PRIVACY POLICY

SIA Synchron – shookout.com

Effective Date: 07.04.2026

Last Updated: 07.04.2026

1. INTRODUCTION AND SCOPE

1.1 About This Policy

This Privacy Policy ("**Policy**") explains how SIA Synchron, a limited liability company incorporated under the laws of the Republic of Latvia, registration number 40203436468, registered address Unijas iela 74A - 45, Riga, Latvia ("**Company**," "**we**," "**us**," or "**our**"), collects, uses, stores, shares, and protects personal data in connection with the shookout.com digital goods marketplace (the "**Platform**").

1.2 Scope

This Policy applies to all individuals who interact with the Platform, including: (a) visitors who browse the Platform without registering ("**Visitors**"); (b) registered users who purchase Digital Goods ("**Buyers**"); (c) registered users who list and sell Digital Goods ("**Sellers**"); and (d) individuals who contact us through customer support, email, or other channels (collectively, "**Users**" or "**you**").

This Policy covers personal data processed through the Platform (including its website, mobile-optimised interfaces, and APIs), email communications, customer support interactions, and any other touchpoints where we collect personal data.

1.3 Data Controller

For the purposes of Regulation (EU) 2016/679 ("**GDPR**"), the Latvian Personal Data Processing Law (*Fizisko personu datu apstrādes likums*), and other applicable data protection laws, Company is the **Data Controller** for the personal data described in this Policy, except as specified in Section 1.4.

Contact details of the Data Controller:

- SIA Synchron
- Unijas iela 74A - 45, Riga, Latvia
- Registration number: 40203436468
- Email: privacy@shookout.com

1.4 Roles in the Marketplace Context

The Platform operates as a marketplace connecting Sellers and Buyers. The allocation of data protection roles is as follows:

(a) Company as Data Controller: Company is the Data Controller for: (i) account registration and management data of all Users; (ii) transaction data processed for Platform operations, payment facilitation, and compliance purposes; (iii) data collected for KYC/AML verification, tax reporting (including DAC7), and sanctions screening; (iv) data used for Platform analytics, improvement, and security; (v) data collected via cookies and tracking technologies; and (vi) customer support communications.

(b) Company as Data Processor: Where Company processes Buyer personal data strictly on behalf of and under the instructions of Sellers for the purpose of fulfilling Seller transactions (e.g., transmitting Buyer contact details to a Seller solely for licence delivery or customer support related to a specific Digital Good), Company acts as a **Data Processor** on behalf of the Seller (who is the Data Controller for that processing). Such processing is governed by a Data Processing Agreement between Company and the Seller, as referenced in the Seller Agreement.

(c) Sellers as Independent Data Controllers: Where Sellers collect or process Buyer personal data independently (e.g., through their own external services, mailing lists, or off-platform communications), such processing is outside the scope of this Policy. Sellers are independent Data Controllers for data they collect or process outside the Platform and are solely responsible for compliance with applicable data protection law.

1.5 Related Documents

This Policy is part of the contractual framework that includes: Terms of Service, Seller Agreement, Refund & Return Policy, and Cookie Policy (/cookies). Capitalised terms not defined herein have the meanings assigned in the Terms of Service.

2. INFORMATION WE COLLECT

2.1 Information You Provide Directly

Category	Buyers	Sellers	All Users
Account Registration	Name, email, password	Legal name or entity name, email, password, address	Same
Profile Information	Display name, avatar (optional)	Display name, avatar, bio, portfolio links, public contact	Same

Identity Verification (KYC)	N/A (unless flagged)	Government-issued ID, proof of address, selfie/video verification, date of birth	On request for compliance
Tax Documentation	N/A	Tax identification number (TIN), VAT registration number, W-8/W-9 forms, tax residency certificates	N/A
Payment Information	Payment card details (processed by Payment Processors), billing address	Bank account/payout details, PayPal or equivalent	Varies
Transaction Data	Purchase history, order details, download records	Sales history, payout records, Commission statements	Varies
Communications	Support tickets, dispute messages, reviews, ratings	Support tickets, dispute responses, Buyer communications	Same
Refund/Withdrawal Data	Refund requests, withdrawal consent records (EU consumers)	Refund dispute responses	Varies
Content Data	User Content (reviews, comments)	Digital Goods metadata, product descriptions, previews, AI content disclosures	Varies

2.2 Information Collected Automatically

When you access the Platform, we automatically collect:

(a) Device and Technical Data: IP address, device type, operating system, browser type and version, screen resolution, device identifiers, and language preferences.

