monefit

Privacy Policy

Version: 2.2

Effective from: 20.07.2026

This Privacy Policy explains how Monefit Investments OÜ (hereinafter also **"Monefit"** or **"we"**) processes personal data in connection with the SmartSaver Website, mobile application (hereinafter the **"SmartSaver App"** or **"App"**) and related services (hereinafter together the **"Services"**). It applies to any natural persons who (1) visit the SmartSaver Website or App; (2) use the Services, or (3) are associated with SmartSaver Users, who are legal entities (e.g. directors, representatives and beneficial owners).

Capitalised terms used in this Privacy Policy that are not defined herein have the meanings given to them in the Terms of Use of Monefit SmartSaver (the **"SmartSaver Terms"**).

1. Who is the controller and the Data Protection Officer?

1.1. The controller of your personal data is Monefit Investments OÜ, registry code 11953111, registered address Kai tn 4, 10111 Tallinn, Estonia, telephone +372 698 8710, e-mail info@monefit.com. Monefit is part of Creditstar Group. The list of companies belonging to the Creditstar Group is available on the website https://creditstar.com/contacts.

1.2. We have appointed a Data Protection Officer (hereinafter **"DPO"**) who is responsible for questions relating to this Privacy Policy.

1.2.1. DPO: Christian Isaksen
1.2.2. DPO e-mail: dpo@monefit.com

1.3. You can contact us or the DPO if you have questions about this Privacy Policy or wish to exercise your rights.

1.4. We process personal data in accordance with Regulation (EU) 2016/679 (hereinafter **"GDPR"**) and the national laws implementing this enactment in each market in which we operate.

2. What personal data do we process?

The personal data we process depends on your relationship with us and how you use the Services. We process the following categories of personal data:

Category	**Personal data processed**
Identity and verification data	Such as first name, last name, personal identification code or national identity number, passport number, date and place of birth, citizenship, country of residence, tax residence, tax identification number, identity document data, copies or photos of identity documents, verification status and results.
Contact details	Such as e-mail address, telephone number, postal address, residential address.

SmartSaver Account information and login data	Such as SmartSaver Account number, status and settings, authentication data, login history, user role, acceptance of the SmartSaver Terms and this Privacy Policy, events and account activity.
Representative and beneficial owner data	Such as proof of representation, power of attorney, director or representative data, beneficial owner identity and ownership information.
KYC, AML, sanctions and fraud prevention data	Such as PEP status, sanctions screening results, source of funds and wealth, purpose of using the Services, bank account ownership evidence, adverse media indicators, insolvency data, investigations, transaction monitoring alerts and fraud prevention records.
Financial data	Such as bank account number and holder name, bank name, payment references, amount, currency, date and status, payment service provider data, tokenised card data (token, last four digits, card network, expiry, issuer country), payment status, chargeback/refund and dispute data.
Use of the SmartSaver	Such as allocated or available funds, SmartSaver Claims acquisition and sale, SmartSaver Price, SmartSaver Account value, returns, rate of return, fees, deductions, transfer instructions.
Communication and support data	Such as customer support chats, messages, phone calls (recorded where notified), complaints, feedback, and reviews.
Marketing and preference data	Such as data about your preferences, participation in campaigns and marketing-related choices.
Device, technical and security data	Such as IP address, device type and identifiers, operating system, browser, SmartSaver App version, language, time zone, network data, log data, session data, security events, error logs, fraud signals, advertising identifiers where permitted, and data on how you use the SmartSaver Website and App.
App permission and feature data	Such as camera, photos and files (for KYC/document upload only); push notification status; approximate location inferred from IP address; network connectivity data collected through OS-level permissions (full network access, internet access and Wi-Fi connection status) used to deliver and secure the App and to support attribution via Play Install Referrer API; biometric sign-in choice and session authentication data: if you enable biometric sign-in, verification is handled entirely by your device operating system; we do not receive or store your fingerprint, face image, biometric template or biometric match result; in-app messaging data.

2.1. We obtain personal data from the following sources:

2.1.1. **directly from you** - when you register, use the Services, contact us or make choices, including data provided by or about directors, representatives and beneficial owners;

2.1.2. **automatically through your device and our technical systems -** including through SDKs and similar technologies when you access the SmartSaver

Website or App (for information about cookies and similar technologies, please see our Cookie Policy);

2.1.3. **from third parties -** including identity verification, KYC, AML, sanctions and fraud prevention service providers, banks and payment service providers, public and official registers, analytics, attribution and marketing partners, professional advisers, authorities and courts.

2.2. Where required by law or to provide the Services, providing personal data is mandatory; optional data is identified as such.

