Mirocard AML/KYC Policy

Last updated: 23 April 2026

Terms and Definitions

For the purposes of this Policy, the following terms shall have the meanings set out below unless the context requires otherwise.

1. **Mirocard** means a service providing users with access to the issuance, management and use of virtual cards through card, payment, technical, crypto-infrastructure and other partner infrastructure.
2. **User** means a natural person or legal entity that registers with Mirocard, undergoes verification, applies for the issuance of a virtual card, uses a virtual card, carries out transactions or otherwise gains access to the service functionality.
3. **Virtual Card** means a digital payment instrument provided to the user through Mirocard under the relevant card programme, BIN, issuer, processor and other card infrastructure participants. A virtual card is not a bank account, deposit, savings product, credit product, electronic money or a means of storing funds with Mirocard.
4. **Available Amount** means the amount displayed in the service interface and available for transactions with the virtual card under the applicable card programme. Display of the available amount does not mean that Mirocard holds the user's funds or accepts them as a deposit.
5. **AML/CFT** means measures for the prevention of money laundering and terrorist financing, including the identification, assessment, monitoring, restriction and mitigation of the relevant risks.
6. **KYC/KYB** means procedures for the identification and verification of natural persons and legal entities, including verification of identity, documents, corporate data, representatives, ownership structure, beneficial owners, the purpose of using the service, source of funds and other necessary information.
7. **Compliance** means the set of rules, procedures, checks, restrictions and decisions aimed at compliance with applicable law, sanctions requirements, AML/CFT requirements, card infrastructure requirements, partner requirements and Mirocard's internal risk management procedures.
8. **Compliance Risk** means any AML/CFT, sanctions, fraud, regulatory, card, operational, reputational or other risk connected with the user, transaction, source of funds, jurisdiction, merchant, virtual card or use of the service.
9. **Risk-Based Approach** means an approach under which the scope of checks, limits, available functionality, monitoring, restrictions and other compliance measures are determined taking into account the risk level of a particular user, transaction, jurisdiction, source of funds, card programme or other circumstances.

10. **Risk Profile** means an assessment of the user's risk level prepared by Mirocard on the basis of KYC/KYB data, jurisdiction, nature of activity, source of funds, transactions, limits, the BIN used, card programme, sanctions, fraud and other compliance indicators.
11. **Sanctions Screening, PEP Screening and Adverse Media Screening** means checks of the user, related persons, transactions, jurisdictions, sources of funds and other data for sanctions matches, politically exposed person status, adverse public information or other compliance indicators.
12. **Enhanced Due Diligence** means additional review of the user, transaction, source of funds, legal entity, beneficial owners or other circumstances where the level of risk is elevated or unacceptable.
13. **Source of Funds and Source of Wealth** means the origin of the specific funds used in connection with the service, and the origin of the overall wealth of the user or beneficial owner.
14. **Beneficial Owner** means a natural person who directly or indirectly owns a legal entity, controls it, or derives benefit from its activities or use of the service.
15. **Related Person** means a representative, director, authorised person, beneficial owner, nominee, counterparty or other person connected with the user, transaction, source of funds or use of the service.
16. **Card Infrastructure** means the set of the card programme, BIN, issuer, processor, card network, card programme partners and other participants that enable the issuance, servicing and use of virtual cards.
17. **BIN** means the bank identification number of a payment card or the related card programme, the terms of which may determine limits, fees, available transactions, MCC restrictions, transaction processing rules and other parameters of card use.
18. **MCC** means the merchant category code used to classify the merchant outlet or type of merchant activity.
19. **Merchant** means the outlet, supplier of goods or services, platform, service or other person with whom the user carries out a transaction using the virtual card.
20. **Transaction** means any action by the user connected with use of the card functionality, including a request to top up the card functionality, authorisation, payment, declined transaction, refund, cancellation, dispute, chargeback or another related procedure.
21. **Fraud and Abuse** means any unlawful, dishonest, improper or prohibited use of the service, account, virtual card, available amount or other Mirocard functionality.
22. **High-Risk Activity** means activity that does not correspond to the user's risk profile, the declared purpose of using the service, the economic rationale of transactions, the terms of the card programme, BIN, MCC, limits or other applicable requirements.
23. **Prohibited or Restricted Jurisdiction** means a country, territory or region whose servicing is prohibited or restricted by Mirocard due to applicable law, sanctions regimes, partner requirements, card infrastructure requirements or internal risk assessment.
24. **Restrictive Measures** means refusal of registration, verification, issuance or use of a virtual card, reduction of limits, restriction of available functionality, decline or

suspension of a transaction, restriction of the available amount, blocking of an account or card, termination of service or other measures applied by Mirocard to manage compliance risks.