(b) Usage Data: Pages visited, features used, search queries, click patterns, time spent on pages, referring URLs, exit pages, and interaction with listings and Digital Goods.

(c) Transaction Metadata: Timestamps, transaction status, payment method type (not full card details), currency, and geolocation data derived from IP address.

(d) Log Data: Server logs, error logs, access logs, and security event logs.

(e) Cookies and Similar Technologies: Cookies, web beacons, pixels, local storage, and similar tracking technologies. See Section 9 and our Cookie Policy (/cookies) for full details.

2.3 Information from Third Parties

We may receive personal data from:

(a) Payment Processors: Transaction confirmation, payment status, chargeback notifications, and fraud screening results from Stripe, PayPal, or other Payment Processors.

(b) Identity Verification Providers: KYC verification results, document authentication, and screening outcomes from third-party identity verification services.

(c) Sanctions and Compliance Databases: Screening results from OFAC, EU, UN, and other sanctions lists and PEP (Politically Exposed Persons) databases.

(d) Tax Authorities: In limited circumstances, tax authorities may provide information relevant to Seller tax compliance verification.

(e) Public Sources: Publicly available business registry information, domain WHOIS data, and publicly available social media profiles where relevant to account verification.

(f) Other Users: Information contained in Buyer reviews, ratings, dispute submissions, and takedown notices.

2.4 Sensitive Data

We do not intentionally collect special categories of personal data (as defined in Article 9 GDPR), including data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic or biometric data, health data, or data concerning sex life or sexual orientation. If such data is incidentally included in documents you provide (e.g., a government ID), we process it solely for the stated verification purpose and apply enhanced security measures. For KYC purposes, biometric data derived from selfie/video verification is processed with your explicit consent (Article 9(2)(a) GDPR) and deleted promptly after verification completion.

3. HOW WE USE YOUR INFORMATION

3.1 Purposes of Processing

We process personal data for the following purposes:

Purpose	Categories of Data Used	Applies to
Account creation and management	Registration data, profile data	All Users
Facilitating transactions	Transaction data, payment data, contact details	Buyers, Sellers
Processing payouts to Sellers	Payout details, tax documentation, transaction history	Sellers
Processing refunds and withdrawal requests	Transaction data, refund request details, EU consent records	Buyers
KYC/AML compliance	Identity documents, verification results, screening data	Sellers (all), Buyers (risk-based)
Tax reporting (including DAC7)	Legal name, address, TIN, transaction data, bank identifiers	Sellers
Sanctions screening	Name, nationality, address, entity details	All Users
Fraud prevention and detection	Transaction patterns, device data, IP address, behavioural signals	All Users
Customer support	Communications, account data, transaction history	All Users
Dispute resolution	Transaction data, communications, Digital Good metadata, evidence submitted	Buyers, Sellers

Content moderation and enforcement	Listings, User Content, AI disclosures, takedown notices	Sellers, reporting parties
Platform improvement and analytics	Usage data, aggregated transaction data, device data	All Users
Personalisation	Usage data, purchase history, preferences	All Users (where consented or legitimate interest)
Marketing and communications	Email, name, preferences, purchase history	All Users (where consented or legitimate interest)
Security and integrity	Log data, device data, IP address, authentication records	All Users
Legal compliance and regulatory obligations	All categories as necessary	All Users
Enforcing Terms of Service and policies	Account data, transaction data, communications	All Users
AI content compliance monitoring	Listing metadata, AI disclosures, content analysis results	Sellers

3.2 No Sale of Personal Data

We do not sell your personal data to third parties. We do not share your personal data with third parties for their direct marketing purposes without your explicit consent.

4. LEGAL BASIS FOR PROCESSING (GDPR)

For Users in the EU, EEA, UK, and Latvia, we process personal data on the following legal bases under Article 6(1) GDPR:

Legal Basis	Processing Activities
Contract Performance	Account registration and management; facilitating transactions between Buyers and Sellers; processing payments and payouts;