3. How and on what legal basis do we process your personal data?

3.1. We process your personal data for the following purposes and on the following legal basis:

How we process your personal data	Legal basis
To verify identity, assess the Application, carry out pre-contractual checks (including KYC, AML, PEP, sanctions, tax residence, bank account, beneficial ownership, insolvency and fraud prevention) and to perform, manage and terminate a customer relationship.	Article 6(1)(b) GDPR
To register SmartSaver Users, create and manage SmartSaver Accounts, and enable authentication including biometric sign-in via the App.	Article 6(1)(b) GDPR
To process payments, pay-outs, chargebacks, SmartSaver Fees, deductions, taxes and payment disputes.	Article 6(1)(b) GDPR
To facilitate SmartSaver Claims acquisition and sale, including processing Tender Offers, Assignment Agreements and SmartSaver Sale Agreements, managing the SmartSaver Account and servicing SmartSaver Claims on behalf of the User.	Article 6(1)(b) GDPR
To prevent fraud, money laundering, terrorist financing and sanctions violations.	Article 6(1)(c) GDPR Applicable anti-money laundering and counter-terrorist financing laws, including the relevant EU AML directives and the national laws implementing them
To maintain, secure and improve the SmartSaver Website, App and Services.	Article 6(1)(f) GDPR
To provide customer support, respond to requests, handle complaints and communications.	Article 6(1)(b) GDPR
To protect our rights, including the establishment, exercise and defence of legal claims.	Article 6(1)(f) GDPR

To collect and process your feedback and reviews about our services and products.	Article 6(1)(f) GDPR
To measure marketing effectiveness, analyse campaign performance and attribution, create user segments, predict users' likely interest in certain Services or offers, and personalise marketing messages, offers and content on the SmartSaver Website, App and other channels.	Article 6(1)(f) GDPR Article 6(1)(a) of the GDPR where consent is required under applicable law for non-essential tracking technologies (see our Cookie Policy).
To send you direct marketing about our similar services or products within the framework of an existing customer relationship.	Article 13(2) of Directive 2002/58/EC and the respective national implementing laws
To send you direct marketing and other offers about our services or products and services or products of companies within the Creditstar Group or our partners, if such offers may be of interest to you.	Article 6(1)(a) GDPR
To comply with legal, tax, accounting, regulatory and reporting obligations.	Article 6(1)(c) GDPR
For ancillary purposes: internal administration, reporting, audits, statistical research, analysing customer and service history, collecting feedback and reviews, and service improvement (anonymised where possible).	Article 6(1)(f) GDPR

3.2. Where we rely on legitimate interests (Article 6(1)(f) GDPR), you may request details of our balancing assessment by contacting the DPO.

3.3. You have the right to object at any time to direct marketing and to profiling related to direct marketing. If you object, we stop processing your personal data for direct marketing. Where we process your personal data for marketing purposes on the basis of your consent, you have the right to withdraw your consent at any time. If you withdraw your consent, we stop processing your personal data for marketing purposes.

4. Do we use profiling and automated decisions to process your personal data?

4.1. We use profiling in the following processes and based on the following logic:

4.1.1. **Identity verification and KYC, AML and sanctions screening:** We use automated tools to verify your identity, validate identity documents and screen your data against sanctions lists, PEP databases, adverse media sources and transaction monitoring rules during onboarding and throughout the customer relationship. Based on this assessment, you may be subject to enhanced due diligence, asked for additional documentation, have transactions delayed or blocked, or have the Services restricted, suspended or terminated, or be reported to authorities as required by law. A qualified person always reviews and confirms any decision that has legal or similarly significant effects on you before it takes effect.

4.1.2. **Marketing personalisation and attribution tracking:** We analyse your data to build profiles used to personalise marketing messages, offers and content across the SmartSaver Website, App and other channels. We also use attribution tools, including AppsFlyer, to measure which campaigns lead to App installs, registrations or other actions and to detect fraudulent installs and fake traffic. This profiling does not produce legal effects concerning you or similarly significantly affect you. You may object to direct marketing and related profiling at any time by contacting us or the DPO.

4.2. We do not make decisions based solely on automated processing, including profiling, that produce legal effects concerning you or similarly significantly affect you, without human involvement. You have the right to request human intervention, to express your point of view and to contest any decision. You may contact the DPO for further information about the logic and safeguards applicable to any profiling activity described in this section.

5. Who do we share your personal data with?

5.1. We share personal data only where necessary for the purposes described in this Privacy Policy, required by law, or where we have another valid legal basis. Where recipients act as our processors, we enter into data processing agreements under Article 28 GDPR. Where they act as independent controllers, their own privacy policy applies. Some recipients may be located outside the EEA; for information on international transfers and safeguards, see section 6. You may contact the DPO to obtain the names of specific recipients.

