DATA PROCESSING ADDENDUM

Last Updated: December 13, 2023

This Data Processing Addendum (the "**Addendum**"), including its Exhibits, forms a part of the UserGems Order Form and Terms and Conditions, Evaluation Agreement or other written agreement entered into by the Parties (the "**Agreement**") between ShelfFlip, Inc. d/b/a UserGems ("**Company**") and Customer (Customer together with Company, the "**Parties**").

1. Subject Matter and Duration

a) **Subject Matter.** This Addendum reflects the Parties' commitment to abide by Data Protection Laws concerning the Processing of Customer Personal Data in connection with Company's execution of the Agreement. All capitalized terms that are not expressly defined in this Addendum will have the meanings given to them in the Agreement. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in the Standard Contractual Clauses; (2) the terms of this Addendum; and (3) the Agreement For purposes of Data Protection Laws, Company is the "data processor" and Customer is the "data controller" with respect to Customer Personal Data.

b) **Duration and Survival.** This Addendum will become legally binding upon the effective date of the Agreement. Company will Process Customer Personal Data until the relationship terminates as specified in the Agreement. Company's obligations and Customer's rights under this Addendum will continue in effect so long as Company Processes Customer Personal Data.

2. Definitions.

For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

a) **"Authorized Persons"** means (i) personnel of Company and (ii) Third Parties engaged by Company in accordance with Sections 3(b)-(d) of this Addendum.

b) "**Customer"** means the entity that entered into the Agreement.

c) "**Customer Personal Data**" means Personal Data Processed by Company on behalf of Customer. The Customer Personal Data and the specific uses of the Customer Personal Data are detailed in **Exhibit A** attached hereto.

d) "**Data Protection Laws**" means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of Personal Data including: (i) California Consumer Privacy Act (Cal. Civ. Code §§ 1798.100 *et seq*.) as amended by the California Privacy Rights Act ("**CPRA**"); (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**") and the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**") (together, collectively, the "**GDPR**"); (iii) the Swiss Federal Act on Data Protection; (iv) the UK Data Protection Act 2018; (v) the Privacy and Electronic Communications (EC Directive) Regulations 2003; and (vi) the Virginia Consumer Data Protection Act (Va. Code §§ 59.1-575 *et seq*.) ("**VCDPA**"); in each case, as updated, amended or replaced from time to time.

e) "**EU SCCs**" means the standard contractual clauses which have been approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of Customer Personal Data to countries not otherwise recognized as offering an adequate level of protection for Customer Personal Data by the European Commission (as amended and updated from time to time), as modified by Section 4(c) of this Addendum.

f) "**ex-EEA transfer**" means the transfer of Customer Personal Data, which is processed in accordance with the GDPR, from Customer to Company (or its premises) outside the European Economic Area (the "**EEA**"), and such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.

g) "**ex-UK Transfer**" means the transfer of Customer Personal Data covered by Chapter V of the UK GDPR, which is processed in accordance with the UK GDPR and the Data Protection Act 2018, from Customer to Company (or its premises) outside the United Kingdom (the "**UK**"), and such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the Data Protection Act 2018.

h) "**Personal Data**" means any information relating to: (i) an identified or identifiable natural person (e.g., a Data Subject or Consumer); (ii) a household under CPRA; and/or (iii) any elements that constitute personal information or a similar construct under applicable law, in each case, where such information is maintained on behalf of the Customer by the Company within its Services environment and is protected similarly as personal data, personal information, or personally identifiable information under Data Protection Laws and Regulations.

i) "**Process**," "**Processes**," "**Processing**," "**Processed**" means any operation or set of operations which is performed on data or sets of data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

j) "**Security Incident(s)**" means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data.

k) "**Services**" means any and all products and services that Company provides and/or performs under the Agreement.

l) **"Standard Contractual Clauses"** means the EU SCCs and the UK SCCs.

m) "**Subprocessor(s)**" means Company's authorized contractors, agents, vendors and third-party service providers (i.e., sub-processors) that Process Customer Personal Data.

n) **"UK Addendum"** means the addendum attached hereto as Exhibit D.

o) "**UK SCCs"** means the EU SCCs, as amended by the UK Addendum.

