



DATA PROCESSING AGREEMENT

Last Modified date 08/10/2026

The Parties have agreed to enter into this Agreement to ensure compliance with the said provisions of Data Protection Legislation in relation to all processing of Service Personal Data by Journey on behalf of the Customer. The terms of this Agreement apply to all processing of Service Personal Data carried out by Journey on behalf of the Customer and to all Service Personal Data processed by Journey in relation to all such processing and are subject to the terms set out in the [Master Services Agreement \(the "MSA"\)](#).

DEFINITIONS

IT IS AGREED as follows:

1. Definitions and Interpretation

- a. 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 Service Personal Data unless expressly stated otherwise;
"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.
"Platform Usage Data"	means data relating to the use of the Platform by the Customer's Authorised Users, including but not limited to: page views, feature interactions, click paths, session duration, navigation patterns, and in-product feedback responses. Platform Usage Data is pseudonymised using opaque user identifiers and does not include the content of any data entered by Authorised Users into the Platform (including but not limited to guest names, booking details, email addresses, or any other Service Data).
"Service Data"	means all Personal Data processed by Journey on behalf of the Customer in the course of providing the Services, including but not limited to the data categories described in Schedule 1. Service Data does not include Platform Usage Data.
"Business Interaction Data"	means Personal Data relating to employees, contractors, representatives and other personnel of the Customer or third parties participating in meetings, calls or other business



communications with Journey, including the categories of Personal Data described in Schedule 4. Business Interaction Data does not include Service Data merely because such Service Data is referred to, displayed or otherwise captured incidentally during a business interaction.

"Business Interaction Processor"	means a processor appointed by Journey to process Business Interaction Data on Journey's behalf in its capacity as Data Controller.
"Platform Usage Sub-Processor"	means a Sub-Processor appointed by Journey specifically for the processing of Platform Usage Data.
"Authorised User"	means an individual authorised by the Customer to access and use the Platform.
"Data Protection Legislation"	means the UK GDPR and Data Protection Act 2018, the EU GDPR (Regulation (EU) 2016/679), where applicable, and any legislation implementing or supplementing the foregoing.
"Service Personal Data"	means Service Data only.
"Platform Usage Personal Data"	means Platform Usage Data only.
"Agency by Journey"	means Journey's hospitality marketing platform, provided with its technology partner, which uses artificial intelligence to generate marketing plans, creative and campaigns.

2. Scope and Application of this Agreement

- a. The provisions of this Agreement shall apply to the processing of the Service 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.
- c. Notwithstanding the foregoing, Journey may process Business Interaction Data as an independent Data Controller in accordance with Clause 10B and Schedule 4. Such processing shall not constitute processing of Service Personal Data on behalf of the Customer.

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).
- b. Notwithstanding Clause 3.a, Journey may collect and process Platform Usage Data for the purposes described in Schedule 3, acting as Data Controller in respect of such data. The Customer acknowledges and agrees that Journey's collection and processing of Platform Usage Data is not subject to the Customer's instructions under Clause 3.a, and is instead governed by the terms set out in Clause 10A and Schedule 3, subject to the Customer's right to disable Platform Usage Data collection under Clause 8.2.3.



- c. Notwithstanding Clause 3.a, Journey may collect and process Business Interaction Data for the purposes described in Schedule 4, acting as an independent Data Controller in respect of such data. The Customer acknowledges that Journey's processing of Business Interaction Data is not subject to the Customer's instructions under Clause 3.a and shall instead be governed by Clause 10B and Schedule 4.
- d. For the avoidance of doubt, Journey shall not collect, access, or process any Service Data for the purposes described in Schedule 3 unless such data has been fully anonymised such that no individual or Customer can be identified from it, whether directly or indirectly.

