DATA PROCESSING AGREEMENT ("**DPA**")

VARIABLES	
Parties' relationships	Processor to Controller
Parties' roles	Customer (as defined in Clause 1 of the Main Agreement) will act as the Controller. BrambleAI (as defined in Clause 1 of the Main Agreement) will act as the Processor.
Main Agreement	The document entered into by the parties entitled "Founding Partner Agreement". For the avoidance of doubt, the Main Agreement together with this DPA collectively form the contract between the Customer and BrambleAI.
Term	This DPA will commence on the commencement date of the Main Agreement and will continue for the term of the Main Agreement.
Breach Notification Period	Without Undue Delay after becoming aware of a personal data breach.
Sub-processor Notification Period	14 days before the new sub-processor is granted access to Personal Data.
Liability Cap	For the avoidance of doubt, this DPA will be subject to the liability limitations and exclusions of liability in the body of the Main Agreement.
Governing Law and Jurisdiction	England and Wales.
Data Protection Laws	All laws, regulations and court orders which apply to the processing of Personal Data, including in the European Economic Area (EEA), the United Kingdom (UK). This includes the: ● European Union Regulation (EU) 2016/679 ● the Data Protection Act 2018

	● UK GDPR each as amended from time to time.
Services related to processing	Provision of the Service
Duration of processing	For the Term of this DPA
Nature and purpose of processing	**Care management solution, including:** ● Rostering and visit scheduling ● Billing ● Call transcription, categorisation, and summarisation ● Product improvement ● Service and support Data must be anonymised when used for any purpose other than those listed above.

Personal Data	The types of personal data processed are:
	The personal data to be processed fall within the categories of data:
	<u>**Client service user:**</u>
	- Full Names - Contact Details - Care Agency Name - Nationality - Date Of Birth - Gender - Address - Visit Information - Profile photo - Leave Details E.G. Temporary Inactivity - Audio recordings of telephone calls made through the Customer's telephony systems - Service delivery records (visit duration, assigned carers, and notes relevant to scheduling only) - Concerns - Funding Source
	<u>**Customer employee /former employees or nominated third party:**</u>
	- Full Names - Contact Details - Hours Worked - Employer - Rostering Information - Payroll Information (including rate card etc) - Visit Information - Carer Availability - Skills, Training and Experience - DOB, Gender, address, transport method - Audio recordings of telephone calls made through the Customer's telephony systems - Covid vaccination status and other medical records - Working hours and absences (e.g., annual / sick leaves) - Termination dates
	<u>**Relatives/nominated third parties**</u>

	- Full Names - Contact Details - Relationship To Service User - Audio recordings of telephone calls made through the Customer's telephony systems **Sensitive data** The personal data to be processed fall within the following categories of sensitive data: - Health Data
Data subjects	The individuals whose Personal Data will be processed are: - Customer's Service users/former users & their relatives/nominated third parties - Customer employees/former employees - Customer's nominated third parties
Special provisions	None
Transfer Mechanism	N/A

ANNEX 1	
Security measures. Technical and organisational measures to ensure the security of Personal Data	https://www.bramble.care/security-measures

ANNEX 2	
Sub-processors. Current sub-processors	https://www.bramble.care/subprocessors

TERMS

1. **What is this agreement about?**
   1.1. **Purpose**. The parties are entering into this Data Processing Agreement (DPA) for the purpose of processing Personal Data (as defined above).
   1.2. **Definitions**. Under this DPA:

(a) **adequate country** means a country or territory that is recognised under Data Protection Laws from time to time as providing adequate protection for processing Personal Data,

(b) **Controller, data subject, personal data breach, process/processing, Processor** and **supervisory authority** have the same meanings as in the Data Protection Laws,

(c) **Sub-Processor** means another processor engaged by the Processor to carry out specific processing activities with Personal Data.

2. **What are each party's obligations?**

2.1. **Controller obligations.** Controller instructs Processor to process Personal Data in accordance with this DPA, and is responsible for providing all notices and obtaining all consents, licences and legal bases required to allow Processor to process Personal Data.

