Privacy Policy — Enrollo

Version: **v1.0.0**

Effective date: **2026-03-01**

Last updated: **2026-03-01**

Data controller

This Privacy Policy explains how Enrollo ("Enrollo", "we", "us", "our") collects, uses, discloses, retains and protects personal data in connection with the Enrollo mobile and web application (the “App”). This Policy is drafted to comply with Regulation (EU) 2016/679 (GDPR/RODO) and applicable Polish law.

If you have questions about this Policy or wish to exercise your rights, contact us at contact@enrollo.pl or at the postal address below.

Scope and principles

We apply the principles of lawfulness, fairness, transparency, data minimisation, purpose limitation, accuracy, storage limitation, integrity and confidentiality. We collect only personal data necessary to provide the App’s services, meet legal obligations, and protect legitimate interests related to security and fraud prevention.

Categories of data we collect

Enrollo collects and processes the following categories of personal data:

- **Account information:** name, email address, profile picture, and other data received from third-party authentication providers such as Google LLC. Passwords are securely hashed by our authentication service and are not readable by us.

- **Payment information (optional):** if you are eligible to receive payouts from Enrollo, you may voluntarily provide your bank account number (IBAN). This information is used solely to identify and process transactions, ensure accurate payouts, and comply with legal and accounting obligations. It is stored securely with appropriate technical and organizational safeguards. Access is restricted and only permitted when necessary for manual or automated payment processing or to comply with legal requirements. Bank account information is never used for marketing or profiling purposes.
- **Technical and usage data:** platform identifiers, tokens for notifications, App version, user agent, IP address, locale, timestamped activity logs, and other technical metadata required for operation, security and troubleshooting.
- **Consent and compliance records:** consent choices (e.g., marketing opt-in), timestamps, accepted document versions, language used, platform, App version/build, user agent, and other metadata necessary to demonstrate lawful consent. Only minimal data required to evidence consent is retained; direct personal identifiers are removed upon account deletion.
- **Transactional and accounting data:** records of payouts, amounts, dates, offer identifiers, internal references and related bookkeeping information.
- **Non-identifying application data:** metrics such as points/XP, counts of accepted offers, total amount of earned bonuses, read notifications, avatar colour or other non-identifying application data.
- **Support correspondence:** messages sent to us when contacting support or submitting a report with categories such as technical issues or feedback.

Legal bases for processing

We process personal data on one or more of the following lawful bases:

- **Performance of a contract** (Article 6(1)(b) GDPR): account creation, authentication, account management, and execution of payouts.
- **Consent** (Article 6(1)(a) GDPR): marketing communications and other optional processing explicitly consented to. Consent is freely given, informed, and can be withdrawn at any time.
- **Legitimate interests** (Article 6(1)(f) GDPR): security, fraud prevention, abuse detection, service improvement, and internal analytics, where such interests are not overridden by your rights.
- **Legal obligation** (Article 6(1)(c) GDPR): retention of transaction and accounting records required by tax, accounting, or other applicable laws.

A mapping of common data items to legal bases is provided in Section 5 below.

Purposes of processing and legal bases (summary)

- Account creation, authentication and account management — **contract**.
- Payouts and payment processing — **contract**.
- Security, fraud prevention and abuse detection — **legitimate interest**.
- Sending marketing/promotion notifications — **consent**.
- Transaction records and legal/accounting retention — **legal obligation**.
- Customer support and communication — **contract / legitimate interest**.

Data processors and third parties

We engage trusted processors who perform services on our behalf under contractual obligations:

- **Supabase** — database and authentication (primary data store; hosted in the EU).

- **Expo** — app infrastructure and push notification delivery.
- **Home.pl** — transactional email delivery and domain hosting with SSL certificate.
- **LeadStar.pl** — affiliate offers distribution and conversion attribution.

We may also rely on cloud infrastructure providers used by these processors. Each processor is **contractually required** to process data solely on our instructions and to implement appropriate technical and organizational measures to protect personal data.

