Carpio Data Processing Agreement

1. Definitions and interpretation

1.1. In this Agreement, capitalised terms shall have the following meaning:

a) **Affiliates**: in relation to a Party, any person which, directly or indirectly (i) is controlled by that party; or (ii) controls that party; or (iii) is under common control with that party;

b) **Agreement**: this data processor agreement and the related Carpio SaaS Terms of Service

c) **Applicable Law**: any legislation applicable to the processing, protection, confidentiality or the privacy of the personal data, including but not limited to English Data Protection laws and the General Data Protection Regulation.

d) **Data Subject**, **Data Processor**, **Data Controller**, **Personal Data** (in this Agreement also referred to as **Data**) have the meaning assigned to them in the European Data Protection Directive 95/46/EC.

e) **Disclosure**: any form of disclosure of the Data or any copies thereof to a Third Party, including, but not limited to, the transfer of Data to a Third Party and the (remote) access to the Data by a Third Party (hereinafter also referred to as a verb "**Disclose**").

f) **Data Processing**: any operation upon the Personal Data, including without limitation accessing, collecting, storing, using, organizing, combining, altering, transferring, disclosing or deleting the Personal Data, carried out in the course of rendering the Services.

g) **Party**; one of the parties to this Agreement (Customer or Carpio as defined in the Terms of Service);

h) **Services**; the Carpio SaaS platform and any services delivered as part of that platform including any managed services;

i) **Third Party**: any party other than the parties to this Agreement. The term includes any affiliate, (sub)contractor, or unauthorized personnel of Processor as well as any public authority.

j) **Transfer of the Personal Data**: forwarding, copying and providing remote access to the Personal Data (hereinafter also referred to as a verb "**transfers**").

1.2. Any obligation in this Agreement of one Party to 'inform' or 'notify' the other Party, means an obligation to inform or notify in writing, which includes informing or notifying per e-mail.

2. Obligations of Processor

General

2.1. Processor shall conduct the Data Processing in accordance with Applicable law and this Agreement with regard to the Data Processing.

2.2. Processor shall perform the Data Processing appropriately and accurately and only insofar as needed to perform or deliver the Services and shall not perform the Data other purposes not specifically authorized by Client (or any of its Affiliates).

2.3. This Agreement is entered into between Client and Processor, on Client's own behalf, and on behalf of and for the benefit of Client Affiliates, on behalf of which Client is entitled to enforce any and all of the provisions of the Agreement. For purposes of the Agreement, "Client" also means each of its Affiliates, unless explicitly provided otherwise. Client Affiliates are entitled to enforce the provisions of the Agreement as though those entities were Client.

Security

2.4. Processor shall take reasonable technical and organizational security measures which are required to secure Personal Data against (accidental) loss, disclosure or alteration or unlawful processing, taking into account the state of the art and the costs of the implementation, ensuring an adequate level of protection taking into account the risks involved in the Data Processing and the nature of the Personal Data to be secured. The applicable security measures have been specified in **Annex 1** to this Agreement, which Processor shall revise if so required to reflect industry standards.

Disclosure

2.5. Save for a disclosure to a competent public authority, Processor shall not Disclose the Data to any Third Party without the prior written approval of a properly authorized employee Client or if this is otherwise allowed pursuant to this Agreement.

2.6. Client hereby authorizes and, where relevant, hereby instructs Processor to Disclose the Personal Data (i) to Processor's affiliates or contractors, but only insofar such affiliates or contractors are directly involved in the provision of the Services or insofar such Disclosure is necessary for the protection, or improvement, audit or review of the Data; and (ii) to a Third Party in order to comply with a legal obligation to which Client, Processor or the Data Subject is subject, provided such Disclosure is directly related to the provision of the Services.

2.7. Any approval by Client of Disclosure of Data by Processor to a Third Party shall be subject to Processor contractually obliging the Third Party to (i) abide by at least the same measures and obligations with regard to the Data Processing that are captured in this Agreement, and (ii) obliging such Third Party not to further process the Personal Data than to the extent allowed under this Agreement.

2.8. Each act or omission of a Third Party engaged by Processor to fulfil its obligations under the Services Agreement, in relation to the obligations set forth in this Agreement shall be deemed to be an act or omission of Processor for which Processor is responsible and fully liable.

Transfer outside the EEA or United Kingdom

2.9. Unless specifically agreed upon in writing between the Parties and taking into account the requirements under Applicable Law, Processor shall not be allowed to process Personal Data outside of the territory of the European Economic Area or the United Kingdom, with the following exceptions:

- Personal data associated with payments is processed by Stripe.com, a payment processor, which may process data outside of the European Economic Area or the United Kingdom

Sub-processors

2.10. Processor shall permit sub-processors to Process Personal Data without the prior written consent of Client. subject to the condition that Processor remains fully liable to Client for the sub-processor's performance of the contract, as well as for any acts or omissions of the sub-processor in regard to its Data Processing. Processor shall ensure that sub-processors are contractually bound to the same obligations with respect to the Data Processing as those which Processor is bound to under the Agreement.