2.2. **Processor obligations**. Processor will:

(a) only process Personal Data in accordance with this DPA and Controller's instructions (unless legally required to do otherwise),

(b) not sell, retain or use any Personal Data for any purpose other than as permitted by this DPA and the Main Agreement,

(c) inform Controller immediately if (in its opinion) any instructions infringe Data Protection Laws,

(d) use the technical and organisational measures described in Annex 1 when processing Personal Data to ensure a level of security appropriate to the risk involved,

(e) notify Controller of a personal data breach within the Breach Notification Period and provide assistance to Controller as required under Data Protection Laws in responding to it,

(f) ensure that anyone authorised to process Personal Data is committed to confidentiality obligations,

(g) without undue delay, provide Controller with reasonable assistance with:
  (i) data protection impact assessments,
  (ii) responses to data subjects' requests to exercise their rights under Data Protection Laws, and
  (iii) engagement with supervisory authorities,

(h) if requested, provide Controller with information necessary to demonstrate its compliance with obligations under Data Protection Laws and this DPA,
  (i) allow for audits at Controller's reasonable request, provided that audits are limited to once a year and during business hours except in the event of a personal data breach, and
  (ii) return Personal Data upon Controller's written request or delete Personal Data by the end of the Term, unless retention is legally required.

2.3. **Warranties**. The parties warrant that they and any staff and/or subcontractors will comply with their respective obligations under Data Protection Laws for the Term.

2.4. **Warranties**. The parties warrant that they and any staff and/or subcontractors will comply with their respective obligations under Data Protection Laws for the Term.

3. **Sub-processing**

3.1. **Use of sub-processors**. Controller authorises Processor to engage other processors (referred to in this section as **sub-processors**) when processing Personal Data. Processor's existing sub-processors are listed in Annex 2.

3.2. **Sub-processor requirements**. Processor will:

   (a) require its sub-processors to comply with equivalent terms as Processor's obligations in this DPA,

   (b) ensure appropriate safeguards are in place before internationally transferring Personal Data to its sub-processor, and

   (c) be liable for any acts, errors or omissions of its sub-processors as if they were a party to this DPA.

3.3. **Approvals**. Processor may appoint new sub-processors provided that they notify Controller in writing in accordance with the Sub-processor Notification Period.

3.4. **Objections**. Controller may reasonably object in writing to any future sub-processor. If the parties cannot agree on a solution within a reasonable time, either party may terminate this DPA.

4. **International personal data transfers**

4.1. **Instructions**. Processor may transfer data outside the UK where:

   (a) a UK data adequacy decision exists for the relevant destination country, or;

   (b) it has implemented a Transfer Mechanism compliant with Data Protection Laws, which for example may include a derogation pursuant to Article 49 of the GDPR applies or an appropriate Transfer Mechanism under UK or EU GDPR is used such as an International Data Transfer Agreement, and;

   (c) transfer is made to a sub processor acting as an employer-of-record for the Processor personnel, and individuals with access are operating directly and exclusively under the Supplier's governance and controls.

4.2. **Transfer mechanism**. Where a party is located outside the UK, the EEA or an adequate country and receives Personal Data:

   (a) that party will act as the data importer,

   (b) the other party is the data exporter, and

   (c) the relevant Transfer Mechanism will apply.

4.3. **Additional measures**. If the Transfer Mechanism is insufficient to safeguard the transferred Personal Data, the data importer will promptly implement supplementary measures to ensure Personal Data is protected to the same standard as required under Data Protection Laws.

4.4. **Disclosures**. Subject to terms of the relevant Transfer Mechanism, if the data importer receives a request from a public authority to access Personal Data, it will (if legally allowed):

    (a) challenge the request and promptly notify the data exporter about it, and

    (b) only disclose to the public authority the minimum amount of Personal Data required and keep a record of the disclosure.

5. Other important information

5.1. **Survival**. Any provision of this DPA which is intended to survive the Term will remain in full force.

5.2. **Order of precedence**. In case of a conflict between this DPA and other relevant agreements, they will take priority in this order:

    (a) DPA,

    (b) Main Agreement.

5.3. **Notices**. Formal notices under this DPA must be in writing.

5.4. **Governing law and jurisdiction**. The Governing Law applies to this DPA and all disputes will only be litigated in the courts of the Jurisdiction.