Mirocard Privacy and Cookies Policy

Last updated: 23 April 2026

1. Introduction

This Mirocard Privacy and Cookies Policy (the "**Policy**") describes what personal data is collected, the purposes for which it is used, to whom it may be disclosed, how such data is protected, how cookies are used, and what rights the user has.

This Policy applies to users of the Mirocard website, personal account, platform, card functionality, KYC/KYB/AML procedures, customer support and other related Mirocard services.

For the purposes of this Policy, **Mirocard** means the service provided by **InnovativeTechnologies OÜ**.

Mirocard is not a bank, payment institution, electronic money issuer, depository, custodian or holder of the user's funds. Processing of data relating to virtual cards, transactions, available amount, checks, top-ups and card functionality may involve third-party providers, including issuers, card programmes, processors, payment systems, KYC/KYB/AML providers, blockchain analytics providers, crypto-infrastructure providers and other mandatory infrastructure participants.

Use of the Mirocard service means that the user has read this Policy.

2. What Data We Collect

Personal data is collected and processed to the extent necessary to provide the service, identify users, comply with compliance requirements, prevent fraud, ensure security, process transactions and fulfil legal obligations.

2.1. Registration and Contact Data

The following may be processed:

- first name and surname;
- email address;
- telephone number;

- country of residence;
- citizenship, where applicable;
- residential or registered address, where applicable;
- account data;
- interface and communication language;
- history of communications with customer support;
- other data provided by the user upon registration or when using the service.

2.2. KYC/KYB and AML Data

For identification, verification, sanctions screening, AML/CFT checks, fraud prevention and other compliance purposes, the following may be processed:

- identity document data;
- copies, images or particulars of documents;
- date of birth;
- citizenship;
- residential address;
- selfie, liveness check, video verification or other data required to confirm identity;
- information on PEP status, sanctions matches and adverse media;
- information on source of funds, source of wealth and the purpose of using the service;
- corporate data of a legal entity;
- data of representatives, directors, shareholders and beneficial owners;
- documents confirming ownership structure, representatives' authority or source of funds;
- results of KYC/KYB/AML checks and internal risk assessment.

If a selfie, liveness check, video identification or other data is used in a manner which, under applicable law, constitutes the processing of biometric data, such processing shall be carried out only where there is an applicable legal basis and the additional conditions required by data protection legislation are satisfied.

2.3. Data on Card Functionality and Transactions

In connection with the use of virtual cards, the following may be processed:

- information on issued virtual cards;
- card status;
- BIN and card programme;
- limits and applicable restrictions;
- transaction history;

- data on successful, declined, cancelled and disputed transactions;
- data on attempted transactions;
- data on refunds, reversals, disputes, chargebacks and user claims;
- information on the available amount displayed in the interface;
- information on fees;
- merchant, MCC, currency, amount, date and transaction status data;
- data required to review disputed, suspicious or unauthorised transactions.

The display of the available amount or transaction history in the Mirocard interface does not mean that Mirocard holds the user's funds.

2.4. Data on Crypto Top-Ups

Where the user has access to crypto top-ups of the card functionality, the following may be processed:

- type of cryptoasset;
- blockchain network;
- sending and receiving addresses;
- transaction hash;
- transaction amount;
- processing status;
- results of blockchain analytics and compliance screening;
- information on wallets, linked addresses and source of funds;
- data required to verify source of funds and prevent unlawful use of the service.

Mirocard does not provide custodial storage of the user's cryptoassets as part of this service.

2.5. Technical Data

When the website, platform and personal account are used, the following may be collected automatically:

- IP address;
- browser type and version;
- device type;
- operating system;
- device, browser or session identifiers;
- date and time of login;
- data on user activity in the interface;
- security logs;

- information on errors, failures and technical events;
- geolocation-type data, where available on the basis of technical signals or user permissions;
- indicators of the use of VPN, proxy, TOR or other technical means, where necessary for security and compliance purposes.

2.6. Cookies and Similar Technologies

Cookies, local storage, pixels, tags, session identifiers and similar technologies may be used. Further details are set out in Section 8 of this Policy.

2.7. Data Received from Third Parties

Data about the user may be received from third parties where necessary to provide the service, verify the user, process transactions, prevent fraud or comply with compliance requirements.

Such sources may include:

- KYC/KYB/AML providers;
- sanctions, PEP and adverse media screening providers;
- blockchain analytics providers;
- issuers, card programmes, BIN partners, processors and payment systems;
- fraud-prevention providers;
- public authorities, courts, regulators or law enforcement agencies, where applicable;
- other partners and Mirocard infrastructure participants.

