Data Processing Agreement

(Version 1st June 2022)

This Data Processing Agreement ("DPA") forms part of and is incorporated into the Master Subscription Agreement ("MSA"). By entering into a Service Order Customer agrees to this DPA.

AGREED TERMS

1. Definitions and Interpretation

The following definitions and rules of interpretation apply in this DPA.

1.1 Definitions:

Authorised Persons: the persons or categories of persons that the Customer authorises to give TripStax written personal data processing instructions and from whom TripStax agrees solely to accept such instructions. In many cases such persons will be Authorised Users who give instructions by accessing the TripStax Services.

Business Purposes: the services to be provided by TripStax to the Customer as described in the MSA and Service Order.

Commissioner: the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).

Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Processing: have the meanings given to them in the Data Protection Legislation.

Controller: has the meaning given to it in section 6, DPA 2018.

Data Protection Legislation:

a) To the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of Personal Data.

b) To the extent the EU GDPR applies, the law of the European Union or any member state of the European Union to which the Customer or TripStax is subject, which relates to the protection of Personal Data.

Data Subject: the identified or identifiable living individual to whom the Personal Data relates.

EU GDPR: the General Data Protection Regulation ((EU) 2016/679).

EEA: the European Economic Area.

Personal Data: means any information relating to an identified or identifiable living individual that is processed by TripStax on behalf of the Customer as a result of, or in connection with, the provision of the services under the MSA; an identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Processing, processes, processed, process: any activity that involves the use of the Personal Data. It includes, but is not limited to, any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring the Personal Data to third-parties.

Personal Data Breach: a breach of security leading to the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data.

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

Records: has the meaning given to it in Clause 12.

Standard Contractual Clauses: means Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

Term: this Agreement's term as defined in Clause 10.

UK GDPR: has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

1.2 This DPA is subject to the terms of the MSA and is incorporated into the MSA. Interpretations and defined terms set forth in the MSA apply to the interpretation of this Agreement.

1.3 The Annexes form part of this DPA and will have effect as if set out in full in the body of this Agreement. Any reference to this DPA includes the Annexes.

1.4 A reference to writing or written includes faxes and email.

1.5 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this DPA and any provision contained in the Annexes, the provision in the body of this DPA will prevail;

(b) the terms of any accompanying invoice or other documents annexed to this DPA and any provision contained in the Annexes, the provision contained in the Annexes will prevail; and

(c) any of the provisions of this DPA and the provisions of the MSA, the provisions of this DPA will prevail.

2. Personal data types and processing purposes

2.1 The Customer and TripStax agree and acknowledge that for the purpose of the Data Protection Legislation:

(a) the Customer is the Controller and TripStax is the Processor.

(b) the Customer retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions it gives to the TripStax.

(c) ANNEX A describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which TripStax may process the Personal Data to fulfil the Business Purposes.

3. TripStax obligations

3.1 TripStax will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's written instructions. TripStax will not process the Personal Data for any other purpose or in a way that does not comply with this DPA or the Data Protection Legislation. TripStax must promptly notify the Customer if, in its opinion, the Customer's instructions do not comply with the Data Protection Legislation.

3.2 TripStax will comply promptly with any Customer written instructions requiring TripStax to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

3.3 TripStax will maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third-parties unless the Customer or this DPA specifically authorises the disclosure, or as required by domestic or EU law, court or regulator (including the Commissioner). If a domestic or EU law, court or regulator (including the Commissioner) requires TripStax to process or disclose the Personal Data to a third-party, TripStax must first inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the domestic or EU law prohibits the giving of such notice.

3.4 TripStax will reasonably assist the Customer with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of TripStax processing and the information available to TripStax, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the Commissioner or other relevant regulator under the Data Protection Legislation. If such assistance is not included in the Services then TripStax shall be entitled to separately charge for any assistance at its normal [day rates].

3.5 TripStax must notify the Customer promptly if it learns of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting TripStax performance of the MSA or this Agreement.

4. TripStax employees

4.1 TripStax will ensure that all of its employees:

(a) are informed of the confidential nature of the Personal Data and are bound by written confidentiality obligations and use restrictions in respect of the Personal Data;

(b) have undertaken training on the Data Protection Legislation and how it relates to their handling of the Personal Data and how it applies to their particular duties; and

(c) are aware both of TripStax duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.

5. Security

5.1 TripStax will at all times implement appropriate technical and organisational measures against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction,

display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in ANNEX B.

5.2 TripStax will implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

6. Personal data breach

6.1 TripStax will within 48 hours and in any event without undue delay notify the Customer in writing if it becomes aware of:

(a) the loss, unintended destruction or damage, corruption, or un-usability of part or all of the Personal Data. TripStax will restore such Personal Data at its own expense as soon as possible.

