DATA PROCESSING AGREEMENT

SIA Synchron - shookout.com

Effective Date: 07.04.2026

Last Updated: 07.04.2026

1. INTRODUCTION AND PARTIES

1.1 Parties

This Data Processing Agreement ("**DPA**") is entered into between:

(a) Data Controller ("Controller," "Seller," "you"): The individual or legal entity registered as a Seller on the shookout.com digital goods marketplace (the "**Platform**"), as identified in the Seller's account registration.

(b) Data Processor ("Processor," "Company," "we," "us"): 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, LV-1084, Latvia.

1.2 Background

The Platform operates as a digital goods marketplace connecting Sellers and Buyers. As described in the Privacy Policy, Section 1.4, Company acts as a Data Processor on behalf of Sellers in limited, defined circumstances: specifically, where Company processes Buyer personal data strictly on behalf of and under the instructions of the Seller 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).

In all other processing activities described in the Privacy Policy (account management, Platform operations, compliance, analytics, security), Company acts as an independent Data Controller. This DPA governs only the processing where Company acts as Data Processor on behalf of the Seller.

1.3 Legal Framework

This DPA is entered into pursuant to Article 28 of Regulation (EU) 2016/679 ("**GDPR**") and is designed to meet the requirements of Article 28(3) GDPR. It supplements the Seller Agreement and the Privacy Policy. In the event of conflict between this DPA and the Seller Agreement regarding data processing matters, this DPA shall prevail.

1.4 Incorporation

This DPA is incorporated into, and forms part of, the Seller Agreement. By accepting the Seller Agreement, the Seller enters into this DPA. No separate signature is required, in accordance with Article 28(9) GDPR (which permits the contract to be in electronic form).

2. DEFINITIONS

2.1 Capitalised terms not defined herein have the meanings assigned in the Seller Agreement, the Terms of Service, or the Privacy Policy. The following definitions apply to this DPA:

"Buyer Data" means the personal data of Buyers that Company processes on behalf of the Seller in the capacity of Data Processor, as described in Schedule 1.

"Data Protection Laws" means the GDPR, the Latvian Personal Data Processing Law (*Fizisko personu datu apstrādes likums*), and all other applicable data protection and privacy laws and regulations in the EU/EEA, the United Kingdom, and any other jurisdiction relevant to the processing of Buyer Data under this DPA.

"Data Subject" means an identified or identifiable natural person whose personal data is processed under this DPA (i.e., a Buyer).

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Buyer Data transmitted, stored, or otherwise processed, as defined in Article 4(12) GDPR.

"Sub-processor" means any third party engaged by Company to process Buyer Data on behalf of the Seller, as described in Section 6.

"Standard Contractual Clauses" or "SCCs" means the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission pursuant to Commission Implementing Decision (EU) 2021/914, as may be amended or replaced.

"Supervisory Authority" means the competent data protection authority, including the Latvian Data State Inspectorate (*Datu valsts inspekcija*) as the lead authority for Company, and any other supervisory authority with jurisdiction over the Seller or the processing of Buyer Data.

3. SCOPE AND PURPOSE OF PROCESSING

3.1 Subject Matter

This DPA governs the processing of Buyer Data by Company in its capacity as Data Processor on behalf of the Seller, in connection with the Seller's use of the Platform to sell and distribute Digital Goods.

3.2 Processing Details

The details of processing are set forth in **Schedule 1** (Description of Processing), which forms an integral part of this DPA and includes: the categories of Data Subjects; the categories of personal data; the nature and purpose of processing; the duration of processing; and the applicable obligations and rights.

3.3 Scope Limitation

This DPA applies solely to the processing of Buyer Data by Company in its capacity as Data Processor. It does not apply to: (a) processing of Seller personal data by Company (where Company is the Data Controller); (b) processing of Buyer personal data by Company for its own purposes as an independent Data Controller (e.g., Platform operations, compliance, analytics, security, fraud prevention); or (c) processing of personal data by the Seller independently of the Platform. The boundaries of these roles are described in the Privacy Policy, Section 1.4.