We **do not sell, rent, or trade** personal data to third parties for their marketing or commercial purposes.

Affiliate links, cookies and tracking

The App displays affiliate offers and may redirect you to partner websites. When you click an affiliate link, the partner may set cookies or tracking identifiers on their site to attribute conversions. Enrollo does not place third-party advertising cookies for profiling or ad targeting within the App. Any tracking performed after redirection is under the partner's control and governed by the partner's privacy policy.

We store minimal local values (locale, consent status, values for skipping warnings and essential technical identifiers). We do not use analytics or advertising tracking by default. If this changes we will inform users and obtain any required consent.

Data retention policy

We retain personal data **for the lifetime of your account**, unless you explicitly request deletion, and in compliance with applicable law:

- **Consent records:** records of user consent are stored in database logs to document and demonstrate compliance with applicable data protection laws. They are retained for the lifetime of the account and may be retained indefinitely for compliance and auditing purposes. These records contain limited metadata associated with the consent event (such as consent identifier, timestamp, language used during acceptance, versions of the agreements accepted, platform or operating system used, App and build versions where available, and device or browser information). These records do not include direct personal identifiers.
- **Account information (email, name, profile picture):** retained for the lifetime of your account. If you request account deletion, this data will be removed, except where retention is required for legal or accounting obligations.
- **Payment information (IBAN):** retained for the lifetime of your account to identify and process transactions, ensure accurate payouts, and comply with applicable legal and accounting obligations. Upon account deletion or after payouts are completed, this data will be irreversibly anonymised, pseudonymised, or masked to protect your privacy.
- **Transactional and accounting data:** retained for the lifetime of your account to maintain a verifiable record of payouts and activity. After account deletion, these records may be retained in pseudonymised, anonymised or masked form (e.g., removing email and name, while retaining anonymous user identifiers and consent metadata) to comply with auditing, accounting, or legal obligations.
- **Non-identifying application data:** retained for the lifetime of your account. If you request account deletion, this data will be removed.
- **Security and event logs:** retained for the lifetime of your account for operational monitoring, security, and fraud-prevention purposes. Some of these logs may remain indefinitely or may be automatically deleted by the database.

- **Support correspondence:** retained for the lifetime of your account to handle inquiries, resolve issues, and document the history of interactions. Upon account deletion, this data will be deleted or anonymised, unless further retention is required for legal or accounting purposes, or unless it was submitted anonymously.

When personal data is no longer necessary or upon your request for deletion, we delete or irreversibly anonymise, pseudonymise or mask it in a manner that prevents re-identification, except where retention is required by law or for auditing, accounting, or fraud-prevention purposes.

Account deletion and anonymisation

You may request deletion of your account and all personal data at any time. When you do:

- **Direct identifiers** (email, name, profile picture) are permanently removed.
- **IBANs** are irreversibly masked, pseudonymised, or anonymised while retaining proof of completed transfers.
- **Transaction, accounting, consent, and security/event logs** required by law or for fraud-prevention may be retained in pseudonymised, anonymised or masked form. All references that could directly identify you as a person (email, name, profile picture) are removed, while the ones that could directly identify you to the deleted account (pseudonymised identifiers such as user ID, consent metadata) may be retained.
- **Deletion logs** record the action, including anonymous identifiers, timestamp, platform, and relevant document versions, without retaining personally identifiable information (PII). These logs serve as an audit trail to demonstrate compliance with deletion requests.

Audit logs and data integrity

To ensure compliance, security, and the integrity of records:

- We keep **logs of changes** to key account data and actions (e.g., consent updates, account deletions, or modifications to account/payment data).
- These logs **do not contain sensitive personal data** (e.g., passwords, IBANs, emails, names, or profile pictures). They record **metadata only**, such as which fields were changed, timestamps, the platform, and relevant document versions.
- Logs may be updated if corrections are necessary; they are not immutable.
- The purpose of these logs is to:
    - Track system changes and support troubleshooting,
    - Demonstrate compliance with data protection obligations, and
    - Support auditing, accounting, or fraud-prevention activities where necessary.
- Logs are stored securely with appropriate technical and organizational measures to prevent unauthorized access or misuse.