3. Data Use and Processing.

a) Documented Instructions. Company and its Subprocessors shall Process Customer Personal Data solely for the purpose of providing the Services to Customer, and solely to the extent necessary to provide the Services to Customer, in each case, in accordance with the Agreement, this Addendum and Data Protection Laws. Company will, unless legally prohibited from doing so, inform Customer in writing if it reasonably believes that there is a conflict between Customer's instructions and applicable law.

b) Authorization to Use Subprocessor. To the extent necessary to fulfill Company's contractual obligations under the Agreement or any Order Form, Customer hereby authorizes Company to engage Subprocessors. Any Subprocessor Processing of Customer Personal Data shall be consistent with Customer's documented instructions and comply with Data Protection Laws. Prior to engaging any Subprocessors, Company shall carry out appropriate due diligence on the Subprocessor and enter into a written agreement with each Subprocessor which provides for sufficient guarantees from the Subprocessor to implement appropriate technical and organizational measures containing substantially the same level of data protection obligations with respect to the protection of Customer Personal Data such that the processing will meet the requirements of applicable Data Protection Laws.

c) Company and Subprocessor Compliance. Company shall (i) enter into a written agreement with Subprocessors regarding such Subprocessor's Processing of Customer Personal Data that imposes on such Subprocessors (and their sub-processors) confidentiality obligations and data protection and security requirements for Customer Personal Data that are at least as restrictive as the obligations in this Addendum; and (ii) remain responsible to Customer for Company's Subprocessors' (and their sub-processors if applicable) failure to perform their obligations with respect to the Processing of Customer Personal Data. Customer approves the Subprocessors referenced in Exhibit B of this DPA.

d) Right to Object to Subprocessor. A list of approved Subprocessors is set forth on **Exhibit A**. Prior to engaging any new Subprocessors that Process Customer Personal Data, Company will notify Customer via email and allow Customer 30 days to object. If Customer has, in good faith, reasonable objections to the appointment of any new

Subprocessor, the Parties will work together in good faith to resolve the grounds for the objection for no less than 30 days, and failing any such resolution, Customer may terminate the part of the Services performed under the Agreement that cannot be performed by Company without use of the objectionable Subprocessor. Company shall refund any pre-paid fees to Customer in respect of the terminated part of the Services.

e) Personal Data Inquiries and Requests. Company agrees to provide reasonable assistance and comply with all reasonable instructions from Customer related to any requests from individuals exercising their rights in Customer Personal Data granted to them under Data Protection Laws.

f) CPRA.

(i) Definitions

(1) For purposes of this Section A, the terms "Business," "Business Purpose," "Commercial Purpose," "Consumer," "Personal Information," "Processing," "Sell," "Service Provider," "Share," and "Verifiable Consumer Request" shall have the meanings set forth in the CPRA.

(2) All references to "Personal Data," "Controller," "Processor," and "Data Subject" in this Addendum shall be deemed to be references to "Personal Information," "Business," "Service Provider," and "Consumer" as defined in the CPRA.

(ii) Obligations

(1) With respect to Customer Personal Data, the parties acknowledge and agree that Customer is a Business and Company is a Service Provider for the purposes of the CPRA (to the extent it applies) and Company is receiving Customer Personal Data from Customer in order to provide the Services pursuant to the Agreement, which constitutes a Business Purpose.

(2) Customer shall disclose Customer Personal Data to Company only for the limited and specified purposes described in **Exhibit A** to this Addendum.

(3) Company shall not Sell or Share Customer Personal Data.

(4) Company shall not retain, use, or disclose Customer Personal Data for any purpose, including a Commercial Purpose, other than as necessary for the specific purpose of performing the Services for Customer pursuant to the Agreement, or as otherwise set forth in the Agreement or as permitted by the CPRA.

(5) Company shall not retain, use, or disclose Customer Personal Data outside of the direct business relationship between Company and Customer, except where and to the extent permitted by the CPRA.

(6) Company shall notify Customer if it makes a determination that it can no longer meet its obligations under the CPRA.

