FLUSSO DYNAMICS GROUP SP. Z O.O.

PRIVACY POLICY

DATA PROTECTION AND PRIVACY NOTICE

Version 1.0 — March 2026
https://flussogroup.com/privacy

1. INTRODUCTION AND DATA CONTROLLER

1.1. Data Controller

FLUSSO DYNAMICS GROUP SP. Z O.O. (hereinafter “Flusso”, “we”, “our”, or “us”), with registered office at ul. Hoża 86, lok. 210, 00-682 Warsaw, Poland, NIP: 7011205258, KRS: 0001105723, is the Data Controller responsible for the processing of personal data collected through the Platform **https://flussogroup.com/** and in connection with the virtual currency services provided.

Flusso is registered as a Virtual Asset Service Provider (VASP) in Poland under registration number RDWW-1317, and maintains operational headquarters in Spain.

1.2. Applicable Legal Framework

This Privacy Policy is governed by the following legislation:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (General Data Protection Regulation – “GDPR”).
- Polish Act of May 10, 2018 on the Protection of Personal Data (Ustawa o ochronie danych osobowych).
- Spanish Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD), applicable to operational activities conducted from Spain.
- Act of March 1, 2018 on Counteracting Money Laundering and Terrorism Financing (Polish AML Act), as it pertains to data processing for AML/CFT compliance.
- Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets (Travel Rule Regulation), as applicable.
- Any other applicable national or EU data protection legislation.

1.3. Contact Information

Purpose	Contact
Data Protection inquiries	compliance@flussogroup.com
GDPR rights requests	compliance@flussogroup.com
General inquiries	support@flussogroup.com
Postal address	ul. Hoża 86, lok. 210, 00-682 Warsaw, Poland

1.4. Scope

This Privacy Policy applies to all personal data processed by Flusso in connection with the operation of the Platform and the provision of virtual currency services, including data collected from Users, prospective Users, Agents, website visitors, and any other individuals whose personal data Flusso processes.

2. PERSONAL DATA WE COLLECT

Flusso collects and processes the following categories of personal data:

2.1. Registration and Identity Data

Data Category	Specific Data	Purpose
Identity information	Full name, date of birth, nationality	KYC verification, regulatory compliance
Identity documents	Passport, national ID, NIE/residence permit	AML/KYC verification via AMLBot
Biometric data	Selfie/live photo for facial recognition matching	Identity verification
Contact information	Email address, mobile phone number	Account creation, 2FA, communications
Address information	Residential address, country of residence	KYC verification, jurisdiction assessment

2.2. Transactional Data

Data Category	Specific Data	Purpose
Transaction records	Order details, amounts, currencies, timestamps, exchange rates	Service provision, regulatory reporting
Payment information	Bank account details, card details (processed by third-party PSPs)	Payment processing
Wallet addresses	Blockchain wallet addresses	Crypto transfers, KYT screening
Beneficiary data	Recipient names, payment details for multi-beneficiary transfers	Service provision

2.3. Technical and Device Data

Data Category	Specific Data	Purpose
Access data	IP address, user agent, browser type, device information	Security, audit trail, fraud prevention
Session data	Login timestamps, session tokens	Authentication, session management
Cookie data	Cookie identifiers, preferences	Platform functionality, analytics

2.4. AML/Compliance Data

Data Category	Specific Data	Purpose
KYC verification results	Verification status, document validation, biometric match results	AML/CFT compliance
KYT screening results	Wallet risk scores (LOW/MEDIUM/HIGH), sanctions screening results	Transaction monitoring
Source of funds	Documentation of income/wealth origin	Enhanced due diligence
Risk assessment	User risk classification, PEP status	Ongoing monitoring

3. LEGAL BASES FOR PROCESSING

Flusso processes personal data on the following legal bases under Article 6 of the GDPR:

