories and Sources of Personal Data

We respect your privacy and process personal data transparently and in accordance with applicable data protection laws.

We may collect personal data from the following sources:

1. Data provided directly by you

You provide personal data to us when you:

- create an account,
- complete forms on the Platform,
- use our services,
- contact us by email or other communication channels,
- undergo identity verification (KYC).

Such data may include:

- Full name
- Date of birth
- Nationality
- PESEL number or other national identification number (if applicable)
- Identity document details (ID card, passport, driver's license)
- Image (including selfie or video verification, where required)
- Residential address and tax residency information
- Politically Exposed Person (PEP) status
- Email address
- Telephone number
- Bank account number
- Transaction-related information

2. Data collected in connection with legal entity clients

Where the Client is a legal entity, we may process personal data relating to:

- Authorized representatives
- Directors
- Beneficial owners (UBOs)
- Persons acting on behalf of the legal entity

This may include:

- Full name
- Nationality
- Residential address
- Tax residency
- PEP status
- Date of birth
- Personal identification number (if required by law)
- Email address
- Telephone number

Such data is processed strictly for identification, AML/CFT compliance, and regulatory purposes.

3. Data obtained indirectly

In certain cases, personal data may be obtained indirectly, including:

- From a person referring a matter to us on your behalf
- From publicly available registers (e.g., company registers)
- From identity verification providers
- From AML/sanctions screening databases
- From payment service providers

In such cases, we process only data necessary for the specific purpose and in compliance with applicable legal requirements.

Contact Data (Find Friends Functionality)

If you choose to use the “Find Friends” or similar feature within the PayPilot mobile application, we may request access to your device contacts.

Access to your contacts is optional and requires your explicit consent.

If you grant permission:

- Contact identifiers (such as phone numbers and/or email addresses) from your contact list may be processed locally on your device and transformed into hashed values before being securely transmitted to our servers.
- Only hashed contact identifiers are transmitted and used exclusively for the purpose of determining whether your contacts are existing PayPilot users.
- We do not transmit, store, or process contact names or other contact details in readable form on our servers.
- Contact data is not used for marketing, profiling, analytics, or advertising purposes.
- We do not sell, rent, or otherwise share contact data with third parties.

The matching process is performed solely using hashed identifiers. Contact identifiers are retained only for the time necessary to perform the matching process, unless a longer retention period is required for security, fraud prevention, or legal compliance purposes.

You may withdraw access to your contacts at any time through your device settings.

The legal basis for processing contact identifiers is your explicit consent pursuant to Article 6(1)(a) of the GDPR.

Use of Cookies and Similar Technologies

The Platform uses cookies and similar technologies (such as SDKs, pixels, and local storage) to ensure proper functioning, security, and performance of the Website and mobile application.

Cookies are small data files stored on your device (computer, tablet, smartphone) when you visit the Platform.

We use the following categories of cookies and similar technologies:

1. Strictly Necessary Cookies

These are required for the proper operation of the Platform and cannot be disabled in our systems. They are used, for example, to:

- maintain user sessions after login,
- ensure security and prevent fraud,
- enable core functionality of the Platform,
- remember privacy preferences and consent choices.

These cookies do not require consent.

2. Functional Cookies

These enable the Platform to remember user preferences, such as:

- interface settings,
- language selection,
- accessibility settings.

Functional cookies are used only where permitted by applicable law.

3. Analytics and Performance Technologies

We may use analytics tools to collect aggregated information about:

- device type,
- operating system,
- browser type,
- session duration,
- pages visited,
- technical performance metrics.

This data is used to improve functionality, stability, and security of the Platform. Where required by law, analytics technologies are activated only after obtaining user consent.

4. Security-Related Technologies

We may use cookies and similar technologies to:

- detect suspicious activity,
- prevent unauthorized access,
- protect against fraud and abuse.

Security-related processing is based on our legitimate interest in protecting users and complying with regulatory obligations.

Data Combination and Identification

Information collected through cookies and similar technologies may be combined with other technical data necessary for security and fraud prevention purposes.

We do not use cookies to directly identify users without a valid legal basis.

Managing Cookies

You can manage or withdraw your consent to non-essential cookies at any time through:

- the cookie consent banner available on the Website,
- your browser settings,
- your device settings (for mobile applications, where applicable).