3.4 Controller Responsibility

The Seller, as Data Controller, is responsible for: (a) ensuring that there is a valid legal basis under Article 6 GDPR for the processing of Buyer Data; (b) providing all required transparency information to Data Subjects under Articles 13 and 14 GDPR; (c) responding to Data Subject requests (with Company's assistance as described in Section 8); and (d) conducting Data Protection Impact Assessments where required under Article 35 GDPR.

4. INSTRUCTIONS FROM THE CONTROLLER

4.1 Processing on Instructions

Company shall process Buyer Data only on documented instructions from the Seller, unless required to process by EU or Latvian law to which Company is subject, in which case Company shall inform the Seller of that legal requirement before processing (unless such law prohibits providing that information on important grounds of public interest) (Article 28(3)(a) GDPR).

4.2 Deemed Instructions

The Seller's instructions to Company regarding the processing of Buyer Data are deemed to be as follows:

(a) **Primary instructions**: Process Buyer Data to the extent necessary to perform Company's obligations under the Seller Agreement and to enable the Seller to sell and distribute Digital Goods through the Platform, including: (i) facilitating the transmission of Buyer Data to the Seller for licence fulfilment and delivery; (ii) providing Buyer Data to the Seller for customer support and dispute resolution related to specific transactions; and (iii) retaining Buyer Data for the purpose of fulfilling existing Buyer licences following account changes.

(b) **Standing instructions**: The Seller Agreement, the Terms of Service, and this DPA collectively constitute the Seller's documented instructions for the processing of Buyer Data. Any additional or modified instructions must be agreed upon in writing (including email) and may require amendment of this DPA. Company reserves the right to decline instructions that, in Company's reasonable opinion, would violate Data Protection Laws or other applicable law.

4.3 Notification of Non-Compliant Instructions

If Company reasonably believes that an instruction from the Seller infringes Data Protection Laws, Company shall promptly notify the Seller and shall be entitled to suspend the relevant processing until the Seller confirms or modifies the instruction (Article 28(3), second subparagraph, GDPR).

5. SECURITY MEASURES

5.1 Obligation

Company shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects (Article 32 GDPR).

5.2 Specific Measures

Without limiting the generality of Section 5.1, Company implements the following categories of security measures (as described in greater detail in the Privacy Policy, Section 10):

(a) Encryption: Encryption of Buyer Data in transit (TLS 1.2 or higher) and at rest (AES-256 or equivalent).

(b) Access Controls: Role-based access controls implementing the principle of least privilege; multi-factor authentication for administrative access to systems processing Buyer Data; unique user accounts for all personnel with access to Buyer Data.

(c) Authentication: Secure password storage using salted cryptographic hashing; account lockout after failed authentication attempts.

(d) Network Security: Firewalls, intrusion detection and prevention systems, DDoS mitigation, and network segmentation separating production systems from development and testing environments.

(e) Application Security: Secure software development lifecycle (SDLC); regular vulnerability assessments and penetration testing; input validation and output encoding to prevent injection attacks.

(f) Physical Security: Company uses professional cloud hosting providers (Sub-processors listed in Schedule 2) that maintain physical security controls (restricted access, surveillance, environmental controls) certified to ISO 27001 or SOC 2 Type II, or equivalent standards.

(g) Personnel: Confidentiality obligations (contractual or statutory) binding all personnel with access to Buyer Data; data protection and security training provided to relevant personnel.

(h) Incident Management: Documented incident response procedures; logging and monitoring of access to systems processing Buyer Data; regular review of security logs.

(i) Business Continuity: Regular backups of Buyer Data; tested disaster recovery procedures; defined recovery time and recovery point objectives.