25. **Partners** means issuers, card programmes, BIN partners, card networks, KYC/AML providers, processing, payment, crypto-infrastructure, technical and other mandatory participants in the Mirocard infrastructure.

1. General Provisions

1.1. Purpose of the Policy

This Mirocard AML/KYC Policy, hereinafter referred to as the "**Policy**", sets out Mirocard's general approach to user identification and verification, risk assessment, sanctions control, transaction monitoring and the prevention of improper use of the service.

This Policy is intended to prevent money laundering, terrorist financing, sanctions circumvention, fraud, abuse of card infrastructure, the use of unlawful, unverified or non-transparent sources of funds, and other conduct creating AML/CFT, sanctions, fraud, regulatory, card, reputational or other compliance risks.

1.2. Scope of Application

This Policy applies to all natural persons and legal entities that register with Mirocard, undergo verification, apply for the issuance of a virtual card, use the card functionality, carry out transactions or otherwise gain access to the service.

This Policy shall apply together with the Usage Policy, the Privacy Policy, the terms of the relevant card programme, and the terms of the issuer, processor, card network, KYC/AML providers and other mandatory partners.

1.3. Service Operating Model

Mirocard provides the user with access to card functionality and an interface for managing virtual cards through the infrastructure of third-party partners.

Mirocard is not a bank, payment institution, electronic money issuer, depository, custodian, provider of a bank account or holder of the user's funds. Mirocard does not accept deposits, does not open bank accounts, does not issue electronic money and does not hold users' funds.

Transactions, including top-ups of the card functionality, settlements, authorisations, debits, refunds, cancellations, disputes, chargebacks and other related procedures, may be processed by third-party infrastructure participants. Mirocard shall be entitled to take into account the decisions, restrictions, refusals, holds, refunds, cancellations or other measures applied by such participants where these are imposed in accordance with their rules, the requirements of the card programme or applicable law.

1.4. Checks through Providers and Partner Infrastructure

Mirocard may conduct KYC/KYB checks, sanctions screening, PEP screening, adverse media screening, fraud checks, checks of crypto addresses and transactions, and other compliance checks through third-party providers, including Sumsub, other KYC/AML providers, sanctions screening providers, fraud-prevention providers, blockchain analytics providers, and card, processing, payment and technical partners.

Use of a third-party provider shall not limit Mirocard's right to make its own decisions concerning user registration, completion of checks, issuance or use of a virtual card, limits, transactions, additional checks, restrictions, blocking or termination of service.

Mirocard shall also be entitled to take into account the requirements of card programmes, BINs, issuers, processors, card networks, KYC/AML providers and other mandatory infrastructure participants.

1.5. No Guarantee of Access to the Service

Registration, submission of documents, successful completion of checks or previously granted access to Mirocard functionality do not guarantee the user:

- issuance of a virtual card;
- access to a specific BIN or card programme;
- completion of a specific transaction;
- retention of limits, fees or other terms;
- absence of additional checks;
- uninterrupted or indefinite provision of the service.

Mirocard shall be entitled to refuse registration, verification, issuance or use of a virtual card, decline or suspend a transaction, restrict functionality, restrict the available amount, block the account or card, suspend service or terminate the relationship with the user where this is necessary or appropriate in light of AML/CFT, sanctions, fraud, card, regulatory, partner or other compliance requirements.

2. KYC/KYB and the Risk-Based Approach

2.1. Mandatory Verification

To use Mirocard, the user must complete KYC/KYB checks to the extent determined by Mirocard, taking into account the risk-based approach, applicable law, the requirements of the card programme, BIN, issuer, processor, card network, KYC/AML provider, other mandatory partners, available functionality, limits and the nature of use of the service.

Checks may be carried out upon registration, submission of an application for issuance of a virtual card, top-up of the card functionality, carrying out transactions, amendment of user data, increase of limits, change of BIN or card programme, detection of suspicious activity,

review of the risk profile, and in other cases where Mirocard considers this necessary for compliance purposes.

Mirocard shall be entitled to refuse registration, card issuance, processing of a transaction or continued service where the user has not passed verification, has provided incomplete, inaccurate, contradictory or outdated information, has refused to provide required documents, or where the results of the checks indicate an unacceptable level of risk.

2.2. Verification of Natural Persons

In relation to natural persons, checks may include:

- identification and verification of identity;
- verification of document, age and legal capacity;
- verification of citizenship, residence and address;
- verification of contact details;
- verification by means of a selfie or liveness procedure;
- sanctions screening;
- PEP screening;
- adverse media screening;
- verification of the purpose of using the service;
- verification of the nature of transactions;
- verification of source of funds or source of wealth.

