MONEYZEN

Privacy Policy

Last updated: 14.07.2026

The purpose of this Privacy Policy (hereinafter referred to as the “Policy”) is to explain the principles on which Moneyzen OÜ processes your personal data.

This Policy applies to personal data collected and processed by us, including personal data that became known to us before the entry into force of these terms, if you have expressed a wish to use our services or if you already use or have previously used our services.

We ensure the confidentiality and security of your data in accordance with the General Data Protection Regulation (GDPR) and other applicable financial and data protection legislation.

1. Data controller and contact information

In this Policy, the terms “we”, “us”, and “our” refer to Moneyzen OÜ.

Moneyzen OÜ is the controller of your personal data and determines the purposes and means of processing your personal data in order to provide our services to you.

Our contact details are:

Moneyzen OÜ (Registry Code: 12541882)
Address: Pronksi 19, 10124 Tallinn, Estonia
Email: info@moneyzen.eu
Telephone: +372 5885 5553
Website: https://moneyzen.eu/

If you have any questions about how we collect, store, share, or use your personal data, or if you wish to exercise any of your legal rights, please contact our Data Protection Specialist at: jana@moneyzen.eu.

2. Scope of application

This Policy applies to any natural person who uses, has used, or has expressed a wish to use our services, or who has any other relationship with us.

In this Policy, such person is referred to as “you” or “your”.

Important information

- This Policy also applies after any agreements related to our products or services have terminated.
- As we reserve the right to amend this Policy at any time, you will be deemed to have accepted such amendments once we have provided you with a corresponding notification.
- We do not disclose information collected about you to any third party, nor do we collect data for purposes other than those specified in this Policy.
- As this Policy contains important information regarding your rights and obligations, we kindly ask you to read it carefully and treat it with due attention.

For matters not specifically regulated in this Policy, we follow the applicable legislation, including, but not limited to, the General Data Protection Regulation (GDPR), the Estonian Personal Data Protection Act, the Creditors and Credit Intermediaries Act, the Money Laundering and Terrorist Financing Prevention Act, and guidelines issued by supervisory authorities.

3. What personal data do we process?

We process your personal data only to the extent necessary for providing our services to you. We collect information about you both directly from you and from external sources when entering into agreements and during the use of our services. The data collected is divided into various categories.

Examples of categories of personal data that we process include:

- **Identity verification and contact information** - full name, personal identification code, date of birth, identity document details, citizenship, postal address, email address, telephone number, preferred communication language.

- **Financial information** - information on income and expenses, financial liabilities, payment transaction data, bank account details, loan history information, employment and educational information, marital status information, information regarding assets and property.

- **Reliability and financial behaviour data** - information regarding your payment behaviour and outstanding debts; information concerning criminal convictions and criminal offences; data enabling us to fulfil our due diligence obligations related to the prevention of money laundering and terrorist financing and to ensure compliance with international sanctions, including information on whether you are a politically exposed person (PEP) or a sanctioned individual. From an investor's perspective, this category may also include information regarding: the origin of assets and funds, investment experience, investment interests, responses to questionnaires assessing the investor's risk tolerance and investment profile.

- **Communication, device and digital data** - video and audio recordings when you visit our office or communicate with us by telephone; information relating to your digital and electronic devices, including: IP address from which your device connects to our services; information regarding your use of our website; device type; operating system; log data; electronic identification data; social media usage data.

We may also collect other information through email, messages, and other communication channels, including when you visit our website.

When you visit our website, we use technology commonly known as "cookies", which can be managed through your internet browser settings. For more information about cookies and the purposes for which they are

used, please refer to our Cookie Policy:
https://moneyzen.eu/wp-content/uploads/2024/04/kupsised.pdf

- **Personal data processed based on your consent** - your consent allowing us to contact you through specific communication channels in order to offer relevant products and services.

- **Other personal data** - Information relating to requests for access, rectification, restriction, deletion, portability of your personal data, as well as complaints submitted by you.

4. How do we obtain your personal data?

We obtain your personal data primarily in three ways:

Directly from you - information that you provide through our website, including when you submit a loan application or provide the information and documentation required for entering into an agreement with us.

During the provision of services - we collect personal data when you use our services, including, for example:

- information regarding payments made to you or by you;
- loan agreement history and related transaction information;
- records generated during the provision of our services;
- information obtained through our communications with you, including telephone call recordings and email correspondence.

From other sources - we may also obtain personal data from public and private registers and databases, including, but not limited to:

- The Estonian population register;
- The Estonian Tax and Customs Board;
- Payment default registers;
- Official Announcements (Ametlikud Teadaanded);
- Sanctions screening databases;
- Internet search engines; and

- Other lawful and reliable information sources.

