GDPR | Data Processing Agreement **("DPA")**

between

_____ - *the "Customer" as indicated on the agreement for Services with Amadeus*

Address:

And

TravelClick, Inc. **("Amadeus")**

Address: 75 New Hampshire Ave, Portsmouth, NH 03801, USA

each a "party"; together "the parties",

GDPR | Data Processing Agreement

The Customer acknowledges and agrees that it will be acting as the Data Controller of Personal Data Processed by Amadeus as a consequence of the provision of Services under the Agreement(s) between the Parties as amended from time to time, and Amadeus will be acting as Data Processor. Notwithstanding the foregoing, Amadeus shall be the Data Controller in respect of activities relating to the administration of the commercial relationship between it and the Customer (e.g., invoicing Customer).

1. DEFINITIONS

For the purpose of this Data Processing Addendum, '**Data Controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; '**Data Processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller; **'Subprocessor'** means any processor engaged by Amadeus in the Processing of Personal Data; '**Data Protection Laws'** shall mean all applicable laws and legally binding regulations relating to the Processing of Personal Data, data protection, and privacy and/or legally binding regulations implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them; '**Personal Data'** means any information relating to an identified or identifiable natural person ('**Data Subject'**) including all data or information that constitutes personal information, personal data, sensitive personal information, personally identifiable information or similar term under any applicable Data Protection Laws; **'EU Restricted Transfer'** means a transfer of Personal Data by Data Controller to the Data Processor (or any onward transfer), in each case, where such transfer would be prohibited by European Data Protection Laws in the absence of the protection for the transferred Personal Data provided by the EU Standard Contractual Clauses as set forth in Annex 1; **'Processing'** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2. SUMMARY OF PROCESSING

The purpose for Amadeus Processing the Personal Data is Amadeus's provision of the Services to the Customer. This Processing includes such activities as specified in the Service Order(s) or as otherwise necessary to perform the obligations and Services set forth therein and which shall in particular determine the duration and the subject-matter of the Processing, the nature and purpose of the Processing, the type of Personal Data and the categories of Data Subjects to which the Personal Data relates, as further detailed in Annex 1.

3. OBLIGATIONS OF AMADEUS AS DATA PROCESSOR

3.1 Amadeus shall only Process the Personal Data in accordance with the Customer's instructions. These instructions will be as set out in the Agreement and this Data Processing Addendum, which is deemed to include any action to perform its obligations or to provide the Services licensed pursuant to the Agreement, and further to any other documented instruction provided by the Customer, except to the extent that any legal requirement prevents Amadeus from complying with

such instructions or requires the Processing of Personal Data other than as instructed by the Customer. Amadeus will inform Customer if, in its opinion, an instruction infringes any Data Protection Laws, as permitted by applicable Data Protection Laws. Customer acknowledges that in the provision of the Services under the Agreement Amadeus may transfer Personal Data in accordance with applicable Data Protection Legislation.

3.2 The Customer agrees that Amadeus may hire other companies to provide Processing Services on its behalf, provided that Amadeus complies with the provisions of this clause. Amadeus has a general authorisation from the Customer to engage Subprocessors from an agreed list. Amadeus remains responsible for its Subprocessors' compliance with the obligations of this Data Processing Addendum and the Agreement as applicable. Any Subprocessor to whom Amadeus transfers Personal Data will have entered into written agreements with Amadeus requiring that the Subprocessor abide by terms in substance that provide for the same data protection obligations as this Data Processing Addendum, as applicable. Amadeus shall inform Customer of any changes to the Subprocessors used in Processing of Personal Data made after the Effective Date of this Data Processing Addendum by notifying Customer.

If Customer, acting reasonably, objects to the use of a Subprocessor, Customer may notify Amadeus promptly in writing within fourteen (14) calendar days after receipt of Amadeus notice in accordance with paragraph above providing details of its objections. Amadeus shall use reasonable endeavours to resolve the reasons for Customer's objections or to procure use of a different Data Processing Subcontractor.