Legal Basis (GDPR Art. 6)	Processing Activities
Art. 6(1)(a) – Consent	Marketing cookies, promotional communications, analytics cookies. Consent is freely given, specific, informed, and unambiguous. Users may withdraw consent at any time.
Art. 6(1)(b) – Performance of Contract	Account creation, identity verification, transaction processing, order execution, transfer services, customer support, API access provision.
Art. 6(1)(c) – Legal Obligation	AML/KYC verification, KYT transaction screening, sanctions screening, suspicious activity reporting to GIIF, data retention for regulatory purposes, tax reporting obligations (CARF).
Art. 6(1)(f) – Legitimate Interest	Fraud prevention, security monitoring, audit trail maintenance, Platform improvement, IT infrastructure security, defense of legal claims.

3.1. Special Categories of Data

Flusso processes biometric data (selfie/facial recognition) for identity verification purposes. This processing is based on the User's explicit consent (GDPR Art. 9(2)(a)) and is necessary for reasons of substantial public interest (GDPR Art. 9(2)(g)) in relation to anti-money laundering compliance. Users are informed and consent is obtained prior to biometric data collection.

4. PURPOSES OF PROCESSING

Flusso processes personal data for the following purposes:

- User registration and account management: creating and maintaining User accounts on the Platform.
- Identity verification (KYC): verifying User identity in compliance with the Polish AML Act, using AMLBot KYC API.
- Transaction processing: executing on-ramp, off-ramp, transfer, and multi-beneficiary payment orders.
- AML/CFT compliance: screening transactions and wallet addresses (KYT), monitoring for suspicious activity, reporting to the General Inspector of Financial Information (GIIF).
- Fraud prevention and security: monitoring access patterns, maintaining audit trails, implementing 2FA, preventing unauthorized access.
- Communication: sending transactional notifications (order confirmations, security alerts, OTP codes), and, where consented, promotional communications.
- Legal compliance: fulfilling obligations under Polish, Spanish, and EU law, including data retention, tax reporting, and regulatory cooperation.
- Platform improvement: analyzing usage patterns (via anonymized analytics) to improve functionality and user experience.
- Defense of legal claims: establishing, exercising, or defending legal claims.

5. DATA SHARING AND RECIPIENTS

Flusso may share personal data with the following categories of recipients, exclusively to the extent necessary for the stated purposes:

Recipient Category	Entity / Service	Purpose	Data Shared
KYC/KYT Provider	AMLBot (Silenca Tech)	Identity verification and transaction screening	Identity documents, selfie, wallet addresses
Custodian	Depasify	Crypto-asset custody, wallet management, withdrawals	Wallet addresses, transaction amounts, User identifiers
Payment Providers	Easy Payment, Chinchin, PMI	Fiat payment processing (SEPA, Pago Móvil)	Payment details, amounts, beneficiary information
Payment Provider	Depasify	Card/PSD2 payment processing	Card details (tokenized), amounts
2FA Provider	Twilio	OTP delivery via SMS	Phone number, OTP code
Error Monitoring	Sentry	Application error tracking	Technical logs (anonymized where possible)
Alerts	Telegram (internal)	Real-time system alerts	System event data (no personal data in alerts)
Hosting	Laravel Cloud (AWS Frankfurt)	Application and database hosting	All Platform data (encrypted at rest)
Regulatory Authorities	GIIF, KNF, AEPD, UODO	Regulatory compliance, suspicious activity reporting	As required by applicable law
Law Enforcement	Police, courts, prosecutors	Legal obligations, court orders	As required by applicable law

Flusso requires all third-party service providers to maintain appropriate technical and organizational security measures and to process personal data only in accordance with Flusso's instructions and applicable data protection law. Data processing agreements (DPAs) are in place with all relevant processors.

6. INTERNATIONAL DATA TRANSFERS

All Platform infrastructure is hosted within the European Union (EU Central region, Frankfurt, Germany). Flusso's primary data processing activities take place within the EEA.