(7) Except and to the extent permitted by the CPRA, Company will not combine Customer Personal Data with Personal Information that it receives from, or on behalf of, another party, or that it collects from its own interaction with the Consumer.

(8) Company shall comply with all obligations applicable to Service Providers under the CPRA, including by providing Customer Personal Data the level of privacy protection required by CPRA.

(9) In the event that Company engages a new sub-processor to assist Company in providing the Services to Customer under the Agreement, Company shall: (i) notify Customer of such engagement via the notification mechanism described in Section 3(d) of this Addendum at least ten (10) days before enabling a new Sub-Processor; and (ii) enter into a written contract with the Sub-processor requiring Sub-processor to observe all of the applicable requirements set forth in the CPRA.

(iii) Consumer Rights

(1) Company shall assist Customer in responding to Verifiable Consumer Requests to exercise the Consumer's rights under the CPRA as set forth in Section 7 of this Addendum.

(iv) Audit Rights

(1) To the extent required by CPRA, Company shall allow Customer to conduct inspections or audits in accordance with Sections 8.3 and 8.4 of this Addendum.

g) VCDPA

(i) Definitions

(1) For purposes of this Section B, the terms "Consumer," "Controller," "Personal data," "Processing," and "Processor" shall have the meanings set forth in the VCDPA.

(2) All references to "Data Subject" in this Addendum shall be deemed to be references to "Consumer" as defined in the VCDPA.

(ii) Obligations

(1) With respect to Customer Personal Data, the parties acknowledge and agree that Customer is a Controller and Company is a Processor for the purposes of the VCDPA (to extent it applies).

(2) The nature, purpose, and duration of Processing, as well as the types of Personal Data and categories of Consumers are described in **Exhibit A** to this Addendum.

(3) Company shall adhere to Customer's instructions with respect to the Processing of Customer Personal Data and shall assist Customer in meeting its obligations under the VCDPA by:

a. Assisting Customer in responding to Consumer rights requests under the VCDPA as set forth in Section 7 of this Addendum;

b. Complying with Section 5 of this Addendum with respect to Customer Personal Data provided by Customer;

c. In the event of a Security Incident, providing information sufficient to enable Customer to meet its obligations pursuant to Va. Code § 18.2-186.6; and

d. Providing information sufficient to enable Customer to conduct and document data protection assessments to the extent required by VCDPA.

(4) Company shall maintain the confidentiality of Customer Personal Data provided by Customer and require that each person Processing such Personal Data be subject to a duty of confidentiality with respect to such Processing;

(5) Upon Customer's written request, Company shall delete or return all Customer Personal Data provided by Customer in accordance with Section 9(b) of this Addendum, unless retention of such Customer Personal Data is required or authorized by law or this Addendum and/or Agreement.

(6) In the event that Company engages any other person a new Sub-processor to assist Company in providing the Services to Customer under the Agreement, Company shall enter into a written contract with the Sub-processor requiring Sub-processor to observe all of the applicable requirements of a Processor set forth in the VCDPA.

(iii) Audit Rights

(1) Upon Customer’s written request at reasonable intervals, Company shall, as set forth in Sections 8 of this Addendum, (i) make available to Customer all information in its possession that is reasonably necessary to demonstrate Company’s compliance with its obligations under the VCDPA; and (ii) allow and cooperate with reasonable inspections or audits as required under the VCDPA.

4. **Cross-Border Transfers of Personal Data**.

a) If Company transfers Customer Personal Data protected under this Addendum outside the EEA to a jurisdiction for which the European Commission has not issued an adequacy decision (each, a “**Restricted Transfer**”), Company represents, warrants, and covenants that (i) Restricted Transfers by Company may only be made to Authorized Persons; (ii) any Restricted Transfer conducted by Company or any Authorized Person shall be undertaken in accordance with the appropriate Standard Contractual Clauses entered into in accordance with Applicable Data Protection Laws; and (iii) that each Restricted Transfer will be made after appropriate safeguards have been implemented for the Restricted Transfer of Customer Personal Data in accordance with Applicable Data Protection Laws.