5. Purposes and legal bases for processing

Regardless of whether we use your personal data to verify your identity, process a loan application, or improve your user experience, we always process your personal data securely and in accordance with this Policy.

The collection and processing of your personal data is based on one or more of the following legal grounds:

Contract - the processing of personal data is necessary for entering into, performing, or securing the performance of a contract, including, for example:

- Assessing creditworthiness;
- Making lending decisions;
- Resolving disputes arising from contractual relationships; and
- Fulfilling other obligations related to contractual performance.

Legal obligation - the processing of personal data is necessary to comply with obligations and exercise rights arising from applicable legislation, including, for example:

- The Money Laundering and Terrorist Financing Prevention Act;
- The Creditors and Credit Intermediaries Act;
- The Law of Obligations Act; and
- Other applicable legal requirements.

Legitimate interest - where appropriate, we may process personal data on the basis of our legitimate interests or those of a third party, provided that such interests are not overridden by your fundamental rights and freedoms. Examples include the use of security camera recordings on our premises for the protection of persons and property. You have the right to object at any time to processing based on legitimate interests. Further information is available in the section “Your Rights”.

Consent - we may request your consent to process certain personal data for specific purposes defined in the consent request, such as sending you marketing communications, including offers based on profiling activities.

We confirm that personal data processed on the basis of consent will only be processed within the scope and for the purposes for which the consent was granted.

You may withdraw your consent at any time. Further information is available in the section “Your Rights”.

The table below describes the general principles governing our processing of personal data, including the purpose of processing, the legal basis, and the source of the information.

General Principles of Personal Data Processing

Purpose	Legal basis	Source of information
Identity verification	Money Laundering and Terrorist Financing Prevention Act; Contract; Consent	Directly from you; From other sources
Provision of services, including assessment of your application and creditworthiness	Contract; Creditors and Credit Intermediaries Act; Law of Obligations Act; Legitimate Interest	Directly from you; From other sources; During the provision of services
Fulfilment of contractual notification obligations	Contract; Law of Obligations Act; Legitimate Interest	Directly from you; During the provision of services
Application of due diligence measures when entering into a contract and monitoring the business relationship	Money Laundering and Terrorist Financing Prevention Act; International Sanctions Act	Directly from you; From other sources; During the provision of services

Disclosure of debt-related information	Legitimate Interest	Directly from you; During the provision of services
Development of our business operations, including improvement of products and services and development of systems	Legitimate Interest	Directly from you; During the provision of services
Sending direct marketing communications (including profiling and offering personalised services and similar products and services)	Consent; Legitimate Interest (for offering similar products and services)	Directly from you; During the provision of services
Ensuring physical security, data security and information security	Cybersecurity Act; Legitimate Interest	During the provision of services
Responding to requests from courts, bailiffs and supervisory authorities	Code of Enforcement Procedure; Code of Civil Procedure; Code of Criminal Procedure; Money Laundering and Terrorist Financing Prevention Act; Bankruptcy Act; Natural Person Insolvency Act	Directly from you; From other sources; During the provision of services

6. With whom do we share your personal data?

We are entitled, without obtaining your separate consent, to disclose your personal data to third parties (including private, public and governmental registers and databases) where such disclosure is required by law and/or is necessary for entering into, performing, or securing the performance of a contract with you.

Based on the above, we may disclose your personal data, among others, to the following third parties:

- For the purpose of assessing creditworthiness and making lending decisions, to the population register, the Estonian Tax and Customs Board, payment default registers (e.g., AS Creditinfo Eesti, OÜ Krediidiregister, or any other entity maintaining a payment default register);
- to companies belonging to the same consolidation group as us, where necessary for the provision of the service, fraud prevention, conducting group-wide risk management, and fulfilling obligations related to the prevention of money laundering and terrorist financing;
- For the performance and administration of contractual obligations, to payment service providers, postal service providers, and similar service providers;
- For debt collection or assignment purposes, to debt collection agencies and similar service providers, or to a new creditor in the event of an assignment of claims;
- To service providers engaged by us, such as auditors, IT service providers, archive service providers, marketing service providers, legal advisers, and other professional service providers;
- For compliance with legal obligations, to courts, bailiffs, prosecutors, police authorities, the Financial Intelligence Unit, supervisory authorities, and other competent authorities.

Further information regarding third parties involved in the processing of your personal data for specific purposes can be found in our list of “Authorised Processors”.

7. Profiling and automated decision-making

Profiling means the automated processing of your personal data for the purpose of analysing and predicting, among other things, your preferences, behaviour, and attitudes.