Most browsers allow you to block or delete cookies. Please note that disabling certain cookies may affect the functionality of the Platform.

Use of the Platform does not constitute consent to non-essential cookies unless such consent has been explicitly provided via a consent management mechanism.

Purpose, Legal Basis and Grounds for Processing Personal Data

We process personal data for the following purposes and on the following legal bases under Article 6 GDPR:

1. Performance of a Contract (Art. 6(1)(b) GDPR)

We process personal data where necessary for the performance of a contract or in order to take steps prior to entering into a contract, including:

- Creating and maintaining a user account;
- Providing access to and operating the Platform;
- Executing cryptocurrency and fiat transactions;
- Delivering services described in the Terms of Service;
- Providing customer support.

2. Compliance with Legal Obligations (Art. 6(1)(c) GDPR)

We process personal data where required to comply with applicable laws and regulatory obligations, including:

- Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) regulations;
- Know Your Customer (KYC) verification requirements;
- Sanctions screening;
- Reporting obligations to competent authorities;
- Accounting and tax regulations.

Where processing is based on legal obligation, consent is not required and cannot be withdrawn in relation to such processing.

3. Legitimate Interests (Art. 6(1)(f) GDPR)

We process personal data based on our legitimate interests, provided that such interests are not overridden by your rights and freedoms, including:

- Ensuring the security of the Platform;
- Preventing fraud, abuse, and unauthorized access;
- Analyzing usage and improving functionality;
- Handling complaints and resolving disputes;
- Establishing, exercising, or defending legal claims.

4. Consent (Art. 6(1)(a) GDPR)

We process personal data based on your explicit consent where required, including:

- Processing contact identifiers for the “Find Friends” functionality;
- Sending marketing communications (where required by applicable law);
- Using non-essential cookies and analytics technologies (where consent is required).

Consent may be withdrawn at any time without affecting the lawfulness of processing based on consent before its withdrawal.

Right to Withdraw Consent

Where processing is based on your consent, you may withdraw that consent at any time:

- by adjusting your device settings (for contact access),
- by managing cookie preferences,
- by unsubscribing from marketing communications,
- or by contacting us at support@paypilot.org.

Withdrawal of consent does not affect processing carried out on other legal bases (such as contractual necessity or legal obligation).

Please note that withdrawal of consent for certain functionalities (e.g., contact matching or marketing communications) may limit or disable related features of the Platform.

Your Rights Under the GDPR

In accordance with the General Data Protection Regulation (GDPR), you have the following rights in relation to your personal data:

1. Right of Access (Art. 15 GDPR)

You have the right to obtain confirmation as to whether we process your personal data and, if so, to request access to that data and receive a copy.

2. Right to Rectification (Art. 16 GDPR)

You have the right to request correction of inaccurate personal data and to complete incomplete data.

3. Right to Erasure (“Right to be Forgotten”) (Art. 17 GDPR)

You may request deletion of your personal data where:

- the data is no longer necessary for the purposes for which it was collected;
- you withdraw consent and no other legal basis applies;
- the processing is unlawful.

However, this right does not apply where processing is required to comply with legal obligations, including AML/CFT retention requirements.

4. Right to Restriction of Processing (Art. 18 GDPR)

You may request restriction of processing, for example, if:

- you contest the accuracy of the data;
- the processing is unlawful but you oppose erasure;
- the data is required for legal claims.

5. Right to Data Portability (Art. 20 GDPR)

Where processing is based on consent or contract and carried out by automated means, you have the right to receive your personal data in a structured, commonly used, and machine-readable format and to transmit it to another controller.

6. Right to Object (Art. 21 GDPR)

You have the right to object to processing based on legitimate interest, including direct marketing. If you object to processing for marketing purposes, we will cease such processing without undue delay.

7. Right to Withdraw Consent

Where processing is based on consent, you may withdraw your consent at any time. Withdrawal does not affect the lawfulness of processing carried out prior to withdrawal.

Please note that withdrawal of consent may limit or disable certain functionalities of the Platform (e.g., contact matching or marketing communications).

Right to Lodge a Complaint

You have the right to lodge a complaint with a supervisory authority in the EU Member State of your habitual residence, place of work, or place of the alleged infringement.

