

# SELLER ONBOARDING AND VERIFICATION POLICY

**SIA Synchron - shookout.com**

**Effective Date:** 07.04.2026

**Last Updated:** 07.04.2026

## 1. INTRODUCTION

### 1.1 Purpose

This Seller Onboarding and Verification Policy ("**Policy**") describes the identity verification, know-your-customer ("**KYC**"), and anti-money laundering ("**AML**") procedures that SIA Synchron, registration number 40203436468, registered address Unijas iela 74A - 45, Riga, LV-1084, Latvia ("**Company**," "**we**," "**us**," or "**our**"), applies to individuals and entities registering as Sellers on the shookout.com digital goods marketplace (the "**Platform**").

### 1.2 Regulatory Framework

Company's verification obligations arise under:

- (a) **Directive (EU) 2015/849** (Fourth Anti-Money Laundering Directive, "**AMLD4**"), as amended by Directive (EU) 2018/843 ("**AMLD5**") and the forthcoming Regulation (EU) 2024/1624 (the single AML Rulebook, applicable from 10 July 2027, with certain provisions in force earlier);
- (b) **The Latvian Law on the Prevention of Money Laundering, Terrorism and Proliferation Financing** (*Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likums*), which transposes AMLD4/5 into Latvian law;
- (c) **Council Directive 2021/514** ("**DAC7**"), which requires platform operators to collect and verify specified Seller information for tax reporting purposes;
- (d) **EU sanctions regulations**, including Council Regulation (EU) No 269/2014, Council Regulation (EU) No 833/2014 (as amended), and all applicable OFAC, UN, UK, and Latvian sanctions programmes, as described in the [Export & Sanctions Compliance Policy](#);
- (e) **Regulation (EU) 2022/2065** (the Digital Services Act, "**DSA**"), Article 30, which requires online marketplaces to obtain and verify certain information from traders before allowing them to offer products;
- (f) **OECD Model Reporting Rules for Digital Platforms**, implemented through DAC7 and equivalent national legislation in non-EU jurisdictions.

### 1.3 Related Documents

This Policy supplements:

- [Seller Agreement](#), Section 2 (Eligibility and Account) and Section 8 (Tax Compliance);
- [Privacy Policy](#), Sections 2-5 (data collection, purposes, legal basis, disclosure);
- [Tax Information for Sellers](#), Section 3 (Information We Collect);
- [Export & Sanctions Compliance Policy](#), Section 5 (Screening).

### 1.4 Current Verification Status (April 2026)

At the current launch stage of the Platform, we are using a **simplified verification process** (primarily Level 1 with basic checks). More comprehensive KYC requirements, including government-issued ID verification, selfie/liveness checks, and enhanced due diligence, will be introduced gradually as the platform grows and in accordance with our risk-based approach. All Sellers will be notified in advance of any material changes to the verification requirements.

## 2. WHY WE VERIFY SELLERS

### 2.1 Legal Obligations

Company is legally required to verify the identity of Sellers to: (a) prevent money laundering and terrorist financing (AMLD4/5, Latvian AML law); (b) comply with economic sanctions (EU, OFAC, UN, UK, Latvia); (c) fulfil tax reporting obligations (DAC7); (d) comply with the DSA trader verification requirements; and (e) ensure the integrity and trustworthiness of the Platform.

### 2.2 Platform Integrity

Verification protects: (a) Buyers, by ensuring they are purchasing from identifiable, accountable Sellers; (b) legitimate Sellers, by reducing competition from fraudulent or infringing actors; (c) Company, by mitigating legal, financial, and reputational risk; and (d) the broader community, by preventing the Platform from being used for illegal purposes.

### 2.3 Risk-Based Approach

Company applies a **risk-based approach** to verification, as required by AMLD4/5 and Latvian AML law. This means that the depth and intensity of verification measures are proportionate to the assessed risk level of the Seller, considering factors including: jurisdiction, transaction volume, product type, and the presence of risk indicators.

## 3. VERIFICATION LEVELS

### 3.1 Tiered Verification Structure

Company operates a tiered verification system. Sellers progress through verification levels based on their activity on the Platform. Higher activity levels require more comprehensive verification.