As a result of profiling, we may:

- Offer products and services that are more relevant to your needs;
- Prevent money laundering and terrorist financing;
- Detect fraud;
- Make automated decisions, such as creditworthiness assessments.

We use **automated decision-making** (i.e., decisions made through technological means without direct human intervention) primarily to ensure that decisions are made quickly, fairly, and efficiently.

Automated decisions and profiling are based on personal data known to us and collected either directly from you or from third parties in accordance with this Policy.

To make our services faster and more convenient, we may use pre-filled fields within our self-service environment. In such cases, information already known to us and previously provided by you (such as your name and contact details) may automatically appear in the relevant fields.

However, you remain responsible for reviewing and verifying the accuracy of all information before confirming or submitting it each time.

8. How long do we retain your personal data?

We retain personal data collected during the course of our business relationship after the relationship has ended in accordance with applicable legal retention requirements and, where necessary, for the establishment, exercise, or defence of legal claims based on our legitimate interests.

As a general rule, we retain your personal data for the following periods:

- Personal data collected in connection with the conclusion and performance of agreements – for up to five (5) years following the termination of all agreements concluded with you, unless applicable law requires or permits a longer retention period.
- Security camera recordings – for up to ninety (90) days, unless applicable law requires or permits a longer retention period.

MONEYZEN

Where we no longer have a legitimate need or legal obligation to retain your personal data, we will promptly delete or anonymise such data.

9. Transfer of personal data to third countries

We may transfer and store personal data collected about you in locations outside the European Economic Area (EEA), including countries where the level of personal data protection may not be equivalent to that provided within the EEA.

Where we choose to use a service provider located outside the EEA for data storage or processing purposes, we will ensure that the transferred personal data is afforded a level of protection equivalent to that required within the EEA and that such transfer is carried out in accordance with applicable legal requirements.

10. Your rights

In relation to the personal data collected and stored about you, you have the following rights:

- **Right of access** – to access the personal data we hold about you and to obtain information regarding how and for what purposes your personal data is processed;
- **Right to rectification** – to request the correction of personal data that is inaccurate, incomplete, or no longer up to date. You are also responsible for informing us of any changes to your contact details or other information previously provided in agreements or through our self-service environment. Maintaining accurate customer information enables us to provide more efficient and reliable services, while inaccurate information may limit your ability to use our products and services.
- **Obtain information about automated decision-making**, including how an automated decision concerning you was made and what impact that decision had on you. In addition, you have the right to request that an assessment based solely on automated processing

be reviewed by a human and not exclusively through automated means;
- **Object to processing** of personal data where such processing is based on our legitimate interests and/or profiling activities;
- **Receive a copy of the personal data you have provided to us** in a structured, commonly used, and machine-readable electronic format (data portability), where the processing is based on your consent or a contract and is carried out by automated means;
- **Request the erasure of your personal data** where we no longer have a legal basis for processing such data or where processing is based on your consent and you withdraw that consent. However, erasure cannot be requested where we have a legal right or obligation to continue processing the personal data (for example, for the performance of a contract or compliance with a legal obligation).

Exercising your rights

To exercise your rights, including the withdrawal of consent, you may:

- Visit our office;
- Contact our DPO (data protection specialist) at jana@moneyzen.eu;
- Submit a digitally signed application to info@moneyzen.eu;
- Contact our customer service by telephone at +372 5885 5553;
- Log in to our self-service environment at https://moneyzen.eu and remove the relevant consent selection within your account settings.

We will respond to your request or application as soon as possible, but no later than one month from the date of receipt. Where additional clarification or verification is required, we may extend the response period in accordance with applicable law.

We seek to resolve any disputes relating to the processing of personal data primarily through negotiations.

You always have the right to lodge a complaint with the Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon) at www.aki.ee if you believe that the processing of your personal data infringes your rights or interests under applicable law. You also have the right to seek judicial remedies before a competent court.

11. How do we protect your personal data?

We have implemented reasonable data security policies and procedures designed to protect personal data against unauthorised access, loss, misuse, alteration, or destruction. To ensure the security of personal data, we use a variety of technical and organisational measures, including encryption. All employees and third parties authorised to process personal data under this Policy are required to comply with applicable standards, including technological security standards, and to implement appropriate measures for the use, protection, and transmission of information. Any person with access to personal data is required to maintain the confidentiality of such information.

12. Amendments to this policy

We may amend this Privacy Policy from time to time to ensure that it remains up to date and compliant with applicable laws and regulations. We will notify you of any amendments by email or through our self-service environment and will make the updated version available on our website. Whenever changes are made to this Policy, the “Last Updated” date shown at the beginning of the document will be revised accordingly.