(Art. 6(1)(b))	processing refunds and withdrawal requests; delivering Digital Goods; customer support related to transactions; enforcing the Terms of Service , Seller Agreement , and Refund Policy .
Legal Obligation (Art. 6(1)(c))	KYC/AML compliance (Directive (EU) 2015/849, Latvian AML law); tax reporting including DAC7 (Council Directive 2021/514); sanctions screening (EU Regulation 269/2014, OFAC); responding to lawful requests from courts, regulators, and law enforcement; DMCA/DSA notice processing; data retention required by Latvian accounting and tax law.
Legitimate Interests (Art. 6(1)(f))	Fraud prevention and detection; Platform security and integrity; analytics and Platform improvement (aggregated/pseudonymised where possible); enforcing policies and investigating violations; direct marketing to existing customers (with opt-out right); defending legal claims. Our legitimate interests do not override your fundamental rights and freedoms. You may object to processing based on legitimate interests (see Section 8).
Consent (Art. 6(1)(a))	Non-essential cookies and tracking technologies; marketing communications (where consent is required under applicable law); processing of biometric data for KYC verification; any other processing where consent is specifically obtained. Consent may be withdrawn at any time without affecting the lawfulness of processing prior to withdrawal (see Section 8).

4.2 Special Categories (Article 9 GDPR)

Where we process special category data (e.g., biometric data from KYC verification), the legal basis is your explicit consent under Article 9(2)(a) GDPR. You may withdraw this consent at any time, though this may affect our ability to verify your identity and maintain your account.

5. SHARING AND DISCLOSURE OF INFORMATION

5.1 Categories of Recipients

We share personal data with the following categories of recipients, only to the extent necessary for the stated purposes:

(a) Buyers and Sellers (Transaction Counterparties)

When a transaction occurs, we share limited information between the Buyer and Seller as necessary to fulfil the transaction and licence:

- Sellers receive: Buyer's username (or display name), and such additional information as reasonably necessary for licence delivery and customer support (e.g., email address, if included in the applicable licence fulfilment flow). Sellers do not receive Buyer payment card details.
- Buyers receive: Seller's display name, public profile information, and licence terms.

(b) Payment Processors

We share transaction data, billing address, and payment instrument details with our Payment Processors (e.g., Stripe, PayPal) for the purpose of processing payments, payouts, chargeback management, and fraud prevention. Payment Processors act as independent Data Controllers for data they process under their own privacy policies.

(c) Identity Verification and KYC Providers

We share identity documents and verification data with third-party KYC service providers who act as Data Processors under our instructions and pursuant to Data Processing Agreements.

(d) Tax Authorities

We are legally obligated to report Seller information and transaction data to tax authorities in accordance with:

- **EU DAC7** (Council Directive 2021/514): Seller legal name, address, TIN, date of birth (individuals) or registration number (entities), financial account identifier, total consideration, number of transactions, fees withheld. Reports are submitted to the Latvian State Revenue Service (*Valsts ieņēmumu dienests*), which may exchange this data with tax authorities in other EU Member States.
- **US IRS reporting**: Where applicable, Seller information may be reported on Form 1099-K or as otherwise required.

- **OECD Model Rules**: Reporting to other jurisdictions implementing the OECD Model Reporting Rules for digital platforms.

(e) Sanctions Screening Services

We share User data with sanctions screening providers to comply with OFAC, EU, UN, and Latvian sanctions obligations.

(f) Law Enforcement and Regulatory Authorities

We may disclose personal data to law enforcement, courts, regulatory authorities, or other governmental bodies: (i) where required by law, subpoena, court order, or binding regulatory request; (ii) to comply with DMCA or DSA obligations; (iii) to prevent, investigate, or report suspected criminal activity; or (iv) to protect the rights, property, or safety of Company, Users, or the public.

(g) Professional Advisors

We may share personal data with our legal counsel, auditors, accountants, and other professional advisors under obligations of confidentiality.

(h) Service Providers (Data Processors)

We engage third-party service providers who process personal data on our behalf under Data Processing Agreements, including: hosting and cloud infrastructure providers; email service providers; analytics providers; customer support tools; content delivery networks; and security services.

(i) Corporate Transactions

In the event of a merger, acquisition, reorganisation, bankruptcy, or sale of all or a portion of our assets, personal data may be transferred to the acquiring entity or successor. We will provide notice of such transfer in accordance with Section 13.

5.2 No Other Sharing

We do not share personal data with any other third parties except as described in this Section 5, or with your explicit consent.

6. INTERNATIONAL DATA TRANSFERS

6.1 Transfer Locations

Company is established in Latvia (EU Member State). Personal data is primarily stored and processed within the EU/EEA. However, some of our service providers, Payment Processors, and recipients listed in Section 5 may be located outside the EU/EEA, including in the United States and other jurisdictions.