3. Purposes for Which Data Is Processed

Personal data is processed for the following purposes.

3.1. Provision of the Service

Data is used for:

- registration and account management;
- providing access to the personal account;
- processing applications for issuance of virtual cards;
- displaying card status, transactions, limits and available amount;
- providing support;
- carrying out actions requested by the user;
- administering user settings and communications.

3.2. KYC/KYB, AML/CFT, Sanctions and Compliance

Data is used for:

- identifying and verifying users;
- verifying legal entities and beneficial owners;
- sanctions screening;
- PEP and adverse media screening;
- assessment of AML/CFT, fraud, sanctions, regulatory and other compliance risks;
- transaction monitoring;
- verification of source of funds and source of wealth;
- prevention of sanctions circumvention, fraud and unlawful activity;
- compliance with the requirements of partners, issuers, card programmes, processors and other infrastructure participants.

3.3. Operation of Virtual Cards and Transactions

Data is used for:

- issuance, activation and servicing of virtual cards;
- transaction processing;
- application of limits and fees;
- review of declined transactions;
- processing refunds, reversals, disputes and chargebacks;
- interaction with issuers, card programmes, BIN partners, processors, payment systems and other infrastructure participants.

3.4. Security and Prevention of Abuse

Data is used for:

- protection of accounts;
- detection of suspicious activity;
- prevention of unauthorised access;
- investigation of fraud, abuse, card testing, account takeover and chargeback abuse;
- prevention of circumvention of KYC/KYB, sanctions, territorial, BIN, MCC, limit and other restrictions;
- ensuring the technical, operational and information security of the service.

3.5. Analytics and Service Improvement

Technical, statistical, aggregated or anonymised data may be used for:

- analysis of website and platform performance;
- improvement of the user interface;
- correction of errors;
- enhancement of the reliability and security of the service;
- assessment of the effectiveness of particular features;
- product development and optimisation.

3.6. Communications

Contact data may be used for:

- sending service notifications;
- security messages;
- notices of amendments to documents;
- responding to user enquiries;
- messages concerning the status of checks, transactions, cards or disputes;
- other mandatory, technical or operational communications.

Marketing communications are sent only where there is an appropriate legal basis and with the possibility to opt out.

3.7. Protection of Rights and Compliance with Obligations

Data may be used for:

- compliance with applicable law;
- accounting, tax and operational record-keeping;
- responding to requests from competent authorities;
- handling claims and disputes;
- protection of the rights, legitimate interests and security of Mirocard, users, partners and third parties.

4. Legal Bases for Processing

Personal data is processed only where there is an applicable legal basis.

4.1. Performance of a Contract

Data is processed where necessary to provide the user with access to the service, account, virtual cards, transactions, support and related functionality.

4.2. Compliance with Legal Obligations

Data is processed where necessary to comply with legal requirements, including KYC/KYB, AML/CFT, sanctions obligations, responses to requests from competent authorities and other legal obligations.

4.3. Legitimate Interest

Data may be processed on the basis of the legitimate interests of Mirocard, users, partners or third parties, including:

- prevention of fraud;
- ensuring the security of the service;
- protection of rights and legitimate interests;
- improvement of the service;
- risk management;
- investigation of breaches;
- defence against claims;
- ensuring the stable operation of the platform and card functionality.

Where data is processed on the basis of legitimate interest, a balance is struck between such interests and the user's rights.

4.4. Consent

User consent is relied upon where required by law, for example for certain cookies, marketing communications or other forms of processing that require consent.

The user may withdraw consent at any time. Withdrawal of consent shall not affect the lawfulness of processing carried out before such withdrawal.

4.5. Special Categories of Data

If, as part of a liveness check, video identification, document verification or other procedures, data is processed that may be regarded as special categories of personal data, such processing shall be carried out only where there is an applicable legal basis.

4.6. Vital Interests and Public Interest

In exceptional cases, data may be processed where necessary to protect the vital interests of a person or for the performance of a task carried out in the public interest, where such basis is applicable.

5. To Whom Data Is Disclosed

Personal data may be disclosed to third parties only to the extent necessary for the purposes set out in this Policy.

Depending on the circumstances, such third parties may act as independent controllers, joint controllers or processors. Their role is determined by the nature of the processing, the contractual arrangements and applicable law.

5.1. KYC/KYB/AML Providers

Data may be disclosed to providers of identification, verification, sanctions screening, PEP and adverse media screening, blockchain analytics, fraud prevention and other compliance checks.

5.2. Issuers, Card Programmes and Processors

Data may be disclosed to issuers, BIN partners, card programmes, processing providers, payment systems and other card infrastructure participants for the issuance, servicing, processing, restriction, monitoring and closure of virtual cards and transactions.