#### Level 1: Basic Registration

Requirement	Details
Trigger	Account creation
Data collected	Email address, display name, password, country of residence
Verification	Email verification (confirmation link)
Capabilities granted	Browse Platform, set up profile, prepare listings (drafts only)
Capabilities restricted	Cannot publish listings, cannot receive payouts

#### Level 2: Identity Verification (Standard KYC)

Requirement	Details
Trigger	Before first listing publication
Data collected (Individuals)	Full legal name, date of birth, residential address, nationality, government-issued photo ID, selfie for biometric matching, Tax Identification Number (TIN)
Data collected (Entities)	Legal entity name, registration number, registered address, country of incorporation, certificate of incorporation or equivalent, identity of beneficial owner(s) holding 25% or more, identity of legal representative, TIN/VAT number
Verification	Automated document verification and biometric matching via third-party KYC provider; cross-referencing against sanctions lists; TIN validation where government tools are available

<b>Capabilities granted</b>	Publish listings, receive Buyer payments (held in escrow)
<b>Capabilities restricted</b>	Payouts subject to holding period; payout limits may apply pending Level 3

### Level 3: Full Verification (Enhanced KYC + Tax)

Requirement	Details
<b>Trigger</b>	Before first payout; or when cumulative gross sales exceed €2,000 or 30 transactions in any calendar year (DAC7 threshold)
<b>Data collected (in addition to Level 2)</b>	Proof of address (utility bill, bank statement, or official correspondence dated within 3 months); bank account or payout method verification (IBAN holder name matching); completed tax forms (W-8BEN/W-8BEN-E for non-US persons, W-9 for US persons, or equivalent); VAT registration certificate (if applicable); financial account identifier for DAC7 reporting
<b>Verification</b>	Address verification via document review; bank account holder name matching; TIN cross-referencing against DAC7 validation tools; Politically Exposed Person (PEP) screening; adverse media screening
<b>Capabilities granted</b>	Full Platform access: publish listings, receive payouts on standard schedule, access all Seller features
<b>Capabilities restricted</b>	None (subject to ongoing monitoring)

### Level EDD: Enhanced Due Diligence









Requirement	Details
<b>Trigger</b>	Risk-based, as described in Section 6

<b>Additional measures</b>	Source of funds inquiry, business activity review, corporate structure analysis (for complex entities), senior management identification, ongoing transaction monitoring with lower thresholds, more frequent periodic reviews
<b>Capabilities</b>	Full access maintained unless risk is unacceptable; additional payout holds or limits may apply during EDD review









#### 4. REQUIRED DOCUMENTS AND INFORMATION

















##### 4.1 Individuals (Natural Persons)





Document / Information	Level 2	Level 3	Purpose
<b>Government-issued photo ID</b>  (passport, national ID card, or driver's licence)	✔ Required	✔ Required	Identity verification
<b>Selfie / liveness check</b>  (live photo or short video for biometric matching)	✔ Required	✔ Required	Biometric matching to prevent identity fraud
<b>Full legal name</b>	✔ Required	✔ Required	Identification, DAC7
<b>Date of birth</b>	✔ Required	✔ Required	Identification, DAC7
<b>Residential address</b>	✔ Required (self-declared)	✔ Required (document-verified)	Jurisdiction, DAC7
<b>Nationality</b>	✔ Required	✔ Required	Sanctions screening
<b>Tax Identification Number (TIN)</b>	✔ Required	✔ Required (validated)	DAC7 reporting

<b>Proof of address</b> (utility bill, bank statement, official letter, dated within 3 months)	 Not required	 Required	Address verification
<b>Bank account / payout method</b>	 Not required	 Required (name-matched)	Payout processing, DAC7
<b>Tax forms</b> (W-8BEN, W-9, or equivalent)	 Not required	 Required (for applicable jurisdictions)	US tax reporting, withholding
<b>VAT registration certificate</b>	 Not required	 If registered for VAT	VAT compliance

#### 4.2 Legal Entities (Companies, Partnerships, etc.)

Document / Information	Level 2	Level 3	Purpose
<b>Certificate of incorporation</b> (or equivalent registration document)	 Required	 Required	Entity verification
<b>Legal entity name and registration number</b>	 Required	 Required	Identification, DAC7
<b>Registered address</b>	 Required	 Required (document-verified)	Jurisdiction, DAC7
<b>Country of incorporation</b>	 Required	 Required	Sanctions screening