2.3. Verification of Legal Entities

In relation to legal entities, checks may include:

- verification of registration and corporate data;
- verification of country of incorporation and actual place of business;
- analysis of the business model and nature of activity;
- verification of representatives, directors and authorised persons;
- verification of ownership structure;
- verification of beneficial owners;
- verification of the purpose of using the service;
- sanctions screening of the legal entity and related persons;
- PEP and adverse media screening of related persons;
- verification of source of funds or source of wealth.

Mirocard shall determine the scope of checks on an individual basis having regard to the user's risk profile, jurisdiction, nature of activity, ownership structure, source of funds, transactions, available limits, applicable BIN, card programme and partner requirements.

2.4. Risk-Based Approach

Mirocard applies a risk-based approach to user registration, verification, access to the service, issuance and use of virtual cards, transaction monitoring, the setting of limits, the application of restrictions and other compliance decisions.

In assessing risk, Mirocard may take into account:

- type of user;
- country of citizenship, residence, incorporation, business activity or actual location;
- results of KYC/KYB checks;
- transparency of the ownership structure;
- information on beneficial owners;
- nature of activity and purpose of using the service;
- source of funds or source of wealth;
- method of topping up the card functionality, including crypto transfers;
- volume, frequency, nature and geography of transactions;
- the BIN, card programme, MCC, limits and available functionality used;
- declined transactions, disputes, refunds, cancellations or chargebacks;
- sanctions, PEP, adverse media, fraud or other compliance indicators;
- requirements of the issuer, KYC/AML provider or other partners;
- applicable law, sanctions regimes and Mirocard's internal risk management procedures.

This list of factors is not exhaustive. Mirocard shall be entitled to take into account any other circumstances that may be relevant to the assessment of AML/CFT, sanctions, fraud, regulatory, card, operational, reputational or other compliance risks.

2.5. Additional and Enhanced Due Diligence

Mirocard shall be entitled at any time to request additional information, documents or explanations from the user, to conduct repeated, additional or enhanced due diligence where this is necessary for identification, risk assessment, verification of source of funds, analysis of a transaction, verification of a legal entity, verification of beneficial owners, compliance with sanctions requirements, prevention of fraud or other compliance purposes.

Such review may include:

- confirmation of source of funds or source of wealth;
- analysis of the economic rationale of transactions;
- verification of crypto addresses;
- review of blockchain data;
- verification of transaction hash;

- verification of linked addresses, counterparties, exchanges, exchangers or other data relating to the origin and movement of funds;
- requests for contracts, invoices, statements, corporate documents, tax documents or other supporting materials.

The user must provide accurate, complete, up-to-date and consistent information and documents. Failure to provide requested information, provision of inaccurate information, concealment of beneficial owners, source of funds, purpose of using the service or connection with a prohibited or restricted jurisdiction may result in refusal of service, restriction of functionality, blocking of the account or card, restriction of a transaction, restriction of the available amount or termination of the relationship with the user.

2.6. Review of the Risk Profile

The user's risk profile may be reviewed throughout the entire period of use of the service, including where there is a change in user data, ownership structure, beneficial owners, nature of activity, country of citizenship, residence, incorporation or actual location, volume or nature of transactions, limits, BIN, card programme, applicable partner requirements or legislation.

Following review of the risk profile, Mirocard shall be entitled to change the available functionality, request additional information or documents, conduct repeated or enhanced checks, amend limits, restrict transactions, block the account or card, restrict the available amount, refuse continued service or take other measures necessary for risk management.

3. Sanctions Screening, PEP and Adverse Media

3.1. General Principle

Mirocard conducts sanctions screening, PEP screening, adverse media screening and other compliance checks in relation to users, representatives, directors, authorised persons, beneficial owners, related persons, jurisdictions, transactions, sources of funds and other data connected with use of the service.

Such checks may be carried out upon registration, KYC/KYB verification, submission of an application for issuance of a virtual card, top-up of the card functionality, carrying out transactions, amendment of user data, repeated or enhanced checks, activity monitoring, review of the risk profile, and in other cases where Mirocard considers this necessary for compliance purposes.

3.2. Sanctions Lists and Regimes

Mirocard may carry out sanctions control by reference to applicable sanctions lists, regimes and sources, including:

- the consolidated sanctions list of the European Union;
- the consolidated list of the United Nations Security Council;

- OFAC sanctions lists;
- United Kingdom sanctions lists;
- sanctions lists, rules and restrictions applicable to the card programme, BIN, issuer, processor, card network, banks, payment providers, KYC/AML providers or other mandatory Mirocard partners.