b) Ex-EEA Transfers. The parties agree that ex-EEA Transfers are made pursuant to the EU SCCs, which are deemed entered into (and incorporated into this Addendum by this reference) and completed under Module Two (Controller to Processor) of the EU SCCs.

c) For each module, where applicable the following applies:

(i) The optional docking clause in Clause 7 does not apply;

(ii) In Clause 9, Option 2 (general prior authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in 3(d) of this Addendum;

(iii) In Clause 11, the optional language does not apply;

(iv) All square brackets in Clause 13 are hereby removed;

(v) In Clause 17 (Option 1), the EU SCCs will be governed by Irish law;

(vi) In Clause 18(b), disputes will be resolved before the courts of Ireland;

(vii) Exhibit B to this Addendum contains the information required in Annex I of the EU SCCs;

(viii) Exhibit C to this Addendum contains the information required in Annex II of the EU SCCs; and

(ix) By entering into this Addendum, the Parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.

d) Ex-UK Transfers. The Parties agree that ex-UK Transfers are made pursuant to the UK SCCs, which are deemed entered into and incorporated into this Addendum by reference, and amended and completed in accordance with the UK Addendum, which is incorporated herein as Exhibit D of this Addendum.

e) Transfers from Switzerland. The Parties agree that transfers from Switzerland are made pursuant to the EU SCCs with the following modifications:

(i) The terms “General Data Protection Regulation” or “Regulation (EU) 2016/679” as utilized in the EU SCCs shall be interpreted to include the Federal Act on Data Protection of 19 June 1992 (the “**FADP**,” and as revised as of 25 September 2020, the “**Revised FADP**”) with respect to data transfers subject to the FADP.

(ii) The terms of the EU SCCs shall be interpreted to protect the data of legal entities until the effective date of the Revised FADP.

(iii) Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information

Commissioner of Switzerland shall have authority over data transfers governed by the FADP and the appropriate EU supervisory authority shall have authority over data transfers governed by the GDPR. Subject to the foregoing, all other requirements of Clause 13 shall be observed.

(iv) The term "EU Member State" as utilized in the EU SCCs shall not be interpreted in such a way as to exclude data subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

f) Supplementary Measures. In respect of any ex-EEA Transfer or ex-UK Transfer, the following supplementary measures shall apply:

(i) As of the date of this Addendum, Company has not received any formal legal requests from any government intelligence or security service/agencies in the country to which the Customer Personal Data is being exported, for access to (or for copies of) Personal Data ("**Government Agency Requests**");

(ii) If, after the date of this Addendum, Company receives any Government Agency Requests, Company shall attempt to redirect the law enforcement or government agency to request that data directly from Customer. As part of this effort, Company may provide Customer's basic contact information to the government agency. If compelled to disclose Company's Personal Data to a law enforcement or government agency, Company shall give Customer reasonable notice of the demand and cooperate to allow Customer to seek a protective order or other appropriate remedy unless Company is legally prohibited from doing so. Company shall not voluntarily disclose Customer Personal Data to any law enforcement or government agency. Customer and Company shall (as soon as reasonably practicable) discuss and determine whether all or any transfers of Customer Personal Data pursuant to this Addendum should be suspended in the light of such Government Agency Requests; and

(iii) The Customer and Company will meet regularly to consider whether:

(1) the protection afforded by the laws of the country of Company to data subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in the EEA or the UK, whichever the case may be;

(2) additional measures are reasonably necessary to enable the transfer to be compliant with the Applicable Data Protection Laws; and

(3) it is still appropriate for Customer Personal Data to be transferred to Company, taking into account all relevant information available to the Parties, together with guidance provided by the supervisory authorities.

(iv) If Data Protection Laws require the Customer to execute the Standard Contractual Clauses applicable to a particular transfer of Customer Personal Data to Company as a separate agreement, Company shall, on request of the Customer, promptly execute such Standard Contractual Clauses incorporating such amendments as may reasonably be required by the Customer to reflect the applicable appendices and annexes, the details of the transfer and the requirements of the relevant Applicable Data Protection Laws.

