DATA PROCESSING AGREEMENT

This Data Processing Agreement (“**DPA**”) is entered into between Grovara, LLC (“**Controller**”) and **Company** (as defined in the Agreement, as such term is itself defined below). This DPA is subject to, and part of, the Brand Management and Distribution Agreement or similar agreement for services between Controller and Company (the “**Agreement**”) and is effective as of the effective date of the Agreement. This DPA applies to the extent Company receives or has access to personal data from the European Economic Area, the United Kingdom, or Switzerland in connection with the Agreement. Controller and Company, intending to be legally bound, agree as follows:

ARTICLE 1. PROCESSING OBJECTIVES

1.1. "**GDPR**" means 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, and repealing Directive 95/46/EC (General Data Protection Regulation), as amended or supplemented from time to time. “**Personal data**,” “**data subject**,” “**personal data breach**,” “**supervisory authority**” and “**processing**” (and variations thereof) shall have the meanings assigned to them in the GDPR.

1.2. Except as required by applicable law, Company shall not use the personal data for any purpose other than those contemplated by the Agreement.

1.3. All personal data shall remain the property of Controller and/or the applicable data subjects.

ARTICLE 2. COMPANY’S OBLIGATIONS

2.1. Company shall process personal data solely in accordance with the Agreement, this DPA and the documented instructions of Controller, including Exhibit A attached hereto.

2.2. Company represents and warrants that it shall comply with applicable Privacy Laws (as defined in Section 4.2 below) as applicable to its activities contemplated by the Agreement.

2.3. Upon reasonable request, Company shall furnish Controller with reasonable information regarding the measures it has adopted to comply with its obligations under this DPA.

2.4. Company shall provide reasonable information and assistance to Controller in fulfilling Controller’s obligations under Privacy Laws, including without limitation GDPR Articles 15-21, and 35-36.

ARTICLE 3. TRANSFER OF PERSONAL DATA

3.1. If Company is certified under the European Union - United States of America Privacy Shield Framework administered by the United States of America Department of Commerce (“**Privacy Shield**”) then, with respect to personal data subject to the GDPR processed by Company, Company shall provide at least the same level of privacy and data protection as is required by the Privacy Shield.

3.2. In the event that Company is not certified under Privacy Shield or Privacy Shield is no longer available for third country transfers under the GDPR, Company hereby enters into Standard Contractual Clauses (processors) (Decision 2010/87/EU) (“**SCCs**”) with Controller, the terms of which are hereby incorporated into this DPA. For the purposes of the SCCs, Controller is the data exporter, Company is the data importer, and the governing law shall be as specified in Section 12.1 below.

3.3. For the purpose of Appendix 1 to the SCCs (i) the data subjects are those individuals whose personal data is accessible or otherwise processed by Company under the Agreement; (ii) the categories of data include first and last name, job title, email address, business and mobile phone numbers, full mailing address and any other personal data relating to the services contemplated by the Agreement; and (iii) no special categories of data will be transferred. The processing operations include actions necessary for Company to utilize Controller's online platform, to perform the services, and to provide the functions contemplated by the Agreement in strict compliance with the Agreement, this DPA and Privacy Laws.

ARTICLE 4. ALLOCATION OF RESPONSIBILITY

4.1. Company is solely responsible for its processing of personal data under this DPA. Company shall only process such personal data in accordance with the Agreement, this DPA, Privacy Laws and Controller's documented instructions.

4.2. Company represents and warrants that it shall comply with all applicable data protection and privacy laws, including the GDPR (collectively, "**Privacy Laws**").

4.3. Company shall indemnify, defend, and hold harmless Controller and its affiliates, and its and their respective managers, directors, officers, employees and representatives from and against all out-of-pocket costs, expenses, fines, fees (including reasonable attorneys' fees) arising from all third-party claims, demands, or proceedings arising from or related to any actual or alleged (i) processing of personal data by Company in violation of Privacy Laws; or (ii) breach by Company of the Agreement or this DPA.

ARTICLE 5. ENGAGING OF THIRD PARTIES OR SUBCONTRACTORS

5.1. Controller authorizes Company to engage third parties and its affiliates as sub-processors, provided that Company has entered into a written agreement with each such sub-processor containing data protection obligations no less protective than those in this DPA with respect to the protection of personal data to the extent applicable to the nature of the services being provided by such third-party sub-processor. Company shall notify Controller in writing of any additional sub-processors to be utilized by Company.

