Privacy Policy

Ram Fintech s.r.o. · Draft for EMI licensing

Company: Ram Fintech s.r.o. Version: 1.2 (Regulatory & Technical Alignment) Last revised: [Enter current date]

1. Introduction and the controller's identification details

The company Ram Fintech s.r.o., ID No.: 245 21 876, with its registered office at Vojtěšská 211/6, Nové Město, 110 00 Prague 1 (hereinafter referred to as "the Company" or "Controller"), hereby informs data subjects of the conditions for the processing of personal data in accordance with Regulation (EU) 2016/679 (GDPR), Act No. 110/2019 Coll., on the Processing of Personal Data, and the CNB Methodology to the Payment System Act (ZPS).

The company is an applicant for an Electronic Money Institution (EMI) license. This document outlines our internal governance systems and ICT security standards (including compliance with PCI DSS and DORA).

2. Point of Contact and Data Protection Officer (DPO)

To protect privacy and facilitate communication with regulatory authorities, we have established a dedicated contact point:

Email: dpo@ram-fintech.com

Data Protection Officer (DPO): The company has appointed an expert DPO to oversee the compliance of all processes with the GDPR and the requirements of the Czech National Bank (ČNB).

3. Scope and Categories of Processed Data

In accordance with our AML/CTF Program and technical architecture, we process:

A. Identification Information (KYC Process):

First name, last name, date and place of birth, social security number, citizenship.

Information from identification documents (including digital copies and photographs).

Biometric data (for the purpose of remote identification via the KYC provider – only with explicit consent).

B. Socio-demographic and AML data:

Information on politically exposed persons (PEPs) and status on sanctions lists (OFAC, EU, UN).

Source of income, occupation, and purpose of the business relationship.

C. Payment and technical data (ICT logs):

Account numbers, transaction details, IP addresses, geolocation data (for fraud monitoring).

Device technical identifiers in accordance with our security report (CIS Hardened Systems).

4. Legal Basis and Purposes of Processing

Compliance with a legal obligation (Article 6(1)(c) of the GDPR):

Act No. 253/2008 Coll. (AML Act): Customer identification, due diligence, and reporting of suspicious transactions (FAÚ).

Act No. 370/2017 Coll. (ZPS): Provision of payment services and management of electronic money.

Performance of a contract (Article 6(1)(b) of the GDPR): Operating multi-currency accounts and issuing payment cards.

Legitimate interest (Article 6(1)(f) of the GDPR):

Fraud prevention (Fraud Monitoring) and ensuring the resilience of ICT systems in accordance with the DORA Regulation.

Internal Control and Audit Trail for the CNB.

5. Data Retention

Due to financial sector regulations, we retain the following data:

10 years after the termination of the business relationship: All documentation relevant to the AML Act and the Payment Services Act.

10 years from the end of the fiscal year: Accounting documents and transaction records.

1 year: Data on prospective clients for whom no account was opened.

6. Data Security and ICT Infrastructure

Your data is stored in the modern cloud environment Amazon Web Services (AWS) in the Frankfurt (Primary) and Ireland (Disaster Recovery) regions.

PCI DSS: Our infrastructure complies with the Payment Card Industry Data Security Standard.

CIS Hardening: Servers are configured according to strict security benchmarks (CIS Red Hat Enterprise Linux 9 Benchmark).

Encryption: Data is encrypted both during transmission (TLS 1.2+) and at rest (AES-256).

7. Recipients of Data and Transfer Abroad

Government agencies: CNB, FAÚ, Czech Police (within the scope of their legal obligations).

Technology partners: Fixosoft (IT management), KYC providers, and card schemes.

Third countries: By default, data does not leave the EEA. If necessary (e.g., for international payments), we use Standard Contractual Clauses (SCCs) and ensure protection in accordance with EU case law.

8. Automated Decision-Making (AML Scoring)

For security purposes, we perform automated transaction scoring. This process is necessary to prevent money laundering. The data subject has the right to a human review of any automated decision that would have legal effects on them.

9. Your rights

You have the right to access, rectify, restrict the processing of, and transfer your data. The right to erasure (the right to be forgotten) is subject to a legal obligation to retain data for a period of 10 years in accordance with AML regulations.

Complaints: Office for Personal Data Protection (Pplk. Sochora 27, 170 00 Prague 7, www.uoou.cz).

10. Conclusion

This Policy is part of our Internal Control Framework. The current version is always available at https://ram-fintech.com.