

Privacy Notice

Last updated: December 3, 2025

This Privacy Notice has been developed by MonetAds Agency OÜ, a legal entity registered under the laws of Estonia, with its registered address at: Harju maakond, Tallinn, Lasnamäe linnaosa, Valukoja tn 8/2, 11415. Registry code: 17283901.

MonetAds Agency OÜ <https://www.moneta-ads.agency> (hereinafter referred to as "Moneta", the "Service", "we", or "us") is committed to protecting our clients' privacy and takes its data protection obligations very seriously.

This Privacy Notice explains how personal data is collected, processed, used, and disclosed when you use the Moneta service.

This Privacy Notice complements our Terms and Conditions and must be considered jointly with them.

1. GENERAL PROVISIONS

1.1. Personal data refers to information that identifies or relates to an identifiable person. This includes information you provide to us, information collected about you automatically, and information we receive from third parties.

2. PURPOSES OF COLLECTING AND PROCESSING PERSONAL DATA

2.1. User data is processed in accordance with the requirements of the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Personal Information Protection and Electronic Documents Act (PIPEDA), Brazilian General Data Protection Law (LGPD), Australia's Privacy Act 1988, and other applicable data protection regulations.

2.2. We collect your personal data directly from you unless it is unreasonable or impractical. We will not collect more data than necessary to provide our services and comply with applicable laws.

We may collect this information when you:

- access or use our website;
- register an account on our website;
- use our products and services;
- contact us through SMS, MMS, instant messaging, email, social media, mail, or telephone.

2.3. We are not responsible for how third-party companies, organizations, and services not affiliated with us collect, store, process, use, or disclose your personal data, even if the user accessed them via our Service.

2.4. The purpose of collecting, storing, processing, and using your personal and other data is to protect the interests of the user and the Service, to provide services to the user, to identify and communicate with the user.

2.5. We retain your personal data for as long as necessary to provide our services, comply with legal requirements, and for our legitimate business purposes.

3. DATA WE COLLECT AND STORE

3.1. When using the Service, the user provides a full name, email address, and Telegram username. These are considered the user's personal data.

3.2. By consenting to the processing of personal data, the user grants us the right to receive, store, process, and use the data mentioned in clause 3.1.

3.3. We have the right to store the user's personal and other data to the extent and for the duration necessary to provide our services or as required by international law, the laws of the user's country of residence, or until the user deletes such data. We may also retain anonymized or aggregated data for statistical or research purposes.

3.4. We do not request additional documents or information unless required by anti-money laundering (AML) laws, law enforcement, or other third parties under applicable law. In such cases, we may request:

- proof of source of funds;
- delivery service information;
- payment purpose details;
- screenshots from the sender's interface;
- full names of the parties to the transaction;
- any other transaction-related information deemed necessary.

In such cases, the user must provide the requested information. The Service does not store this data but receives it solely for processing the transaction.

3.5. Where permitted by law, we may collect certain types of information automatically whenever you interact with us or use our services. This helps us improve customer support, performance, user experience, and prevent unauthorized access.

3.6. We may collect device-related data including IP address, location, browser type and settings, time zone, operating system, device type, unique device ID, screen size, mobile network info, mobile OS, mobile browser type, and date/time/duration of visit.

3.7. We may receive information from payment systems, payment service providers, card schemes, card program managers, authorities, law enforcement, and public sources. This data is stored securely and confidentially.

4. ACCESS TO INFORMATION

4.1. We will not share personal data with third parties for commercial purposes without user consent.

Data may be shared only:

- after obtaining user consent;
- if necessary to fulfill a user's request;
- upon lawful requests from law enforcement.

4.2. The user agrees that we may share data with third parties providing services or goods under clause 3.4. Data controllers and processors must ensure protection from loss, destruction, or unauthorized processing.

4.3. The user acknowledges that Internet data transmission is not guaranteed to be secure, and we are not liable for unauthorized third-party access beyond our technical control. Although we implement HTTPS and SSL encryption at nearly every point of contact with the user, no method of transmission over the Internet or method of electronic storage is 100% secure.

4.4. The user has the right to request, modify, or delete their personal data in our possession, unless otherwise required by law.

5. DATA SUBJECT RIGHTS

5.1. As a data subject, the user has the right to:

- know the source, purpose, and location of their personal data;
- access information on data sharing conditions and third-party recipients;
- access their personal data;

- receive a response within 30 calendar days about whether their data is being processed and the content of such data;
- object to data processing;
- request corrections or deletion of their personal data;
- protect personal data from unlawful processing and accidental loss, destruction, or damage;
- file complaints with the data protection authority or court;
- use legal remedies if personal data protection laws are violated;
- limit consent to processing of specific data categories;
- withdraw consent for data processing;
- understand automated processing mechanisms;
- be protected from automated decisions with legal consequences.

6. PERSONAL DATA SECURITY

- 6.1. We use industry-standard technical and operational security measures to protect data from loss, misuse, alteration, or destruction. However, absolute security cannot be guaranteed.
- 6.2. We apply all relevant confidentiality obligations and technical/organizational security measures to prevent unauthorized or unlawful disclosure or processing.
- 6.3. Personal data may be disclosed without consent only as required by law and when necessary for national security, public interest, or human rights.
- 6.4. User data is not encrypted; only passwords on the platform are encrypted.
- 6.5. In case of a data breach, we will take all necessary steps to mitigate any harm.
- 6.6. If the breach threatens user rights and freedoms, we will notify users as soon as possible.

7. DATA STORAGE

- 7.1. Data from clause 3.1 is securely stored in our cloud storage.
- 7.2. This data is stored for the duration of the contractual relationship (until account closure).
- 7.3. It may also be stored for one month after deactivation of the account or longer if required by law or financial institutions we work with.

8. COOKIES

- 8.1. The Service does not use its own cookies or tracking technologies for personal data. However, third parties (e.g., Google Ads) integrated into our platform may use cookies for analytics or advertising. These are governed by their own privacy policies.
- 8.2. Users are informed of cookie purposes and asked for explicit consent. Consent can be managed or withdrawn at any time. The Service uses third-party cookies (e.g., Google Ads, analytics systems).
- 8.3. For more information on third-party cookies and privacy policies, see:
Google Ads: <https://policies.google.com/privacy>

9. ADDITIONAL TERMS

- 9.1. The Service may amend this Privacy Notice. All important changes will be reflected in a new version published on the Service. By using the Service, users confirm acceptance of the updated version. For major updates, the Service will notify users via email or platform notifications.

10. DATA PROTECTION OFFICER (DPO)

- 10.1. The DPO is responsible for ensuring the company's compliance with data protection laws and acts independently to safeguard personal data and privacy rights.
- 10.2. If the Company becomes aware of a suspected or actual data breach, the DPO must investigate and take corrective action.
- 10.3. You may contact the DPO via email: business.and.compliance@gmail.com

MonetAds Agency OÜ

Registry code: 17283901

Address: Harju maakond, Tallinn, Lasnamäe linnaosa, Valukoja tn 8/2, 11415

Management Board Member: Dennis Kryvablotski

Email: business.and.compliance@gmail.com