SCHEDULE C
DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is entered into between Pisano Limited ("Company") and the Customer identified in the applicable Order Form and/or General Terms for Pisano Services ("GTS").

This DPA supplements the Order Form, General Terms for Pisano Services (together with its applicable schedules, exhibits, annexes, and attachments, including all SOWs) and any future agreements (collectively, the "Agreement") between Company and Customer for the purposes of providing services outlined in the Agreement. This DPA applies to the Company's Processing of Personal Data and is effective as of the date of the last signature ("DPA Effective Date").

1. DEFINITIONS.

All capitalized terms used in this DPA will have the meanings given to them below. Capitalised terms used in this DPA that are not defined in this Section 1 (Definitions) shall have the meaning ascribed to them elsewhere in this DPA and/or the Agreement or in applicable Data Protection Laws unless otherwise specified.

"Adequate Country" means, as applicable, (i) where the EU GDPR applies, the EEA or a country or territory which is deemed to ensure an adequate level of protection by the European Commission; (ii) where the UK GDPR applies, the UK or a country or territory recognized as ensuring adequate data protection pursuant to Section 17A of the UK Data Protection Act 2018 as amended or replaced; and (iii) where the Swiss FADP as amended or replaced applies, Switzerland or a country or territory outside Switzerland which has been recognized to provide an adequate level of protection by the Federal Data Protection and Information Commissioner.

"Business Purpose means the limited purpose specifically identified in Annex I for which Company receives or accesses Personal Data.

"Data Protection Laws" means all applicable data protection and privacy laws and regulations, as applicable to a party, including, but not limited to, where applicable, the EU Data Protection Laws, and the US Data Protection Laws, and any other state or national data protection, data privacy or data security laws applicable to the scope of the Services, in each case as amended, superseded, or replaced from time to time.

"EU Data Protection Laws" means (i) Regulation 2016/679 of the European Parliament and of the Council 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 or "EU GDPR"), (ii) the EU GDPR as incorporated into United Kingdom domestic law pursuant to Section 3 of the European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (the "UK GDPR"); (iii) the Swiss Federal Act on Data Protection of 19 June 1992 and its corresponding ordinances ("FADP"); (iv) the EU Directive 2002/58/EC on Privacy and Electronic Communications; and (v) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i) – (iv); in each case as amended, superseded or replaced from time to time.

"EEA" means the member states of the European Union as well as Iceland, Liechtenstein and Norway.

References to "instructions" or "written instructions" and related terms mean instructions from Customer for Processing of Personal Data, which consist of: (i) the terms of the Agreement and this DPA; (ii) Processing enabled by Customer through the Services; and (iii) other reasonable written instructions of Customer consistent with the terms of the Agreement and this DPA.

"Personal Data" means any information of Customer obtained, accessed, or received by Company in connection with an engagement under the Agreement that constitutes "personal data", "personal information" or its equivalent term under the applicable Data Protection Laws.

"Process" or "Processing", "Data Subjects", "Data Controller" (or "Controller"), "Data Processor" (or "Processor"), "Business", "Service Provider", and "Sell" and "Share" have the meaning given to those terms or equivalent or similar terms under the applicable Data Protection Laws. Notwithstanding the foregoing, Process or Processing shall include any collection, acquisition, access to, use, modification, disclosure, transmission, storage, or destruction of Personal Data.

"Security Specifications" means the appropriate technical and organizational security measures employed by Company to protect any Personal Data in the custody and control of Company in connection with delivering the Services to Customer, as further set out in Annex II.

"Services" means the services, systems and documentations provided by Company to Customer pursuant to the Agreement.

"Sub-Processor" means any third-party entity engaged by Company, including its Affiliates, as set out in Annex III, to assist in fulfilling its obligations with respect to providing parts of the Services pursuant to the Agreement or this DPA.

"Standard Contractual Clauses" means (i) where the EU GDPR and/or the Swiss FADP applies, the standard contractual clauses annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021 ("EU SCCs"), currently available at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en; and (ii) where the UK GDPR applies, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("UK SCCs"), currently available at https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf; in each case, as may be amended, superseded, or replaced from time to time. The EU SCCs and UK SCCs are incorporated by reference and form an integral part of this DPA.

"Transfer Risk Assessment" means the additional guarantees to supplement the guarantees provided by the SCCs and UK Addendum as included in this DPA in Annex IV;

"US Data Protection Laws" means all applicable laws and regulations of any jurisdiction in the United States relating to privacy, data protection or data security (in each case, as amended, superseded or replaced from time to time), including, without limitation, as applicable, the California Consumer Privacy Act, as amended by the California Privacy Rights Act, together with the regulations promulgated thereunder (collectively, the "CCPA"); the Virginia Consumer Data Protection Act; the Colorado Privacy Rights Act, when effective; the Connecticut Data Privacy Act, when effective; and the Utah Consumer Privacy Act, when effective.