6.2 Safeguards for International Transfers

Where personal data is transferred outside the EU/EEA to a country that has not received an adequacy decision from the European Commission, we implement appropriate safeguards in accordance with Chapter V of the GDPR, including:

(a) Standard Contractual Clauses (SCCs): We execute the European Commission's Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914) with recipients in non-adequate countries, supplemented by additional technical and organisational measures where necessary following a transfer impact assessment.

(b) Adequacy Decisions: Where the European Commission has issued an adequacy decision for the recipient country (e.g., the EU-U.S. Data Privacy Framework for certified US organisations), we rely on that adequacy decision.

(c) Binding Corporate Rules: Where applicable, we rely on the recipient's approved Binding Corporate Rules.

(d) Derogations: In limited circumstances, transfers may be based on the derogations set forth in Article 49 GDPR (e.g., explicit consent, necessity for contract performance, important reasons of public interest).

6.3 Transfer Impact Assessments

For transfers to jurisdictions without an adequacy decision, we conduct transfer impact assessments to evaluate the level of data protection in the recipient country, considering the laws and practices of that country (including government access to data), and implement supplementary measures where necessary.

6.4 Your Right to Information

You may request information about the specific safeguards applied to transfers of your personal data by contacting us at privacy@[domain.com].

7. DATA RETENTION

7.1 General Principles

We retain personal data only for as long as necessary to fulfil the purposes described in this Policy, unless a longer retention period is required or permitted by law. When determining retention periods, we consider: (a) the purpose of processing; (b) applicable legal, tax, and regulatory retention requirements; (c) contractual obligations; (d) ongoing legitimate business needs; and (e) the data subject's interests.

7.2 Specific Retention Periods

Category of Data	Retention Period	Legal Basis for Retention

Account registration data	Duration of account + 3 years after deletion	Contract performance; legitimate interest (defence of claims); Latvian limitation period
Transaction records	7 years from the date of transaction	Latvian Accounting Law (*Grāmatvedības likums*); EU VAT Directive; DAC7
KYC/AML verification data	5 years after the end of the business relationship	Directive (EU) 2015/849, Art. 40; Latvian AML/CTF Law
Tax documentation (Sellers)	7 years from the reporting period	DAC7; Latvian tax law; IRS requirements
Sanctions screening records	5 years after the screening event	EU sanctions regulations; Latvian AML law
Customer support communications	3 years from resolution of the inquiry	Legitimate interest; defence of claims
Refund and dispute records	5 years from resolution	Contract performance; legal obligation; defence of claims
EU withdrawal consent records	5 years from the date of transaction	Directive 2011/83/EU; evidence of valid consent
Cookie and consent records	3 years from the date of consent (or until withdrawal)	ePrivacy Directive; GDPR accountability
Server logs and security data	12 months from collection	Legitimate interest (security); Latvian cybersecurity requirements

Marketing consent records	Duration of consent + 3 years after withdrawal	GDPR accountability (Art. 5(2), Art. 7(1))
Aggregated/anonymised analytics	Indefinitely (no personal data)	N/A (not personal data)

7.3 Post-Account Deletion

When you delete your account, we will: (a) delete or anonymise your personal data within thirty (30) days, except for data that we are required or permitted to retain under Section 7.2; (b) retain transaction records, tax data, and compliance records for the applicable retention periods; and (c) retain anonymised or aggregated data that can no longer identify you.

7.4 Seller-Specific Retention

Due to regulatory obligations (including DAC7, AML, and tax law), Seller data is subject to longer retention periods than Buyer data. By registering as a Seller, you acknowledge that certain personal data and transaction records will be retained for up to seven (7) years after the end of the business relationship, regardless of account deletion.

8. YOUR RIGHTS

8.1 GDPR Rights (EU/EEA/UK/Latvia Users)

Under the GDPR and applicable national law, you have the following rights:

Right	Description	How to Exercise
Right of Access (Art. 15)	Obtain confirmation of whether we process your personal data and, if so, access to that data and supplementary information (purposes, categories, recipients, retention, etc.)	Email privacy@shookout.com or use the "Download My Data" feature in account settings
Right to Rectification (Art. 16)	Have inaccurate personal data corrected and incomplete data completed	Update your account settings directly, or email privacy@shookout.com