(v) If either (i) any of the means of legitimizing transfers of Customer Personal Data outside of the EEA or UK set forth in this Addendum cease to be valid or (ii) any supervisory authority requires transfers of Customer Personal Data pursuant to those means to be suspended, Company agrees to amend the means of legitimizing transfers or alternative arrangements with Customer, with effect from the date set out in such notice, amend or put in place alternative arrangements in respect of such transfers, as required by Applicable Data Protection Laws.

5. **Information Security Program**.

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 natural persons, Company shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing Customer Personal Data. **Exhibit C** sets forth additional information about Company's technical and organizational security measures.

6. **Security Incidents**.

a) Security Incident Procedure. Company will deploy and follow policies and procedures to detect, respond to, and otherwise address Security Incidents including procedures to (i) identify and respond to reasonably suspected or known Security Incidents, mitigate harmful effects of Security Incidents, document Security Incidents and their outcomes, and (ii) restore the availability or access to Customer Personal Data in a timely manner.

b) Notice. Company agrees to provide prompt written notice without undue delay (and in any event within 48 hours) to Customer's Designated POC if it verifies that a Security Incident has taken place. Such notice will include all available details required under Data Protection Laws for Customer to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident.

7. **Rights of Data Subjects**

a) Company shall, to the extent permitted by law, notify Customer upon receipt of a request by a Data Subject to exercise the Data Subject's rights of: access, rectification, erasure, data portability, restriction or cessation of processing, withdrawal of consent to processing, and/or objection to being subject to processing that constitutes automated decision-making (such requests individually and collectively "**Data Subject Request(s)**"). If Company receives a Data Subject Request in relation to Customer Personal Data, Company will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. Customer is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of processing, or withdrawal of consent to processing of any Personal Data are communicated to Company, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject.

b) Company shall, at the request of the Customer, and taking into account the nature of the processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Customer in complying with Customer's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, *provided that* (i) Customer is itself unable to respond without Company's assistance and (ii) Company is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

8. **Audits**.

a) Right to Audit; Permitted Audits. In addition to any other audit rights described in the Agreement, Customer and its regulators shall have the right, upon at least 30 days' prior written notice, to an on-site audit (at a date and time mutually agreed upon) of Company's architecture, systems, policies and procedures relevant to the security and integrity of Customer Personal Data, or as otherwise required by a governmental regulator: (i) following any notice from Company to Customer of an actual or reasonably suspected Security Incident involving Customer Personal Data; (ii) as required by governmental regulators; and (iii) for compliance purposes, once annually.

b) Audit Terms. Any audits described in this Section shall be: (i) conducted by Customer or its regulator, or through a third-party independent contractor selected by one of these parties and paid for by Customer; (ii) conducted during reasonable times; (iii) to the extent possible, conducted upon reasonable advance notice (but no less than 30 days' prior notice) to Company; and (iv) of reasonable duration and shall not unreasonably interfere with Company's day-to-day operations.

c) Third Parties Auditor. In the event that Customer conducts an audit through a third party independent auditor or a third party accompanies Customer or participates in such audit, such third party shall be required to enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect Company's and Company's customers' confidential and proprietary information. For the avoidance of doubt, regulators shall not be required to enter into a non-disclosure agreement.

d) Audit Results. Upon Company's request, after conducting an audit, Customer shall notify Company of the manner in which Company does not comply with any of the applicable security, confidentiality or privacy obligations or Data Protection Laws herein. Upon such notice, Company shall make any reasonably necessary changes to ensure compliance with such obligations at its own expense and without unreasonable delay and shall notify Customer when such changes are complete. Notwithstanding anything to the contrary in the Agreement, Customer may conduct a follow-up audit within six 6 months of Company's notice of completion of any necessary changes. To the extent that a Company audit and/or Customer audit identifies any material security vulnerabilities, Company shall remediate those vulnerabilities within a commercially reasonable amount of time of the completion of the applicable audit, unless any vulnerability by its nature cannot be remedied within such time, in which case the remediation must be completed within a mutually agreed upon time.