5.3 Security Review

Company shall regularly test, assess, and evaluate the effectiveness of the technical and organisational measures implemented under this Section 5 (Article 32(1)(d) GDPR). The measures shall be updated as necessary to address evolving threats, vulnerabilities, and changes in the state of the art.

6. SUB-PROCESSORS

6.1 General Authorisation

The Seller hereby grants Company a **general written authorisation** to engage Sub-processors for the processing of Buyer Data, subject to the conditions set forth in this Section 6 (Article 28(2) GDPR).

6.2 Current Sub-processors

The list of Sub-processors currently engaged by Company for the processing of Buyer Data is set forth in **Schedule 2** and is also maintained at shookout.com/sub-processors, which is updated on an ongoing basis.

6.3 Notification of Changes

Company shall notify the Seller of any intended changes concerning the addition or replacement of Sub-processors at least **fifteen (15) days** before the new Sub-processor begins processing Buyer Data, by: (a) updating the Sub-processor list at shookout.com/sub-processors; and (b) sending an email notification to the Seller's registered email address.

6.4 Objection Right

The Seller may object to the appointment of a new Sub-processor by notifying Company in writing (including email to privacy@shookout.com) within **ten (10) days** of receiving

the notification under Section 6.3, provided the objection is based on reasonable, documented data protection concerns. If the Seller objects:

(a) Company will use reasonable efforts to make available a change in the processing or to suggest a commercially reasonable alternative Sub-processor;

(b) If Company cannot accommodate the Seller's objection within thirty (30) days, the Seller may terminate the Seller Agreement with respect to the services that require the use of the objected-to Sub-processor, without penalty. This termination right is the Seller's sole remedy for an unresolved Sub-processor objection.

6.5 Sub-processor Obligations

Company shall: (a) enter into a written agreement with each Sub-processor imposing data protection obligations no less protective than those set forth in this DPA (Article 28(4) GDPR); (b) ensure that each Sub-processor provides sufficient guarantees to implement appropriate technical and organisational measures; and (c) remain fully liable to the Seller for the performance of each Sub-processor's obligations.

7. INTERNATIONAL DATA TRANSFERS

7.1 Location of Processing

Buyer Data is primarily stored and processed within the EU/EEA. The location of each Sub-processor is identified in Schedule 2.

7.2 Transfer Safeguards

Where the processing of Buyer Data involves a transfer to a country outside the EU/EEA that has not received an adequacy decision from the European Commission, Company shall ensure that such transfer is subject to appropriate safeguards in accordance with Chapter V GDPR, including:

(a) **Standard Contractual Clauses (SCCs):** Commission Implementing Decision (EU) 2021/914, Module 3 (Processor to Sub-processor), supplemented where necessary by additional technical and organisational measures identified through a transfer impact assessment;

(b) **Adequacy Decisions:** Where the European Commission has adopted an adequacy decision for the recipient country (e.g., the EU-U.S. Data Privacy Framework for certified organisations);

(c) **Other Mechanisms:** Binding Corporate Rules, or derogations under Article 49 GDPR where applicable.

7.3 Transfer Impact Assessments

Company conducts transfer impact assessments for Sub-processors located outside the EU/EEA, evaluating the legal regime of the recipient country and implementing supplementary measures where necessary, as described in the Privacy Policy, Section 6.3.

8. ASSISTANCE WITH DATA SUBJECT RIGHTS

8.1 Obligation

Company shall assist the Seller, by appropriate technical and organisational measures, insofar as possible, in fulfilling the Seller's obligation to respond to requests from Data Subjects exercising their rights under Chapter III GDPR (Articles 15-22), including the rights of access, rectification, erasure, restriction, portability, and objection (Article 28(3)(e) GDPR).