Right to Erasure (Art. 17)	Request deletion of your personal data where: (a) no longer necessary; (b) you withdraw consent; (c) you object and no overriding grounds exist; (d) processing is unlawful; or (e) required by law. Subject to exceptions in Art. 17(3) (legal obligations, defence of claims, etc.)	Email privacy@shookout.com or use "Delete My Account" in settings
Right to Restriction (Art. 18)	Restrict processing where: (a) accuracy is contested; (b) processing is unlawful but you oppose erasure; (c) we no longer need the data but you need it for legal claims; or (d) you have objected pending verification	Email privacy@shookout.com
Right to Data Portability (Art. 20)	Receive your personal data in a structured, commonly used, machine-readable format (e.g., JSON, CSV) and transmit it to another controller, where processing is based on consent or contract and carried out by automated means	Email privacy@shookout.com or use "Export My Data" in account settings
Right to Object (Art. 21)	Object to processing based on legitimate interests (Art. 6(1)(f)) or for direct marketing purposes. We will cease processing unless we demonstrate compelling legitimate grounds that override your interests	Email privacy@shookout.com or use the unsubscribe link for marketing
Right Not to Be Subject to Automated Decision-Making	Not be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly	Email privacy@shookout.com

(Art. 22)	significantly affects you. See Section 12	
Right to Withdraw Consent (Art. 7(3))	Withdraw consent at any time, without affecting the lawfulness of processing prior to withdrawal	Cookie settings; unsubscribe links; email privacy@shookout.com
Right to Lodge a Complaint	Lodge a complaint with a supervisory authority	Latvian Data State Inspectorate (*Datu valsts inspekcija*): www.dvi.gov.lv ; or the supervisory authority in your EU Member State of habitual residence

8.2 Responding to Requests

We will respond to all valid data subject requests within **one (1) month** of receipt, in accordance with Article 12(3) GDPR. This period may be extended by **two (2) additional months** where necessary, considering the complexity and number of requests. We will inform you of any extension within one month, with reasons. Requests are free of charge, unless manifestly unfounded or excessive (Article 12(5) GDPR).

We may request reasonable verification of your identity before fulfilling a request, to prevent unauthorised access to personal data.

8.3 CCPA/CPRA Rights (California Residents)

If you are a California resident, you have additional rights under the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("**CCPA**"):

(a) Right to Know: You have the right to request disclosure of: (i) the categories and specific pieces of personal information we have collected about you; (ii) the categories of sources from which we collected personal information; (iii) the business or commercial purpose for collecting or selling personal information; and (iv) the categories of third parties with whom we share personal information.

(b) Right to Delete: You have the right to request deletion of personal information we have collected from you, subject to statutory exceptions.

(c) Right to Correct: You have the right to request correction of inaccurate personal information.

(d) Right to Opt-Out of Sale/Sharing: We do not sell personal information or share it for cross-context behavioural advertising. If this changes, we will provide a "Do Not Sell or Share My Personal Information" link.

(e) Right to Non-Discrimination: We will not discriminate against you for exercising your CCPA rights.

(f) Authorised Agent: You may designate an authorised agent to make requests on your behalf with proper verification.

To exercise CCPA rights, email privacy@shookout.com with subject line "CCPA Request" or use the Privacy section in your account settings. We will verify your identity and respond within 45 days (extendable by an additional 45 days with notice).

8.4 Categories of Personal Information (CCPA Disclosure)

In accordance with CCPA § 1798.100, the following categories of personal information have been collected in the preceding twelve (12) months:

CCPA Category	Examples	Collected	Sold	Shared for Cross-Context Behavioural Advertising
Identifiers	Name, email, IP address, account ID	Yes	No	No
Personal information (Cal. Civ. Code § 1798.80)	Name, address, payment information	Yes	No	No
Commercial information	Purchase history, transaction records	Yes	No	No

Internet/electronic activity	Browsing history, search queries, interactions	Yes	No	No
Geolocation data	Approximate location from IP address	Yes	No	No
Professional/employment information	Seller business details	Yes	No	No
Inferences	User preferences, fraud risk scores	Yes	No	No

9. COOKIES AND TRACKING TECHNOLOGIES

9.1 Types of Cookies

We use the following categories of cookies and similar technologies:

Category	Purpose	Consent Required	Examples
Strictly Necessary	Essential Platform functionality: authentication, security, shopping cart, cookie consent preferences	No (Art. 5(3) ePrivacy Directive exception)	Session cookies, CSRF tokens, consent records
Functional	Enhanced functionality and personalisation: language preferences, display settings, remembering user choices	Yes	Language/currency preference cookies

Analytics	Understanding Platform usage, performance monitoring, aggregated statistics	Yes	Google Analytics (or privacy-friendly alternatives), Plausible, server-side analytics
Marketing	Delivering relevant advertisements, measuring ad effectiveness, remarketing	Yes	Facebook Pixel, Google Ads (if used)

9.2 Consent Management

Upon your first visit to the Platform, we present a cookie consent banner that: (a) clearly identifies each category of non-essential cookies; (b) does not use pre-ticked boxes; (c) allows you to accept or reject each category individually; (d) does not set non-essential cookies until you provide affirmative consent; (e) provides a link to this Policy and our Cookie Policy (/cookies); and (f) allows you to change or withdraw your preferences at any time through the "Cookie Settings" link available in the Platform footer.