5.3. Crypto-Infrastructure Providers

Where the user uses crypto top-ups or related functions, data may be disclosed to providers involved in the processing, verification, conversion, compliance analysis or technical support of such transactions.

5.4. Technical Suppliers

Data may be disclosed to providers of hosting, cloud infrastructure, analytics, cyber security, email distribution, CRM, customer support, monitoring, logging and other technical services.

5.5. Legal and Professional Advisers

Data may be disclosed to lawyers, auditors, accountants, consultants and other professional advisers where necessary to protect rights, fulfil obligations, manage risks or conduct Mirocard's business.

5.6. Public Authorities and Mandatory Recipients

Data may be disclosed to public authorities, courts, regulators, law enforcement agencies, financial intelligence units, sanctions authorities or other mandatory recipients where required by law, by a request from a competent authority, or where necessary to protect the rights of Mirocard, users, partners or third parties.

6. International Data Transfers

Given the international nature of the service, card infrastructure, KYC/KYB/AML providers, blockchain analytics providers, issuers, processors, card programmes, crypto-infrastructure providers and technical suppliers, the user's personal data may be transferred to and processed outside the user's country of residence, including in countries outside the European Economic Area.

Where data is transferred to a country that does not ensure an adequate level of protection of personal data, the safeguards required by law are applied, which may include:

- standard contractual clauses;
- contractual obligations with data recipients;
- technical and organisational security measures;
- transfer risk assessments;
- other lawful safeguards permitted by applicable law.

7. How Data Is Protected

Technical and organisational measures are applied to protect personal data against unauthorised access, disclosure, alteration, loss, destruction or unlawful use.

Such measures may include:

- encryption of data transmission;
- access control;
- two-factor authentication;
- activity logging;
- role-based access restriction;
- monitoring of suspicious activity;
- backup procedures;
- supplier due diligence;
- internal security procedures;
- training of employees and contractors;
- contractual confidentiality and data protection obligations.

Despite the measures taken, no method of data transmission or storage can be completely secure. The user must comply with account security rules, use a strong password, refrain

from disclosing access data to third parties and report suspicious activity in a timely manner.

In the event of a personal data breach, steps shall be taken to assess the incident, minimise possible harm and notify users or competent authorities where such notification is required by applicable law.

8. Cookies and Similar Technologies

8.1. What Cookies Are

Cookies are small files stored on the user's device when visiting a website or using a platform. Similar technologies may include local storage, pixels, tags, SDKs, device identifiers and session identifiers.

8.2. What Cookies Are Used

The following categories of cookies may be used.

Strictly necessary cookies
These are required for the operation of the website and platform, including authorisation, security, session management, fraud prevention and access to protected sections. These cookies do not require separate consent where they are strictly necessary for providing the service requested by the user.

Functional cookies
These help remember user settings, such as interface language, region or preferences. Such cookies are used where there is an applicable legal basis.

Analytical cookies
These are used to analyse website performance, understand user behaviour, improve the interface and enhance service quality. Where such cookies are not strictly necessary, they are used only after the user's consent has been obtained.

Marketing cookies
These are used to display relevant advertising, measure the effectiveness of advertising campaigns and tailor marketing communications. Such cookies are used only after the user's consent has been obtained.

8.3. Managing Cookies

Upon the first visit to the website, the user may be shown a cookie banner or cookie settings centre.

The user may:

- accept all cookies;
- reject non-essential cookies;
- configure cookie categories;

- change or withdraw consent at a later stage.

Non-essential cookies are not placed before the user's consent is obtained, where such consent is required by law.

The user may also manage cookies through browser settings. Disabling certain cookies may affect the operation of some website or platform features.

8.4. Withdrawal of Consent

The user may change cookie settings or withdraw consent through the available cookie management tool, where such a tool is available, or through browser settings.

9. Automated Processing and Risk Assessment

For the purposes of KYC/KYB/AML, sanctions screening, fraud prevention, risk management, security and compliance with card infrastructure requirements, automated or partially automated analytical tools may be used.

Such tools may help identify:

- sanctions matches;
- PEP or adverse media indicators;
- suspicious transactions;
- inconsistency with the risk profile;
- indicators of fraud, abuse, account takeover or card testing;
- indicators of chargeback abuse;
- connection with prohibited or restricted jurisdictions;
- indicators of use of the service in breach of rules, limits, BIN, MCC or compliance requirements.

The results of automated or partially automated analysis may affect the need for additional checks, document requests, restriction of functionality, refusal to issue a card, suspension of a transaction, blocking of a card or account, or refusal of service.