<b>Articles of association / memorandum</b>  (or equivalent constitutional document)	 Not required	 Required	Ownership structure, legal authority
<b>Beneficial ownership declaration</b>  (all individuals holding ≥25% direct or indirect ownership)	 Required (self-declared)	 Required (document-verified)	AML4/5, sanctions
<b>ID of each beneficial owner</b>  (per Individual requirements above)	 Required	 Required	AML4/5, sanctions
<b>ID of legal representative</b>  (person authorised to act for the entity)	 Required	 Required	Authority verification
<b>Proof of authorisation</b>  (board resolution, power of attorney, or equivalent)	 Not required	 Required	Legal representative authority
<b>Proof of registered address</b>	 Not required	 Required	Address verification
<b>TIN / VAT registration</b>	 Required (self-declared)	 Required (validated)	DAC7, VAT
<b>Bank account</b>  (in entity name)	 Not required	 Required (name-matched)	Payout, DAC7

<b>Tax forms</b> (W-8BEN-E, W-9, or equivalent)	 Not required	 Required (for applicable jurisdictions)	US tax reporting
<b>Corporate structure chart</b> (for entities with complex ownership)	 Not required	 If applicable (EDD trigger)	AMLD4/5, sanctions

### 4.3 Document Requirements

All submitted documents must: (a) be clear, legible, and unredacted (except for information not required, which may be redacted by the Seller); (b) be in the original language, accompanied by a certified or sworn translation into English or Latvian if the original is in another language; (c) not be expired (government IDs must be valid at the time of submission); (d) be in colour (for photo IDs); and (e) be in an accepted format: JPEG, PNG, PDF (maximum 10MB per file).

## 5. VERIFICATION PROCESS AND TIMELINES

### 5.1 Process Flow

Step	Description	Timeline
<b>1. Submission</b>	Seller submits required documents and information through the Seller dashboard (Settings → Verification)	Seller-initiated
<b>2. Automated checks</b>	Documents are processed by Company's third-party KYC provider: document authenticity, biometric matching, data extraction, sanctions screening, PEP/adverse media screening	Typically within minutes to 1 hour
<b>3. Automated decision</b>	If automated checks return a clear pass (high confidence, no risk flags), the verification level is granted automatically	Immediate upon completion of Step 2

<b>4. Manual review</b>	If automated checks return inconclusive results, potential matches (fuzzy hits), or risk flags, the case is escalated to Company's compliance team for manual review	Target: 2 business days
<b>5. Additional information request</b>	If manual review requires additional documentation or clarification, Company contacts the Seller via email and dashboard notification	Seller has <b>14 calendar days</b> to respond
<b>6. Decision</b>	Company approves, conditionally approves (with restrictions), or rejects the verification	Communicated within 2 business days of receiving all required information
<b>7. Ongoing monitoring</b>	Verified Sellers are subject to ongoing monitoring: re-screening against updated sanctions lists, periodic review (risk-based), and transaction monitoring	Continuous

## 5.2 Standard Timelines

<b>Verification Level</b>	<b>Typical Processing Time (from complete submission)</b>
<b>Level 1</b> (email verification)	Instant
<b>Level 2</b> (standard KYC, auto-approved)	Minutes to 1 hour
<b>Level 2</b> (standard KYC, manual review required)	1-3 business days
<b>Level 3</b>	1-2 business days

(full verification, auto-approved)	
<b>Level 3</b> (full verification, manual review)	3-5 business days
<b>EDD</b> (enhanced due diligence)	5-15 business days

Processing times depend on document quality, completeness, and the complexity of the case. Company will notify the Seller if additional time is needed.

### 5.3 Periodic Re-Verification

Verified Sellers are subject to periodic re-verification to ensure continued accuracy and compliance:

(a) **Annual review:** Company conducts an automated re-screening of all verified Sellers against updated sanctions lists, PEP databases, and adverse media at least once per calendar year;

(b) **Triggered re-verification:** Company may require updated documents or information upon: (i) a material change in the Seller's information (name, address, ownership, tax status); (ii) a sanctions list update resulting in a potential match; (iii) a significant change in the Seller's transaction volume or patterns; (iv) a risk indicator identified through transaction monitoring; or (v) a regulatory requirement or law enforcement request;

(c) **Document expiry:** Sellers must provide updated government-issued photo ID before or promptly after the expiry of the ID previously submitted. Company will notify Sellers sixty (60) days before the expiration date of their submitted ID.