9.3 Do Not Track

We currently respond to Do Not Track (DNT) browser signals by disabling non-essential tracking where technically feasible. We also honour the Global Privacy Control (GPC) signal as an opt-out of sale/sharing under the CCPA.

9.4 Detailed Information

For a complete list of cookies, their providers, purposes, and expiration periods, see our Cookie Policy (/cookies).

10. SECURITY MEASURES

10.1 Technical Measures

We implement appropriate technical security measures to protect personal data against unauthorised access, alteration, disclosure, or destruction, including: (a) encryption of data in transit (TLS 1.2 or higher) and at rest (AES-256 or equivalent); (b) secure authentication mechanisms, including hashed and salted passwords; (c) regular security testing, including vulnerability assessments and penetration testing; (d) firewalls, intrusion detection/prevention systems, and DDoS protection; (e) access logging and monitoring; (f) secure software development practices; and (g) regular security patches and updates.

10.2 Organisational Measures

We implement organisational measures including: (a) access controls based on the principle of least privilege; (b) employee and contractor confidentiality obligations; (c) data protection training for personnel handling personal data; (d) incident response procedures and breach notification processes; (e) regular review of data protection policies and procedures; (f) Data Processing Agreements with all Data Processors; and (g) vendor due diligence for service providers processing personal data.

10.3 Breach Notification

In the event of a personal data breach that is likely to result in a risk to your rights and freedoms, we will: (a) notify the Latvian Data State Inspectorate (*Datu valsts inspekcija*) within 72 hours of becoming aware of the breach (Article 33 GDPR); and (b) notify affected individuals without undue delay where the breach is likely to result in a high risk to their rights and freedoms (Article 34 GDPR).

10.4 No Guarantee

While we implement commercially reasonable security measures, no method of electronic transmission or storage is 100% secure. We cannot guarantee absolute security of your personal data.

11. CHILDREN'S PRIVACY

11.1 The Platform is not directed at, and we do not knowingly collect personal data from, children under the age of sixteen (16) in the EU/EEA/UK (or under the applicable age in other jurisdictions, including thirteen (13) in the United States under COPPA). The minimum age for creating an account is eighteen (18) years, as specified in the Terms of Service.

11.2 If we become aware that we have collected personal data from a child below the applicable age without valid parental consent, we will take reasonable steps to delete such data promptly. If you believe that a child has provided personal data to us, please contact us at privacy@shookout.com.

12. AI AND AUTOMATED DECISION-MAKING

12.1 Automated Processing Activities

We use automated processing, including algorithmic and AI-assisted systems, in the following contexts:

(a) Fraud Detection and Prevention: Automated analysis of transaction patterns, device fingerprints, behavioural signals, and account activity to identify potentially fraudulent transactions or suspicious behaviour. This may result in temporary transaction holds, additional verification requirements, or account restrictions.

(b) Content Moderation: Automated tools to detect potentially infringing, illegal, or policy-violating content in Digital Good listings. Automated detection is supplemented by human review before enforcement action is taken (except in clear cases of illegal content requiring immediate removal).

(c) Sanctions and AML Screening: Automated screening of User data against sanctions lists, PEP databases, and adverse media. Matches are verified by human review before enforcement action.

(d) AI-Generated Content Detection: Automated tools to identify undisclosed AI-generated content in Digital Good listings, in support of the AI content disclosure requirements in the Terms of Service and Seller Agreement.

(e) Search and Recommendation: Algorithmic ranking and recommendation of Digital Goods based on relevance, popularity, recency, and User preferences.

(f) Refund Risk Assessment: Automated scoring of refund requests based on transaction history, account behaviour, and claim patterns to prioritise review and detect potential abuse.

