SCARF SYSTEMS, INC.
DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") and the schedules to this DPA apply to the Processing of Customer Personal Data on behalf of Customer (the "**Customer**") in order to provide Services Customer may have ordered from Company as set forth in the applicable agreement between Customer and Company (the "**Agreement**"). In the event of a conflict between the terms of this DPA and the terms of the Agreement, the terms of this DPA will prevail, unless the Agreement explicitly provides otherwise, identifying the relevant portion of the DPA that it is superseding. For purposes of this DPA, Customer and Company agree that Customer may be a Data Controller of Customer Personal Data and Company may be a Data Processor of such data, except when Customer acts as a Data Processor of Customer Personal Data, in which case Company is a subprocessor. In the course of providing Services to Customer pursuant to the Agreement, Company may Process Customer Personal Data on behalf of Customer. Company agrees to comply with the following provisions with respect to any Customer Personal Data submitted by or on behalf of Customer for the Services or collected and Processed through the Services.

1. **DEFINITIONS.** Any capitalized term used but not defined in this DPA has the meaning provided to it in the Agreement or in the Applicable Data Protection Law.
    a. "**Applicable Data Protection Law**" refers to all laws and regulations applicable to Company's Processing of Personal Data under the Agreement including, without limitation, the GDPR.
    b. "**Customer Personal Data**" means any Personal Data Processed by Company on behalf of Customer pursuant to or in connection with the Agreement, with the explicit exclusions of any information provided by Customer to Company in connection with the creation or administration of its account(s) or billing information for the Services.
    c. "**CCPA**" means the California Consumer Privacy Act 2018 Cal. Civ. Code 1798.100 et seq., including any amendments and any implementing regulations thereto that become effective on or after the effective date of this Data Processing Addendum.
    d. "**GDPR**" means the EU General Data Protection Regulation 2016/679 and to the extent the GDPR is no longer applicable in the United Kingdom, any implementing legislation or legislation having equivalent effect in the United Kingdom. References to "Articles" or "Chapters" of the GDPR will be construed accordingly.
    e. "**Personal Data**" shall have the meaning ascribed to it, or to substantially similar phrases, in Applicable Data Protection Law.
    f. "**SCCs**" means the standard contractual clauses for international transfers annexed to the European Commission's commission implementing decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, published on June 4, 2021, including as incorporated into the UK Transfer Addendum, if applicable
    g. "**Services**" means those services and activities to be supplied to or carried out by or on behalf of Company for Customer pursuant to the Agreement.
    h. "**Subprocessor**" means any third party appointed by or on behalf of Company to Process Customer Personal Data.
    i. "**Transfer**" means the transfer of Customer Personal Data outside the United Kingdom or EU/European Economic Area ("**EEA**").
    j. "**UK GDPR**" means the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018.
    k. "**UK Transfer Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, published by the UK Information Commissioner's Office on March 21, 2022.
2. **PROCESSING OF CUSTOMER PERSONAL DATA.** Company will in the course of providing Services, including with regard to Transfers of Personal Data to a third country, Process Customer Personal Data only on behalf of and under the documented Instructions of Customer unless required to do so otherwise under Applicable Data Protection Law; in such a case, Company will inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. Schedule 1 specifies the duration of the Processing, the nature and purpose of the Processing, and the types of Personal Data and categories of data subjects. Customer is responsible for ensuring that (a) it has complied, and will continue to comply, with Applicable Data Protection Law in its use of the Services and its own Processing of Customer Personal Data and (b) it has, and will continue to have, the right to Transfer, or provide access to, Customer Personal Data to Company for Processing in accordance with the terms of the Agreement and this DPA. Customer appoints Company as a Data Processor to Process Customer Personal Data on behalf of, and in accordance with, Customer's instructions (a) as set forth in the Agreement, this DPA, and as otherwise necessary to provide the Services to Customer (which may include investigating security incidents and preventing spam or fraudulent activity,

and detecting and preventing network exploits and abuse); (b) as necessary to comply with applicable law; and (c) as otherwise agreed in writing by the parties ("**Permitted Purposes**"). Customer will ensure that its instructions comply with Applicable Data Protection Law. Customer acknowledges that Company is not responsible for determining which laws are applicable to Customer's business nor whether Company's provision of the Services meets or will meet the requirements of such laws. Customer will ensure that Company's Processing of Customer Personal Data, when done in accordance with Customer's instructions, will not cause Company to violate any applicable law, regulation, or rule, including Applicable Data Protection Law. Company will inform Customer if it becomes aware or reasonably believes that Customer's data Processing instructions violate any applicable law, regulation, or rule, including Applicable Data Protection Law. Customer is responsible for ensuring that suitable safeguards are in place prior to transmitting or Processing, or prior to permitting Customer's end users to transmit or Process, any Personal Data via the Services. Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Customer Personal Data, to the extent applicable under the CCPA.