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 make available to the Customer the ability to export Service Personal Data using the standard data export functionality provided within the Platform during the term of the Services. The Customer acknowledges that it is responsible for exporting its Service Personal Data prior to termination or expiry of the Services using such functionality. Journey shall not be required to provide Service Personal Data in any bespoke format or via any method other than the standard export tools made available within the Platform, except where required by applicable law.
- c. Journey shall ensure that all persons authorised to access or process Service Personal Data are subject to a binding obligation of confidentiality, whether contractual or statutory.
- d. Both Parties shall comply at all times with the Data Protection Legislation and other applicable laws and shall not perform their obligations under this Agreement or any other agreement or arrangement between themselves in such a way as to cause either Party to breach any of its applicable obligations under the Data Protection Legislation.
- e. The Customer hereby warrants, represents, and undertakes that the Personal Data shall comply with the Data Protection Legislation in all respects including, but not limited to, its collection, holding, and processing.
- f. Journey does not process special category Personal Data through Agency by Journey unless the Parties have agreed it in writing with additional safeguards. The Customer warrants that it will not connect or enable an integration or data source that supplies special category Personal Data (for example health, dietary, accessibility, religious or biometric information about guests) to Agency by Journey without first notifying Journey and agreeing the safeguards, and will configure its connected systems to exclude such data where Journey asks.
- g. 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 Data Protection Legislation) and any best practice guidance issued by the ICO.
- h. Journey will keep records of its Processing activities in accordance with the Data Protection Legislation
- i. Journey confirms 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;
- j. Each Party shall provide all reasonable assistance to the other Party in complying with its obligations under the Data Protection Legislation 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.
- k. The Customer hereby provides general written authorisation for Journey to appoint Sub-Processors and to make international transfers of Service Personal Data in accordance with this Clause 4 and Clause 8. Journey operates a cloud-based infrastructure and may



process Service Personal Data in the United Kingdom, the European Economic Area, and other jurisdictions where it or its Sub-Processors maintain operations.

- i. Journey may transfer Service Personal Data outside the United Kingdom where:
 - a. the transfer is to a country or territory that is subject to a UK adequacy regulation;
 - b. the transfer is subject to appropriate safeguards in accordance with Article 46 of the UK GDPR or, where applicable, Article 46 of the EU GDPR, including but not limited to:
 - i. the UK International Data Transfer Agreement (IDTA);
 - ii. the UK Addendum to the EU Standard Contractual Clauses;
 - iii. the Standard Contractual Clauses adopted by the European Commission pursuant to Commission Implementing Decision (EU) 2021/914; or
 - iv. any other valid transfer mechanism recognised under applicable Data Protection Legislation.

Journey shall ensure that all such transfers are subject to appropriate technical and organisational safeguards to ensure a level of protection essentially equivalent to that guaranteed under the Data Protection Legislation.

Where EU GDPR applies to the processing of Service Personal Data, references in this Agreement to appropriate safeguards shall include the Standard Contractual Clauses adopted under Commission Implementing Decision (EU) 2021/914, as amended or replaced from time to time.

- ii. Journey shall not transfer any Service Personal Data to any third party other than an authorised Sub-Processor appointed in accordance with Clause 8, unless otherwise required by law. For Platform Usage Data, Journey may transfer such data to Platform Usage Sub-Processors listed in Schedule 3, subject to the provisions of Clause 8A;
- iii. process the Service 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 Service 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 Data Protection Legislation;
- 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 Data Protection Legislation. Audits shall be conducted no more than once per calendar year (unless required by law or following a material breach), during normal business hours, without unreasonable disruption, and at the Customer's expense.
- viii. inform the Customer without undue delay if it is asked to do anything that infringes the Data Protection Legislation 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 Data Protection Legislation. 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 without undue delay and in any event within seventy-two (72) hours of becoming aware of the Personal Data Breach and shall provide available information required under Article 33(3) UK GDPR as such information becomes available, including details of any unauthorised or unlawful access, processing, loss, damage or destruction of the Personal Data, and in addition, Journey shall 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. Where a Personal Data Breach originates with a Sub-Processor, Journey's obligation under this Clause 5 runs from the time Journey becomes aware of it, which depends on the Sub-Processor notifying Journey. The Customer acknowledges that, as controller, its own awareness under Article 33 of the UK GDPR may arise before Journey's notification reaches it, and that it remains responsible for its own regulatory notifications.
- f. Journey should notify the Customer of any communications from Information Commissioner or any other regulatory authority in connection with the Customer Personal Data.
- g. 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.
- h. 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 Data Protection Legislation 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 Data Protection Legislation 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 Data Protection Legislation.
 - d. The liability of the Parties under this Agreement shall be subject to the limitations and exclusions of liability set out in the MSA.
 - e. For the avoidance of doubt, Journey shall be responsible for its compliance with Data Protection Legislation in respect of its processing of Platform Usage Personal Data in its capacity as Data Controller. Such processing shall remain subject to the liability limitations set out in the Master Services Agreement.