12.2 Decisions with Significant Effects

Where an automated process produces a decision that has legal effects or similarly significantly affects you (e.g., account suspension based on fraud scoring, refund denial based on automated risk assessment), you have the right under Article 22 GDPR to: (a) obtain human intervention in the decision; (b) express your point of view; and (c) contest the decision. To exercise this right, contact privacy@shookout.com or use the appeal mechanism described in the Terms of Service and Seller Agreement.

12.3 Transparency

We are committed to transparency in our use of automated decision-making. Upon request, we will provide meaningful information about the logic involved in automated decisions affecting you, the significance of such processing, and the envisaged consequences.

13. CHANGES TO THIS PRIVACY POLICY

13.1 We may update this Policy from time to time to reflect changes in our practices, applicable law, or regulatory guidance. Material changes will be communicated by: (a) posting the updated Policy on the Platform with a revised "Last Updated" date; (b) sending an email notification to registered Users at least **thirty (30) days** before the effective date of material changes; and (c) displaying a prominent notice on the Platform.

13.2 For changes required by law or regulatory authority that must take effect immediately, we will provide notice as soon as practicable.

13.3 Your continued use of the Platform after the effective date of any changes constitutes your acknowledgement of the updated Policy. If you do not agree with a material change, you may exercise your right to delete your account and personal data in accordance with Section 8.

14. CONTACT INFORMATION AND SUPERVISORY AUTHORITY

14.1 Data Controller Contact

SIA Synchron Unijas iela 74A - 45, Riga, Latvia Registration number: 40203436468 Email: **privacy@shookout.com** General support: **support@shookout.com**

14.2 Data Protection Officer

[If DPO is appointed:] Data Protection Officer: [NAME/TITLE] Email: **dpo@shookout.com**

[If DPO is not appointed:] Company has assessed its processing activities and determined that the appointment of a Data Protection Officer is not mandatory under Article 37 GDPR. For all data protection inquiries, please contact: **privacy@shookout.com**.

Note: if Company's core activities involve regular and systematic monitoring of data subjects on a large scale, or large-scale processing of special categories of data, a DPO appointment may become required. This should be assessed periodically.

14.3 Supervisory Authority

You have the right to lodge a complaint with a data protection supervisory authority. The lead supervisory authority for Company is:

Datu valsts inspekcija (Data State Inspectorate) Elijas iela 17, Riga, LV-1050, Latvia Website: www.dvi.gov.lv Email: pasts@dvi.gov.lv Phone: +371 67223131

You may also lodge a complaint with the supervisory authority in your EU Member State of habitual residence or place of work, in accordance with Article 77 GDPR.

VERSION 2: UX-FRIENDLY PRIVACY POLICY

Privacy Policy shookout.com by SIA Synchron

Last Updated: 07.04.2026

This policy explains what personal data we collect, why, how we protect it, and what rights you have. We have written it in plain language, but it is legally binding.

We are **SIA Synchron**, a company registered in Latvia. We operate the shookout.com digital marketplace.

What Data We Collect

When you create an account:

- Name, email, password
- Sellers also provide: legal name or business name, address, tax ID, government ID (for verification), bank details (for payouts)

When you use the Platform:

- What you browse, search for, and click on
- Your purchases, downloads, and sales history
- Your IP address, device type, browser, and approximate location
- Reviews, comments, support messages

When you buy or sell:

- Payment details (processed securely by our payment partners, not stored by us)
- Transaction records, refund requests, dispute details

From other sources:

- Payment processors (transaction status, fraud checks)
- Identity verification services (KYC results)
- Sanctions screening databases

Why We Use Your Data

We use your data to...	**Legal basis (GDPR)**
Run your account and process transactions	Contract with you
Process payouts to Sellers	Contract
Handle refunds and disputes	Contract
Verify Seller identities (KYC/AML)	Legal obligation
Report Seller data to tax authorities (DAC7)	Legal obligation
Screen against sanctions lists	Legal obligation

Detect and prevent fraud	Legitimate interest
Keep the Platform secure	Legitimate interest
Improve the Platform and understand usage	Legitimate interest
Send you marketing (with your permission)	Consent
Set non-essential cookies	Consent

We do not sell your data. Ever.

Who We Share Your Data With

- **Buyers and Sellers**: Limited info needed to complete transactions (username, email for licence delivery)
- **Payment processors** (Stripe, PayPal, etc.): to process your payments securely
- **Identity verification services**: to verify Seller identities
- **Tax authorities**: Seller data as required by law (EU DAC7, US IRS)
- **Sanctions screening providers**: to comply with sanctions law
- **Law enforcement**: only when legally required
- **Our service providers**: hosting, email, analytics, support tools (under strict contracts)

We do not share your data with anyone else unless you explicitly agree.

