DATA PROCESSING AGREEMENT

Last Modified date 02/07/2024

The Parties have agreed to enter into this Agreement to ensure compliance with the said provisions of UK GDPR in relation to all processing of the Personal Data by the Customer for Journey. The terms of this Agreement are to apply to all processing of Personal Data carried out for Journey by the Customer and to all Personal Data held by the Customer in relation to all such processing and is subject to the terms set out in the Master Services Agreement (the "MSA").

DEFINITIONS

IT IS AGREED as follows:

1.Definitions and Interpretation

1.1 In this Agreement, unless the context otherwise requires, the following expressions have the following meanings:

"Data Controller", "Customer", "Data Processor", "Processing", and "Data Subject"	shall have the meanings given to the terms "controller", "processor", "processing", and "data subject" respectively in Article 4 of the UK GDPR;
"ICO"	means the UK's supervisory authority, the Information Commissioner's Office;
"Personal Data"	means all such "personal data", as defined in Article 4 of the UK GDPR, as is, or is to be, processed by the Customer on behalf of Journey, as described in Schedule 1;
"Services"	means those services and facilities which are provided by Journey to the Customer and which Journey uses for the purposes for discharging The Service Agreement;
"Sub-Processor"	means a sub-processor appointed by Journey to process the Personal Data; and
"Sub-Processing Agreement"	means an agreement between Journey and a Sub-Processor governing the Personal Data processing carried out by the Sub-Processor, as described in Clause 8.

2. **Scope and Application of this Agreement**
    a. The provisions of this Agreement shall apply to the processing of the Personal Data described in Schedule 1, carried out for the Customer by Journey, and to all Personal Data held by Journey in relation to all such processing whether such Personal Data is held at the date of this Agreement or received afterwards.
    b. This Agreement shall continue in full force and effect for so long as Journey is processing Personal Data on behalf of the Customer, and thereafter as provided in Clause 9.

3. **Provision of the Services and Processing Personal Data**
    a. Journey is only to carry out the Services, and only to process the Personal Data received from the Customer:

i. for the purposes of those Services and not for any other purpose;
ii. to the extent and in such a manner as is necessary for those purposes; and
iii. strictly in accordance with the express written authorisation and instructions of the Customer (which may be specific instructions or instructions of a general nature or as otherwise notified to Journey by the Customer).

4. **Data Protection Compliance**

a. Journey shall promptly comply with any request from the Customer requiring Journey to amend, transfer, delete, or otherwise dispose of the Personal Data.
b. Journey shall transfer all Personal Data to the Customer on their request in the formats, at the times, and in compliance with the Customer's written instructions.
c. Both Parties shall comply at all times with the UK GDPR 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 the UK GDPR.
d. The Customer hereby warrants, represents, and undertakes that the Personal Data shall comply with the UK GDPR in all respects including, but not limited to, its collection, holding, and processing.
e. Each Party agrees to comply with any reasonable measures required by the other Party 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 (including, but not limited to, the UK GDPR) and any best practice guidance issued by the ICO.
f. Journey will keep records of its Processing activities in accordance with the Data Protection Legislation
g. Journey confirm that all employees have undertaken training on the Data Protection Legislation relating to handling Personal Data and are aware of their personal duties and obligations under the Data Protection Legislation and this Agreement;
h. Each Party shall provide all reasonable assistance to the other Party in complying with its obligations under the UK GDPR with respect to the security of processing, the notification of personal data breaches, the conduct of data protection impact assessments, and in dealings with the ICO.
i. When processing the Personal Data on behalf of the Customer, Journey shall:
    i. data should not be transferred outside of the UK or to any international organisation (as defined in the UK GDPR) (together "Restricted Countries") without the prior written consent of the customer and shall ensure that any Processing or transfer of Partner Organisation Personal Data in or to any Restricted Countries complies with all requirements of the Data Protection Legislation.
    ii. not transfer any of the Personal Data to any third party without the written consent of the Customer;
    iii. process the Personal Data only to the extent, and in such manner, as is necessary in order to comply with its obligations to the Customer or as may be required by law;
    iv. implement appropriate technical and organisational measures, as described in Schedule 2, and take all steps necessary to protect the Personal Data against unauthorised or unlawful access, processing, accidental loss, destruction, damage, alteration, or disclosure;
    v. if so requested by the Customer 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;
    vi. make available to the Customer any and all such information as is reasonably required and necessary to demonstrate the Journey's compliance with the UK GDPR;

vii. on reasonable prior notice, submit to audits and inspections and provide the Customer 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 the UK GDPR.

viii. inform the Customer immediately if it is asked to do anything that infringes the UK GDPR or any other applicable data protection legislation.