2. ROLES AND SCOPE OF PROCESSING.

2.1. Roles of the Parties. Customer shall be the Controller and/or Business (as applicable) and Company shall be the Processor and/or Service Provider (as applicable) with respect to Personal Data Processed by Company on Customer's behalf in performing its obligations under this DPA.

2.2. Scope of Processing. Each party will comply with all applicable Data Protection Laws and its obligations under the Agreement and this DPA in relation to its Processing of the Personal Data. Without limiting the foregoing, Company shall provide the same level of privacy protection as is required of Businesses (as defined in the CCPA) by the CCPA. Customer and Company acknowledge and agree that Annex I describes the subject matter and details of the processing of Personal Data.

3. CUSTOMER'S OBLIGATIONS.

3.1. Customer's Data Protection Obligations. Customer shall be solely responsible for determining the purposes for which and the manner in which Personal Data are, or are to be, Processed. Customer has the right, including upon notice in accordance with Sections 4.1(e) and/or 4.1(f) below, to take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Data by Company or any authorized Sub-Processor. In addition:

(a) Customer confirms that it has complied with its obligations for the lawful processing and sharing of the Personal Data with Company and its authorized Sub-Processors, if any.

(b) Additional instructions not consistent with the scope of the Agreement require prior written agreement of the parties, including agreement on any additional fees payable by Customer.

4. COMPANY'S OBLIGATIONS.

4.1. Company's Processing Obligations. Without prejudice to Section 2 above, Company shall in respect of the Processing of the Personal Data:

(a) only Process the Personal Data for the Business Purpose and in accordance with Customer's instructions as provided from time to time and comply promptly with all such instructions and directions received from Customer;

(b) treat Personal Data as Confidential Information (as defined by the parties in the Agreement) and Process it only to the extent, and in such a manner, as is necessary for the purposes described in this DPA and shall not process the Personal Data for any other purpose;

(c) provide all assistance reasonably required by Customer to enable Customer to take reasonable and appropriate steps to ensure that Company and any authorized Sub-Processors effectively Process Personal Data in a manner consistent with Customer's obligations under all applicable Data Protection Laws;

(d) assist Customer in ensuring compliance with its obligations under the Data Protection Laws, which could include, but is not limited to, in conducting any required privacy impact assessment, risk analysis, or prior consultation with the relevant data protection authorities upon request from Customer;

(e) immediately inform Customer if, in its opinion, Company´s implementation or execution of an instruction from Customer would infringe the Data Protection Laws;

(f) promptly, and in any event within five (5) business days, notify Customer of any determination made by Company that it can no longer meet its obligations under this DPA or Data Protection Laws whereupon Customer may terminate this DPA in accordance with Section 12.2;

(g) keep or cause to be kept full and accurate records relating to all Processing of Personal Data on behalf of Customer as part of the Services ("Records");

(h) promptly notify Customer and in any event within five (5) working days of any requests, complaints or any communication it receives from Data Subjects, or a supervisory authority, government authority, law enforcement authority or any other third party that relates to the Personal Data, unless and only to the extent prohibited under applicable law;

(i) promptly provide such cooperation and assistance as reasonably required by Customer to fulfil its obligations under Data Protection Laws in relation to Data Subject requests or any request from applicable government regulator or supervisory authority;

(j) Notwithstanding the foregoing, to the extent permitted by the Data Protection Laws, Company may use aggregated and anonymized data derived from Personal Data ("Anonymized Data") internally to build and improve the quality of the Services it is providing to Customer, provided that such Anonymized Data does not constitute Personal Data under the applicable Data Protection Laws, and Company does not use such Anonymized Data to perform services on behalf of another person or business.

4.2. Prohibited Processing Activities by Company. Company shall not:

(a) disclose Personal Data to any third party individual other than for the purposes of complying with a request from a Data Subject to access (including a copy of) their Personal Data in accordance with the Data Protection Laws and in accordance with the above Sections 4.1(h) and 4.1(i), as applicable;

(b) Sell or Share (as defined in the CCPA) Personal Data or retain, use, or disclose the Personal Data for any Commercial Purposes (as defined by the CCPA) or outside of its direct business relationship with Customer and under Customer's prior written authorization only;

(c) include Personal Data in any product or service offered by Company to third parties;

(d) co-mingle or combine Personal Data with its own data or the data of any third party, other than as strictly required to perform the Services;

(e) attempt to or actually re-identify any previously aggregated, deidentified, or anonymized data and will contractually prohibit downstream data recipients from attempting to or actually re-identifying such data; or

(f) with the exception of those pre-approved Sub-Processors listed in Annex III or added pursuant to Section 7.2, share or allow access to files containing Personal Data to any third party for further Processing by that third party or its agents (except for the purposes of mere routing of Personal Data through a third party such as routing through a telecommunications carrier, or any use of cloud hosting or infrastructure Sub-Processors (e.g. AWS) that are restricted to computation, storage and content delivery that will not include any other form of Processing unless agreed in writing in advance).

