GDPR Policy

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

Internal Guidelines on Personal Data Protection

Company: Ram Fintech s.r.o.

Intended for: Employees, statutory bodies, and internal control functions

Verze: 1.0 (Regulatory Draft for ČNB)

Effective date: [Enter date]

Document sponsor: Data Protection Officer (DPO)

1. Purpose and Scope of the Directive

This policy establishes binding rules for the handling of personal data within Ram Fintech s.r.o. (hereinafter referred to as the “Company”). The policy is an integral part of the Internal Control Framework and is designed to meet the following requirements:

General Data Protection Regulation (GDPR).

The Payment Services Act (ZPS) No. 370/2017 Coll.

AML Act No. 253/2008 Coll.

Cybersecurity standards (DORA, PCI DSS) described in the Company’s technical documentation.

2. Organizational Structure and Responsibilities

2.1. Data Protection Officer (DPO)

The company has appointed a DPO who:

It monitors compliance with legal regulations.

It serves as a point of contact between the Office for Personal Data Protection (ÚOOÚ) and data subjects.

It conducts regular employee training sessions.

2.2. AML Officer (Alena Bulachová)

He is responsible for ensuring compliance with data processing requirements within the KYC (Know Your Customer) processes and sanctions list monitoring. Close cooperation with the DPO is mandatory when conducting data protection impact assessments (DPIAs) for new products.

2.3. IT a Security (Fixosoft / Internal IT)

He is responsible for ensuring data security in the AWS environment, managing access rights, and monitoring logs.

3. Data Classification and Technical Infrastructure

V souladu s dokumentem Internal Control and ICT Systems Description:

Data storage: Primary AWS region: Frankfurt (eu-central-1); backup AWS region: Ireland (eu-west-1).

Security: All production data is encrypted (AES-256). Access to the database is permitted only via an encrypted VPN connection with multi-factor authentication (MFA).

Classification: Clients' personal data is classified as "Confidential" and is subject to the strictest security measures.

4. Data Access Rules (Access Control)

The company applies the "need-to-know" and "least privilege" principles:

Customer Support: Access to basic identification data only to the extent necessary to process the request.

Compliance/AML Team: Access to transaction history and identification documents for the purpose of reporting to the Financial Intelligence Unit (FAÚ).

Administrators: Access to raw data is logged and regularly reviewed (CIS Hardened Reports).

5. Document Management and Retention Periods

In accordance with the Company’s AML program:

Client file (KYC): Must include copies of identification documents, a record of the sanctions list check, and PEP status.

Retention: Documents are retained for a period of 10 years following the termination of the business relationship. Upon expiration of this period, the data must be permanently deleted or anonymized, unless there is another legal basis for retaining it.

6. Data Breach Protocol

In the event of a data breach or unauthorized access (e.g., an AWS security breach or an attack on an end device):

Detection: Report the incident to [dpo@ram-fintech.com] and the IT Security team.

Assessment: The DPO will assess the risk to the rights and freedoms of data subjects.

Notification to the Office for Personal Data Protection: If there is a risk, the DPO shall notify the Office within 72 hours.

Client notifications: If there is a high risk, clients are notified without undue delay (via email or in the app).

Documentation: Every incident must be recorded in the “Incident Log,” including the corrective actions taken.

7. Data Subjects’ Rights – Internal Handling

A request for access to data must be processed within 30 days.

Request for deletion: Before deletion, the Compliance Department must confirm that there is no longer an obligation to retain the data under the AML Act.

8. Training and Confidentiality

Every employee signs a non-disclosure agreement (NDA) as part of their employment contract.

Training on data protection and cybersecurity is conducted at least once a year.

9. Inspection and Penalties

Compliance with this policy is subject to internal audit. Violations of these rules may be classified as serious breaches of employment duties, with consequences in accordance with the Labor Code.

Approved by the management of Ram Fintech s.r.o.