5. **Data Subject Access, Complaints, and Breaches**

a. Journey shall assist the Customer in complying with its obligations under the UK GDPR. In particular, the following shall apply to data subject access requests, complaints, and data breaches.

b. Journey should notify the customer without undue delay if they receive:

i. a subject access request from a data subject; or

ii. any other complaint or request relating to the processing of the Personal Data.

c. Journey should notify the customer and assist as required in relation to any subject access request, complaint, or other request, including by providing the requesting Party:

i. with full details of the complaint or request;

ii. the necessary information and assistance in order to comply with a subject access request;

iii. with any Personal Data they hold in relation to a data subject; and

iv. any other information requested.

d. Journey shall notify the Customer immediately if it becomes aware of any form of Personal Data breach, including any unauthorised or unlawful access, processing, loss of, damage to, or destruction of any of the Personal Data, in addition Journey will provide assistance and co-operation to the customer in relation to Personal Data Breach including with Personal Data Breach notifications to Data Subjects and supervisory authorities.

e. Journey should notify the customer of any communications from Information Commissioner or any other regulatory authority in connection with the customer Personal Data.

f. The customer should be notified of a request from any third party for disclosure of Customer Personal Data where compliance with such request is required or purported to be required by Law.

g. For further details on Subject Access Requests please refer to Journey's Subject Access Request Procedure.

6. **Liability and Indemnity**

a. The Customer shall be liable for, and shall indemnify (and keep indemnified) Journey in respect of any and all action, proceeding, liability, cost, claim, loss, expense, reasonable legal fees, or demand suffered or incurred by, awarded against, or agreed to be paid by, Journey and any Sub-Processor arising directly or in connection with:

i. any non-compliance by the Customer with the UK GDPR or other applicable legislation;

ii. any Personal Data processing carried out by Journey or Sub-Processor in accordance with instructions given by the Customer that infringe the UK GDPR or other applicable legislation; or

iii. any breach by the Customer of its obligations under this Agreement, except to the extent that Journey or any Sub-Processor is liable under sub-Clause 6.2.

b. Journey shall be liable for, and shall indemnify the Customer in respect of any and all action, proceeding, liability, cost, claim, loss, expense, reasonable legal fees or demand suffered or incurred by, awarded against, or agreed to be paid by Journey arising directly or in

connection with Journey's Personal Data processing activities that are subject to this Agreement:

i. only to the extent that the same results from the Journey's or a Sub-Processor's breach of this Agreement; and

ii. not to the extent that the same is or are contributed to by any breach of this Agreement by the Customer.

c. Nothing in this Agreement (and in particular, this Clause 6) shall relieve either Party of, or otherwise affect, the liability of either Party to any data subject, or for any other breach of that Party's direct obligations under the UK GDPR.

7. Confidentiality

a. Journey shall maintain the Personal Data in confidence, and in particular, unless the Customer has given written consent for Journey to do so, Journey shall not disclose any Personal Data supplied to them by, for, or on behalf of the Customer to any third party. Journey shall not process or make any use of any Personal Data supplied to it by the Customer otherwise than in connection with the provision of the Services to the Customer.

b. Journey 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.

8. Appointment of Sub-Processors

a. Journey shall not sub-contract any of its obligations or rights under this Agreement without the prior written consent of the Customer (such consent not to be unreasonably withheld).

b. In the event that Journey appoints a Sub-Processor, Journey shall:

i. enter into a Sub-Processing Agreement with the Sub-Processor which shall impose upon the Sub-Processor the same obligations as are imposed upon Journey by this Agreement and which shall permit both Journey and the Customer to enforce those obligations; and

ii. ensure that the Sub-Processor complies fully with its obligations under the Sub-Processing Agreement and the UK GDPR.

c. In the event that a Sub-Processor fails to meet its obligations under any Sub-Processing Agreement, the Journey shall remain fully liable to the Customer for failing to meet its obligations under this Agreement.

d. Sub-Processors at this current time that are engaged to supply certain products and services on our behalf or to facilitate the running of our business and contracts include payment processing, delivery, IT support, consultancy services, service providers, data centres, security and back-up. In some cases, those third parties may require access to some or all of your personal data that we hold.