Individuals

2.11. Processor shall promptly inform Client of any complaints, requests or enquiries received from Data Subjects, including but not limited to requests to correct, delete or block Personal Data. Processor shall not respond to the Data Subjects directly except where specifically instructed by Client, in which case Processor shall respond within a reasonable period of time, and in any case within three (3) weeks after receipt of the respective complaint, request or enquiry.

Processor shall in any event cooperate with Client to address and resolve any complaints, requests or enquiries from Data Subjects.

Data leakage

2.12. As soon as Processor has become aware of a security incident involving the Data (such as but not limited to leakage, unauthorized access, use, destruction, loss, alteration, disclosure), Processor shall (i) promptly, and in any case within forty-eight (48) hours, inform Client summarizing in reasonable detail (a) the likely impact on Client of the security incident, and (b) the corrective actions taken or to be taken by Processor; (ii) take all necessary and appropriate corrective actions to remedy any deficiencies in its security measures; and (iii) take any action pertaining to such security incident as far as required by Applicable Law.

Inform

2.13. Processor shall promptly inform Client if Processor (i) cannot for any reason comply with its obligations under the Agreement; (ii) becomes aware of any circumstance or change in Applicable Law that is likely to have a substantial adverse effect on Processor's ability to meet its obligations under the Agreement; or (iii) any inspection or inquiry made by any public authority with regard to the Data or the Data Processing.

Data retention

2.14. Processor shall not keep Data any longer than necessary for the purpose of performing or having performed the Services. Subject to Processor's legal and regulatory obligations with regard to the Data, Processor shall securely delete all the Data together with all copies in its possession or control. Client may require Processor to promptly confirm and warrant to it in writing that Processor deleted Data. Data may be stored in backups for up to 31 days following deletion and will expire from those backups after that time period.

3. Obligations of Client

3.1. Client shall (i) provide Processor with specific written instructions with regard to the security and confidentiality of the Personal Data in accordance with Applicable Law; (ii) inform Processor of any legitimate inspection or audit of the Data Processing by any competent authority which relates to the Data Processing by Processor; and (iii) inform Processor as soon as reasonably possible of any access request, request for correction or blocking of Personal Data or any objection related to the Data Processing by the Processor.

4. Notices

4.1. All notices, confirmations and other statements made by the Parties in connection with this Agreement shall be via email and shall be sent to info@carpio.tech or to the email address of the Client's designated Admin users within the Carpio platform.

5. Miscellaneous

5.1. Carpio retains the right to update this Agreement from time to time as required. Any changes to the this document will be communicated to the Client either via electronic mail, posted on the Website or within the Platform. Where the changes to the Agreement have a material impact on the Customer, the sole remedy of the Customer is to terminate the Agreement.

6. Governing Law

6.1. This Agreement is governed by and construed in accordance with the laws of the England and Wales.

6.2. Any disputes arising out of, or in connection with this Agreement shall be settled by the in accordance with procedure provided for in the SaaS Agreement, or - in the absence of such procedure – be brought for the competent court in England and Wales.

Annex 1: Technical and organizational security measures

1. The Processor is using a policy document that explicitly addresses measures to protect data processing, as well as privacy safeguards.
2. Employees of the Processor involved in the processing of Personal Data are bound by a confidentiality code.
3. All employees of the organization and, as appropriate, hired staff and external users get appropriate training and regular refresher about IT information security policy and the organization's information security procedures for as relevant to their function.
4. IT facilities and equipment are physically protected against unauthorized access and against damage and malfunctions.
5. There are procedures to allow authorized users access to the information systems and services they need for the performance of their duties.
6. There are procedures for the acquisition, development, maintenance and destruction of data and information systems.
7. Activities performed by users (with Personal Data) are recorded in log files. The same goes for other relevant events, such as attempts to unauthorized access to personal data and disturbances that may result to the loss or loss of personal data.
8. Security systems are incorporated in all application systems including an appropriate access control.
9. The network and information systems are actively monitored and managed.
10. There are procedures for the timely and effective handling of information security incidents and weaknesses in security as soon as they are reported.

Record of Processing activities:

Description processing activities by Processor:	Carpio will maintain a list of Client users for the purposes of authentication, authorization, audit, and notifications. The user list will be created by Clients, or their agents such as a marketplace agency, when creating their accounts in the platform or by inviting additional users to access their account.
Purpose of processing:	Authentication, authorisation, audit, notifications
Sub Processor(s)	Amazon Web Services (Ireland)
Description of the categories of data subjects:	Current and former platform users
Description of the categories of personal data:	Name, email address, company name
Description of the categories of recipients to whom the personal data have been or will be disclosed:	Other users within the Carpio platform who have shared access to the same accounts
Retention period:	Retained for audit purposes for up to 1 year after Client deletes their account