(b) any accidental, unauthorised or unlawful processing of the Personal Data; or

(c) any Personal Data Breach.

6.2 Where TripStax becomes aware of (a), (b) and/or (c) above, it will, without undue delay, also provide the Customer with the following written information:

(a) description of the nature of (a), (b) and/or (c), including the categories of in-scope Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;

(b) the likely consequences; and

(c) a description of the measures taken or proposed to be taken to address (a), (b) and/or (c), including measures to mitigate its possible adverse effects.

6.3 Immediately following any accidental, unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Further, TripStax will reasonably co-operate with the Customer at no additional cost to the Customer (if the Data Breach is caused by TripStax), in the Customer's handling of the matter, including but not limited to:

(a) assisting with any investigation;

(b) providing the Customer with physical access to any facilities and operations affected;

(c) facilitating interviews with TripStax employees, former employees and others involved in the matter including, but not limited to, its officers and directors;

(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and

(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Personal Data processing.

6.4 TripStax will not inform any third-party of any accidental, unauthorised or unlawful processing of all or part of the Personal Data and/or a Personal Data Breach without first obtaining the Customer's written consent, except when required to do so by domestic or EU law.

6.5 TripStax agrees that the Customer has the sole right to determine:

(a) whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Commissioner, other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice; and

(b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

6.6 TripStax will cover reasonable expenses associated with the performance of its obligations under clause 6.1 to clause 6.3 unless the matter arose from the Customer's instructions, negligence, default or breach of this Agreement, in which case the Customer will cover all reasonable expenses including those incurred by TripStax.

7. Cross-border transfers of personal data

7.1 TripStax (and any subcontractor) will not transfer or otherwise process the Personal Data outside the UK or, the EEA without obtaining the Customer's prior written consent.

7.2 If it is required or requested that a transfer of Personal Data is made outside of the EEA or UK then, subject to the additional terms to be agreed, the Parties shall comply with the additional terms and the Standard Contractual Clauses sections I, II, III and IV (as applicable).

8. Subcontractors

8.1 Other than those subcontractors as set out in ANNEX A, TripStax will not authorise any other third-party or subcontractor to process the Personal Data.

8.2 Those subcontractors approved as at the commencement of this DPA are as set out in ANNEX A. TripStax must list all approved subcontractors in Annex A and include any subcontractor's name and location. TripStax may engage additional subcontractors or substitute subcontractors by amending Annex A and giving not less than 15 days' notice to the Customer.

8.3 Where the subcontractor fails to fulfil its obligations under the written agreement with TripStax which contains terms substantially the same as those set out in this Agreement, TripStax shall inform the Customer and take such reasonable action against the subcontractor as the Customer determines to ensure or require the subcontractor's performance of its agreement obligations.

8.4 The Parties agree that TripStax will be deemed by them to control legally any Personal Data controlled practically by or in the possession of its subcontractors.

8.5 On the Customer's written request, TripStax will substitute a subcontractor for another subcontractor where the original subcontractor is in default of its agreement with TripStax or is responsible for a data breach or breach of security.

9. Complaints, data subject requests and third-party rights

9.1 TripStax will take such technical and organisational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

(a) the rights of Data Subjects under the Data Protection Legislation, including, but not limited to, subject access rights, the rights to rectify, port and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

(b) information or assessment notices served on the Customer by the Commissioner [or other relevant regulator] under the Data Protection Legislation.

9.2 TripStax will notify the Customer as soon as reasonably possible in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

9.3 TripStax will notify the Customer within 3 days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation.

9.4 TripStax will give the Customer its reasonable co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.5 TripStax will not disclose the Personal Data to any Data Subject or to a third-party other than in accordance with the Customer's written instructions, or as required by domestic or EU law.

10. Term and termination

10.1 This DPA will remain in full force and effect so long as:

(a) the MSA remains in effect; or

(b) TripStax retains any of the Personal Data related to the MSA in its possession or control (**Term**).

10.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the MSA in order to protect the Personal Data will remain in full force and effect.

10.3 TripStax material failure to comply with the terms of this DPA may amount to a material breach of the MSA. In such event, the Customer may require TripStax remedy the breach or terminate the MSA in accordance with clause 10.2 thereof on written notice to TripStax.

10.4 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its MSA obligations, the parties may agree to suspend the processing of the Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation within 30 days, either party may terminate the MSA on not less than 20 working days written notice to the other party.

11. Data return and destruction

11.1 At the Customer's request, TripStax will give the Customer, or a third-party nominated in writing by the Customer, a copy of or access to all or part of the Personal Data in its possession or control in the format and on the media reasonably specified by the Customer.