(g) Company certifies that it understands and will comply with the restrictions on the use of Personal Data in connection with the Services set forth in this DPA. Company further certifies that it will ensure that any employees, subcontractors, and agents involved in performing Services under the Agreement comply with the terms of this DPA.

5. RIGHTS OF DATA SUBJECTS.

Access, Correction, Restrict, Opting-Out, Deletion and Data Portability. To the extent Customer, in its use of the Services under the Agreement, does not have the ability to enable accessing, correcting, amending, restricting, opting-out, deleting, or porting Personal Data, as required by the Data Protection Laws, Company shall comply with any commercially reasonable request by Customer to facilitate such actions.

Requests of Data Subjects. If Company receives any complaint, notice or communication, which relates directly or indirectly to the Processing of the Personal Data from a Data Subject ("Data Subject Request"), Company shall promptly notify Customer and in any event within five (5) working days from receiving such Data Subject Request. Company shall not respond to any such Data Subject Request without Customer's prior written consent except as required by applicable laws to which Company is subject, in which case Company shall to the extent permitted by applicable laws inform Customer of that legal requirement and consult Company before responding to the request. Company shall provide Customer with commercially reasonable cooperation and assistance in relation to a Data Subject's Request.

6. COMPANY'S PERSONNEL.

6.1. Confidentiality. Company shall be fully responsible for any of Company's employees (including its agents and contractors) and Sub-Processors who have access to Personal Data and, without prejudice to any existing contractual arrangements between the Parties, Company shall treat all Personal Data as strictly confidential and it shall inform all its employees, agents, contractors and/or approved Sub-Processors engaged in Processing the Personal Data of the confidential nature of the Personal Data. Company shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality and have undertaken appropriate training relating to the handling of Personal Data. Company shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

6.2. Limitation of Access. Company shall ensure that access to Personal Data is limited to (i) those personnel who require such access to meet Company´s obligations under the Agreement and (ii) such part or parts of the Personal Data as is necessary for the performance of that personnel's duties.

7. SUB-PROCESSORS.

7.1. Appointment of Sub-Processors. Customer agrees that Company is authorized to use Company's Affiliates as Sub-Processors to Process the Personal Data. This being said, the engagement of any other agents, sub-contractors or third parties besides Company's Affiliates or those listed as approved Sub-Processors in the Data Processing Schedule are subject to requirements set under Section 7.2 below. Company will impose on its Sub-Processors the same and appropriate data protection obligations as set out in this DPA and the Agreement by way of a written agreement taking into consideration the type of Personal Data Processed by a Sub-Processor and Company shall remain fully responsible for the Processing activities of its Sub-Processors.

7.2. New or Replacement Sub-Processors. In the event Company intends to add or replace any Sub-Processors, Company will promptly notify Customer of such additional or replacement Sub-Processor. Such notice from Company shall be done in writing or by email and must be sent by and to the parties' contact persons as listed in the Agreement or any other applicable statement of work documents or order forms. Customer may notify Company of any objections (on reasonable grounds related to Data Protection Laws) to the proposed Sub-Processor or Annex IV ("Objection") within thirty (30) business days of the notice. Company and Customer shall negotiate in good faith to agree to further measures including contractual or operational adjustments relevant to the appointment of the proposed Sub-Processor or operation of the services to address Customer's Objection. Where such further measures cannot be agreed between the parties within forty-five (45) business days from Company's receipt of the Objection (or such greater period agreed by Customer in writing), Customer may, by written notice to Company with immediate effect, terminate that part of the Services which require the use of the proposed Sub-Processor.

7.3. Liability. Company shall be liable for the acts, errors and omissions of its Sub-Processors as if they were Company´s own acts, errors and omissions, except as otherwise set forth in the Agreement.

8. INTERNATIONAL TRANSFERS.

8.1. In General. Subject to appropriate data protection standards and security measures, Company may store, Process and transfer Personal Data anywhere in the world where Company, its Affiliates or approved Sub-Processors maintain data processing operations. Company shall ensure that such transfers of the Personal Data are carried out in compliance with the Data Protection Laws. Where EU, UK or Swiss Personal Data is transferred outside the EEA, the UK or Switzerland, Company shall only Process or permit the Processing of EU, UK or Swiss Personal Data outside of the EEA, the UK or Switzerland if one of the following conditions is met:

(a) the EU, UK or Swiss Personal Data are transferred to an Adequate Country; or

(b) the Standard Contractual Clauses and the Transfer Risk Assessment are in place between Customer and Company and/or between Company and the Sub-Processor, as appropriate.

