**CAPPFINITY**

**DATA PROCESSING AGREEMENT**

**THIS AGREEMENT** is made the [ ] day of [ ]

**BETWEEN:**

(1) **[Client Entity]** a company registered in England under number[registered number], whose registered office is at [registered address] (“Client”) and

(2) **Cappfinity Limited,** a company registered in England under number 06802155 whose registered office is at Birmingham Business Park, 2230-2235 Regents Court The Crescent, Birmingham B37 7YE (“Cappfinity”).

**WHEREAS:**

1. The parties agree that Client is at all times the data controller and Cappfinity is the data processor in relation to the Personal Data that Cappfinity processes in the course of providing the Data Processing Services to the Client.
2. Under an agreement [add date or other relevant detail to connect this DPA with the relevant SOW] between the Client and Cappfinity (“the Cappfinity Standard Terms”) Cappfinity will process personal data on the beahalf of the Client in accordance with the Data Processing Services described in Schedule 1.

(3) The Parties have agreed to enter into this Agreement to ensure compliance with applicable Data Protection Law in relation to all processing of the Personal Data by Cappfinity for the Client.

(4) The terms of this Agreement are to apply to all processing of Personal Data carried out for the Client by Cappfinity and to all Personal Data held by Cappfinity in relation to all such processing.

**IT IS AGREED** as follows:

1. Definitions and Interpretation
   * 1. In this Agreement, unless the context otherwise requires, the following expressions have the following meanings:

|  |  |
| --- | --- |
| **“Data Protection Law”**  **“Data Controller”, “Data Processor”, “processing”, and “data subject”** | means the UK GDPR and other applicable data protection legislation, including but not limited to the EU GDPR 2016. This also includes any replacement legislation that may come into affect from time to time.  shall have the meanings given to the terms “controller”, “processor”, “processing”, and “data subject” respectively under data protection law; |
| **“Supervisory Authority”** | means the UK’s supervisory authority, the Information Commissioner’s Office or other applicable supervisory authority; |
| **“Personal Data”** | means all such “personal data”, as defined under data protection law, as is, or is to be, processed by Cappfinity on behalf of the Client, as described in Schedule 1; |
| **“Data Processing Services”** | means the data processing activities described in Schedule 1 which are provided by Cappfinity to the Client in connection to the main agreement agreed to by Client and Cappfinity |
| **“Sub-Processor”** | means a sub-processor appointed by Cappfinity to process the Personal Data; and |
| **“Sub-Processing Agreement”** | means an agreement between Cappfinity and a Sub-Processor governing the Personal Data processing carried out by the Sub-Processor, as described in Clause 9. |

* + 1. Unless the context otherwise requires, each reference in this Agreement to:
       - 1. “writing”, and any cognate expression, includes a reference to any communication effected by electronic or facsimile transmission or similar means;
         2. a statute or a provision of a statute is a reference to that statute or provision as amended or re-enacted at the relevant time;
         3. “this Agreement” is a reference to this Agreement and each of the Schedules as amended or supplemented at the relevant time;
         4. a Schedule is a schedule to this Agreement; and
         5. a Clause or paragraph is a reference to a Clause of this Agreement (other than the Schedules) or a paragraph of the relevant Schedule.
         6. a "Party" or the "Parties" refer to the parties to this Agreement.
    2. The headings used in this Agreement are for convenience only and shall have no effect upon the interpretation of this Agreement.
    3. Words imparting the singular number shall include the plural and vice versa.
    4. References to any gender shall include all other genders.
    5. References to persons shall include corporations.