8.2 Procedure

(a) If Company receives a request from a Data Subject directly, and the request relates to the Seller's processing of that Data Subject's data (i.e., a Buyer contacting Company about data the Seller controls), Company shall promptly forward the request to the Seller and shall not respond directly unless instructed by the Seller or required by applicable law;

(b) Company shall provide the Seller with such information and cooperation as is reasonably necessary for the Seller to respond to the Data Subject request within the time limits prescribed by the GDPR (one month, extendable by two additional months);

(c) Where technically feasible, Company shall provide self-service tools through the Platform enabling the Seller to access, export, rectify, or delete Buyer Data within the scope of the Seller's processing.

8.3 Costs

Company shall not charge the Seller for routine assistance with Data Subject requests. For requests requiring substantial effort beyond standard Platform functionality (e.g., manual data extraction from archived systems), Company may charge the Seller reasonable costs, notified in advance.

9. BREACH NOTIFICATION

9.1 Notification to Controller

Company shall notify the Seller **without undue delay**, and in any event within **forty-eight (48) hours**, after becoming aware of a Personal Data Breach affecting Buyer Data (Article 28(3)(f) and Article 33(2) GDPR).

9.2 Content of Notification

The notification shall include, to the extent available at the time of notification (with additional information to follow as it becomes available):

(a) A description of the nature of the Personal Data Breach, including where possible: the categories and approximate number of Data Subjects concerned; and the categories and approximate number of personal data records concerned;

(b) The name and contact details of Company's contact point for further information;

(c) A description of the likely consequences of the Personal Data Breach;

(d) A description of the measures taken or proposed to be taken by Company to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

9.3 Controller Obligations

The Seller, as Data Controller, retains responsibility for: (a) determining whether the Personal Data Breach must be notified to the Supervisory Authority under Article 33 GDPR (within 72 hours of becoming aware); (b) determining whether affected Data Subjects must be notified under Article 34 GDPR; and (c) making such notifications. Company shall cooperate with and assist the Seller in these obligations.

9.4 Limitation

Company's obligation under Section 9.1 applies only to Personal Data Breaches affecting Buyer Data processed by Company in its capacity as Data Processor. Breaches affecting personal data processed by Company in its capacity as Data Controller are handled directly by Company in accordance with the Privacy Policy, Section 10.3.

10. DELETION OR RETURN OF DATA

10.1 Upon Termination

Upon termination of the Seller Agreement, Company shall, at the Seller's choice: (a) return all Buyer Data to the Seller in a structured, commonly used, machine-readable format; or (b) delete all Buyer Data and certify such deletion in writing. The Seller must communicate their choice within **thirty (30) days** of termination. If no choice is communicated, Company shall delete the Buyer Data.

10.2 Exceptions

Company may retain Buyer Data beyond termination to the extent required by: (a) applicable EU or Latvian law (including tax, accounting, and AML record-keeping obligations); (b) fulfilment of existing Buyer licences granted prior to termination; (c) resolution of pending disputes, refund claims, or chargebacks; or (d) a lawful hold or preservation request from a regulatory authority or court. Company shall inform the

Seller of any such retention requirement and shall limit the processing to what is strictly necessary for the applicable legal obligation.

10.3 Timeline

Subject to Section 10.2, deletion or return of Buyer Data shall be completed within **sixty (60) days** of the Seller's request or the expiry of the 30-day election period under Section 10.1.

11. AUDITS AND INSPECTIONS

11.1 Audit Right

Company shall make available to the Seller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and this DPA, and shall allow for and contribute to audits, including inspections, conducted by the Seller or an auditor mandated by the Seller (Article 28(3)(h) GDPR).

11.2 Conditions

Audits under Section 11.1 are subject to the following conditions:

(a) **Written notice:** The Seller shall provide at least **thirty (30) days'** written notice of an intended audit, including the proposed scope, duration, and start date;

(b) **Scope:** Audits shall be limited to the processing of Buyer Data under this DPA and shall not extend to Company's processing as Data Controller or to the data of other Sellers;

(c) **Frequency:** The Seller may conduct no more than **one (1) audit per twelve (12) month period**, unless a Personal Data Breach has occurred or a Supervisory Authority has ordered or requested an audit;

(d) **Confidentiality:** The Seller and its auditor(s) shall execute confidentiality undertakings acceptable to Company before the audit. Auditors must be independent and not competitors of Company;

(e) **Disruption:** Audits shall be conducted during normal business hours and in a manner designed to minimise disruption to Company's operations;

(f) **Costs:** The Seller shall bear the costs of the audit. Company shall bear its own internal costs of cooperating with the audit;

(g) **Regulatory audits:** Audits conducted by, or at the request of, a Supervisory Authority are not subject to the frequency or notice limitations above.