3. **SECURITY.** Company will ensure that its employees (including subprocessors) who Process Customer Personal Data for Company or who have access to Customer Personal Data are authorized to Process this Personal Data, and have undertaken to, or are contractually bound to observe confidentiality. 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 will in relation to Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as required by Art. 32 GDPR. As appropriate, this may include: the pseudonymization and encryption of Personal Data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; and the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident. In assessing the appropriate level of security, Company will take into account the risks presented by Processing, in particular from a Personal Data Breach. Company's technical and organizational measures are subject to technical advancements and development. Company will use commercially reasonable efforts to regularly test, assess and evaluate the effectiveness of technical and organizational measures to reasonably ensure the security of the Processing.
4. **SUBPROCESSING.** Customer agrees that Company may use Subprocessors to fulfill its contractual obligations under the Agreement. Information about Subprocessors, including their functions and locations, is available at: https://about.scarf.sh/subprocessors (as may be updated by Provider from time to time) or such other website address as Provider may provide to Customer from time to time (the "**Subprocessor Site**"). Where Company authorizes any Subprocessor as described in this Section 4, Company agrees to impose data protection terms on any Subprocessor it appoints that require it to protect Customer Personal Data to the standard required by Applicable Data Protection Law. Customer provides a general consent for Company to engage Subprocessors, conditioned on the following requirements: Company will provide details of any change in Subprocessors as soon as reasonably practicable by updating the Subprocessor Site or by other written means. If Company provides notice by updating the Subprocerssor Site, Customer may subscribe to such notices by sending an email to privacy@scarf.sh. If Customer objects to such engagement in a written notice to Company within 30 days after being informed of the engagement on reasonable grounds relating to the protection of Personal Data, Customer and Company will work together in good faith to find a mutually acceptable resolution to address such objection. If the parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Customer may, as its sole and exclusive remedy, terminate the Agreement and cancel the Services by providing written notice to Company and pay Provider for all amounts due and owing under the Agreement as of the date of such termination.
5. **DATA RIGHTS REQUESTS.** If Company receives a request from a Data Subject that relates to Customer Personal Data and identifies Customer (a "**Data Subject Request**"), Company will (a) advise the Data Subject to submit the Data Subject Request to Customer, and (b) promptly notify Customer of the Data Subject Request. Where required by Applicable Data Protection Law, to the extent Customer is unable through its use of the Services to address a particular Data Subject Request, Company will, upon Customer's request and taking into account the nature of Customer Personal Data Processed, provide reasonable assistance to Customer in fulfilling the Data Subject Request. To the extent permitted by Applicable Law, Customer will be responsible for any costs arising from Company's assistance.
6. **PERSONAL DATA BREACH.** Upon becoming aware of a Personal Data Breach, Company will without undue delay inform Customer and provide written details of the Personal Data Breach reasonably required to fulfill Customer's notification obligations under Applicable Data Protection Law. Where possible, such details will include, the nature of the Personal Data Breach, the categories and approximate number of data subjects concerned and the categories and approximate number of Customer Personal Data records concerned, the likely consequences, and the measures taken or proposed to be taken to mitigate any possible adverse effects. Company will promptly work to recover Customer Personal Data which is lost, damaged, destroyed or distorted as a result of the Personal Data Breach, and take such reasonable

commercial steps as may be directed by Customer to assist in the investigation, mitigation, and remediation of each such Personal Data Breach.