1. Scope and Application of this Agreement
   * 1. The provisions of this Agreement shall apply to the processing of the Personal Data described in Schedule 1, carried out for the Client by Cappfinity, and to all Personal Data held or accessed by Cappfinity in relation to all such processing whether such Personal Data is held at the date of this Agreement or received afterwards.
     2. This Agreement shall continue in full force and effect for so long as Cappfinity is processing Personal Data on behalf of the Client, and thereafter as provided in Clause 10.
2. Provision of the Data Processing Services and Processing Personal Data

Cappfinity is only to carry out the Data Processing Services described in Schedule 1, and only to process the Personal Data received from the Client:

* + 1. for the purposes of those Data Processing Services and not for any other purpose;
    2. to the extent and in such a manner as is necessary for those purposes; and
    3. strictly in accordance with the express written authorisation and instructions of the Client (which may be specific instructions or instructions of a general nature or as otherwise notified by the Client to Cappfinity).

1. Data Protection Compliance
   * 1. All instructions given by the Client to Cappfinity shall be made in writing and shall at all times be in compliance with applicable data protection law . Cappfinity shall act only on such written instructions from the Client unless the Cappfinity is required by law to do otherwise..
     2. Cappfinity shall promptly comply with any request from the Client requiring Cappfinity to amend, transfer, delete, or otherwise dispose of the Personal Data.
     3. Cappfinity shall transfer all Personal Data to the Client on the Client’s request in the formats, at the times, and in compliance with the Client’s written instructions.
     4. Both Parties shall comply at all times with applicable data protection law and other applicable laws and shall not perform their obligations under this Agreement or any other agreement or arrangement between themselves in such way as to cause either Party to breach any of its applicable obligations under data protection law.
     5. Cappfinity agrees to comply with any reasonable measures required by the Client to ensure that its obligations under this Agreement are satisfactorily performed in accordance with any and all applicable legislation from time to time in force and any best practice guidance issued by the ICO or other supervisory authority.
     6. Cappfinity shall provide all reasonable assistance to the Client in complying with its obligations under data protection law respect to the security of processing, the notification of personal data breaches, the conduct of data protection impact assessments, and in dealings with supervisory authorities.
     7. When processing the Personal Data on behalf of the Client, Cappfinity shall:
        + 1. not process the Personal Data outside the UK or European Economic Area (all EU member states, plus Iceland, Liechtenstein, and Norway) (“EEA”) without the prior written consent of the Client and, where the Client consents to such a transfer to a country that is outside of the UK or EEA, to comply with the obligations of Cappfinity under the provisions applicable to transfers of Personal Data to third countries providing an adequate level of protection to any Personal Data that is transferred;
          2. not transfer any of the Personal Data to any third party without the written consent of the Client and, in the event of such consent, the Personal Data shall be transferred strictly subject to the terms of a suitable agreement, as set out in Clause 9;
          3. process the Personal Data only to the extent, and in such manner, as is necessary in order to comply with its obligations to the Client or as may be required by law (in which case, Cappfinity shall inform the Client of the legal requirement in question before processing the Personal Data for that purpose unless prohibited from doing so by law);
          4. implement appropriate technical and organisational measures and take all steps necessary to protect the Personal Data against any unauthorised processing, including any accidental or unlawful loss, destruction, damage, alteration, disclosure or access. In assessing the appropriate level of security, the Parties shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks for Data Subjects. Cappfinity shall at least implement the technical and organisational measures specified in Schedule 2 and shall inform the Client in advance of any material changes to such measures:
          5. if so requested by the Client acting reasonably (and within the timescales required by the Client) supply further details of the technical and organisational systems in place to safeguard the security of the Personal Data held and to prevent unauthorised access;
          6. keep detailed records of all processing activities carried out on the Personal Data;
          7. make available to the Client any and all such information as is reasonably required and necessary to demonstrate Cappfinity’s compliance with data protection law;
          8. on reasonableprior notice, submit to audits and inspections and provide the Client with any information reasonably required in order to assess and verify compliance with the provisions of this Agreement and both Parties’ compliance with the requirements of data protection law.ClientCappfinity; and
          9. inform the Client immediately if it is asked to do anything that infringes any applicable data protection legislation.
2. Data Subject Access, Complaints, DPIAs and Breaches
   * 1. Cappfinity shall assist the Client in complying with its obligations under data protection law. In particular, the following shall apply to data subject access requests, complaints, and data breaches.
     2. Cappfinity shall notify the Client without undue delayif it receives:
        + 1. a subject access request from a data subject; or
          2. any other complaint or request relating to the processing of the Personal Data.
     3. Cappfinity shall cooperate fully with the Client and assist as required in relation to any subject access request, complaint, or other request, including by:
        + 1. providing the Client with full details of the complaint or request;
          2. providing the necessary information and assistance in order to comply with a subject access request;
          3. providing the Client with any Personal Data it holds in relation to a data subject upon reasonable noticeClient; and
          4. providing the Client with any other information reasonably requested by the Client.
     4. Cappfinity shall notify the Client as soon as possible if it becomes aware of any form of Personal Data breach, including any unauthorised or unlawful processing, loss of, damage to, or destruction of any of the Personal Data.
     5. Cappfinity shall provide reasonable assistance with any Data Protection Impact Assessments (DPIAs) requested by the Client upon reasonable written notice.
3. Liability and Indemnity