7. Confidentiality

- a. Journey shall maintain all Service Data in confidence, and shall not disclose any Service Data supplied to them by, for, or on behalf of the Customer to any third party without the Customer's prior written consent. Journey shall not process or make any use of any Service Data supplied to it by the Customer otherwise than in connection with the provision of the Services to the Customer.
- b. Journey may disclose Platform Usage Data to Platform Usage Sub-Processors listed in Schedule 3 for the purposes described therein, provided that Journey has entered into appropriate data processing agreements with each such Sub-Processor in accordance with Clause 8A.
- c. Journey shall ensure that all Platform Usage Sub-Processors are contractually obliged to keep Platform Usage Data confidential and to process it only for the purposes specified in Schedule 3.
- d. Journey may disclose Business Interaction Data to Business Interaction Processors appointed for the purposes described in Schedule 4, provided that Journey has entered into appropriate written data processing agreements with such processors.
- e. Journey shall ensure that Business Interaction Processors are contractually obliged to maintain the confidentiality and security of Business Interaction Data and to process such data only on Journey's documented instructions.

8. Sub-Processors

- 1. Service Data Sub-Processors (Processor Role)
 - a. The Customer provides general written authorisation for Journey to appoint Sub-Processors to process Service Personal Data.
 - b. Journey shall:
 - i. enter into a written Sub-Processing Agreement imposing obligations no less protective than those set out in this Agreement and compliant with Article 28 UK GDPR;
 - ii. ensure that the Sub-Processor complies with such obligations;
 - iii. remain fully liable for the acts and omissions of any Sub-Processor processing Service Personal Data.
 - iv. ensure that its agreements with Sub-Processors enable Journey to comply with its audit and information obligations under this Agreement.
 - c. Journey shall maintain an up-to-date list of Sub-Processors processing Service Personal Data and shall notify the Customer of any material changes at least thirty (30) days in advance. Where a Sub-Processor must be replaced urgently on security or service-continuity grounds, Journey may make the replacement immediately and



shall notify the Customer as soon as practicable and in any event within five (5) Business Days.

- d. Advertising Platforms. Notwithstanding Clause 4 and Clause 7, where the Customer enables audience matching or campaign delivery, Journey may disclose Service Personal Data to an advertising platform (including Meta Platforms and Google Ads) on the Customer's instruction. The platform handles that data under the terms the Customer agreed with it in the Customer's own account. Journey does not name the platform and it is not a Sub-Processor, and is not listed on the Sub-Processor register. The Customer is responsible, as controller, for the lawful basis and transparency for that disclosure. The Customer's enablement of the relevant feature constitutes its written consent and instruction for the purposes of Clause 7. Where the Customer uploads or connects a list of guests or customers for audience matching, the Customer warrants that it holds the lawful basis and has given the transparency information required for that disclosure.
- 2. Platform Usage Sub-Processors (Controller Role)
 - a. Journey may appoint Platform Usage Sub-Processors to process Platform Usage Personal Data on its behalf.
 - b. Journey shall:
 - i. enter into a written data processing agreement with each Platform Usage Sub-Processor;
 - ii. remain fully liable for their acts and omissions;
 - iii. notify the Customer at least thirty (30) days prior to engaging a new Platform Usage Sub-Processor.
 - c. If the Customer objects on reasonable data protection grounds, the Customer may disable Platform Usage Data collection without penalty.
- 3. Business Interaction Processors (Controller Role)
 - a. Journey may appoint Business Interaction Processors to process Business Interaction Data on its behalf.
 - b. Journey shall enter into a written data processing agreement with each Business Interaction Processor in accordance with applicable Data Protection Legislation.
 - c. Journey shall remain responsible for ensuring that Business Interaction Processors process Business Interaction Data only on Journey's documented instructions and subject to appropriate confidentiality, security and international transfer safeguards.