5.2. The categories of recipients may include:

5.2.1. Creditstar Group Companies;
5.2.2. Identity verification, KYC, AML, sanctions, adverse media and fraud prevention providers;
5.2.3. Banks, card issuers, payment service providers and payment intermediaries;
5.2.4. IT, hosting, cloud, cybersecurity, App development, analytics, attribution, crash reporting service providers;
5.2.5. Auditors, accountants, tax advisers, legal advisers, compliance advisers and other professional advisers;
5.2.6. Public authorities, supervisory authorities, tax authorities, financial intelligence units, courts, law enforcement and other competent bodies;
5.2.7. Advertising and social media platforms;
5.2.8. Marketing, analytics and attribution service providers.

6. Do we transfer your personal data outside the European Economic Area?

6.1. As a general rule, we process personal data in the European Economic Area (EEA). Some recipients, including certain cloud, analytics and attribution providers, may be located outside the EEA. We transfer personal data to countries outside the EEA only where there is a valid transfer mechanism and appropriate safeguards are in place. The specific non-EEA countries to which we transfer personal data are available from the DPO on request. Where transfers are made to countries covered by a European Commission adequacy decision, we rely on that decision. Where transfers are made to countries not covered by an adequacy decision, we rely on the European Commission standard contractual clauses (SCCs) adopted under Article 46(2)(c) GDPR.

6.2. You may contact the DPO to obtain more information about international transfers and, where applicable, a copy of the relevant safeguards, including standard contractual clauses, subject to necessary redactions.

7. How long do we retain your personal data?

7.1. We retain your personal data only for as long as needed for the purposes for which it was collected and under a valid legal basis. Accordingly, personal data is retained for relevant periods prescribed by applicable legislation or on the basis of legitimate interest in order to protect the interests of Monefit, including in cases where it might be necessary to prepare and submit any legal claims. For example, the statutory retention period for accounting and tax records is seven (7) years from the end of the financial year in which the relevant accounting document was recorded.

7.2. When the data retention conditions stipulated in Clause 7.1. are no longer applicable your personal data will be deleted or anonymised.

8. How do we protect your personal data?

8.1. We implement appropriate technical and organisational security measures to protect your personal data against unauthorised or unlawful access, accidental loss, destruction, alteration or disclosure in accordance with Article 32 of the GDPR. We regularly review our security measures and update them as necessary, taking into account technological developments, risks, and regulatory expectations.

9. What are your rights in relation to the processing of personal data?

9.1. Subject to GDPR conditions and limitations, you have the right to:

9.1.1. **receive a confirmation whether we process your personal data and, if so, access the personal data and receive a copy of it;**
9.1.2. **correct inaccurate or incomplete data;**
9.1.3. **request the erasure of data** where it is no longer necessary, consent is withdrawn or processing is unlawful, however, we may refuse such request where we have a valid legal basis to continue processing, e.g. we must keep the data by law or need it to bring legal claims;
9.1.4. **request a restriction of processing**, whereby you contest the accuracy of the data, the processing is unlawful or we no longer need the data;
9.1.5. **data portability**, where You can ask to receive personal data you provided to us in a structured, commonly used and machine-readable format, if processing is based on consent or contract performance and carried out by automated means;
9.1.6. **object to processing based on legitimate interests;**
9.1.7. **object at any time to direct marketing and related profiling;**
9.1.8. **withdraw consent** at any time without affecting prior processing;
9.1.9. **request human intervention and contest** any automated decision with legal or similarly significant effects (see Section 4).

10. How to exercise your rights?

10.1. To exercise your rights, contact us or the DPO at dpo@monefit.com. We will respond within one month, extendable by two months for complex requests. You may also manage marketing preferences and App permissions directly in your device or App settings.

11. How can you lodge a complaint?

11.1. If you have concerns about how we process your personal data, please contact us or the DPO first. You have the right to lodge a complaint with the Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon):

11.1.1. website: www.aki.ee;

11.1.2. e-mail: info@aki.ee;
11.1.3. postal address: Tatari 39, 10134 Tallinn, Estonia;
11.1.4. telephone: +372 627 4135.

11.2. You may also lodge a complaint with the supervisory authority in the Member State of your habitual residence, place of work or place of the alleged infringement.

12. Changes to this Privacy Policy

12.1. The current version of this Privacy Policy is available on the SmartSaver Website or App. We can update this Privacy Policy to reflect changes in the Services, data processing or applicable law. If changes are material, we will notify you in advance by e-mail, in-app message, SmartSaver Website notice or other appropriate means where required by law, so that you have a reasonable opportunity to review the changes and exercise your rights before they take effect.