5.2. The parties will cooperate in good faith to resolve any concerns Controller has in connection with sub-processors utilized by Company.

5.3. Company shall be liable for the acts and omissions of its sub-processors to the same extent as if Company were performing the services of each sub-processor directly under the terms of this DPA.

ARTICLE 6. DUTY TO REPORT

6.1. Company shall notify Controller without undue delay (in no event more than 48 hours) after becoming aware of a personal data breach, as defined by Article 4 of the GDPR. Such notice shall include, to the extent reasonably available to Controller, the information required for Controller to fulfill its obligations under Articles 33 and 34 of the GDPR.

6.2. Controller shall be responsible for complying with Articles 33 and 34 of the GDPR. However, Company shall provide reasonable assistance in accordance with the GDPR in the notification of the relevant supervisory authorities and/or data subjects by Controller.

ARTICLE 7. SECURITY

7.1. Company shall implement and maintain such appropriate technical and organisational measures as are required by Article 32 of the GDPR that are designed to ensure a level of security that is appropriate to the risk for the rights and freedoms of natural persons, including, as appropriate, pseudonymization and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems, the ability to restore the availability of personal data in a timely manner in the event of a physical or technical incident, and a process for regularly evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

ARTICLE 8. HANDLING REQUESTS FROM INVOLVED PARTIES

8.1. If a data subject contacts Company with respect to the data subject rights under the GDPR, Company shall promptly (in any event within five days) notify Controller in writing. Controller and Company shall each be responsible for complying with a data subject's rights request under the GDPR with respect to personal data in its possession or the possession of its sub-processors.

ARTICLE 9. NON DISCLOSURE AND CONFIDENTIALITY

9.1. Company shall ensure the confidentiality of the personal data to the extent required by the Agreement or contemplated by the services provided under the Agreement. All persons authorized to access personal data by Company shall have committed themselves to confidentiality where applicable.

ARTICLE 10. AUDIT

10.1. Company shall permit Controller (or its appointed third-party auditors) to audit Company's compliance with this DPA, and shall make available to Controller information, systems and staff reasonably necessary for Controller to conduct such audit. Such audit shall be conducted at Company's place of business, provided that Controller gives Company a minimum of 10 (ten) days' prior written notice of its intention to perform such audit, the auditors conduct the audit during Company's normal business hours, and the auditors take all reasonable measures to prevent unnecessary disruption to Company's operations. Controller may not request more than one audit in any twelve (12) calendar month period. Controller agrees to treat all information acquired during the course of any audits and audit results as confidential information of Company under the Agreement.

10.2. Additionally, a supervisory authority may conduct an audit of Company to the extent required or permitted by the GDPR.

ARTICLE 11. DURATION AND TERMINATION

11.1. Company shall, at Controller's choice, destroy or return to Controller all personal data in Company's possession after the Agreement terminates or expires for any reason, unless otherwise required by applicable law.

11.2. This DPA is entered into for the duration set out in the Agreement. This DPA shall automatically terminate upon the later of (i) the termination or expiration of the Agreement, or (ii) no personal data of Controller being in the custody or control of Company or its sub-processors.

11.3. This DPA may only be amended by a written agreement signed by both parties.

11.4. The parties will reasonably cooperate with each other to amend this DPA as necessary to comply with applicable new privacy legislation or regulations.

ARTICLE 12. MISCELLANEOUS

12.1. This DPA shall be governed by the laws of the jurisdiction specified in the Agreement. Venue for any dispute arising between the parties in connection with this DPA shall be in the courts of the jurisdiction specified in the Agreement.

12.2. This DPA shall be construed to enable the parties to be compliant with the terms of the GDPR.

12.3. In the case of any conflict between the Agreement and this DPA, this DPA shall control with respect to the matter in conflict.

EXHIBIT A
DATA AND DATA SUBJECTS

1. Nature and purpose of the processing

The purpose of the processing is to enable the parties to provide and participate in the Grovara B2B online international commerce platform and related services and transactions, in accordance with the Agreement.

2. Categories of Data Subjects

Individuals whose personal data is accessible to or otherwise processed by Company under the Agreement.

3. Types of Personal Data

- First and last name
- Job title
- Email address
- Business and mobile phone numbers
- Full mailing address
- Any other personal data relating to the services contemplated by the Agreement