Mirocard shall also be entitled to take into account territorial, sectoral, goods, technology, financial and other sanctions restrictions, even where a specific person is not included on a personal sanctions list.

3.3. PEP and Adverse Media

Mirocard shall be entitled to screen the user and related persons for politically exposed person status and to take into account adverse public information which may indicate AML/CFT, sanctions, fraud, corruption, regulatory, reputational or other compliance risk.

The existence of PEP status or adverse public information does not always mean an automatic refusal of service, but may result in additional review, a request for source of funds or source of wealth, enhanced due diligence, manual review, imposition of additional limits or restrictions, enhanced monitoring or refusal of service where the level of risk is unacceptable.

3.4. Sanctions Matches and Prohibition on Circumvention

Where a sanctions match, possible match, connection with a prohibited or restricted jurisdiction, risk of sanctions circumvention, PEP indicators, adverse public information or other material compliance indicators are identified, Mirocard shall be entitled to refuse registration, issuance or use of a virtual card, decline or suspend a transaction, restrict functionality, request additional documents, block the account or card, restrict the available amount, terminate service or take other measures necessary to comply with applicable requirements and manage risks.

The user is prohibited from using Mirocard for the direct or indirect circumvention of sanctions, territorial restrictions, KYC/KYB checks, card restrictions, BIN conditions, MCC restrictions, limits or other compliance requirements.

In particular, the service must not be used for the benefit of a sanctioned person, organisation or jurisdiction, through nominees, front structures, another person's data, linked accounts, VPN, proxy, TOR or other means where this is intended to conceal identity, location, source of funds, beneficial owner, actual user or the nature of the transaction.

3.5. Non-Disclosure of Screening Details

Mirocard shall be entitled not to disclose to the user details of sanctions screening, PEP screening, adverse media screening or other compliance checks, including screening sources, match results, internal risk assessment, escalation rules, risk indicators, thresholds, scoring models or the specific reasons for a decision, where such disclosure may breach applicable law, sanctions requirements, card programme rules, partner requirements, service security, third-party rights or the effectiveness of compliance procedures.

4. Prohibited and Restricted Jurisdictions

4.1. General Principle

Mirocard does not provide the service to users who are located in, incorporated in, are citizens or residents of, carry on business in or are otherwise connected with prohibited or restricted jurisdictions where such servicing would be contrary to applicable law, sanctions regimes, AML/CFT requirements, the requirements of the card programme, BIN, issuer, processor, card network, other mandatory partners or Mirocard's internal risk assessment.

Mirocard shall be entitled to refuse registration, KYC/KYB verification, issuance or use of a virtual card, processing of a transaction or continued service where a connection is identified between the user, transaction, source of funds, merchant, account or card and a prohibited or restricted jurisdiction.

4.2. List of Prohibited and Restricted Jurisdictions

As of the last update of this Policy, Mirocard does not provide the service to users who are citizens or residents of, are incorporated in, are actually located in, carry on business in, have a source of funds in, or are otherwise connected with the following countries and territories:

- Islamic Republic of Afghanistan – AF;
- Republic of Angola – AO;
- Belarus – BY;
- Bosnia and Herzegovina – BA;
- Republic of Botswana – BW;
- Commonwealth of The Bahamas – BS;
- Kingdom of Cambodia – KH;
- Republic of Burundi – BI;
- Democratic Republic of the Congo – CD;
- Central African Republic – CF;
- Republic of the Congo – CG;
- People's Democratic Republic of Algeria – DZ;
- Republic of Ecuador – EC;
- State of Eritrea – ER;
- Federal Democratic Republic of Ethiopia – ET;
- Republic of Ghana – GH;
- Republic of Guinea – GN;
- Republic of Guinea-Bissau – GW;
- Co-operative Republic of Guyana – GY;
- Republic of Haiti – HT;

- Republic of Iraq – IQ;
- Islamic Republic of Iran – IR;
- Japan – JP;
- Republic of Kenya – KE;
- Democratic People's Republic of Korea – KP;
- Republic of Cuba – CU;
- Lebanese Republic – LB;
- Republic of Liberia – LR;
- Libya – LY;
- Republic of the Union of Myanmar – MM;
- Federal Republic of Nigeria – NG;
- Islamic Republic of Pakistan – PK;
- Republic of Serbia – RS;
- Russian Federation – RU;
- Republic of the Sudan – SD;
- Democratic Socialist Republic of Sri Lanka – LK;
- Federal Republic of Somalia – SO;
- Republic of South Sudan – SS;
- Syrian Arab Republic – SY;
- Republic of Tunisia – TN;
- Republic of Trinidad and Tobago – TT;
- Ukraine – UA;
- Republic of Uganda – UG;
- United States of America – US;
- Republic of Vanuatu – VU;
- Bolivarian Republic of Venezuela – VE;
- Republic of Yemen – YE;
- Republic of Zimbabwe – ZW;
- People's Republic of China – CN.