Certain third-party service providers may process data outside the EEA. In such cases, Flusso ensures that appropriate safeguards are in place in accordance with Chapter V of the GDPR, including:

- Standard Contractual Clauses (SCCs) approved by the European Commission.
- Adequacy decisions of the European Commission, where applicable.
- Binding Corporate Rules (BCRs), where applicable.

Users may request information about the specific safeguards applied to international transfers by contacting compliance@flussogroup.com.

7. DATA RETENTION

Flusso retains personal data for the minimum period necessary to fulfill the purposes for which it was collected, subject to applicable legal retention obligations:

Data Category	Retention Period	Legal Basis
KYC/Identity verification data	5 years after end of business relationship	Polish AML Act (Art. 49)
Transaction records	5 years after end of business relationship	Polish AML Act (Art. 49)
KYT screening results	5 years after the transaction	Polish AML Act
Suspicious activity reports	5 years after submission (or as required by GIIF)	Polish AML Act
Tax and invoicing records	5 years (Poland) / 4 years (Spain)	Polish Tax Code / Spanish tax law
Audit trail (security logs)	3 years	Legitimate interest / Security
Cookie consent records	Duration of consent + 1 year	GDPR accountability
Marketing consent records	Duration of consent + 3 years	GDPR accountability
Account data (inactive accounts)	1 year after inactivity declaration, then anonymized or deleted	Contractual / Legitimate interest

Upon expiry of the retention period, personal data shall be securely deleted or irreversibly anonymized, unless further retention is required by law or necessary for the defense of legal claims.

8. YOUR RIGHTS

Under the GDPR and applicable national law, you have the following rights regarding your personal data:

Right	Description
Right of Access (Art. 15)	You may request confirmation of whether we process your personal data and obtain a copy of such data.
Right to Rectification (Art. 16)	You may request the correction of inaccurate personal data or the completion of incomplete data.
Right to Erasure (Art. 17)	You may request the deletion of your personal data where no legal obligation requires its retention (e.g., AML retention obligations).
Right to Restriction (Art. 18)	You may request the restriction of processing under certain circumstances.
Right to Data Portability (Art. 20)	You may request to receive your personal data in a structured, commonly used, machine-readable format.
Right to Object (Art. 21)	You may object to processing based on legitimate interest, including profiling. You may object to direct marketing at any time.
Right to Withdraw Consent (Art. 7(3))	Where processing is based on consent, you may withdraw consent at any time without affecting the lawfulness of processing prior to withdrawal.
Right to Lodge a Complaint	You may lodge a complaint with a supervisory authority (UODO in Poland or AEPD in Spain).

8.1. How to Exercise Your Rights

To exercise any of the above rights, please contact us at:

Email: compliance@flussogroup.com

Postal: Flusso Dynamics Group Sp. z o.o., ul. Hoża 86, lok. 210, 00-682 Warsaw, Poland

Flusso shall respond to your request within one (1) month of receipt. This period may be extended by two (2) further months where necessary, taking into account the complexity and number of requests. We shall inform you of any such extension within one month of receipt.

Flusso may request proof of identity before processing your request to ensure the security of your personal data.

8.2. Limitations

Certain rights may be limited where Flusso is required by law to retain or process personal data, in particular under AML/CFT obligations. In such cases, Flusso shall inform you of the applicable limitation and the legal basis for it.

9. COOKIES AND SIMILAR TECHNOLOGIES

The Platform uses cookies and similar technologies. The following categories of cookies are used:

Category	Default	Description	Examples
Necessary	Active (mandatory)	Essential for login, session management, payment processing, and security. Cannot be disabled.	Session ID, CSRF token, authentication tokens
Functional	Active	User preferences such as language, display settings.	Language selection, UI preferences
Analytics	Disabled	Platform usage metrics and performance monitoring.	Page views, feature usage, error rates
Marketing	Disabled	Personalized communications and advertising.	Campaign tracking, referral source

Technical specifications: session cookies are configured as HTTP-only with SameSite=Lax attribute. Analytics and marketing cookies are set only upon explicit User consent.

