

PRIVACY POLICY

Last Updated: July 27, 2026

Introduction

This Privacy Policy describes how we collect, process, use and disclose your information, including any personal data we collect from you, or which you provide to us through the website www.mirocard.com (hereinafter referred to as the Website). When you contact us via the Website, complete any forms or submit any details using the Website, we will collect, use and disclose your personal information as described in this Privacy Policy.

What is personal data?

Personal Data means any information relating to an identified or identifiable natural person.

Personal data is processed exclusively for legitimate business and legal purposes, including providing the Services, verifying user identity, ensuring the security and integrity of the platform, preventing fraud and financial crime, processing transactions, and complying with applicable laws, regulations, and other legal obligations.

What are the Services?

For the purposes of this Privacy Policy, "Services" means all products, services, features, functionalities, content, applications, and other offerings provided by us through the Website, including the customer support and any related services that we make available from time to time.

Personal Data We Collect and Process

We collect personal data directly from you, automatically through your use of the Services, and from trusted third-party sources where permitted by applicable law.

1. Information You Provide When You Register

When you create an account, we may collect:

- first name and last name;
- email address;
- hashed password.

2. Identity Verification Information

To verify your identity and comply with applicable legal and regulatory requirements, we may collect:

- mobile phone number;

- identity document information, including the document type, issuing country, document number, issue and expiry dates, information contained in machine-readable zones or barcodes, and document security features;
- photographs or scans of identity documents;
- facial images, including selfies, liveness verification images
- biometric information derived from facial images, where permitted by applicable law and necessary for identity verification. biometric information processed by our identity verification providers.

3. Compliance and Source of Funds Information

To comply with AML/CFT requirements, prevent fraud, and assess the legitimacy of transactions, we may collect:

- information and documents demonstrating the source of funds or source of wealth, including bank statements, supporting documents, explanations, and screenshots;
- information regarding the purpose, nature, and economic rationale of transactions;
- Information you provide in questionnaires to prove your capacity and understanding of the consequences of your actions.

4. Communications with Us

When you contact us, we may collect:

- your contact details, including your email address;
- the content of your communications, including messages, attachments, and other materials you provide;
- support ticket identifiers and case reference numbers;
- technical information relating to your communications, such as timestamps, device information, browser details, language settings, and other diagnostic information.

5. Transaction Information

When you use the Services, we may collect information relating to your transactions, including:

- wallet information and unique account identifiers within the System;
- virtual card information necessary to provide card-related services;
- transaction details, including the date, time, amount, currency, transaction status, counterparties, merchant information, payment method, transaction references, and any messages associated with a transaction;

6. Device and Technical Information (Cookies)

We use cookies and similar technologies, including web beacons, pixels, tags, local storage, and similar tracking technologies (collectively, "Cookies"), to collect information about your use of the Website and the Services. Cookies are small text files stored on your device when you visit the Website.

Cookies enable us to operate the Website and the Services, recognize your device, remember your preferences, improve functionality and performance, analyze how the Website and the Services are used, enhance security, prevent fraud, comply with our legal obligations, and, where applicable, provide personalized content or advertising.

Information We Collect Through Cookies

Through Cookies, we may collect and process information including, but not limited to:

- IP address;
- browser type and version;
- device type, operating system, and device identifiers;
- language and regional preferences;
- date, time, and duration of your visits;
- pages viewed and navigation paths;
- referring and exit URLs;
- interactions with the Website and the Services;
- session identifiers;
- network and connection information; and
- other technical, diagnostic, and usage information.

Some of the information collected through Cookies may constitute Personal Data under applicable data protection laws.

Types of Cookies We Use

Cookies may be classified as follows:

- By origin
 - ⇒ First-party Cookies are placed directly by us through the Website or the Services.
 - ⇒ Third-party Cookies are placed by trusted third-party service providers, including analytics, security, payment processing, fraud prevention, customer support, and advertising providers that assist us in operating, maintaining, securing, and improving the Website and the Services.