8.2. EU Personal Data Transfers. For the purposes of Section 8.1(b), Customer and Company (on its behalf and/or on behalf of its Affiliates) agree to enter into the EU SCCs (module two: Transfer controller to processor), for transfers of EU Personal Data to Company outside of the EEA, as set forth below. Each Party's signature to this DPA shall be considered as signature to the EU SCCs. If needed by a supervisory authority or by Data Protection Laws, the Parties will cooperate and sign the EU SCCs separately.

(a) Customer shall be the data exporter, and Company and its Affiliates shall be the data importer;

(b) Clauses 7(a) – (c) shall apply;

(c) Option 1 of Clause 9(a) shall apply, and the data importer shall submit the request for specific authorisation at least 30 days prior to the engagement of the Sub-Processor;

(d) Clause 11(a) shall not include an additional redress mechanism for Data Subject, as set out in the second optional paragraph of Clause 11(a);

(e) Option 2 of Clause 17 shall apply, and the EU SCCs shall be governed by the law specified in the Agreement, provided that law is an EEA Member State recognizing third party beneficiary rights, otherwise the law of the Netherlands shall apply;

(f) Clause 18(b) disputes shall be resolved before the courts specified in the GTS, provided these courts are located in an EAA Member State, otherwise those courts shall be the courts of the Netherlands. In any event, Clause 17 and 18 (b) shall be consistent in that the choice of forum and jurisdiction shall fall on the country of the governing law;

(g) The Annexes of the EU SCCs shall be populated with the relevant information set out in Annex I, Annex II and Annex III of this DPA; and

(h) If and to the extent the EU SCCs conflict with any provision of this DPA, the EU SCCs will prevail to the extent of such conflict.

8.3. Swiss Data Transfers. For the purpose of Section 8.1(b), and in order to allow the parties to lawfully transfer Swiss Personal Data in accordance with the FADP, the version of the EU SCCs referenced in Section 8.2 above shall apply and shall include all necessary amendments to make them legally effective in Switzerland, including but not limited to the following:

(a) References to the GDPR will be deemed to be references to the equivalent provisions of the FADP;

(b) The competent supervisory authority in Annex I.C of the EU SCCs under Clause 13 is the Federal Data Protection and Information Commissioner of Switzerland;

(c) The applicable law for contractual claims under Clause 17 of the EU SCCs is Swiss law or the law of a country that allows and grants rights as a third party beneficiary;

(d) The term "member state" used in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland form the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c); and

(e) The EU SCCs also protect the data of legal entities until the entry into force of the revised FADP.

8.4. UK Data Transfers. For the purpose of Sections 8.1(b), and in order to allow the parties to lawfully transfer UK Personal Data in accordance with the UK GDPR, the version of the EU SCCs referenced in Section 8.2 above shall apply together with the UK Addendum. Each Party's signature to this DPA shall be considered as signature to the UK Addendum. If needed by a supervisory authority or by Data Protection Laws, the Parties will cooperate and sign the UK Addendum separately. The parties further agree that for the purpose of the Addendum:

(a) Customer shall be the data exporter, and Company shall be the data importer (on behalf of itself and its Affiliates), and the parties' details as set out in the Agreement shall be incorporated into Table 1 of Part 1 of the UK Addendum (Parties);

(b) The first option of Table 2 of Part 1 of the UK Addendum (Selected SCCs, Modules and Selected Clauses) shall be selected and the date shall be the DPA Effective Date of this DPA;

(c) Table 3 of Part 1 of the UK Addendum (Appendix Information) shall be populated with the relevant information set out in Annex I, Annex II and Annex III to this DPA; and

(d) Either the importer or the exporter may end the UK Addendum, and Table 4 of Part 1 of the UK Addendum shall be completed accordingly.

Company agrees to provide the same level of protection for Personal Data as is required by the Standard Contractual Clauses, as applicable and specified in this DPA, and to notify Customer if it or any of its Sub-Processors can no longer provide those protections. To the extent that there is any conflict between the Standard Contractual Clauses, this DPA or the Agreement, the Standard Contractual Clauses shall prevail.

9. DATA SECURITY.

9.1. Data Security. Company shall:

(a) promptly notify Customer if it makes a determination that it can no longer meet its obligations under this DPA or to provide the same level of protection as is required by Data Protection Laws, and in such event, to work with Customer to promptly take reasonable and appropriate steps to stop and remediate any Processing until such time as the Processing meets the level of protection as is required by the Data Protection Laws;

(b) implement and maintain throughout the term of this DPA appropriate technical and organizational security measures to protect Personal Data against unauthorized or unlawful processing and accidental destruction or loss (including ensuring the reliability of employees), so as to allow Customer to comply with the requirement to implement appropriate technical and organizational security measures (including without limitation pseudonymization, encryption and application of retention rules), in accordance with the Security Specifications and other applicable provisions of the Data Protection Laws; and

(c) at Customer's sole election, cease Processing Personal Data promptly if in Customer's reasonable discretion, Company is not providing the same level of protection to Personal Data as is required by Data Protection Laws.