For the purposes of this Policy, a connection with a prohibited or restricted jurisdiction may include citizenship, residence, incorporation, actual location, place of business, source of funds, source of wealth, the location of representatives, directors, beneficial owners, related persons, merchants, counterparties or other material elements of the transaction in such jurisdiction.

Mirocard shall also be entitled to restrict or prohibit the servicing of users connected with other countries, territories or regions where such restriction is required by applicable law,

sanctions regimes, FATF requirements, the card programme, BIN, issuer, processor, card network, other mandatory partners or Mirocard's internal risk assessment.

The inclusion of a country or territory in this list does not necessarily mean that such country or territory is fully prohibited under applicable law. The restriction may result from partner requirements, card infrastructure requirements, sanctions, AML/CFT, fraud, operational, regulatory or other compliance risks.

4.3. Updating the List

Mirocard shall be entitled at any time to update, supplement or amend the list of prohibited and restricted jurisdictions without any separate re-execution of this Policy or other user documents.

Amendments may result from changes in sanctions regimes, applicable law, regulatory requirements, the requirements of the card programme, BIN, issuer, processor, card network, other partners, service geography, technical availability or Mirocard's internal risk assessment.

The updated list shall apply from the time of its publication on the Mirocard website, in the service interface, in this Policy or from such other date as Mirocard may specify.

Continued use of the service after update of the list constitutes the user's acceptance of the applicable restrictions, unless otherwise provided by mandatory provisions of applicable law.

4.4. User Obligations

The user must independently ensure that the user is entitled to use Mirocard in accordance with the law of the user's jurisdiction and is not subject to the restrictions established by the list of prohibited and restricted jurisdictions, the rules of the card programme, sanctions regimes or the requirements of applicable partners.

The user is prohibited from using the service from a prohibited or restricted jurisdiction, providing inaccurate information regarding citizenship, residence, incorporation, actual location or connection with such jurisdiction, or using third parties, nominees, another person's accounts, VPN, proxy, TOR or other means to circumvent territorial, sanctions or compliance restrictions.

Where this section is breached, Mirocard shall be entitled to refuse registration, verification, issuance or use of a virtual card, decline or suspend a transaction, restrict functionality, block the account or card, restrict the available amount, terminate service or take other measures necessary to comply with AML/CFT, sanctions, card, regulatory or other compliance requirements.

5. Transaction Monitoring and Prohibited Use

5.1. Transaction Monitoring

Mirocard shall be entitled to conduct ongoing monitoring of users, accounts, top-ups of the card functionality, transactions, virtual cards, card behaviour, technical signals, sources of funds and other actions within the service in order to identify and prevent AML/CFT, sanctions, fraud, card, operational and other compliance risks.

Monitoring may be carried out before a transaction is made, during its processing, after it is made, and throughout the period of use of the service.

In carrying out monitoring, Mirocard may take into account:

- volume, frequency, nature and geography of transactions;
- method and source of top-up of the card functionality, including crypto transfers;
- blockchain data, crypto addresses and linked addresses;
- BIN, MCC, limits and merchant categories used;
- declined transactions, disputes, refunds, cancellations and chargebacks;
- technical data, IP address, device, geolocation signals and indicators of VPN, proxy or TOR use;
- the results of KYC/KYB checks;
- source of funds or source of wealth;
- sanctions, PEP, adverse media, fraud and other compliance indicators.

Mirocard shall be entitled to use automated and manual monitoring methods, internal procedures, and data from third-party providers, the card programme, issuer, processor, card network, KYC/AML provider, blockchain analytics providers, crypto-infrastructure counterparties and other mandatory partners.

5.2. Prohibited Use

The user is prohibited from using Mirocard, the account, virtual cards, the available amount or other service functionality for:

- money laundering, terrorist financing, sanctions circumvention or other unlawful activity;
- fraud, deception of third parties, abuse, mass or automated card testing, account takeover, abuse of transaction disputes or other unlawful conduct;
- use of unlawful, unverified, non-transparent or economically unexplained sources of funds;
- circumvention of KYC/KYB verification, verification of source of funds or source of wealth, limits, BIN conditions, MCC restrictions, sanctions, territorial, technical or other compliance restrictions;

- use of the service in the interests of third parties, through nominees, another person's accounts, linked accounts, front structures or other means of circumventing checks and restrictions;
- carrying out transactions that do not correspond to the declared purpose of using the service, the user's risk profile or the economic rationale of the transactions;
- carrying out transactions in breach of this Policy, the Usage Policy, the terms of the card programme, the requirements of the issuer, partners or applicable law.