In Poland, the competent supervisory authority is:

President of the Personal Data Protection Office (PUODO)
ul. Stawki 2
00-193 Warsaw, Poland
Phone: +48 22 531 03 00
Website: https://uodo.gov.pl

Important Notice Regarding Regulatory Obligations

Please note that certain personal data must be retained and processed to comply with legal and regulatory obligations, including anti-money laundering (AML) and counter-terrorist financing (CFT) requirements. In such cases, deletion or restriction of processing may not be possible until statutory retention periods have expired.

Recipients of Personal Data

We may disclose personal data to the following categories of recipients, where necessary and in accordance with applicable law:

1. Public Authorities and Regulators

We may disclose personal data to public authorities where required by law or regulatory obligation, including but not limited to:

- Supervisory authorities (including the President of the Personal Data Protection Office – PUODO);
- Financial supervisory authorities;
- Tax authorities;
- Courts;
- Law enforcement agencies (e.g., police, prosecutor's office).

Such disclosures are made strictly to the extent required by applicable legal provisions.

2. Financial Institutions and Payment Service Providers

We may share personal data with:

- Banks and financial institutions;
- Payment service providers (PSPs);
- Electronic money institutions (EMIs);
- Cryptocurrency exchanges and liquidity providers;
- Card scheme partners (where applicable);

This is necessary to execute transactions, comply with AML/CFT requirements, and provide the services requested by you.

3. Identity Verification and Compliance Providers

To comply with legal and regulatory obligations, we may share personal data with:

- KYC/identity verification service providers;
- AML and sanctions screening providers;
- Fraud prevention service providers;
- Blockchain analytics providers (where applicable).

Such providers act as processors on our behalf or as independent controllers where required by law.

4. IT and Infrastructure Providers

We may engage trusted third-party service providers that process personal data on our behalf, including:

- Cloud hosting providers;
- Data storage providers;
- IT support and cybersecurity service providers;
- Email and communication service providers;
- Analytics service providers (where applicable).

These entities process data under data processing agreements compliant with GDPR and are bound by confidentiality and security obligations.

5. Professional Advisors

We may disclose personal data to:

- Legal advisors;
- Auditors;
- Accounting and tax advisors;

where necessary for compliance, risk management, or legal claims.

6. Transfers Based on Consent

Where processing is based on your explicit consent, personal data may be shared with specific third parties indicated at the time consent is obtained.

Data Retention

We retain personal data only for as long as necessary for the purposes for which it was collected and in accordance with applicable legal and regulatory requirements.

Personal data is retained for the following periods:

1. Contractual Relationship

Personal data processed for the performance of a contract is retained for the duration of the contractual relationship and until the account is closed or services are terminated.

2. Regulatory and Legal Obligations

Where required by applicable law, including Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) regulations, personal data may be retained for a minimum period of 5 years following the termination of the business relationship, or longer if required by law.

Such retention is mandatory and cannot be shortened upon request.

3. Legal Claims

Personal data may be retained beyond the contractual period where necessary to establish, exercise, or defend legal claims.

4. Consent-Based Processing

Where processing is based on consent (e.g., contact matching or marketing communications), data will be processed until consent is withdrawn, unless another legal basis applies.

5. Cookies and Similar Technologies

Retention periods for cookies depend on their category:

- Session cookies are deleted when the browsing session ends.
- Persistent cookies remain on your device until they expire or are manually deleted.
- Analytics data is retained only for the period necessary to analyze and improve Platform performance.

International Transfers of Personal Data

Personal data may be processed within the European Economic Area (EEA).

In certain cases, personal data may be transferred to countries outside the EEA where this is necessary for the provision of services (for example, through the use of cloud infrastructure providers, payment institutions, or compliance service providers).

Where such transfers occur, we ensure that appropriate safeguards are implemented in accordance with Chapter V of the GDPR, including:

- transfers to countries subject to an adequacy decision by the European Commission;
- the use of Standard Contractual Clauses (SCCs);

- implementation of appropriate technical and organizational safeguards.

We take reasonable steps to ensure that personal data transferred outside the EEA receives an adequate level of protection.

Personal Data Breach Notifications

In the event of a personal data breach, the Company shall notify the competent supervisory authority without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons, in accordance with Article 33 of the GDPR.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Company shall inform affected individuals without undue delay, in accordance with Article 34 of the GDPR.

The Company maintains internal procedures designed to detect, assess, investigate, and respond to personal data breaches.