Where a decision is made solely on the basis of automated processing and produces legal effects concerning the user or similarly significant effects, the user shall have the rights provided by applicable law, including the right to request human involvement in the review of the decision, express the user's point of view and challenge the decision, where such rights apply.

10. Data Retention Periods

Personal data is retained only for as long as is necessary for the purposes for which it was collected, and to comply with legal obligations, resolve disputes, prevent fraud, conduct checks, process transactions and protect Mirocard's rights.

Retention periods depend on the category of data, the purpose of processing, applicable law, AML/CFT requirements, sanctions compliance, card infrastructure requirements and the need to protect rights.

10.1. Account Data

Account data is retained for the duration of use of the service and, after use has ceased, for the period necessary to comply with legal obligations, protect rights, prevent fraud and address potential claims.

10.2. KYC/KYB/AML Data

KYC/KYB/AML data, verification documents, screening results, source of funds information, risk-profile records and related compliance records may be retained for the period prescribed by applicable law, AML/CFT requirements, sanctions compliance requirements, card infrastructure requirements and internal retention procedures.

10.3. Transaction Data

Data on transactions, virtual cards, available amount, fees, refunds, reversals, disputes and chargebacks may be retained for the period necessary to comply with contractual, accounting, tax, AML/CFT, sanctions and other legal obligations, and to review claims and disputes.

10.4. Technical Data

Technical logs, security data and information on use of the service may be retained for the period necessary to ensure security, investigate incidents, prevent fraud and maintain operation of the platform.

10.5. Cookies

The retention period for cookies depends on their category and specific purpose. Session cookies are deleted after the session ends, while persistent cookies may be stored for longer within the period specified in cookie settings, the cookie banner or another available cookie management tool.

Once the applicable retention period has expired, data is deleted, anonymised or archived, unless further retention is required by law or for the protection of rights.

11. User Rights

Depending on applicable law, the user may have the following rights in relation to personal data.

11.1. Right of Access

The user may request confirmation as to whether personal data is being processed, as well as information about such processing and a copy of the data.

11.2. Right to Rectification

The user may request correction of inaccurate or incomplete personal data.

11.3. Right to Erasure

The user may request deletion of personal data where there are legal grounds for doing so.

Deletion may be restricted where the data is necessary for compliance with a legal obligation, KYC/KYB/AML requirements, sanctions requirements, protection of rights, dispute handling, fraud prevention or other lawful purposes.

11.4. Right to Restrict Processing

The user may request restriction of data processing in cases provided for by law, for example where the user disputes the accuracy of the data or objects to the processing.

11.5. Right to Data Portability

The user may obtain personal data provided by the user in a structured, commonly used and machine-readable format, where applicable and technically feasible.

11.6. Right to Object

The user may object to processing based on legitimate interest where the user has grounds relating to the user's particular situation.

The user may object at any time to processing of data for direct marketing purposes.

11.7. Right to Withdraw Consent

Where processing is based on consent, the user may withdraw such consent at any time. Withdrawal of consent shall not affect the lawfulness of processing carried out before withdrawal.

11.8. Rights in Relation to Automated Decisions

In cases provided for by applicable law, the user may request human involvement in the review of a decision, express the user's point of view and challenge the decision where such decision was taken solely on the basis of automated processing and has legal or similarly significant effects.

12. How to Exercise Rights

To exercise rights, the user may contact Mirocard at:

Email: [insert email]

Additional information may be requested in order to confirm the user's identity and protect data against unauthorised disclosure.

Requests are answered without undue delay and, as a rule, no later than one month from receipt of the request. If the request is complex or multiple requests have been received, the response period may be extended by a further two months. In such case, the user shall be informed of the extension and the reasons for the delay within one month from receipt of the request.

A request may be refused in whole or in part where such refusal is permitted by applicable law, for example due to KYC/KYB/AML obligations, sanctions requirements, card infrastructure requirements, protection of rights, fraud investigation or the need to retain data by law.

13. Data of Minors

The Mirocard service is not intended for persons who have not reached the age of majority in their jurisdiction.

Data of minors is not knowingly collected. If it becomes known that data of a minor has been provided without a proper basis, reasonable steps shall be taken to delete or restrict the processing of such data, unless otherwise required by law.

14. Amendments to this Policy

This Policy may be amended due to changes to the service, card functionality, partner infrastructure, legislation, compliance requirements, technical processes or business practice.

The updated version of the Policy may be published on the website, in the service interface, in the user's personal account or otherwise communicated to the user by any available means.

Amendments shall take effect from the date of publication unless another date is specified in the updated version.