5.3. Prohibited and Restricted Categories of Transactions

The user is prohibited from using Mirocard and virtual cards for transactions connected with prohibited or restricted categories, including:

- transactions equivalent to cash withdrawals or transfers of funds;
- cash equivalents and quasi-cash transactions;
- gambling, betting, lotteries and gaming services;
- adult goods and services;
- purchase of cryptocurrency, tokens, digital assets, exchange services, P2P platforms or other crypto services where such transactions are prohibited by the terms of the relevant card programme, BIN, MCC or Mirocard rules;
- high-risk merchants;
- high-risk MCCs;
- pyramid schemes, fraudulent schemes, investment fraud or misleading practices;
- darknet markets, mixers, tumblers, ransomware, hacking, stolen data, unlawful marketplaces or other prohibited or high-risk activity;
- sanctioned persons, prohibited or restricted jurisdictions, sanctioned goods, services, sectors or activities;
- terrorism, extremism, trafficking in weapons, drugs, persons, unlawful content or other criminal activity.

The specific availability or prohibition of particular transactions may depend on the card programme, BIN, MCC, issuer, processor, card network, partner requirements and Mirocard's internal risk assessment.

5.4. High-Risk Activity

Mirocard shall be entitled to regard as suspicious or high-risk any activity that does not correspond to the user's risk profile, the declared purpose of using the service, the economic rationale of transactions, the terms of the card programme, BIN, limits, MCC restrictions or other applicable requirements.

High-risk activity may include:

- unusual or repeated transactions;

- a high proportion of declined transactions;
- frequent disputes, refunds, cancellations or chargebacks;
- transactions with high-risk merchants;
- indicators of mass card testing;
- indicators of account takeover;
- abuse of transaction disputes;
- attempts to circumvent restrictions;
- use of multiple accounts;
- use of nominees;
- use of VPN, proxy or TOR to conceal the actual location;
- a connection between transactions, addresses, sources of funds, merchants or the user and sanctions, fraud, AML/CFT or other compliance risks.

5.5. Measures Following Monitoring

Where prohibited use, high-risk activity, suspicious activity or other compliance indicators are identified, Mirocard shall be entitled to:

- request additional information or documents;
- conduct repeated or enhanced checks;
- reduce limits;
- restrict functionality;
- decline or suspend a request to top up the card functionality;
- decline or suspend a card transaction;
- restrict the processing of a refund, cancellation, dispute or chargeback where permitted by applicable rules;
- restrict the available amount;
- block the account or virtual card;
- refuse further service;
- disclose information to partners or competent authorities where required or permitted by applicable requirements;
- take other measures necessary to comply with AML/CFT, sanctions, fraud, card, regulatory, partner or Mirocard internal requirements.

Where the relevant transaction, available amount, cryptoasset, refund, cancellation or card procedure is processed by a third-party infrastructure participant, Mirocard shall be entitled to take into account the decisions, restrictions, holds, refusals, refunds, cancellations or other measures applied by that participant.

6. Restrictions, Blocking and Refusal of Service

6.1. Right to Apply Restrictions

Mirocard shall be entitled at any time to apply temporary or permanent restrictions in relation to the user, account, virtual card, available amount, top-up of the card functionality, transaction or particular service functions where this is necessary or appropriate to comply with AML/CFT, sanctions, fraud, card, regulatory, partner or internal risk management requirements.

Such measures may be applied on Mirocard's own initiative and also at the request of, or taking into account the requirements of, the card programme, BIN, issuer, processor, card network, KYC/AML provider, crypto-infrastructure counterparty, bank, payment provider, competent authority or other mandatory infrastructure participant.

6.2. Grounds for Restrictions

Restrictions may be applied, in particular, where there is or is suspected to be:

- failure to pass KYC/KYB verification;
- refusal to undergo repeated checks;
- failure to provide requested documents;
- provision of inaccurate, incomplete, contradictory, outdated or forged information;
- an unverified, non-transparent or economically unexplained source of funds or source of wealth;
- AML/CFT, sanctions, fraud, regulatory, card, operational, reputational or other compliance risk;
- a connection with a sanctioned person, prohibited or restricted jurisdiction, prohibited merchant, MCC or prohibited transaction category;
- fraud, abuse, mass card testing, account takeover, abuse of transaction disputes or unauthorised activity;
- circumvention or attempted circumvention of KYC/KYB, sanctions, territorial, BIN, MCC, limit, technical or other restrictions;
- breach of this Policy, the Usage Policy, the terms of a particular card, the terms of the card programme, the requirements of the issuer, partners or applicable law;
- a requirement, recommendation or restriction from the issuer, card programme, BIN partner, processor, card network, KYC/AML provider, crypto-infrastructure counterparty, bank, payment provider, regulator, law enforcement authority or other competent person.