Where Your Data Goes

We are based in Latvia (EU), so your data is primarily stored in the EU. Some of our service providers are in the US or other countries. When data leaves the EU, we protect it using:

- **EU Standard Contractual Clauses** (approved by the European Commission)
- **Adequacy decisions** (e.g., EU-U.S. Data Privacy Framework for certified companies)
- Additional safeguards as needed

How Long We Keep Your Data

Data type	How long	Why
Your account data	While your account is active + 3 years	Defence of legal claims
Transaction records	7 years	Tax and accounting law
KYC/AML documents	5 years after relationship ends	Anti-money laundering law
Seller tax data (DAC7)	7 years	EU tax reporting
Support conversations	3 years after resolution	Dispute resolution
Refund and EU withdrawal records	5 years	Legal compliance
Security logs	12 months	Platform security

When you delete your account, we remove your data within 30 days, except what we are legally required to keep.

Sellers: Due to tax and AML regulations, your data may be kept for up to 7 years after you leave, even if you delete your account.

Your Rights

If you are in the EU, EEA, UK, or Latvia (GDPR):

Right	What it means	How to use it
Access	See what data we have about you	Account settings → "Download My Data" or email us
Correction	Fix inaccurate data	Update your account settings or email us

Deletion	Delete your data (with legal exceptions)	Account settings → "Delete My Account" or email us
Restriction	Limit how we use your data	Email us
Portability	Get your data in a standard format	Account settings → "Export My Data" or email us
Object	Stop processing based on legitimate interest, or stop marketing	Email us, or click "Unsubscribe" in emails
Automated decisions	Get a human review of automated decisions that significantly affect you	Email us
Withdraw consent	Take back consent at any time	Cookie settings, unsubscribe links, or email us
Complain	File a complaint with a regulator	Latvian Data State Inspectorate: www.dvi.gov.lv , or your local EU data protection authority

We respond to requests within **1 month** (may extend to 3 months for complex cases). Requests are free.

If you are in California (CCPA/CPRA):

You have the right to: know what we collect, request deletion, request correction, and opt out of data sales (we do not sell your data). We do not discriminate against you for exercising these rights. Email us at privacy@shookout.com with "CCPA Request."

Cookies

We use cookies for:

- **Essential functions** (login, security, cart): always on
- **Preferences** (language, settings): only with your consent

- **Analytics** (how the Platform is used): only with your consent
- **Marketing** (ads, if applicable): only with your consent

You choose which cookies to allow when you first visit. Change your preferences any time via "Cookie Settings" in the footer. See our full Cookie Policy (/cookies) for details.

We honour Do Not Track and Global Privacy Control signals.

Security

We protect your data with:

- Encryption in transit (TLS) and at rest (AES-256)
- Secure password storage (hashed + salted)
- Regular security testing
- Access controls (only staff who need it can see your data)
- Breach notification procedures (we notify authorities within 72 hours and you without undue delay if there is a high risk)

No system is 100% secure, but we take commercially reasonable measures to protect your data.

Children

The Platform is for users 18 and older. We do not knowingly collect data from anyone under 16 (EU) or 13 (US). If we learn we have, we will delete it promptly.

AI and Automated Decisions

We use automated systems for:

- **Fraud detection**: analysing transaction patterns to flag suspicious activity
- **Content moderation**: detecting potentially infringing or policy-violating listings
- **Sanctions screening**: checking names against sanctions lists
- **AI content detection**: identifying undisclosed AI-generated products
- **Search and recommendations**: showing you relevant products

When an automated decision significantly affects you (e.g., account suspension), you can always request a human review. Email privacy@shookout.com or use the appeal process described in our Terms of Service.

Changes to This Policy

We may update this policy. For material changes, we will email you at least 30 days in advance. The updated version will be posted here with a new "Last Updated" date.

Contact Us

- **Privacy questions**: privacy@shookout.com
- **General support**: support@shookout.com
- **Legal inquiries**: legal@shookout.com

Data protection regulator: Latvian Data State Inspectorate (*Datu valsts inspekcija*) Elijas iela 17, Riga, LV-1050, Latvia www.dvi.gov.lv

SIA Synchron | Latvia | Registration No. 40203436468

Related documents: Terms of Service · Seller Agreement · Refund Policy · Cookie Policy (/cookies)