Subject to any limitations of liability in the Cappfinity Standard Terms or any other terms and conditions entered into between the parties, Cappfinity shall indemnify, the Client, against all losses suffered or incurred by the Client arising out of the failure by Cappfinity or its employees or agents to comply with of its obligations under this Agreement (“Claims”). Each party acknowledges that Claims include any claim or action brought by a data subject arising from Cppfinity’sbreach of its obligations under this Agreement.

1. Intellectual Property Rights

All copyright, database rights, and other intellectual property rights subsisting in the Personal Data (including but not limited to any updates, amendments, or adaptations to the Personal Data made by either the Client or Cappfinity) shall belong to the Client or to any other applicable third party from whom the Client has obtained the Personal Data under licence (including, but not limited to, data subjects, where applicable). Cappfinity is licensed to use such Personal Data under such rights only for the purposes of the Data Processing Services, and in accordance with this Agreement.

1. Confidentiality
   * 1. Cappfinity shall maintain the Personal Data in confidence, and in particular, unless the Client has given written consent for Cappfinity to do so, Cappfinity shall not disclose any Personal Data supplied to by, for, or on behalf of, the Client to any third party. Cappfinity shall not process or make any use of any Personal Data supplied to it by the Client otherwise than in connection with the provision of the Data Processing Services to the Client.
     2. Cappfinity shall ensure that all personnel who are to access and/or process any of the Personal Data are contractually obliged to keep the Personal Data confidential.
     3. The obligations set out in in this Clause 8 shall continue for a period of six years after the cessation of the provision of software or services by Cappfinity to the Client.
     4. Nothing in this Agreement shall prevent either Party from complying with any requirement to disclose Personal Data where such disclosure is required by law. In such cases, the Party required to disclose shall notify the other Party of the disclosure requirements prior to disclosure, unless such notification is prohibited by law.
2. Appointment of Sub-Processors
   * 1. The Client consents to Cappfinity engaging third party subprocessors to process the Data for the Permitted Purpose provided that Cappfinity:

(i) maintains an up-to-date list of its subprocessors at [Cappfinity-Personal-Data-Subprocessors-Notice.pdf](https://www.cappfinity.com/global/wp-content/uploads/sites/3/2022/05/Cappfinity-Personal-Data-Subprocessors-Notice.pdf), which it shall update with details of any change in subprocessors at least 10 days prior to any such change;

(ii) imposes data protection terms on any subprocessor it appoints that require it to protect the Data to the standard required by Applicable Data Protection Law; and

(iii) remains liable for any breach of this Clause that is caused by an act, error or omission of its subprocessor.

9.2 The Client may object to Cappfinity's appointment or replacement of a subprocessor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to the Client's ability to comply with Applicable Data Protection Laws. In such event, Cappfinity will either not appoint or replace the subprocessor or, if this is not possible, the Client may suspend or terminate the relevant Order(s) (without prejudice to any fees incurred by the Client prior to suspension or termination).