9. Data Storage and Deletion.

a) Data Storage. Company will not store or retain any Customer Personal Data except as necessary to perform the Services under the Agreement.

b) Data Deletion. Company will abide by the following with respect to deletion of Customer Personal Data:

(i) Within a reasonable amount of time after the Agreement's expiration or termination, or sooner if requested by Customer, Company will securely destroy (per subsection (iii) below) all copies of Customer Personal Data (including automatically created archival copies).

(ii) Upon Customer's request, Company will promptly return to Customer a copy of all Customer Personal Data within 30 days and, if Customer also requests deletion of the Customer Personal Data, will carry that out as set forth above.

(iii) Customer Personal Data shall be disposed of in a method that prevents any recovery of the data in accordance with industry best practices for shredding of physical documents and wiping of electronic media.

(iv) Upon Customer's request, Company will provide a "Certificate of Deletion" certifying that Company has deleted all Customer Personal Data. Company will provide the "Certificate of Deletion" within 30 days of Customer's request.

10. Limitation of Liability.

Each Party's liability, including the liability of all of its affiliates, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference to the liability of a Party means the total liability of that Party and all of its affiliates under the Agreement and all DPAs together.

11. Contact Information.

a) The Customer Designated POC shall be the contact specified for the Data Exporter in Exhibit B.

Exhibit A

1.1 Subject Matter of Processing	The subject matter of Processing is the Services pursuant to the Agreement.
1.2 Duration of Processing	The Processing will continue until the expiration or termination of the Agreement.
1.3 Categories of Data Subjects	May include, but is not limited to, the following: • Prospects, leads, champions, and current and past customers of Customer (who may be natural persons) • Employees or contact persons of Customer's prospects, leads, champions and current and past customers • Customer's users authorized by Customer to use the Services
1.4 Nature and Purpose of Processing	The purpose of Processing of Customer Personal Data by Company is the performance of the Services pursuant to the Agreement.
1.5 Types of Personal Data	May include, but is not limited to, the following: ● First and last name, ● Title ● Position ● Employer ● Email Address
1.6 Sensitive Personal Data or Special Categories of Data	None.

Exhibit B

The following includes the information required by Annex I and Annex III of the EU SCCs, and Table 1, Annex 1A, and Annex 1B of the UK Addendum.

1. **The Parties**

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: ... As designated by Customer in the Order Form to the Agreement

Address: ... As designated by Customer in the Order Form to the Agreement

Contact person's name, position and contact details: As designated by Customer in the Order Form to the Agreement

Activities relevant to the data transferred under these Clauses: The provision of the Services under the Agreement.

Signature and date: By entering into this Addendum, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date of the Agreement.

Role (controller/processor): Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: ShelfFlip, Inc. d/b/a UserGems

Trading Name (if different): N/A

Address: 2443 Fillmore St. #308-3416, San Francisco, CA 94115

Official Registration Number (if any) (company number or similar identifier): N/A

Contact person's name, position and contact details: Stephan Kletzl, DPO, stephan@usergems.com

Activities relevant to the data transferred under these Clauses: The provision of the Services under the Agreement.

Signature and date: ... By entering into this Addendum, Data Importer is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date of the Agreement.

Role (controller/processor): Processor

2. **Description of the Transfer**

Data Subjects	As described in Exhibit A of the Addendum.
Categories of Personal Data	As described in Exhibit A of the Addendum.
Special Category Personal Data (if applicable)	None.

Nature of the Processing	As provided in Exhibit A of the Addendum.
Purposes of Processing	As described in Exhibit A of the Addendum.
Duration of Processing and Retention (or the criteria to determine such period)	As described in Exhibit A of the Addendum.
Frequency of the transfer	As necessary to perform the Services.
Recipients of Personal Data Transferred to the Data Importer	As described in Section 4 below and as supplemented by any Third Parties added in accordance with Section 3(d) of the Addendum.

3. Competent Supervisory Authority

The supervisory authority shall be the supervisory authority of the Customer, as determined in accordance with Clause 13 of the EU SCCs. The supervisory authority for the purposes of the UK Addendum shall be the UK Information Commissioner's Officer.