If Amadeus is unable to or fails to resolve the reasons for Customer's objections or to procure use of a different Data Processing Subcontractor within a reasonable period of time, Customer may terminate the Services which cannot be provided by Amadeus without the use of the Data Processing Subcontractor to which Customer objects by providing written notice to Amadeus, provided Customer will not be entitled to claim damages in respect such termination.

3.3 Amadeus shall Process Personal Data subject to appropriate technical and organizational measures against unauthorized or unlawful Processing of the Personal Data and against accidental loss or destruction of, or damage to, the Personal Data in accordance with Data Protection Laws as more fully described in this document.

3.4 Amadeus shall use personnel authorized by Amadeus to access the Personal Data who are subject to a duty of confidentiality in respect of the Personal Data.

3.5 Amadeus shall, at the choice of the Customer, delete or return all Personal Data to the Customer after the end of the Processing of Personal Data under the Agreement and in accordance with the terms of the Agreement, unless Amadeus is required to retain the Personal Data by applicable law.

3.6 Where Amadeus processes Personal Information as a Service Provider under the California Consumer Privacy Act, as amended and replaced ("**CCPA**"), the following shall apply:

3.6.1 For purposes of this Section 3.6.1, the terms "**Service Provider**," "**Business",** "**Business Purpose**," "**Commercial Purpose**," "**Collect**," "**Personal Information**", "**Process**" and "**Sell**" shall have the meanings set forth in the CCPA.

3.6.2 **Service Provider Obligations and Restrictions**. The parties agree that Amadeus is a Service Provider to Customer with respect to Personal Information Processed by Amadeus.

3.6.3 As a Service Provider, Amadeus will not retain, use, Sell, or disclose the Personal Information for any purpose other than for the specific purpose of performing the services specified in the Service Order, including retaining, using, Selling or disclosing the Personal Information for a Commercial Purpose other than providing the services specified in the Service Order.

3.6.4 As a Service Provider, Amadeus will not retain, use, Sell, or disclose Personal Information outside of the direct business relationship between the parties except under the following limited circumstances:

a) To perform services on behalf of Customer for a Business Purpose as specified in the Agreement or applicable Service Order;

b) To retain and employ a Sub-Processor that meets the requirements for a Service Provider under the CCPA.

c) For internal use by Amadeus to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles, or correcting or augmenting Personal Information acquired from another source.

d) To detect data security incidents or protect against fraudulent or illegal activity.

e) To collect, use, retain, sell, or disclose Personal Information that is deidentified or aggregated information.

f) As otherwise permitted by applicable law, including, compliance with federal, state, or local laws; compliance with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities; cooperating with law enforcement agencies concerning conduct or activity that Amadeus reasonably and in good faith believes may violate federal, state, or local law; exercising or defending legal claims.

3.6.5. Amadeus certifies that it understands the restrictions under this Section 3.5 and will comply with them.

4. ASSISTANCE

4.1 Amadeus shall:

(a) inform Customer of any requests or queries from a Data Subject, regulatory authority or any other law enforcement authority regarding Processing of Personal Data under the Agreement and this Data Processing Addendum and provide Customer with any information and assistance that may reasonably be required to respond to any such requests or queries;

(b) assist the Customer with its obligations to comply with Articles 32 to 36 of the applicable Data Protection Laws taking into account the nature of processing and the information available to Amadeus;

(c) notify Customer without undue delay on becoming aware of any Security Incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise Processed by Amadeus in connection with the Agreement and this Data Processing Addendum; and