11.2 On termination of the MSA for any reason or expiry of its term, TripStax will securely delete or destroy or, if directed in writing by the Customer, return and not retain, all or any of the Personal Data related to this DPA in its possession or control, except for one copy that it may retain and use for 3 years for evidential and security purposes only.

11.3 If any law, regulation, or government or regulatory body requires TripStax to retain any documents, materials or Personal Data that TripStax would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the documents, materials or Personal Data that it must retain, the legal basis for such retention, and establishing a specific timeline for deletion or destruction once the retention requirement ends.

11.4 TripStax will certify in writing to the Customer that it has deleted or destroyed the Personal Data within 7 days after it completes the deletion or destruction.

11.5 TripStax shall be entitled to charge the Customer for the effort required to comply with this clause 11. In the absence of an agreed charge TripStax shall be entitled to charge at its normal day rate.

12. Records

12.1 TripStax will keep detailed, accurate and up-to-date written records regarding any processing of the Personal Data, including but not limited to, the access, control and security of the Personal Data, approved subcontractors, the processing purposes, categories of processing, and a general description of the technical and organisational security measures referred to in Clause 5.1 (**Records**).

12.2 TripStax will make the Records available to enable the Customer to verify TripStax compliance with its obligations under this DPA and the Data Protection Legislation and TripStax will provide the Customer with copies of the Records upon reasonable request.

13. Audit

13.1 TripStax will permit the Customer and its third-party representatives to audit TripStax compliance with its obligations under this Agreement, on at least 20 working days' notice, once in each year of the Term. TripStax will give the Customer and its third-party representatives necessary assistance to conduct such audits. Each party shall bear its own costs of audit.

13.2 The notice requirements in Clause 13.1 will not apply if the Customer reasonably believes that a Personal Data Breach has occurred or is occurring, or TripStax is in material breach of any of its obligations under this DPA or any of the Data Protection Legislation.

13.3 If a Personal Data Breach occurs or is occurring, or TripStax becomes aware of a breach of any of its obligations under this DPA or any of the Data Protection Legislation, TripStax will:

(a) within 5 working days of the triggering event, conduct its own audit to determine the cause;

(b) produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;

(c) provide the Customer with a copy of the written audit report; and

(d) remedy any deficiencies identified by the audit within the number days specified in the report.

13.4 Customer acknowledges that TripStax provides services to other Customers. Customer and its third-party representatives will prior to conducting any audit or receiving any audit report prepared in accordance with this clause 13 enter into a confidentiality agreement with TripStax to preserve the confidentiality of TripStax information and that belonging to other TripStax customers. Customer shall not be entitled to see information that relates to other TripStax customers or their clients.

13.5 Upon the request of the Customer but not more than once a year, TripStax will conduct site audits of its Personal Data processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this Agreement.

13.6 On the Customer's written request but subject to clause 13.4, TripStax will make relevant audit reports available to the Customer for review.

13.7 TripStax will promptly address any exceptions noted in the audit reports with the development and implementation of a corrective action plan by TripStax management.

14. Notice

14.1 Any notice or other communication given to a party under or in connection with this DPA must be in writing and delivered as specified in the TripStax Service Order.

14.2 Clause 14.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

This DPA is entered into as part of the TripStax Service Order.

ANNEX A Personal Data processing purposes and details

Subject matter of processing:

The subject matter of the processing is data including Personal Data input into the Services by Authorised Users in accordance with the Service Order and MSA.

Duration of Processing:

TripStax will Process Personal Data for the duration of the Term specified in the Service Order, unless otherwise agreed upon in writing.

Nature of Processing:

The performance of the Services pursuant to the Service Order.

Business Purposes:

TripStax will Process Personal Data as necessary to perform the Services pursuant to the Service Order, as further specified in the Service Order and MSA, and as further instructed by Customer in its use of the Services.

Personal Data Categories:

The Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

● Customers and Customer End Users (who are natural persons) and their chosen contacts.

● Contact persons, travelers, assistants, agents, employees and other natural persons of Customer End Users.

● Employees, agents, advisors, freelancers of Customer (who are natural persons)

● Customer's Users authorised by Customer to use the Services.

Data Subject Types:

The Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

● First and last name

● Title

● Position

● Employer

● Contact information (company, email, phone, physical business address)

● ID data

● Professional life data

● Personal life data

●Travel related data

●Encrypted credit/charge/debit card data

● Localisation data

Authorised Persons: Authorised Users.

Approved Subcontractors:

- Microsoft Azure -datacentre located in the Netherlands
- Or as separately notified by an updated list made available to the Customer.

ANNEX B Security measures

TripStax maintains administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services. TripStax will not materially decrease the overall security of the Services during the Term.