Users may manage cookie preferences at any time through the cookie settings banner available on the Platform. Withdrawal of consent for non-essential cookies does not affect the lawfulness of processing prior to withdrawal.

10. SECURITY MEASURES

Flusso implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 of the GDPR. These measures include:

- Encryption of data in transit (TLS/HTTPS) and at rest.
- Two-factor authentication (OTP via email and SMS) with bcrypt-hashed codes.
- Password hashing with bcrypt (12 rounds).
- Security headers: X-Frame-Options: DENY, HSTS, X-Content-Type-Options: nosniff, strict Referrer-Policy.
- Role-based access control (RBAC) with four granular roles.
- HMAC webhook signature validation for all payment provider callbacks.
- CSRF protection via Laravel/Sanctum framework.
- Rate limiting on authentication and OTP endpoints.
- Circuit breaker pattern for external service provider resilience.
- Mandatory KYC verification gate enforced by application middleware.
- Sentry error monitoring and Telegram-based real-time alerts.
- Comprehensive audit trail for all KYC/KYT events and financial operations.

All infrastructure is hosted within the EU (Frankfurt, Germany) on Laravel Cloud with PostgreSQL 17 Serverless and Redis cache.

11. DATA BREACH NOTIFICATION

In the event of a personal data breach, Flusso shall:

- Notify the competent supervisory authority (UODO in Poland and/or AEPD in Spain, as applicable) without undue delay and, where feasible, within seventy-two (72) hours of becoming aware of the breach, in accordance with Article 33 of the GDPR.
- Notify affected Users without undue delay where the breach is likely to result in a high risk to their rights and freedoms, in accordance with Article 34 of the GDPR.
- Document all data breaches, including the facts, effects, and remedial action taken, as part of Flusso's accountability obligations.

Flusso maintains monitoring systems (Sentry, Telegram alerts, and audit trails) designed to detect potential data breaches promptly.

12. AUTOMATED DECISION-MAKING AND PROFILING

Flusso employs certain automated processes in the provision of its services:

- KYT Risk Scoring: automated screening of blockchain wallet addresses assigns a risk classification (LOW, MEDIUM, HIGH). Transactions involving HIGH-risk addresses may be automatically flagged or suspended.
- KYC Verification: automated document and biometric verification via AMLBot, with results reviewed where necessary.

These automated processes may produce legal effects or similarly significantly affect Users (e.g., refusal to process a transaction). In accordance with Article 22 of the GDPR, Users have the right to:

- Obtain human intervention in automated decisions.
- Express their point of view.
- Contest the decision.

To exercise these rights, contact compliance@flussogroup.com.

13. CHILDREN'S PRIVACY

Flusso's services are not directed to persons under eighteen (18) years of age. Flusso does not knowingly collect personal data from children. If Flusso becomes aware that personal data has been collected from a minor, such data shall be promptly deleted.

14. SUPERVISORY AUTHORITIES

Users may lodge complaints regarding the processing of their personal data with the following supervisory authorities:

Authority	Jurisdiction	Contact
UODO (Prezes Urzędu Ochrony Danych Osobowych)	Poland	https://uodo.gov.pl/ – ul. Stawki 2, 00-193 Warsaw
AEPD (Agencia Española de Protección de Datos)	Spain	https://www.aepd.es/ – C/ Jorge Juan 6, 28001 Madrid

Users may also lodge complaints with the supervisory authority of their habitual residence or place of work within the EEA.

15. CHANGES TO THIS PRIVACY POLICY

Flusso reserves the right to update this Privacy Policy at any time. Material changes shall be notified to Users via email and through the Platform with a minimum of thirty (30) calendar days' advance notice.

The updated Privacy Policy shall be published on the Platform with the date of last modification. Continued use of the Platform after the effective date of changes constitutes acceptance of the updated Privacy Policy.

Users who do not agree with the changes may terminate their account in accordance with the Terms and Conditions.

— End of Privacy Policy —

VASP Registration RDWW-1317 | Warsaw, Poland | compliance@flussogroup.com