9. Deletion and/or Disposal of Personal Data

a. Journey shall, at the written request of the Customer, delete (or otherwise dispose of) the Personal Data or return it to the Customer within a reasonable time after the earlier of the following:

i. the end of the provision of the Services under the Service Agreement; or

ii. the processing of that Personal Data by Journey is no longer required for the performance of the Journey's obligations under this Agreement and/or the Service Agreement.

b. Following the deletion, disposal, or return of the Personal Data, Journey shall delete (or otherwise dispose of) all further copies of the Personal Data that it holds, unless retention of such copies is required by law, in which case Journey shall inform the Customer of such requirements in writing.

c. All Personal Data to be deleted or disposed of under this Agreement shall be deleted or disposed of using certified confidential waste providers if held in hard copy format or upon advice from specialist IT Providers for all electronic data held.

d. Journey will confirm in writing to the customer once customer data has been deleted from all systems including backups.

10. Data Protection

The parties agree that the Client is a Controller and that Journey is a Processor for the purposes of processing Personal Data pursuant to the Contract. The parties acknowledge and agree to the terms of Journey's data processing agreement.

Each Party shall comply with the Data Protection Legislation and the data protection clauses of this Agreement are in addition to, and do not relieve, remove or replace the Parties' obligations under the Data Protection Legislation.

11. **Law and Jurisdiction**

a. This Agreement shall be governed by, and construed in accordance with, the laws of England and Wales.

SCHEDULE 1

Personal Data

Categories of Data Subject	Type of Personal Data	Nature of Processing Carried Out	Purpose(s) of Processing	Duration of Processing
Employees	Name, Email Address, Phone Numbers, Gender (optional: picture, date of birth, nationality)	Collection and Storage in Processors Systems	Managing employees delivering well-being activities	Duration of service contract
Customers	Name, Email Address, Phone Numbers, Gender	Collection and Storage in Processors Systems	Taking bookings & delivering well-being activities to customers	Duration of service contract
Customers	Name, Email Address, Other relevant preference options	Storage, Uploading and segmentation of data	Email Marketing	Duration of service contract
Customers	Name, Email Address, other custom form fields	Data Storage	Product & Website form entries for email marketing and or provision of information	Duration of service contract
Customers	Phone numbers	Data Storage and tracking	Analytical statistics	Duration of service contract

SCHEDULE 2

Technical and Organisational Data Protection Measures

1. Journey shall ensure that, in respect of all Personal Data it receives from or processes on behalf of the Customer, it maintains security measures to a standard appropriate to:
    a. the harm that might result from unlawful or unauthorised processing or accidental loss, damage, or destruction of the Personal Data; and
    b. the nature of the Personal Data.
2. In particular, Journey shall have in place, and comply with, a security policy which:
    a. defines security needs based on a risk assessment;
        i. 2.1.1 is provided to the Customer on written request;
        ii. 2.1.2 is disseminated to all relevant staff.
    b. ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the Personal Data in accordance with best industry practice;
    c. prevent unauthorised access to the Personal Data;
    d. protect the Personal Data using pseudonymisation, where it is practical to do so;
    e. ensure that its storage of Personal Data conforms with best industry practice and access by personnel to Personal Data is strictly monitored and controlled;
    f. have secure methods in place for the transfer of Personal Data whether in physical form (for example, by using couriers rather than post) or electronic form (for example, by using encryption);
    g. encrypt data in transit: All data transmitted between systems must be encrypted using industry-standard encryption protocols, such as TLS (Transport Layer Security) 1.2 or higher. This includes data transferred over public and private networks to prevent unauthorised access during transmission.
    h. encryption of data at dest: All sensitive data stored within the systems must be encrypted using an industry-standard algorithm with sufficient key length, for example AES 256. This applies to all databases, file storage systems, and backup media.
    i. password protect all computers and other devices on which Personal Data is stored, ensuring that all passwords are secure and that passwords are not shared under any circumstances;
    j. take reasonable steps to ensure the reliability of personnel who have access to the Personal Data;
    k. have in place methods for detecting and dealing with breaches of security (including loss, damage, or destruction of Personal Data) including:
        i. having a proper procedure in place for investigating and remedying breaches of the UK GDPR; and
        ii. notifying the Customer as soon as any such security breach occurs.
    l. have a secure procedure for backing up all electronic Personal Data and storing back-ups separately from originals;
    m. have a secure method of disposal of unwanted Personal Data including for back-ups, disks, print-outs, and redundant equipment;