This list of grounds is not exhaustive. Mirocard shall be entitled to apply restrictions in any other cases where continued service, processing of a transaction or provision of functionality creates or may create a compliance risk for Mirocard, users, partners or the card infrastructure.

6.3. Types of Measures

Depending on the nature of the risk, Mirocard shall be entitled to apply one or more measures, including:

- refusal of registration, verification, issuance or use of a virtual card;
- a request for additional information, documents, explanations, source of funds or source of wealth;
- repeated, additional or enhanced checks;
- reduction of limits;
- amendment of available functionality;
- restriction of particular BINs or card programmes;
- decline, cancellation or suspension of a transaction;
- refusal to process or suspension of a top-up of the card functionality;
- restriction of the available amount;
- blocking of the virtual card or account;
- refusal to process particular user requests where permitted by applicable rules;
- termination of service to the user;
- disclosure of information to partners, the issuer, the card programme, a regulator, law enforcement authorities or other competent persons where required or permitted by applicable requirements;
- other measures necessary to comply with AML/CFT, sanctions, fraud, card, regulatory, partner or Mirocard internal requirements.

Mirocard does not hold users' funds. Where a restriction concerns a transaction, available amount, refund, cancellation, dispute, chargeback or other procedure, the actual processing of that procedure may depend on the third-party infrastructure participant and its rules.

6.4. Application of Measures without Prior Notice

Restrictive measures may be applied without prior notice to the user where such prior notice may:

- create a risk of circumvention of checks or restrictions;
- breach applicable law or sanctions requirements;
- conflict with partner requirements or card infrastructure requirements;
- hinder fraud prevention;
- reduce the effectiveness of AML/KYC, sanctions or other compliance procedures;
- infringe the rights of third parties or the security of the service.

6.5. Non-Disclosure of Reasons

Mirocard shall be entitled not to disclose to the user the specific reasons for refusal, restriction, blocking, suspension of a transaction, restriction of the available amount or termination of service where disclosure may breach applicable law, sanctions requirements, card programme rules, partner requirements, service security, third-party rights or the effectiveness of AML/KYC, sanctions, fraud and other risk management procedures.

7. Processing and Disclosure of AML/KYC Data

7.1. General Principle

For the purposes of KYC/KYB, AML/CFT, sanctions compliance, fraud prevention, transaction monitoring, risk assessment, processing of card transactions and compliance with partner requirements, Mirocard shall be entitled to collect, use, verify, analyse, store and disclose user data to the extent necessary to provide the service, carry out checks, make compliance decisions and comply with applicable requirements.

Such data may include:

- identification data and documents;
- information on the legal entity, representatives and beneficial owners;
- KYC/KYB check results;
- sanctions screening results;
- PEP and adverse media screening results;
- information on source of funds or source of wealth;
- information on top-ups of the card functionality, transactions, virtual cards, BIN, MCC, declined transactions, disputes, refunds, cancellations and chargebacks;
- blockchain data;
- technical and security data;
- risk indicators, monitoring results and internal risk assessment.

Detailed terms of processing of personal data, including legal bases, retention periods, international data transfers, user rights and the procedure for exercising such rights, are set out in the Mirocard Privacy Policy.

7.2. Disclosure of Data to Partners and Providers

Mirocard shall be entitled to disclose AML/KYC and compliance data to third parties where this is necessary or appropriate for carrying out checks, providing the service, issuing and servicing virtual cards, processing transactions, monitoring, risk management, prevention of fraud, compliance with partner requirements or compliance with applicable law.

Such third parties may include:

- KYC/AML providers, including Sumsub;

- providers of sanctions screening, PEP screening, adverse media screening, fraud prevention and identity verification;
- issuers, card programmes, BIN partners, processing providers and card networks;
- blockchain analytics providers, crypto-infrastructure providers, exchange, liquidity or settlement counterparties, banks and payment providers;
- cloud, hosting, security, analytics, support, technical and outsourcing providers;
- auditors, legal advisers, consultants and other professional representatives of Mirocard;
- regulators, law enforcement authorities, courts, sanctions authorities, public authorities or other competent persons where such disclosure is required or permitted by applicable requirements.