9.2. Controls for the Protection of Personal Data. Company shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Personal Data, as set forth in the Security Specifications. Company regularly monitors compliance with these safeguards. Company will not materially decrease the overall security of the Services during the term of the Agreement.

10. SECURITY INCIDENT MANAGEMENT AND DATA BREACH NOTIFICATION.

10.1. Security Incident Notification. Company maintains security incident management policies and procedures as indicated in the Security Specifications and shall, to the extent permitted by law, promptly notify Customer after becoming aware of any actual or reasonably suspected breach, accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to its System or any related systems or networks, involving the (possible) loss or unauthorized disclosure of Personal Data, Customer's Confidential Information and/or any electronic files as created by Company or in control of Company or its Sub-Processors of which Company becomes aware of that is transmitted, stored, or otherwise processed (a "Security Incident").

10.2. Data Breach Notification. In the event a Security Incident impacting Personal Data is discovered on or in connection with Company's systems or any other type of electronic medium or storage device, that depending on the facts and circumstances may lead to a data breach notification pursuant to applicable law to any applicable government regulator or supervisory authority for compliance with Data Protection Laws, Company shall:

(a) promptly, but in any event within forty-eight (48) business hours thereof, notify Customer of such a Security Incident in writing (or by telephone and e-mail if such is quicker) along with any actions that have been taken to mitigate the effects of such loss or disclosure and will take such further actions as it deems reasonably necessary to prevent a reoccurrence of a similar loss or disclosure;

(b) reasonably cooperate with Customer to investigate and resolve the Security Incident;

(c) make reasonable efforts to identify and remediate the cause of such Security Incident;

(d) provide Customer with a description of the Security Incident (including the date of the Security Incident, if known, and the date of its discovery), the type of data and the extent to which Personal Data, has been or reasonably believed to have been the subject of the breach, the scope of the Security Incident, and other information Customer may reasonably request concerning the affected Data Subjects; and

(e) keep Customer up-to-date about developments in connection with the Security Incident.

Unless otherwise required under Data Protection Laws, the parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected Data Subjects and/or notices to the relevant supervisory authorities. The costs of any notifications to Data Subjects or a government regulator or supervisory authority that is legally required by the Data Protection Laws shall be borne by Company.

11. THIRD-PARTY CERTIFICATIONS AND AUDITS.

11.1. By Supervisory Authorities. Company shall provide Customer with reasonable access to its documentation and systems in the event of an audit required by a government regulator or supervisory authority for compliance with Data Protection Laws.

11.2. By Customer. At Customer's request, and subject to Company's reasonable confidentiality and security constraints:

(a) Company shall make available to Customer relevant documentation regarding Company's Processing of Personal Data under this DPA to demonstrate compliance with the obligations under Data Protection Laws such as but without limitation in the form of Company's most recent ISO 27001, ISO 27017, or ISO 27018 certifications and/or audit reports and/or security questionnaires ("Third Party Reports").

(b) No more than once per calendar year (except in case of an actual or suspected Security Incident), , Company shall provide Customer with written responses to all reasonable requests for information made by Customer or appointed representatives relevant to the Processing of Personal Data under this DPA, and allow for and contribute to annual audits or assessments of compliance through review of Company systems that are used to Process or access Personal Data, policies, and technical and organizational information security and other measures, including inspections conducted during normal business hours with advance prior written notice by Customer or another auditor as mandated by Customer who will have entered into a confidentiality undertaking covering the audit at any time.11 Company shall grant to Customer all reasonable access rights and information required to perform such audits.

11.3. Audits of Company's Sub-Processors. In relation to any Sub-Processors that are engaged pursuant to the

Agreement and this DPA, Customer acknowledges and agrees that it is sufficient, for the purposes of satisfying the requirements of this section, that Company has a right to audit those Sub-Processors on behalf of Customer, subject to reasonable restrictions.

11.4. Company Confidential Information. Any information provided by Company under this Section 11 constitutes Company's Confidential Information under the Agreement. Company will not be required to disclose any commercial secrets, including algorithms, source code, trade secrets and similar information.

12. TERM; TERMINATION; SURVIVAL.

12.1. Term. This DPA is effective as of the DPA Effective Date and shall continue in full force and effect unless and until it is terminated in accordance with this Section. This DPA shall terminate automatically upon the termination or expiration of the Agreement.

12.2. Termination for Convenience. Customer may (without prejudice to any other right or remedy) terminate this DPA at any time on immediate notice to Company.