## 6. ENHANCED DUE DILIGENCE (EDD)

### 6.1 Triggers

Company applies Enhanced Due Diligence measures where the risk assessment indicates a higher-than-standard risk. EDD is triggered by one or more of the following:

(a) The Seller is located in or has significant connections to a jurisdiction identified as high-risk by: the European Commission's list of high-risk third countries (delegated acts under AMLD4, currently Commission Delegated Regulation (EU) 2016/1675, as amended); the FATF list of jurisdictions under increased monitoring ("grey list") or those subject to a call for action ("black list"); or Company's internal risk assessment;

- (b) The Seller (individual) is a Politically Exposed Person (PEP) or a family member or known close associate of a PEP;
- (c) The Seller's ownership structure involves multiple layers of corporate entities, nominee shareholders, bearer shares, trusts, or foundations that obscure the ultimate beneficial owner;
- (d) The Seller's transaction volume, patterns, or Buyer profile present unusual risk indicators (e.g., large volumes of small transactions, concentration of sales to high-risk jurisdictions, rapid escalation in sales volume without corresponding business justification);
- (e) Adverse media screening identifies credible negative information regarding the Seller (fraud allegations, prior sanctions, criminal proceedings, regulatory actions);
- (f) A Supervisory Authority, Financial Intelligence Unit, or law enforcement authority has requested or required enhanced measures;
- (g) The Seller's products fall into a higher-risk category (e.g., encryption tools, security software, AI models with dual-use potential).

## **6.2 EDD Measures**

Enhanced Due Diligence may include, in addition to standard verification:

- (a) **Source of funds and source of wealth inquiry:** Requesting documentation or a declaration regarding the origin of the Seller's funds and the economic activity generating the income flowing through the Platform;
- (b) **Detailed corporate structure analysis:** Requiring a complete ownership chart, identifying all intermediate entities and ultimate beneficial owners (including those below the 25% standard threshold);
- (c) **Senior management identification:** Identifying and verifying the senior management (directors, officers) of entity Sellers, beyond the legal representative;
- (d) **Enhanced transaction monitoring:** Applying lower thresholds and more frequent automated alerts for the Seller's transactions;
- (e) **More frequent periodic reviews:** Increasing the re-verification frequency from annual to quarterly or semi-annual;
- (f) **Independent verification:** Cross-referencing Seller-provided information against independent databases, public registries, or third-party intelligence services;
- (g) **In-person or video verification:** Requiring a live video call with the Seller or legal representative for identity confirmation.

## **6.3 Outcome**

Following EDD, Company may: (a) approve the Seller with no additional restrictions; (b) approve with conditions (e.g., payout limits, transaction monitoring thresholds, mandatory periodic re-verification); (c) decline the application or terminate the account, where the risk level is unacceptable or cannot be adequately mitigated; or (d) file a Suspicious Activity Report (SAR) with the Latvian Financial Intelligence Unit (*Finanšu izlūkošanas dienests*) where required by law. Company is prohibited from disclosing the filing of a SAR to the Seller ("tipping-off" prohibition under AMLD4/5 and Latvian AML law).

## 7. CONSEQUENCES OF FAILED OR INCOMPLETE VERIFICATION

### 7.1 Failure to Complete Verification

Situation	Consequence
Seller does not complete Level 2 verification	Cannot publish listings or receive payouts
Seller does not complete Level 3 within 14 days of request	Existing listings suspended; payouts held
Seller does not respond to additional information requests within 14 days	Account suspended pending receipt of documentation
Seller fails to provide updated documents upon expiry or triggered re-verification within 14 days	Account restrictions (listing suspension, payout hold) until compliance

### 7.2 Verification Rejection

Company may reject a Seller's verification application where: (a) the submitted documents are fraudulent, altered, or forged; (b) biometric matching fails (the selfie does not match the ID); (c) the Seller matches a sanctions list entry that cannot be resolved as a false positive; (d) the Seller is identified as a PEP and the associated risk cannot be adequately mitigated; (e) the Seller provides false, misleading, or inconsistent information; (f) the EDD process identifies unacceptable risk; or (g) Company is otherwise unable to satisfy itself of the Seller's identity, legitimacy, or compliance with applicable law.