9. Deletion and/or Disposal of Service Personal Data

- a. Journey shall, following termination or expiry of the Services, delete Service Personal Data in accordance with this Clause 9.
- b. During the term of the Services, Journey shall make available to the Customer the ability to export Service Personal Data using the standard export functionality within the Platform.
- c. The Customer acknowledges and agrees that it is responsible for exporting its Service Personal Data prior to termination or expiry of the Services using such functionality.
- d. "Following the deletion or disposal of the Service Personal Data, Journey shall delete remaining copies of the Service 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.
- e. 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.
- f. Journey will confirm in writing to the Customer once Customer data has been deleted from all systems including backups.



- g. For the avoidance of doubt, this Clause 9 applies only to Service Personal Data and shall not apply to Platform Usage Personal Data or Business Interaction Data processed by Journey in its capacity as Data Controller, which shall instead be retained in accordance with Schedule 3 and Schedule 4 respectively.

10. Data Protection

The Parties agree that, in respect of Service Personal Data, the Customer is the Data Controller and Journey is the Data Processor.

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.

a. Platform Usage Personal Data – Independent Controller Role

- i. Notwithstanding Clause 10, the Parties acknowledge and agree that, in respect of Platform Usage Data as defined herein:
 - a. Journey acts as an independent Data Controller in respect of Platform Usage Personal Data in accordance with Schedule 3.
- ii. Journey shall process Platform Usage Data in compliance with the Data Protection Legislation, including but not limited to:
 - a. maintaining a lawful basis for processing (legitimate interest in product improvement, as documented in Journey's Legitimate Interest Assessment);
 - b. providing appropriate transparency to Authorised Users through an in-product privacy notice, including the identity of Journey as Controller, the purposes of processing, the categories of data collected, any third parties to whom data is disclosed, retention periods, and the rights of data subjects;
 - c. implementing appropriate technical and organisational measures to protect Platform Usage Data;
 - d. conducting a Data Protection Impact Assessment where required under Article 35 of the UK GDPR; and
 - e. responding to data subject access requests and other rights requests from Authorised Users in respect of Platform Usage Data.
- iii. The Customer shall not be liable for Journey's processing of Platform Usage Data in its capacity as Controller, except to the extent that the Customer has failed to comply with its own obligations under this Agreement.
- iv. Journey shall implement and maintain the following data minimisation measures in respect of Platform Usage Data:
 - a. use pseudonymised user identifiers rather than directly identifying information (such as email addresses) where technically feasible;
 - b. collect only such data as is necessary for the purposes stated in Schedule 3;
 - c. disable or not enable any vendor features that capture the content of form fields, free-text inputs, or any data entered by Authorised Users into the Platform;
 - d. apply a bounded retention period as specified in Schedule 3, after which Platform Usage Data shall be deleted or fully anonymised; and
 - e. not attempt to re-identify anonymised or pseudonymised Platform Usage Data, or combine it with Service Data, for any purpose.
- v. Clause 10 shall continue to apply in full to all Service Data. The Customer remains the sole Data Controller for all Service Data, and Journey remains the Data Processor in respect of such data.

b. Business Interaction Data – Independent Controller Role

- i. Notwithstanding Clause 10, the Parties acknowledge and agree that Journey acts as an independent Data Controller in respect of Business Interaction Data processed for the purposes described in Schedule 4.
- ii. Journey shall process Business Interaction Data in accordance with applicable Data Protection Legislation, including by:
 - a. maintaining an appropriate lawful basis for the processing, including legitimate interests where applicable and supported by Journey's