12.3. Effect of Termination; Survival. Termination or expiry of this DPA shall not release:

(a) Company from its confidentiality obligations relating to the Personal Data. Company's obligations under this DPA shall remain in full force and effect for as long as Company holds Personal Data.

(b) Either of the parties from any other liability, which at the time of termination has already accrued to the other party, nor affect in any way the survival of any other right, duty or obligation of the parties, which is expressly stated elsewhere in this DPA to survive such termination.

13. RETURN AND DELETION OF PERSONAL DATA.

13.1. Return or Deletion of Personal Data. Subject to Section 13.3 below, on termination or expiration of the Agreement or of this DPA for any reason, or upon Customer's request at any time, Company and its Sub-Processors (if any) shall promptly return any Personal Data it still holds to Customer or its agent, in a format reasonably notified by them, and/or securely delete and/or destroy it from its servers or third-party servers, whatever may apply (at Customer´s option). Company shall provide reasonable cooperation and assistance to export any Personal Data from its systems.

13.2. Sub-Processors. Where Customer elects to have the Personal Data securely deleted or destroyed, Company shall procure that all Sub-Processors return or delete the Personal Data they hold.

13.3. Compliance with Applicable Laws. After the termination of the Agreement or of this DPA or upon the Customer´ request to delete/destroy the Personal Data, Company may only retain Personal Data to the extent and for such period as required by applicable laws and always provided that Company and any Sub-Processor shall ensure the confidentiality of all such Personal Data and shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

14. MISCELLANEOUS.

14.1. Hierarchy of Documents. In the event of any inconsistency or conflict between the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail to the extent of that conflict in connection with the Processing of Personal Data.

14.2. Updates to DPA. In the event of changes to applicable Data Protection Laws, including, but not limited to, the amendment, revision, or introduction of new laws, regulations, or other legally binding requirements to which either party is subject, the parties agree to revisit the terms of this DPA, and negotiate any appropriate or necessary updates in good faith, including the addition, amendment, or replacement of any Appendix and/or Annex.

14.3. Limitation of Liability. All activities under this DPA (including without limitation Processing of Personal Data) remain subject to the applicable limitations of liability set forth in the Agreement. In no event does Company limit or exclude its liability towards data subjects or competent data protection authorities.

14.4. Governing Law. This DPA will be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

ANNEX I – DESCRIPTION OF DATA PROCESSING

A. LIST OF PARTIES

Data exporter(s): The **Customer Name**, as specified in the Service Subscription Order Form

Address: The **Customer Address**, as specified in the Service Subscription Order Form

Contact person's name, position, and contact details: Authorized Signatory, as specified in the Service Subscription Order Form

Activities relevant to the data transferred under these Clauses: Any activities relevant for the purposes of receiving the services provided by Company in connection with an engagement under the Agreement.

Signature and date: By entering into the DPA, data exporter is deemed to have signed these Standard Contractual Clauses and Annexes incorporated herein as of the DPA Effective Date

Role: Controller

Data importer(s): Pisano Limited

Address: 9th Floor 107 Cheapside, EC2V 6DN London United Kingdom

Contact person's name, position and contact details: dpo@pisano.com and alphan.dinc@pisano.com , Alphan Dinc, Data Protection Committee Manager

Activities relevant to the data transferred under these Clauses: Any activities relevant for the purposes of providing the services to Controller in connection with an engagement under the Principal Agreement.

Signature and date: By entering into the DPA, data importer is deemed to have signed these Standard Contractual Clauses and Annexes incorporated herein as of the DPA Effective Date

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer´s prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer´s employees authorized by Customer to use the Services

Categories of personal data transferred

Personal details, including any information that identifies the data subject and their personal characteristics, including: name, address, and contact details.

Goods or services provided and related information, including details of the goods or services supplied, licenses issued, and contracts.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The data is transferred on a continuous basis.

Nature of the processing

The performance of the Services pursuant to the Agreement

Purpose(s) of the data transfer and further processing

Company will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified below, and as further instructed by Customer in its use of the Services.

The Company will use the Personal Data to send surveys and analyze the survey responses to present reports, analysis, and insights to Customer through it Experience Management Platform as specified in the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The duration of the DPA, plus the period from the end date of the DPA until deletion of all Personal Data by Company in accordance with the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

The subject matter and duration of processing is outline above within this Annex. The nature of the specific sub-processing services are further described in Annex III.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:

The Dutch Data Protection Authority, unless required otherwise by Section 8 of the DPA.

ANNEX II – TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Company shall employ the following technical and organizational measures to safeguard the limitation Personal Data as well Customer´s Confidential Information and Records it has under its control.