7.3. International Data Transfers

Given the international nature of the service, card infrastructure, crypto top-ups, KYC/AML providers, issuers, processing providers, card networks and technical partners, user data may be transferred to and processed outside the user's country of residence, including outside the European Economic Area.

Such transfers shall be carried out in accordance with the Mirocard Privacy Policy, applicable data protection law and the contractual, organisational or technical safeguards used by Mirocard.

7.4. Retention of AML/KYC Data

Mirocard shall be entitled to retain AML/KYC and compliance data for the period necessary to provide the service, comply with AML/CFT, sanctions, fraud, card, regulatory, tax, accounting, contractual and other applicable requirements, process transactions, disputes, refunds, cancellations, chargebacks, claims, internal reviews, investigations and protect the rights of Mirocard, users, partners or third parties.

Mirocard may continue to retain certain AML/KYC and compliance data after termination of service to the user where such retention is required or permitted by applicable law, partner requirements, card infrastructure requirements, internal risk management procedures or the need to protect the rights and legitimate interests of Mirocard.

7.5. Confidentiality of Compliance Information

Mirocard shall be entitled not to disclose to the user internal AML/KYC and compliance information, including the results of risk assessment, scoring, thresholds, risk indicators, sanctions screening, PEP screening, adverse media screening, blockchain analysis, fraud checks, monitoring, manual review, internal escalation or the specific grounds for individual compliance decisions.

Disclosure of such information may be restricted where it may breach applicable law, sanctions requirements, the requirements of competent authorities, card programme rules,

the requirements of the issuer or partners, service security, third-party rights or reduce the effectiveness of AML/KYC, sanctions, fraud or other risk management procedures.

8. Final Provisions

8.1. Priority of Compliance Requirements

Mirocard shall be entitled to apply any measures necessary or appropriate to comply with AML/CFT, sanctions, fraud, card, regulatory, partner and other risk management requirements.

Where use of the service by the user creates or may create AML/CFT, sanctions, fraud, regulatory, card, operational, reputational or other compliance risk, Mirocard shall be entitled to restrict or terminate provision of the service regardless of whether the specific situation is expressly provided for in this Policy.

In the event of any conflict between the user's interests and the need to comply with applicable compliance requirements, the requirements of the card programme, BIN, issuer, processor, card network, KYC/AML provider, competent authority or other mandatory partner, Mirocard shall be entitled to adopt the stricter approach.

8.2. Non-Disclosure of Internal Procedures

This Policy is a public document and does not disclose Mirocard's internal procedures, including internal verification rules, risk scoring, thresholds, risk indicators, monitoring rules, escalation matrix, sanctions and fraud scenarios, blockchain analytics rules, decision-making criteria, internal review materials and other elements of the compliance model.

Mirocard shall be entitled not to disclose such information to the user, nor the specific grounds for individual compliance decisions, where disclosure may breach applicable law, sanctions requirements, the requirements of competent authorities, card programme rules, the requirements of the issuer or partners, service security, third-party rights or reduce the effectiveness of AML/KYC, sanctions, fraud or other risk management procedures.

8.3. Amendment of the Policy

Mirocard shall be entitled at any time to amend, supplement or update this Policy, including provisions on KYC/KYB checks, sanctions control, prohibited and restricted jurisdictions, transaction monitoring, prohibited use, restrictions, blocking, data processing and other compliance measures.

Amendments may result from changes in applicable law, sanctions regimes, FATF lists, the requirements of the card programme, BIN, issuer, processor, card network, KYC/AML provider, partners, the operating model, internal risk assessment or service functionality.

The updated version of the Policy shall apply from the time of its publication on the Mirocard website, in the service interface, in the user's personal account or from such other date as Mirocard may specify.

Continued use of the service after update of the Policy constitutes the user's acceptance of the updated version, unless otherwise required by applicable law.

8.4. Language and Interpretation

This version of the Policy is drafted in English. If the Policy is provided in several languages, the English version shall be deemed the governing and prevailing version unless Mirocard expressly specifies another prevailing version.

Section headings are included for convenience only and shall not affect the interpretation of this Policy.

If any provision of this Policy is held to be invalid, unlawful or unenforceable, this shall not affect the validity and enforceability of the remaining provisions.

8.5. Relationship with Other Documents

This Policy shall apply together with the Usage Policy, the Privacy Policy, the terms of the relevant card programme, and the terms of the issuer, processor, card network and other partners.

In the event of any inconsistency between this Policy and other Mirocard user documents in relation to AML/CFT, sanctions compliance, KYC/KYB, transaction monitoring, restrictions, blocking or refusal of service, this Policy shall prevail unless otherwise required by applicable law or mandatory card infrastructure rules.