1. Deletion and/or Disposal of Personal Data
   1. Subject to the provisions of the Terms, upon termination or expiry of the relevant Order(s), Cappfinity shall (at the Client's election) destroy or return to the Client all Personal Data in its possession or control.
   2. This requirement shall not apply to the extent that Cappfinity is required by applicable law to retain some or all of the Personal Data, or to Personal Data it has archived on back-up systems, which Personal Data Cappfinity shall securely isolate and protect from any further processing except to the extent required by law.
2. Law and Jurisdiction
   * 1. This Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall be governed by, and construed in accordance with, the laws of England and Wales.
     2. Any dispute, controversy, proceedings or claim between the Parties relating to this Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall fall within the jurisdiction of the courts of England and Wales.

SIGNED for and on behalf of the Client by:

[insert name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Authorised Signature

Date: [ ]

SIGNED for and on behalf of the Cappfinity by:

[insert name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Authorised Signature

Date: [ ]

**SCHEDULE 1**

**Data Processing Information**

**Nature and purpose of processing operations**

Nature and purpose of data processing is as follows (please specify):

*[ ]*

**Categories of data subject**

The Personal Data transferred concern the following categories of data subjects (please specify):

*[ ]*

**Categories of data**

The Personal Data transferred concern the following categories of data (please specify):

*[… ]*

**Special categories of data (if appropriate)**

The Personal Data transferred concern the following special categories of data (please specify):

*Insert details if relevant]*

**Duration of Processing**

*The* Personal Data *shall be processed for the term of the DPA or for such longer or shorter period as the Supplier provides data processing services under the DPA.*

**List of Sub-processors**

Client approves the following sub-processors to process Personal Data on behalf of the Supplier:

**SCHEDULE 2**

**Technical and Organisational Security Measures**

Cappfinity currently observes the security practices described in this Annex. Notwithstanding any provision to the contrary otherwise agreed to by Client, Cappfinity may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices. All capitalised terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

a) Access Control

i) Preventing Unauthorized Product Access

Outsourced processing: Cappfinity hosts its Service with outsourced cloud infrastructure providers. Additionally, Cappfinity maintains contractual relationships with vendors in order to provide the Service in accordance with our Data Processing Agreement.

Cappfinity relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: Cappfinity hosts its product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications, as per https://azure.microsoft.com/en-gb/overview/trusted-cloud/compliance and https://aws.amazon.com/compliance/

Authentication: Cappfinity has implemented a strong password policy for its Service. Customers who interact with the Service must authenticate before accessing its Service.

Authorisation: Customer data is stored in multi-tenant storage systems accessible to customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure.

The authorisation model in each of Cappfinity products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customisation options. Authorisation to data sets is performed through validating the user’s permissions against the attributes associated with each data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key.

ii) Preventing Unauthorised Product Use

Cappfinity implements industry standard access controls and detection capabilities for the internal networks that support its Service.

Security reviews of code stored in Cappfinity source code repositories is performed, checking for coding best practices and identifiable software flaws.

iii) Limitations of Privilege & Authorisation Requirements

Product access: A subset of Cappfinity employees have access to the product and to personal data via controlled interfaces, based on a business need to know. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through “just in time” requests for access; all such requests are logged. Employees are granted access by role.

Code of conduct: All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

b) Transmission Control

In-transit: Cappfinity makes HTTPS encryption (also referred to as SSL or TLS) mandatory on every one of its login interfaces. Cappfinity HTTPS implementation uses industry standard algorithms and certificates.

At-rest: Cappfinity stores user passwords following policies that follow industry standard practices for security.

c) Input Control

Detection: Cappfinity has designed its infrastructure to log extensive information about the system behaviour, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Cappfinity personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: Cappfinity maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, Cappfinity will take appropriate steps to minimize damage or unauthorized disclosure.

Communication: If Cappfinity becomes aware of unlawful access to data stored within its products, Cappfinity will notify those affected promptly per the GDPR requirements described in Article 34.