1.	Physical access controls employed for preventing unauthorized persons from gaining access to data processing systems within which personal data is processed or used.	Internally Hosted Data center physical controls include: • Electronic access card reading system. • Management of keys. • Front desk with required sign in for all visitors. • CCTV Video Recording building management system. • Patch and vulnerability management processes • Managed Network Firewalls
2.	Admission control measures taken for preventing data processing systems from being used without authorization.	• Personal and individual user log-in when entering the system and / or the corporate network, with MFA required for sensitive systems. • Password require a minimum of 10 characters, from at least 3 of the following categories: 1) Uppercase letter, 2) Lowercase Letter, 3) Number, 4) Non-alphanumeric special character, 5) Any unicode character that is categorized as an alphabetic character but isn't uppercase or lowercase. If the user account has five invalid logon attempts, the account will be locked out. User passwords expire after 180 days. • Automated screen locks after a defined period of inactivity, requiring password to unlock. • Service account passwords are managed electronically, with access granted using least-privilege principles and access is logged. • User accounts are audited quarterly and constantly monitored. • Personal Accounts and credentials are prohibited from being shared • Where shared accounts/tokens/keys are needed, they are required to be stored in a password management system (such as Secret Server, Akeyless, AWS Secrets manager, Lastpass)
3.	Virtual access control measures taken to ensure that persons entitled to use a data processing system have access only to personal data to which they have a right of access, and that personal data cannot be read, copied, modified, or removed without authorizations in the course of processing or use and after storage.	• User authentication is based on username and password. • All transactional records contain identifiers to distinguish client records.
4.	Transmission control measures taken to ensure that personal data cannot be read, copied, modified, or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged.	• All data on untrusted systems are encrypted in flight using TLS 1.2 or better. • Network activity is logged and archived for at least one year. • Removable storage is not used.
5.	Input control measures taken to ensure that it is possible to check and establish whether and by whom personal data have been entered into data processing systems, modified, or removed.	• Record entry is restricted to a defined set of roles • Firewalls and intrusion prevention systems are in place to prevent unauthorized access.
6.	Assignment control measures employed to ensure that, in the case of commissioned processing of	• Confidentiality agreements are in place for all individuals with data access.

	personal data, the data are processed strictly in accordance with the instructions of the principal.	• Security training is conducted during onboarding and on a regular basis. • Additional training may be provided based on role, such as code security training for software developers. • Employees review and agree to a code of conduct and acceptable use policies annually. • Privacy policy describes rights and obligations of agent and principal. • A data handling policy exists which outlines the security requirements for systems based on the type of data they contain.
7.	Availability control measures taken to ensure that personal data are protected from accidental destruction or loss.	• Systems employ redundancies such as RAID arrays and redundant equipment. • Backups are stored in alternate location from primary processing. • Multiple air conditioning units are installed to provide redundant capacity in a N+1 configuration. • High sensitivity smoke detection. • UPS backed generator. • Diverse fiber routing and multiple carriers.
8.	Internal Audits, monitoring and risk Identification & assessment taken for preventing unauthorized access to data processing systems	• Company meets all requirements for regulatory compliance (ISO27001) which are audited annually. • Company leverages an internal penetration testing team for routine internal vulnerability discovery • Annual a security audit is conducted by an external security team • Company has a bug bounty program • Company has a dedicated security team for security program management for the company. • Logs are forwarded to a central Security Operations Center. • Logs are automatically parsed to look for anomalies which are then flagged for review and follow-up if needed. • Endpoint Detection and Response (EDR) agent installation is required for all endpoints with alerts/logs forwarded to the SOC. • Prior to engaging new third-party service providers or vendors who will have access to Personal Data, a risk assessment of vendors' data security practices is conducted
9.	Internal Security Standards	In addition to complying with appropriate regulatory standards such as ISO27001 and HIPAA, Company maintains internal Security Standards in the following categories: • Public Cloud Security Requirements • Software Development Requirements • Operational Security Standards

ANNEX III – LIST OF APPROVED SUB-PROCESSORS

The data exporter has authorized the use of the following sub-processors:

Name Sub-Processors	**Address**	**Description of Processing**
Pisano Musteri Iletisim Cozumleri ve Bilgi Teknolojileri Anonim Sirketi (Pisano Limited's 100% owned subsidiary) (a.k.a Pisano Turkey)	Resitpasa Mahallesi Katar Caddesi ITU ARI TEKNOKENT 4 NO 2/50 IC KAPI NO: 6 SARIYER ISTANBUL	Pisano Turkey is the Company's 100% owned subsidiary to conduct technical and customer service to the Company and its customers.
Google Cloud EMEA Limited	70 Sir John Rogerson's Quay, Dublin 2, Ireland	Pisano Server Provider
Microsoft Ireland Operations Limited	One Microsoft Place, South County Business Park, Leopardstown, Dublin, 18, D18 P521, Ireland	Pisano Server Storage Provider
Buinsoft Technology s.r.o.	Na Folimance 2155/15 120 00 Praha Czechia	Group IT, Integration and Technical Service Company
Mailgun Technologies, Inc.	112 E. Pecan Street #1135 San Antonio, Texas 78209	Email Gateway Provider
OpenAI Ireland Ltd	1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland	Pisano LLM and Generative AI Solutions Provider
AWS Turkey Pazarlama Teknoloji ve Danışmanlık Hizmetleri Limited Şirketi (Amazon AWS S3)	Esentepe Mahallesi Bahar Sk. Özdilek/River Plaza No: 13/52 Şişli, Istanbul, 34394, TR	Pisano Server Storage Provider