- documented Legitimate Interests Assessment;
 - b. providing appropriate transparency information to affected Data Subjects;
 - c. implementing appropriate technical and organisational measures to protect Business Interaction Data;
 - d. responding to applicable Data Subject rights requests relating to Business Interaction Data;
 - e. carrying out a Data Protection Impact Assessment where required by Data Protection Legislation; and
 - f. ensuring that any Business Interaction Processors are appointed under written agreements containing appropriate confidentiality, security and data protection obligations.
- iii. Where Business Interaction Data includes special category Personal Data or Personal Data relating to criminal convictions or offences, Journey shall only process such data where an applicable condition under Data Protection Legislation is satisfied.
 - iv. For the avoidance of doubt, Service Data shall remain Service Personal Data for the purposes of this Agreement notwithstanding that it may be referred to, displayed, discussed or otherwise captured incidentally in a meeting, recording or transcript. Journey shall continue to act as Data Processor in respect of such Service Data unless Journey has a separate lawful basis, independent of the provision of the Services, to process that Personal Data in its capacity as Data Controller (for example, where the individual is also Journey's own business contact).
 - v. The Customer shall not be responsible for Journey's processing of Business Interaction Data in Journey's capacity as independent Data Controller, except to the extent that the Customer has failed to comply with its own obligations under applicable 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
Guests and customers of the Customer	Name, email, phone, booking and stay details, marketing preferences	Ingestion, transformation into a knowledge graph, rule-based inference	Generating and running marketing campaigns for the Customer	Duration of service contract
Guests and customers of the Customer	Hashed or pseudonymised guest identifiers	Transmission to advertising platforms to build custom audiences and customer-match lists. The advertising platform acts as an independent controller; see Clause 8.1.d	Audience matching for the Customer's campaigns	Duration of service contract
Individuals identifiable in creative and brand assets	Images and likenesses	Ingestion of brand and creative assets, and analysis by an AI model	Generating creative for the Customer's campaigns	Duration of service contract



Authorised users; the Customer's marketing and billing contacts	Name, email, business contact details	Prompt construction and inference	Generating marketing plans and creative	Duration of service contract
---	---------------------------------------	-----------------------------------	---	------------------------------

Note on inference: Guest and marketing inference uses pseudonymised identifiers and derived facts. Identities are resolved locally. Brand and creative analysis sends assets, which may contain likenesses of identifiable individuals, to an AI model in an authorised EEA region.

Special category Personal Data is not processed through Agency by Journey; see Clause 4.



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 rest: 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 Data Protection Legislation; and
 - ii. notifying the Customer in accordance with Clause 5.
 - 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;



SCHEDULE 3

Platform Usage Data

1. **Data Controller:** Journey Hospitality Ltd
2. **Data Subjects:** Authorised Users of the Platform (employees and contractors of the Customer who access the Platform's administration tools)
3. **Categories of Platform Usage Data:**

Category	Examples	Excluded
Navigation data	Pages viewed, features accessed, click paths, time on page	Content of pages viewed (e.g. guest names, booking details)
Feature interaction data	Buttons clicked, workflows completed, features used/not used, search queries within admin tools	Search results content, data displayed on screen
Session data	Session start/end times, session duration, browser type, screen resolution, operating system	IP addresses (not collected or stored by analytics vendor)
User attributes	Pseudonymised user identifier, role category (e.g. "reception", "spa manager", "admin"), property identifier, product context (e.g. "EMS", "ecommerce")	Name, email address, phone number, or any directly identifying information
Feedback data	In-product survey responses, satisfaction scores, feature requests submitted through in-product prompts	Any feedback containing guest PII (technical controls to prevent submission)

4. **Purposes of processing:**
 - a. Product improvement: understanding how Authorised Users interact with the Platform to inform product development priorities
 - (b) Onboarding optimisation: identifying where Authorised Users encounter difficulty during initial setup and training
 - (c) Feature adoption measurement: understanding which features are used and which are underutilised to inform product investment decisions
 - (d) User experience research: collecting direct feedback from Authorised Users to improve Platform usability
 - (e) Platform reliability: identifying errors, performance issues, and workflow failures experienced by Authorised Users
5. **Lawful basis:** Legitimate interest (Article 6(1)(f) UK GDPR) - Journey's legitimate interest in improving the Platform for the benefit of all Customers and Authorised Users. Documented in Journey's Legitimate Interest Assessment (maintained separately).
6. **Retention period:** Platform Usage Data shall be retained for a maximum of twenty-four (24) months from the date of collection. After this period, Platform Usage Data shall be either



deleted or fully anonymised such that no individual or Customer can be identified.