4. List of Authorized Subprocessors

Name of Authorized Subcontractor (Sub-processor)	Description of processing	Country in which subprocessing will take place
Azure by Microsoft Corporation	Hosting Services	US
AWS by Amazon, Inc.	Hosting Services	US

Exhibit C

Description of the Technical and Organisational Security Measures implemented by the Data Importer

The following includes the information required by Annex II of the EU SCCs and Appendix II of the UK Addendum.

1. Adopting and implementing reasonable policies and standards related to security;

2. Assigning responsibility for information security management;

3. Devoting adequate personnel resources to information security;

4. Conducting appropriate background checks and requiring employees, vendors and others with access to the Personal Data to enter into written confidentiality agreements;

5. Conducting training to make employees and others with access to Personal Data aware of information security risks and to enhance compliance with its policies related to data protection;

6. Preventing unauthorized access to Personal Data through the use, as appropriate, of physical and logical entry controls, secure areas for data processing, procedures for monitoring the use of data processing, audit trails, use of secure passwords, network intrusion detection technology, authentication technology, secure log-on procedures, and virus protection, on-going monitoring of compliance with its policies related to data protection, including:

    6.1 Appropriate physical access control measures (e.g., access ID cards, card readers, desk officers, alarm systems, motion detectors, burglar alarms, video surveillance and exterior security);

    6.2 Denial-of-use control measures to prevent unauthorized use of data protection systems (e.g., automatically enforced password complexity and change requirements, firewalls, etc.);

    6.3 Requirements-driven authorization scheme and access rights, and monitoring and logging of system access to identify unauthorized Processing of Personal Data by Authorized Personnel;

    6.4 Data transmission control measures to ensure that Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission, transport or storage on data media, and transfer and receipt records.

    6.5 Encryption of any Personal Data transmitted electronically to a person outside Vendor's IT system, transmitted over a wireless network, or stored on any movable or portable media.

    6.6 Data entry control measures to ensure that it is possible to check and establish whether and by whom Personal Data has been input into data processing systems, modified, or removed;

    6.7 Subcontractor supervision measures to ensure compliance with the Addendum;

    6.8 Measures to ensure that Personal Data is protected from accidental destruction or loss including, as appropriate and without limitation, data backup, retention and secure destruction policies; secure offsite storage of data sufficient for disaster recovery; and disaster recovery programs; and

    6.9 Measures to ensure that data collected for different purposes can be processed separately including, as appropriate, physical or adequate logical separation of client data.

Exhibit D
UK Addendum

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Part 1: Tables

Table 1: Parties

Start Date	This UK Addendum shall have the same effective date as the Addendum.	
The Parties	Exporter	Importer
Parties' Details	Customer	Company
Key Contact	*See* Exhibit B of this Addendum	*See* Exhibit B of this Addendum

Table 2: Selected SCCs, Modules and Selected Clauses

EU SCCs	The Version of the Approved EU SCCs which this UK Addendum is appended to as defined in the Addendum and completed by Sections 4(c) and 4(d) of the Addendum.

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this UK Addendum is set out in:

Annex 1A: List of Parties	As per Table 1 above
Annex 2B: Description of Transfer	*See* Exhibit B of this Addendum
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	*See* Exhibit C of this Addendum
Annex III: List of Sub processors (Modules 2 and 3 only):	*See* Exhibit B of this Addendum

Table 4: Ending this UK Addendum when the Approved UK Addendum Changes

Ending this UK Addendum when the Approved UK Addendum changes	☐ Importer ☒ Exporter ☐ Neither Party

Entering into this UK Addendum:

1. Each party agrees to be bound by the terms and conditions set out in this UK Addendum, in exchange for the other party also agreeing to be bound by this UK Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making ex-UK Transfers, the Parties may enter into this UK Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this UK Addendum. Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this UK Addendum

3. Where this UK Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

UK Addendum	means this International Data Transfer Addendum incorporating the EU SCCs, attached to the Addendum as Exhibit D.
EU SCCs	means the version(s) of the Approved EU SCCs which this UK Addendum is appended to,

	as set out in Table 2, including the Appendix Information
Appendix Information	shall be as set out in Table 3
Appropriate Safeguards	means the standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making an ex-UK Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved UK Addendum	means the template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as may be revised under Section 18 of the UK Addendum.
Approved EU SCCs	means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time).
ICO	means the Information Commissioner of the United Kingdom.
ex-UK Transfer	shall have the same definition as set forth in the Addendum .
UK	means the United Kingdom of Great Britain and Northern Ireland
UK Data Protection Laws	means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	shall have the definition set forth in the Addendum.