### 7.3 Fraudulent Documents

Submission of fraudulent, forged, or materially altered identification documents constitutes: (a) immediate and permanent account termination; (b) a violation of the [Seller Agreement](#) and [Terms of Service](#); (c) grounds for reporting to law enforcement and the Latvian Financial Intelligence Unit; and (d) grounds for forfeiture of any pending payouts, to the extent permitted by applicable law.

## 8. DATA PROTECTION AND RETENTION

### 8.1 Legal Basis

The processing of personal data for KYC/AML verification is based on: (a) **legal obligation** (Article 6(1)(c) GDPR), to comply with AMLD4/5, Latvian AML law, DAC7, DSA Article 30, and sanctions regulations; and (b) **explicit consent** (Article 9(2)(a) GDPR), for the processing of biometric data derived from selfie/liveness verification. Consent for biometric processing may be withdrawn at any time, though withdrawal may prevent Company from verifying the Seller's identity and maintaining the account.

### 8.2 Data Collected

The categories of personal data collected for verification are listed in Section 4 and are further described in the [Privacy Policy](#), Section 2.

### 8.3 Third-Party KYC Providers

Verification documents and biometric data are processed by Company's third-party KYC service providers, who act as Data Processors under Data Processing Agreements in accordance with Article 28 GDPR. These providers are listed in the Sub-processor list maintained at [shookout.com/sub-processors](https://shookout.com/sub-processors) and referenced in the [Data Processing Agreement](#), Schedule 2.

### 8.4 Retention

Data Category	Retention Period	Legal Basis
KYC/AML verification data (ID documents, biometric data, screening results)	<b>5 years</b> after the end of the business relationship	AMLD4/5 Art. 40; Latvian AML Law
Biometric data (selfie/liveness)	Deleted promptly after verification completion, unless retention is required for dispute resolution	GDPR Art. 9; data minimisation

Tax documentation (TIN, W-8/W-9, VAT certificates)	<b>7 years</b> from the reporting period	DAC7; Latvian tax law
Sanctions screening records	<b>5 years</b> after the screening event	EU sanctions regulations; Latvian AML law
Verification decision records (approved/rejected, reasons)	<b>5 years</b> after the decision	AMLD4/5; accountability

### 8.5 Data Subject Rights

Sellers may exercise their data protection rights (access, rectification, erasure, restriction, portability, objection) as described in the [Privacy Policy](#), Section 8. Certain rights may be limited where the processing is required by law (e.g., AML record-keeping obligations override the right to erasure during the mandatory retention period, per Article 17(3)(b) GDPR).

### 9. UPDATES TO THIS POLICY

Company may update this Policy to reflect changes in applicable AML/KYC law, DAC7 requirements, sanctions regulations, regulatory guidance, or Company's verification procedures. Material changes will be communicated by: (a) posting the updated Policy with a revised "Last Updated" date; (b) email notification to registered Sellers; and (c) a prominent notice in the Seller dashboard, at least **fifteen (15) days** before the effective date.

### 10. CONTACT

Purpose	Contact
<b>Verification questions and document submission</b>	Seller Dashboard → Settings → Verification
<b>Verification support</b>	<a href="mailto:verification@shookout.com">verification@shookout.com</a>
<b>Privacy and data protection inquiries</b>	<a href="mailto:privacy@shookout.com">privacy@shookout.com</a>
<b>Compliance inquiries</b>	<a href="mailto:compliance@shookout.com">compliance@shookout.com</a>

**Legal inquiries**

[legal@shookout.com](mailto:legal@shookout.com)

**Company:** SIA Synchron **Registration number:** 40203436468 **Address:** Unijas iela 74A  
- 45, Riga, LV-1084, Latvia

**Related documents:** [Seller Agreement](#) · [Privacy Policy](#) · [Tax Information for Sellers](#) ·  
[Export & Sanctions Compliance Policy](#) · [Data Processing Agreement](#)