7. **DPIA AND CONSULTATION**. Taking into account the nature of the Processing and the information available to Company, Company will, when required by Data Protection Laws, assist Customer with its obligations related to data protection impact assessments (where related to the Services, and only to the extent that Customer does not otherwise have access to the relevant information) and prior consultation with supervisory authorities, including by providing the information contained in the Audit Report as set forth in Section 9 below.
8. **RETURN AND DELETION OF CUSTOMER PERSONAL DATA.** Company will delete all Customer Personal Data upon the completion of the Permitted Purpose or request by Customer, whichever is earlier. Company may retain Customer Personal Data to the extent required by applicable laws, and only to the extent and for such period as required by applicable laws and provided that Company will maintain the confidentiality of all such Customer Personal Data and will ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.
9. **AUDITS.** Company will make available information to Customer at Customer's request which is necessary to demonstrate compliance with this DPA and allow for any audits, including inspections, conducted by Customer or another auditor, as requested by Customer on reasonable, legitimate grounds for suspecting a breach of this DPA. Company will provide for such audits by allowing Customer to review confidential summary reports ("**Audit Report**") prepared by third-party security professionals at Company's selection and expense. If Customer can demonstrate that it requires additional information, beyond the Audit Report, then Customer may request, at Customer's cost, Company to provide for an audit subject to reasonable confidentiality procedures, which will: (i) not include access to any information that could compromise confidential information relating to other Company clients or suppliers, Company's technical and organizational measures or any trade secrets; and (ii) be performed upon no less than sixty (60) days' notice, during regular business hours and in such a manner as not to unreasonably interfere with Company's normal business activities.
10. **INTERNATIONAL DATA TRANSFERS.** Customer authorizes Company and its subprocessors to Transfer Customer Personal Data across international borders, including from the UK or European Economic Area to the United States:
    a. Transfers from the EEA. Where a Transfer is made from the European Economic Area ("**EEA**"), the SCCs are incorporated into this DPA and apply to the transfer as follows:
        i. with respect to Transfers from Customer to Company, Module One applies where both Customer and Company are Controllers, Module Two applies where Customer is a Controller and Company is a Processor, and Module Three applies where both Customer and Company are Processors;
        ii. in Clause 7, the optional docking clause does not apply;
        iii. in Clause 9(a) of Modules Two and Three, Option 2 applies, and the period for prior notice of subprocessor changes is set forth in Section 6 of this DPA;
        iv. in Clause 11(a), the optional language does not apply;
        v. in Clause 17, Option 1 applies with the governing law being that of Ireland;
        vi. in Clause 18(b), disputes will be resolved before the courts in Dublin, Ireland;
        vii. Annex I of the SCCs is completed with the information in Schedule A to this DPA;
        viii. Annex II of the SCCs is completed with the information in Section 3 above of this DPA; and
        ix. Annex III of the SCCs is completed with the information in Section 4 of this DPA.
    b. Transfers from Switzerland. Where a Transfer is made from Switzerland, the SCCs are incorporated into this DPA and apply to the transfer as modified in Section 10(a) above, except that:
        i. in Clause 13, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner if the Transfer is governed by the Swiss Federal Act on Data Protection;
        ii. references to "Member State" in the SCCs refer to Switzerland, and data subjects located in Switzerland may exercise and enforce their rights under the SCCs in Switzerland; and
        iii. references to the "General Data Protection Regulation," "Regulation 2016/679," and "GDPR" in the SCCs refer to the Swiss Federal Act on Data Protection (as amended or replaced).
    c. Transfers from the UK. Where a Transfer is made from the UK, the UK Transfer Addendum is incorporated into this DPA and applies to the transfer. The UK Transfer Addendum is completed with the information in Section 10(a) above, the Annexes to this DPA; and both "Importer" and "Exporter" are selected in Table 4.
    d. Specific application of the SCCs. The following terms apply to the SCCs:
        i. Customer may exercise its audit rights under the SCCs as set out in Section 9 above.
        ii. Company may appoint Subprocessors under the SCCs as set out in Section 4 above.
        iii. With respect to Transfers made to Company, Company may neither participate in, nor permit any Subprocessor to participate in, any further Transfer unless the further Transfer is made in full compliance

with Data Protection Laws and in accordance with applicable SCCs or an alternative legally compliant transfer mechanism adopted by the importer.

iv. If any provision of this Section 10 is inconsistent with any terms in the SCCs, the SCCs will prevail

11. **LIABILITY** Each Party's liability taken together in the aggregate, 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 provisions of the Agreement
12. **GENERAL** This DPA will continue in force until the termination of the Agreement, unless earlier terminated as provided herein. In the event of a conflict or inconsistency between the Agreement, this DPA, and the SCCs, the terms of the following documents will prevail (in order of precedence): the SCCs; then this DPA; and then the Agreement.

SCHEDULE A
Details of Processing

Data Exporter	• Name: The Customer entity identified in the Agreement. • Address: The Customer address specified in the Agreement or on the applicable order form. • Contact person's name, position and contact details: The Customer's contact specified in the Agreement or on the applicable order form. • Activities relevant to the data transferred under the SCCs: The data exporter is a customer of the data importer and utilizing the data importer's services as described in more detail in the Agreement. • Role: Controller and/or Processor
Data Importer	• Name: Scarf Systems, Inc. • Address: 548 Market St, PMB 17568, San Francisco, CA 94104 • Contact person's name, position and contact details: Avi Press, CEO, avi@scarf.sh • Activities relevant to data transferred under the SCCs: The data importer is providing certain services to the data exporter, as described in more detail in the Agreement. • Role: Processor
Categories of Data Subjects	Users and visitors of Customer's who reside in the EEA, Switzerland or UK
Categories of Personal Data	IP addresses
Sensitive data transferred	N/A
Frequency of the transfer	At the data exporter's discretion using the Services, during the term of the Agreement
Nature of Processing	Customer Personal Data will be Processed to provide the Services in accordance with the Agreement, including the following Processing activities: (1) provision of the Services in accordance with the Agreement, (2) technical support, issue diagnosis and error correction, and (3) disclosures in accordance with the Agreement or as compelled by Applicable Data Protection Law.
Purpose(s) of data transfer and further processing	Customer Personal Data is Processed for the purposes of providing the Services in accordance with the Agreement and any applicable order form.
Period for which Licensee Personal Data will be retained	Customer Personal Data will be retained in accordance with Section 8 of the DPA
Competent Supervisory Authority	Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located shall act as competent supervisory authority.