- By duration
 - ⇒ Session Cookies are temporary Cookies that are automatically deleted when you close your browser or end your browsing session.
 - ⇒ Persistent Cookies remain stored on your device for a specified period or until they expire or are manually deleted. These Cookies allow us to recognize your device across multiple visits and remember your preferences and settings.
- By purpose
 - ⇒ Strictly Necessary Cookies are essential for the operation of the Website and the provision of the Services. These Cookies enable core functionality such as authentication, security, fraud prevention, network management, and payment processing.
 - ⇒ Functional Cookies allow the Website to remember your preferences and settings, providing enhanced functionality and a more personalized user experience.

Managing Cookies

You can manage or disable Cookies through your browser settings. Please note that disabling certain Cookies may affect the functionality, availability, security, or performance of the Website or the Services, and some features may not operate properly.

Where required by applicable law, we will obtain your consent before placing non-essential Cookies on your device. You may withdraw or modify your consent at any time through our cookie preference settings or by changing your browser settings.

Personal Data Received from Third Parties

We may also receive personal data from trusted third-party sources, including:

- payment service providers, financial institutions, and payment processors;
- card networks, issuing banks, fraud prevention providers, credit reference agencies, identity verification providers, and sanctions screening providers;
- government authorities, regulators, law enforcement agencies, and other competent public authorities where permitted or required by law;
- publicly available sources, including company registers, sanctions lists, beneficial ownership registers, and other publicly accessible databases used for customer due diligence, enhanced due diligence, fraud prevention, and compliance purposes.

How We Share Personal Data

We share personal data with the following categories of recipients, in each case only to the extent necessary and subject to appropriate contractual and technical safeguards:

- **Financial Partners** — including, but not limited to, the Issuer, issuing banks, programme managers, card networks, acquirers, payment processors, digital asset exchanges, and fiat on-ramp/off-ramp providers. We may disclose personal data to these partners where necessary to enable the issuance and administration of Cards, process, authorize, and settle Transactions, comply with applicable legal and regulatory obligations, and detect, prevent, and manage fraud and other risks.
- **Verification and Compliance Providers** — such as identity verification providers, KYC and AML service providers, sanctions and PEP screening vendors, adverse media screening providers, and fraud prevention partners. We share personal data with these providers where necessary to verify identities, comply with applicable legal and regulatory obligations, and detect and prevent fraud.
- **Technology providers** — cloud hosting, email, messaging, customer-support tooling, analytics, security monitoring and other SaaS providers that support the System.
- **Professional advisers** — legal counsel, auditors, accountants and insurers, where necessary for the establishment, exercise or defense of legal claims or for compliance with legal obligations.
- **Public authorities** — we may disclose your information to comply with our legal obligations, to respond to requests relating to criminal investigation, alleged or suspected illegal activities, or any other activities that may expose us or other users to legal liabilities, as well as to enforce our site policies and protect our or others' rights, property or safety.

International Data Transfers

Some of the recipients with whom we share personal data may be located in jurisdictions outside the country where your personal data was originally collected. Consequently, your personal data may be transferred to, stored in, or otherwise processed in countries that may provide a different level of data protection than your jurisdiction.

Where required by applicable law, we implement appropriate safeguards to ensure that international transfers of personal data are carried out in accordance with applicable data protection laws and that your personal data remains adequately protected.

Additional Disclosures

Where we intend to disclose your personal data in circumstances that are not described in this Privacy Policy or are not otherwise permitted by applicable law, we will obtain your consent before doing so, unless the disclosure:

1. is required or requested by a competent governmental authority, regulator, court, or law enforcement agency;
2. is necessary to protect your vital interests or those of another individual where obtaining your consent is not reasonably practicable;

3. is necessary to respond to an emergency involving a serious threat to the life, health, or safety of any individual; or
4. is otherwise required, permitted, or authorized under applicable laws and regulations.

How we keep your data secure

We are committed to safeguarding your personal data and take appropriate measures to protect it whenever you submit information through our website or otherwise provide it to us.

To protect your information from unauthorized access, disclosure, alteration, or destruction, we apply a range of technical and organizational security measures. These include encryption technologies, authentication mechanisms, and other security controls designed to secure our systems and the personal data they contain. Physical access to facilities where personal data is processed and stored is restricted to authorized personnel only, and such facilities are subject to continuous monitoring.