11.3 Alternative Compliance Evidence

Company may satisfy audit requests by providing: (a) a copy of the most recent SOC 2 Type II report or ISO 27001 certificate covering the systems used to process Buyer Data; (b) a summary report prepared by an independent third-party auditor covering the matters relevant to this DPA; or (c) responses to a reasonable audit questionnaire provided by the Seller. The Seller retains the right to conduct an on-site audit under Section 11.2 if the alternative evidence is insufficient to address the Seller's documented concerns.

12. LIABILITY AND INDEMNIFICATION

12.1 Allocation

Each party shall be liable for damages caused by processing that infringes the GDPR, in accordance with the allocation of responsibility set forth in Articles 82 and 83 GDPR:

(a) The Seller (Controller) is liable for damages caused by processing that does not comply with the GDPR obligations specifically directed to Controllers;

(b) Company (Processor) is liable for damages caused by processing where it has not complied with GDPR obligations specifically directed to Processors, or where it has acted outside or contrary to lawful instructions of the Seller.

12.2 Indemnification

(a) The Seller shall indemnify and hold harmless Company from and against any claims, damages, losses, costs, and expenses arising from: (i) the Seller's breach of Data Protection Laws; (ii) the Seller's unlawful or unauthorised instructions; (iii) the Seller's failure to fulfil its obligations as Data Controller (including failure to obtain valid legal bases, provide transparency information, or respond to Data Subject requests); or (iv) any processing carried out by the Seller outside the Platform.

(b) Company shall indemnify and hold harmless the Seller from and against any claims, damages, losses, costs, and expenses arising from: (i) Company's breach of this DPA; (ii) Company's processing of Buyer Data outside or contrary to the Seller's lawful instructions; or (iii) a Personal Data Breach caused by Company's failure to implement appropriate security measures under Section 5.

12.3 Liability Cap

Company's total aggregate liability under this DPA shall be subject to the limitation of liability set forth in the Seller Agreement, Section 13, except to the extent such limitation is prohibited by applicable mandatory law.

13. DURATION AND TERMINATION

13.1 Duration

This DPA shall remain in effect for the duration of the Seller Agreement and for as long as Company processes Buyer Data on behalf of the Seller, including any post-termination retention period described in Section 10.2.

13.2 Termination

This DPA terminates automatically upon termination of the Seller Agreement, subject to the surviving provisions of this DPA (Sections 9, 10, 11, 12, and 14).

14. GENERAL PROVISIONS

14.1 Governing Law

This DPA shall be governed by the laws of the Republic of Latvia, without regard to its conflict of law principles, consistent with the Seller Agreement, Section 14.

14.2 Severability

If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions shall remain in full force. The invalid provision shall be replaced by a valid provision that achieves, to the extent possible, the original purpose.

14.3 Amendments

This DPA may be amended by Company to reflect changes in Data Protection Laws, Supervisory Authority guidance, or Company's processing practices, upon thirty (30) days' notice to the Seller (fifteen (15) days for changes required by law). The Seller's continued use of the Platform after the effective date of an amendment constitutes acceptance.

14.4 Entire Agreement

This DPA, together with the Schedules hereto, the Seller Agreement, the Privacy Policy, and the Terms of Service, constitutes the entire agreement between the parties regarding the processing of Buyer Data.

14.5 Contact

For questions regarding this DPA: **privacy@shookout.com**

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