AML & COMPLIANCE

AML & Compliance Policy

Effective: 1 February 2026 · Version 1.0

> This policy sets out HansePay's obligations under EU anti-money laundering legislation and explains what we require from our customers. As a regulated payment institution, we are subject to the EU Anti-Money Laundering Directives (AMLD) and are obligated to take active steps to prevent our platform from being used for financial crime.

1. Regulatory Framework

Atrya Technologies SIA (HansePay) is subject to the following key regulatory instruments:

- **Directive (EU) 2015/849** (4th AMLD), as amended by **Directive (EU) 2018/843** (5th AMLD) — customer due diligence and AML/CFT obligations
- **Directive (EU) 2018/1673** (6th AMLD) — harmonisation of money-laundering criminal offences across the EU
- **Regulation (EU) 2023/1113** — information accompanying transfers of funds and certain crypto-assets (recast "Transfer of Funds" Regulation)
- **Latvian Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing**
- Supervision by **Latvijas Banka** (Bank of Latvia)

The EU's new anti-money-laundering package — Regulation (EU) 2024/1624 (the single AML Rulebook, "AMLR"), Directive (EU) 2024/1640, and the new Anti-Money Laundering Authority (AMLA) — applies progressively from 2027. We are preparing for this transition.

2. Know Your Customer (KYC)

Before opening an account or activating payment services, we are required to verify the identity of all customers. This process exists to prevent our platform from being used for money laundering, terrorist financing, tax evasion, and sanctions violations.

2.1 Individual customers
We collect and verify:

- Full legal name, date of birth, and nationality
- Residential address
- Government-issued photo identification (passport or national ID)
- Source of income and employment status
- Account purpose and expected transaction volumes

2.2 Business customers

For legal entities we collect and verify:

- Company name, registration number, jurisdiction, and legal form
- Articles of incorporation and governance documents
- Register of shareholders / proof of ownership
- Identity of all directors and authorised signatories
- Identity and residential address of all Ultimate Beneficial Owners (UBOs) — persons owning or controlling 25% or more of the entity
- Business activity description, NACE industry classification
- Source of business funds and expected payment flows
- Account purpose and main counterparty countries

3. Enhanced Due Diligence (EDD)

We apply additional verification measures where we identify higher risk. This includes, but is not limited to:

- Customers who are Politically Exposed Persons (PEPs) or close associates of PEPs
- Customers or transactions with connections to higher-risk countries (as identified by FATF or EU-designated high-risk third countries)
- Customers operating in higher-risk sectors (crypto-assets, gambling, arms, cash-intensive businesses)
- Complex corporate structures or high transaction volumes relative to stated business activity
- Customers who are subject to adverse media or have previously been flagged by a financial institution

Enhanced due diligence may include requests for source of wealth documentation, additional corporate structure clarification, or senior management approval before account activation.

4. Politically Exposed Persons (PEPs)

A Politically Exposed Person (PEP) is an individual who holds, or has held, a prominent public function. This includes heads of state, government ministers, senior judges, senior military officers, executives of state-owned enterprises, and members of senior governing bodies of international organisations. In line with EU requirements, we continue to apply enhanced measures for at least 12 months after a person ceases to hold such a function, and for longer where the risk remains.

Close associates and immediate family members of PEPs are also subject to enhanced scrutiny. We ask all customers to self-declare PEP status during onboarding, and we additionally screen all customers and beneficial owners against PEP databases.

Being a PEP does not automatically prevent you from using HansePay, but additional review and documentation will be required.

5. Sanctions Screening

We screen all customers and beneficial owners against the following sanctions lists upon onboarding and on an ongoing basis:

- European Union Consolidated Sanctions List
- United Nations Security Council Sanctions List
- US Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) List
- UK Office of Financial Sanctions Implementation (OFSI) Consolidated List
- Latvian national sanctions registers

We are prohibited by law from processing transactions for or with any sanctioned party. If a customer is matched to a sanctions list, we are obligated to freeze their funds and report to the relevant authority. We cannot provide advance notice of such actions.

6. Transaction Monitoring

We monitor transactions on an ongoing basis for indicators of suspicious activity, including:

- Transactions inconsistent with a customer's stated business activity or expected volumes
- Unusual patterns such as rapid structuring to avoid reporting thresholds
- Payments to or from high-risk jurisdictions without a clear business rationale
- Transactions involving counterparties flagged in adverse media or sanctions databases

7. Suspicious Activity Reporting

We are legally required to report suspicious transactions to the relevant financial intelligence unit (FIU). In Latvia, this is the **Financial Intelligence Unit (Finanšu izlūkošanas dienests — FID)**. We are prohibited by law ("tipping off" provisions) from informing customers that a report has been, or is being, made.

8. Your Obligations as a Customer

By using HansePay, you agree to:

- Provide accurate and complete information during onboarding and on any ongoing request
- Promptly notify us of any material changes to your circumstances, ownership structure, or business activity
- Not use our platform to process funds derived from criminal activity or to circumvent legal obligations
- Cooperate fully with any enhanced due diligence request we make
- Ensure that you are not subject to sanctions and that your transactions do not involve sanctioned parties or jurisdictions

Failure to comply with these obligations may result in account restriction, account closure, and reporting to relevant authorities.

9. Record Keeping

In accordance with EU AML legislation, we retain all customer due diligence records and transaction records for a minimum of **five years** from the date of the transaction or the end of the business relationship. Extended retention may apply in the case of ongoing legal or regulatory proceedings.

10. Contact

For compliance-related enquiries: compliance@hansepay.com