4. The UK Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the UK Addendum amend the Approved EU SCCs in any way which is not permitted under the Approved EU SCCs or the Approved UK Addendum, such amendment(s) will not be incorporated in the UK Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and the UK Addendum, UK Data Protection Laws applies.

7. If the meaning of the UK Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after the UK Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for ex-UK Transfers, the hierarchy in Section 10 below will prevail.

10. Where there is any inconsistency or conflict between the Approved UK Addendum and the EU SCCs (as applicable), the Approved UK Addendum overrides the EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved UK Addendum.

11. Where this UK Addendum incorporates EU SCCs which have been entered into to protect ex-EU Transfers subject to the GDPR, then the parties acknowledge that nothing in the UK Addendum impacts those EU SCCs.

Incorporation and Changes to the EU SCCs:

12. This UK Addendum incorporates the EU SCCs which are amended to the extent necessary so that:

a) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b) Sections 9 to 11 above override Clause 5 (Hierarchy) of the EU SCCs; and

c) the UK Addendum (including the EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales**.**

13. Unless the parties have agreed alternative amendments which meet the requirements of Section 12 of this UK Addendum, the provisions of Section 15 of this UK Addendum will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 of this UK Addendum may be made.

15. The following amendments to the EU SCCs (for the purpose of Section 12 of this UK Addendum) are made:

a) References to the "Clauses" means this UK Addendum, incorporating the EU SCCs;

b) In Clause 2, delete the words: "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679",

c) Clause 6 (Description of the transfer(s)) is replaced with: "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d) Clause 8.7(i) of Module 1 is replaced with: "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e) Clause 8.8(i) of Modules 2 and 3 is replaced with: "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f) References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of

"Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g) References to Regulation (EU) 2018/1725 are removed;

h) References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i) The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j) Clause 13(a) and Part C of Annex I are not used;

k) The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l) In Clause 16(e), subsection (i) is replaced with: "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m) Clause 17 is replaced with: "These Clauses are governed by the laws of England and Wales.";

n) Clause 18 is replaced with: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The parties agree to submit themselves to the jurisdiction of such courts."; and

o) The footnotes to the Approved EU SCCs do not form part of the UK Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to the UK Addendum

16. The parties may agree to change Clauses 17 and/or 18 of the EU SCCs to refer to the laws and/or courts of Scotland and Northern Ireland.

17. If the parties wish to change the format of the information included in Part 1: Tables of the Approved UK Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved UK Addendum which:

a) makes reasonable and proportionate changes to the Approved UK Addendum, including correcting errors in the Approved UK Addendum; and/or

b) reflects changes to UK Data Protection Laws;

The revised Approved UK Addendum will specify the start date from which the changes to the Approved UK Addendum are effective and whether the parties need to review this UK Addendum including the Appendix Information. This UK Addendum is automatically amended as set out in the revised Approved UK Addendum from the start date specified.

19. If the ICO issues a revised Approved UK Addendum under Section 18 of this UK Addendum, if a party will as a direct result of the changes in the Approved UK Addendum have a substantial, disproportionate and demonstrable increase in:

c) its direct costs of performing its obligations under the UK Addendum; and/or

d) its risk under the UK Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that party may end this UK Addendum at the end of a reasonable notice period, by providing written notice for that period to the other party before the start date of the revised Approved UK Addendum.

20. The parties do not need the consent of any third party to make changes to this UK Addendum, but any changes must be made in accordance with its terms.

Previous Data Processing Addendums:

- Effective as of November 2023
- Effective as of May 2022
- Effective as of September 2021
- Effective as of September 2020