Access to personal data is granted only to employees who require such access to perform their job responsibilities, such as members of our customer support team. All personnel with access to personal data are subject to confidentiality obligations under non-disclosure agreements. In addition, we provide ongoing training to our employees on data protection, information security, and confidentiality requirements.

We regularly review and enhance our security practices to ensure they remain aligned with recognized industry standards and continue to provide an appropriate level of protection for your personal data.

You also play an important role in protecting your account. We recommend using a unique, strong password for your account that includes a combination of uppercase and lowercase letters, numbers, and special characters, and avoiding the reuse of passwords across different services. Never disclose your password to anyone. Please note that our employees will never ask you to provide your password or other login credentials. If anyone claiming to represent Mirocard requests this information, do not disclose it and contact us immediately by email to support@mirocard.com.

Personal Data Retention

We retain personal data only for as long as necessary for the purposes for which it was collected, or for such longer period as is required by applicable law. In particular:

- data collected for the purposes of AML/CFT compliance (including identification documents, Verification records, Transaction records, suspicious-activity reports and sanctions-screening records) is retained for a minimum of five (5) years following the end of the business relationship or longer if required by applicable law.
- communications with Customer Support are retained for a reasonable period following the closure of the relevant ticket, to resolve recurring issues and to defend against potential disputes;

- marketing-consent records and evidence of consent are retained for as long as the consent remains active, and for a reasonable period after withdrawal.

When the retention period expires, personal data is deleted or irreversibly anonymized, except where continued retention is required by applicable law, or where the data is necessary for the establishment, exercise or defense of legal claims.

Your Rights

You have the right to exercise control over the way in which your personal data is processed:

- **Right to be informed.** You have the right to be informed about how and why we collect, use, process, store, and disclose your personal data. This Privacy Policy explains our data processing practices, and you may contact us at any time if you require further information.
- **Right of access.** You have the right to request confirmation as to whether we process your personal data and to obtain access to that data, together with information about the purposes of processing, the recipients with whom it is shared, and other information required under applicable law.
- **Right to rectification.** You have the right to request that we correct or update any inaccurate, incomplete, or outdated personal data that we hold about you.
- **Right to erasure.** You may request the deletion of your personal data by submitting a request by contacting us via email. Please note that, where we are required to retain certain information to comply with legal, regulatory, accounting, fraud prevention, or other statutory obligations, we may not be able to erase all of your personal data. In such cases, we will retain only the information that is legally required and delete any data that is no longer necessary.
- **Right to restrict or object to processing.** You have the right, in the circumstances provided by applicable law, to request the restriction of the processing of your personal data or to object to certain types of processing.
- **Right to data portability.** Where applicable, you may request that your personal data be transferred to another service provider. Where technically feasible and legally permitted, we will provide your data in a structured, commonly used, and machine-readable format.
- **Right to withdraw consent.** You may withdraw that consent at any time by updating your account settings or by contacting us via email and specifying the consent you wish to withdraw. The withdrawal of consent does not affect the lawfulness of processing carried out before the withdrawal. You may also opt out of receiving marketing communications by clicking the "unsubscribe" link included in our emails.

We will reply to your request within 30 days once we receive it. If we expect that responding to you will take longer, we will let you know.

You may exercise your rights described above by sending an e-mail to support@mirocard.com. Before we provide you with any confidential information, we must ensure that you are indeed the person you claim to be. For example, we will ask you to send a request from the mail associated with your Mirocard account

Kindly note that there may be legal reasons when we will not be able to fulfil your request.

Security

We implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data.

Policy Changes

We reserve the right to modify, amend, or update this Privacy Policy at any time, in our sole discretion. Any changes will become effective immediately upon posting the updated Privacy Policy on the Website, unless otherwise required by applicable law.

We encourage you to review this Privacy Policy periodically to stay informed of any updates. Your continued access to or use of the Website or the Services after any changes have been posted constitutes your acceptance of the revised Privacy Policy.

We may, but are not obligated to, notify you of material changes to this Privacy Policy by email, through the Website, or by other reasonable means. Except where required by applicable law, we assume no obligation to provide individual notice of any changes.