Data security and access control

We apply appropriate technical and organisational measures to protect personal data, including but not limited to:

- **Encryption:** Sensitive data is encrypted at rest (including, where feasible, IBANs) and in transit using HTTPS/TLS.
- **Database security:** Row-level security (RLS) and strict database policies to prevent unauthorized READ/INSERT/UPDATE/DELETE operations.

- **Document protection:** Bank statement files or payment documents are securely stored, and access is provided via signed, time-limited URLs.
- **Personnel access:** Access to personal data is restricted to authorized personnel only.

International transfers

Your personal data is primarily processed and stored within the EU. Some service providers (e.g., providers of push notification or infrastructure services) may be located or process data outside the EU. Where personal data is transferred outside the EU/EEA we use appropriate safeguards such as EU Standard Contractual Clauses (SCCs) or other legally recognized transfer mechanisms to ensure an adequate level of protection.

Your rights

Under GDPR you have the right to:

- Request access to your personal data.
- Request rectification of inaccurate data.
- Request erasure of your personal data, subject to legal exceptions (see Sections 8–9).
- Request restriction of processing.
- Object to processing based on legitimate interests (including profiling) — if you object we will cease processing unless we have overriding legitimate grounds.
- Request portability of data you have provided in a structured, commonly used, machine-readable format.

- Withdraw consent at any time where processing is based on consent (withdrawal does not affect processing that occurred before withdrawal).
- Lodge a complaint with a supervisory authority.

To exercise your rights, contact us at contact@enrollo.pl. We will respond within the timeframes required by law (generally within one month).

Consent management and policy versioning

- We record the specific version of the Privacy Policy, Terms of Service and Disclaimer you agreed to at the time of consent (version identifiers and timestamp).
- If the Privacy Policy or Terms change materially, we will notify you and, where required, request renewed consent prior to processing that relies on the new terms.
- We store consent evidence both locally (on the device as applicable) and persistently in our database so that consent history is demonstrable and auditable.

Marketing, notifications and opting out

- Marketing notifications and promotional messages are sent only with your explicit consent. You may withdraw consent at any time via the App settings or your device settings. Withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.
- We do not use personal data for third-party advertising or profiling.

Children’s data

The App is intended exclusively for users who are at least 18 years of age and is not directed to children. We do not knowingly collect or process personal data of individuals below the applicable age of digital consent under local law. If we become aware that personal data has been collected from a child without a valid legal basis, we will promptly suspend the account and delete or irreversibly anonymise such data, unless retention is required by law.

Data breach notification

In the event of a personal data breach that is likely to result in a risk to the rights and freedoms of individuals, we will notify the competent supervisory authority, Urząd Ochrony Danych Osobowych (UODO), and affected users where required by applicable law, without undue delay and within statutory time limits (including the 72-hour period where applicable under GDPR).

We take reasonable technical and organisational measures to prevent, detect and mitigate security incidents and will respond appropriately if a breach occurs.

Changes to this Privacy Policy

We may update this Policy to reflect changes in our practices, legal requirements, or features of the App. Material changes will be communicated to users, and where required by law, renewed consent will be obtained prior to continued use. All users are deemed bound by the most recent version of this Policy once it is published in the App. The latest Policy is also available from our contact point below.

Contact information and complaints

If you have questions, wish to exercise your rights, or want to submit a complaint:

Data Controller: Mateusz Jakub Muszarski

Address: Osiedle Konstytucji 3 Maja 21/4, Starogard Gdański 83-200, Pomorskie, Poland

Email: mat.muszarski@gmail.com

You also have the right to lodge a complaint with the supervisory authority: **Urząd Ochrony Danych Osobowych**.