ANNEX IV – TRANSFER RISK ASSESSMENT

The European Commission, the United Kingdom Information Commissioner's Office, the Swiss Federal Information Commission, and other data protection authorities have approved the use of EU SCCs or UK SCCs (as applicable) (hereinafter together, "SCCs") to safeguard personal data transferred to "third countries" with dissimilar privacy laws only when the parties conduct a risk assessment and adopt supplementary measures to the extent necessary to assure an equivalent level of protection for the data. This Annex 5 provides information in support of the representations and warranties of the Data Importer and Data Exporter (as outlined in Annex 1 above) in data transfer agreements such as Clause 14(a) of the SCCs:

1. The Data Importer will assist the Data Exporter by assessing and monitoring whether the laws applicable to it provide adequate protection under Data Protection Laws. To the extent that it determines that any such laws are not in line with the requirements of the SCCs and Data Protection Laws, it undertakes to comply with the safeguards set out in paragraphs 2 to 5 below.

2. The Data Importer will adopt supplementary measures to protect the Personal Data received under the SCCs from the Data Exporter in accordance with the requirements of Data Protection Laws, including by implementing appropriate technical and organizational safeguards to protect personal data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defence and public security. Such technical and organisational measures may include, as relevant and necessary in light of the nature, scope and circumstances of the transfer: (a) encryption or similar technologies to protect Personal Data in-transit and at-rest; (b) pseudonymization of Personal Data; (c) access and confidentiality controls and policies; and/or (d) access logs and other similar audit trails.

3. The Data Importer warrants that: (a) it has not purposefully created any means by which a public authority can bypass the Data Importer's security mechanisms, authentication procedures and/or software to gain access to and/or use its systems and/or the Personal Data, such as a back door or similar programming; (b) it has not purposefully created or changed its business processes, security mechanisms, software and/or authentication procedures in a manner that facilitates access to its systems and/or the Personal Data by public authorities; and (c) it is not required by national law or government policy to create or maintain any means to facilitate access to its systems and/or the Personal Data by public authorities, such as a back door, or for the Data Importer to be in possession or to hand over the encryption key to access such data.

4. Any audits, including requests for reports or inspections, carried out by the Data Exporter or a qualified independent assessor selected by the Data Exporter ("Independent Assessor") of the processing activities will include, at the choice of the Data Exporter and/or Independent Assessor, verification as to whether any Personal Data has been disclosed to public authorities and, if so, the conditions under which such disclosure has been made.

5. In the event that the Data Importer receives a legally binding request for access to the Personal Data by a public authority, the Data Importer will:

(a) promptly notify the Data Exporter of such request to enable the Data Exporter to intervene and seek relief from such disclosure, unless the Data Importer is otherwise prohibited from providing such notice, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. If the Data Importer is so prohibited and in the event that, despite having used its reasonable best efforts, the Data Importer is not permitted to notify the Data Exporter, it will make available on an annual basis general information on the requests it received to the Data Exporter and/or the competent supervisory authority of the Data Exporter;

(b) promptly inform the public authority if, in the Data Importer's opinion, such request is inconsistent and/or conflicts with its obligations pursuant to the SCCs. The Data Importer will document any such communication with the public authorities relating to the inconsistency and/or conflict of such request with the SCCs;

(c) have in place and comply with its data disclosure related policies;

(d) not make any disclosures of the Personal Data to any public authority that are determined to be massive, disproportionate and indiscriminate in a manner that it would go beyond what is necessary in a democratic society; and

(e) upon request from the Data Exporter, provide general information on the requests from public authorities it received in the preceding 12 month period relating to Personal Data. Where possible, such information will include the following: (i) an overview of laws and regulations that permit access to the Personal Data in the jurisdiction to which the Data Importer is subject, to the extent the Data Importer is reasonably aware of such laws and regulations; (ii) any measures taken to prevent access by public authorities to the Personal Data; (iii) information about the nature and number of such requests received by the Data Importer; (iv) the type of Personal Data requested; (v) the requesting body; (vi) the legal basis to disclose the Personal Data to the public authority; and (vii) whether the Data Importer reasonably believes that it is legally prohibited to provide the information in subsections (i) to (vi) above and, if so, the extent to which such prohibition applies.