

PRIVACY POLICY

Privacy Policy

Effective: 1 February 2026 · Version 1.0

This Privacy Policy explains how Atrya Technologies SIA (trading as HansePay) collects, uses, and protects your personal data in accordance with Regulation (EU) 2016/679 (GDPR) and applicable Latvian and German data protection law.

1. Data Controller

The data controller is **Atrya Technologies SIA**, Marijas iela 2A, Rīga, LV-1050, Latvia, operating under the brand HansePay from Stadtdeich 2–4, 20097 Hamburg, Germany.

Data Protection contact

privacy@hansepay.com

General enquiries

hello@hansepay.com

2. Data We Collect

2.1 Account and identity data

- Full name, date of birth, nationality
- Government-issued identification documents (passport or national ID)
- Residential address and proof of address
- Email address and phone number
- Profile photograph (from ID documents)

2.2 Business account data (additional)

- Company name, registration number, registered address, legal form
- NACE industry codes and business description
- Details of directors, authorised signatories, and beneficial owners (UBOs)
- Corporate structure and ownership information
- Company financial information (source of funds, account purpose)

2.3 Transaction data

- Payment amounts, currencies, dates, and reference information
- Sender and recipient account details (IBANs, SWIFT codes, names)
- Transaction purpose and payment references

2.4 Usage and technical data

- IP address, browser type and version, operating system
- Device identifiers
- Pages visited, time spent, click-through paths
- Login timestamps and session data

2.5 Compliance data

- Politically Exposed Person (PEP) status and sanctions screening results
- Source of wealth and source of funds declarations
- Risk assessment scores and customer due diligence records
- Correspondence with us relating to your account

3. How We Collect Data

- **Directly from you** — when you apply for an account, fill in forms, upload documents, or communicate with us
- **From identity verification providers** — our KYC partner (Signicat) processes your biometric and document data to verify your identity
- **From sanctions and PEP databases** — we screen your details against EU, UN, OFAC, and UK consolidated sanctions lists
- **Automatically** — when you use our website or platform, via cookies and server logs (see our Cookie Policy)
- **From third-party payment networks** — when receiving payments, counterparty data arrives via SEPA and SWIFT messaging

4. Why We Process Your Data (Legal Basis)

Purpose	Legal basis
Opening and operating your payment account	Contract (Art. 6(1)(b) GDPR)
Processing payment transactions	Contract (Art. 6(1)(b) GDPR)
Identity verification (KYC)	Legal obligation (Art. 6(1)(c) GDPR) — EU AML Directive
Sanctions and PEP screening	Legal obligation (Art. 6(1)(c) GDPR)
Transaction monitoring for AML	Legal obligation (Art. 6(1)(c) GDPR)
Regulatory reporting	Legal obligation (Art. 6(1)(c) GDPR)
Fraud prevention and security	Legitimate interests (Art. 6(1)(f) GDPR)
Service improvement and analytics	Legitimate interests (Art. 6(1)(f) GDPR)
Marketing communications	Consent (Art. 6(1)(a) GDPR) — you can opt out at any time

5. Automated Decision-Making

In line with our AML and KYC obligations, we use automated processing — including sanctions-list screening and risk scoring — to assess the risk profile of applicants and transactions. Some of these decisions may be made solely by automated means within the meaning of **Article 22 GDPR**, where this is necessary for entering into or performing our contract with you, or to comply with a legal obligation to which we are subject. Where this is the case, you have the right to obtain human intervention, to express your point of view, and to contest the decision by contacting privacy@hansepay.com.

6. Sharing Your Data

We share your personal data only where necessary:

- **Signicat** (Norway, within the EEA) — identity verification and KYC processing under a Data Processing Agreement
- **Correspondent banks and payment networks** — required to execute your payment instructions (SEPA, SWIFT)
- **Sanctions screening providers** — to comply with AML obligations
- **Latvijas Banka and other regulatory authorities** — when required by law
- **Law enforcement agencies** — when legally required or to prevent serious crime
- **Professional advisers** (lawyers, auditors) — under strict confidentiality
- **Successors in business** — in the event of a merger, acquisition, or sale of assets

We do not sell your personal data. We do not share your data for third-party marketing purposes.

7. International Data Transfers

Most of our processing takes place within the European Economic Area (EEA). Service providers located in the EEA — including our identity-verification partner Signicat (Norway) — are not subject to third-country transfer restrictions. Where we do transfer personal data to a country outside the EEA, we rely on one of the following safeguards:

- European Commission adequacy decisions
- Standard Contractual Clauses (SCCs) approved by the European Commission
- Binding Corporate Rules where applicable

You may request a copy of the relevant transfer safeguards by contacting privacy@hansepay.com.

8. Data Retention

We retain your personal data for as long as necessary to provide our services and to comply with our legal obligations. Key retention periods include:

- **Account and KYC data:** 5 years from account closure (EU AML Directive requirement)
 - **Transaction records:** 5 years from the date of the transaction
 - **Compliance and risk records:** Up to 10 years where required by regulatory or legal proceedings
 - **Marketing preferences:** Until you withdraw consent
 - **Technical logs:** 12 months
-

9. Your Rights Under GDPR

You have the following rights regarding your personal data:

- **Right of access (Art. 15):** Request a copy of the personal data we hold about you
- **Right to rectification (Art. 16):** Request correction of inaccurate data
- **Right to erasure (Art. 17):** Request deletion of your data where we no longer have a legal basis to retain it
- **Right to restriction (Art. 18):** Request that we limit processing of your data in certain circumstances
- **Right to data portability (Art. 20):** Receive your data in a structured, machine-readable format
- **Right to object (Art. 21):** Object to processing based on legitimate interests
- **Right to withdraw consent:** Where processing is based on consent, you may withdraw it at any time without affecting the lawfulness of prior processing

Note that some rights are subject to limitations — for example, we may be unable to delete data we are required to retain for AML or regulatory purposes.

To exercise any of these rights, contact privacy@hansepay.com. We will respond within 30 days.

10. Supervisory Authority

If you believe we have not handled your personal data in accordance with GDPR, you have the right to lodge a complaint with the relevant supervisory authority:

Datu valsts inspekcija (Latvian Data State Inspectorate)

Elijas iela 17, Rīga, LV-1050, Latvia

www.dvi.gov.lv

You may also contact the supervisory authority in your country of residence.

11. Cookies

We use cookies and similar tracking technologies on our website. Please see our [Cookie Policy](#) for full details.

12. Policy Updates

We may update this Privacy Policy from time to time. We will notify you of material changes by email or prominent notice on our platform before the changes take effect. The current version is always available at this page.