7. Platform Usage Sub-Processors:

- a. Journey maintains a consolidated register of all sub-processors engaged across the Platform (the "Platform Sub-Processor Register"), which sets out the name, purpose, processing location, and categories of data processed by each sub-processor. The Platform Sub-Processor Register is available to Customers on written request.
- b. Not all sub-processors listed in the Platform Sub-Processor Register will process data for all Customers. Journey will only share a Customer's data with a sub-processor where the relevant feature or integration has been enabled for that Customer's account.
- c. Journey shall notify the Customer at least fourteen (14) days prior to adding a new entry to the Platform Sub-Processor Register. Where a new sub-processor is engaged solely in connection with a feature or integration that the Customer has not enabled, the fourteen (14) day notice period shall apply from the date of addition to the Register but shall not restrict Journey from making that sub-processor available on the Platform during that period.

Sub-Processor	Purpose	Location	Data categories processed
UserPilot	In-product analytics, user guidance, and feedback collection	AWS eu-west	All categories listed in Section 3 above

8. Technical safeguards:

- a. Pseudonymised user identifiers generated by Journey; directly identifying information (including name, email address, or IP address) is not collected or transmitted to Platform Usage Sub-Processors unless strictly necessary for a documented and specific purpose, and only where no less intrusive alternative exists.
- b. Form field content capture is disabled at the vendor configuration level
- c. Platform Usage Data is logically separated from Service Data in all systems
- d. Encryption in transit (TLS 1.2 or higher) and at rest for all Platform Usage Data
- e. Access to Platform Usage Data is restricted to Journey personnel with a legitimate business need



SCHEDULE 4

Business Interaction Data

Data Controller: Journey Hospitality Limited.

Data Subjects: Employees, contractors, representatives and other personnel of the Customer or third parties participating in meetings or communications with Journey.

Categories of Personal Data: Name, role and organisation; voice and, where applicable, image; audio or video recordings; meeting and call metadata; transcripts; AI-generated summaries, notes and action points; and other information voluntarily disclosed during the meeting or communication.

Purposes of Processing: Maintaining accurate business records; documenting decisions, commitments and actions; delivery and management of the Services; account and relationship management; service quality and training; dispute resolution; and improving Journey's internal operating processes.

Lawful Basis: Journey's legitimate interests in effectively delivering and managing its Services, maintaining accurate records and improving service quality, subject to Journey's documented Legitimate Interests Assessment and the rights and interests of affected individuals.

Retention: Business Interaction Data shall be retained only for as long as reasonably necessary for the purposes for which it was collected, in accordance with Journey's documented retention policy, after which it shall be securely deleted or anonymised. Longer retention may apply where reasonably necessary for the establishment, exercise or defence of legal claims or to comply with applicable law.

Third-Party Processing: Journey may appoint appropriately vetted Business Interaction Processors to provide recording, transcription, storage and AI-assisted summarisation services. Such processors shall be subject to written data processing, confidentiality and security obligations and appropriate safeguards for any international transfers.

Business Interaction Data shall not be used to train third-party general-purpose artificial intelligence models unless separately assessed and expressly authorised by Journey.

Service Data Boundary: For the avoidance of doubt, Service Data does not become Business Interaction Data merely because it is referred to, displayed, discussed or otherwise captured incidentally during a meeting, call, recording or transcript. Journey shall continue to process such Service Data in its capacity as Data Processor in accordance with this Agreement, unless Journey has a separate lawful basis, independent of the provision of the Services, to process that Personal Data in its capacity as Data Controller, as described in Clause 10.b.iv.