(d) make available to Customer information reasonably necessary to demonstrate compliance with Amadeus's Personal Data Processing obligations under the Agreement and this Data Processing Addendum. If Customer, acting reasonably, considers that Amadeus has not provided sufficient evidence of its compliance, Customer must notify Amadeus in writing providing evidence of such concerns, and Amadeus shall use reasonable endeavours to resolve Customer's concerns. If Amadeus is unable to resolve Customer's concerns, Customer may, as required under Data Protection Laws, audit Amadeus's control environment and security practices relevant to the Personal Data Processed under the Agreement and this Data Processing Addendum for Customer. Any audits conducted by Customer or a mutually agreed upon third party auditor pursuant to this provision shall be subject to: the execution of an appropriate confidentiality agreement with Amadeus, compliance with Amadeus's on-site or other applicable security policies and the following conditions: unless required or otherwise requested by a regulator: (i) audits shall be limited to once annually; (ii) audits will be carried out during normal working hours, without disturbing business operations; (iii) Customer will provide at least thirty (30) days prior written notice; and (iv) a Customer will provide Amadeus with a copy of the audit report.

4.2 Amadeus reserves the right to charge Customer a reasonable fee for the assistance provided by Amadeus under **Section 4.1**.

5. Restricted Transfers.

5.1 In respect of any EU Restricted Transfer, the parties with effect from the commencement of the relevant transfer hereby enter into the EU Standard Contractual Clauses in Annex 1.

6. General Terms

6.1 **Precedence.** The provisions of this Data Processing Addendum are supplemental to the relevant Agreement. In the event of inconsistencies between the provisions of this Data Processing Addendum and the provisions of the relevant Agreement the provisions of this Data Processing Addendum shall prevail.

6.2 **Compliance with Data Protection Laws.** Each Party to this Data Processing Addendum shall comply with Data Protection Laws as applicable to such Party.

Customer	**Amadeus**
Name:……..…..…	Name: Meghan Norwood – Global head of operations
Authorised Signature: ……...…	Authorised Signature: 
Date:……..…..……	Date:……

TravelClick
an AMADEUS company

ANNEX I

STANDARD CONTRACTUAL CLAUSES

MODULE TWO: Transfer Controller to Processor (C2P)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 - Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

Intentionally deleted

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same

time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least fifteen (15) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects[3]. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III - LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination- including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent

supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authorities, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent suspensory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request

if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV - FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall

certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Member State in which the data exported is established.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Member State in which the data exported is established.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

TravelClick
an AMADEUS company

APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES

ANNEX A

A. LIST OF PARTIES

Data exporter(s):

1.	**Name:**	*"Customer" as indicated on the services agreement with Amadeus*
	Address:	*"Address" as indicated on the services agreement with Amadeus*
	Contact person's name, position and contact details:	*"Signatory and contact details" as indicated on the services agreement with Amadeus*
	Activities relevant to the data transferred under these Clauses:	*Amadeus service provision to the Customer*
	Signature and date:	*"Signature and date" as indicated and incorporated by reference on the services agreement with Amadeus*
	Role (controller/processor):	*Controller*

Data importer(s):

1.	**Name:**	Amadeus
	Address:	55 West, 46th Street, 27th Floor, New York, USA
	Contact person's name, position and contact details:	Wiiliam Sintiris - COO
	Activities relevant to the data transferred under these Clauses:	*Amadeus service provision to the Customer*
	Signature and date:	*"Signature and date" as indicated and incorporated by reference on the services agreement with Amadeus*
	Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER*

Categories of data subjects whose personal data is transferred	Customer's hotel guests.
Categories of personal data transferred	Guest information: First and last name; email address; position salutation, last name, first mail, title, email, company, address 1, address2, city, state, postal code, country, phone, frequent guest id, initial_, phoneday, phoneevening, rawstreetaddr, lastupdate, users, unsubscribe, gsource, groupconame, birthdate, corpid, frequent_guestid, lastccno, contacttitle, contactfirstname, contactlastname, contactemail, airtravelerid, cartravelerid, guest profile, IP, tracking technology (e.g. cookies) – as applicable. Payment information (if applicable): credit card type, credit card number, expiration date, name on card, billing address 1, billing address 2, billing city, billing country, billing state, billing postal code, billing code,
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.	The personal data transferred does not concern nor require to provide the services no special categories of data
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	Continous basis
Nature of the processing	Processing of the Customer data for the provision of the services described in the service agreement between the processor and the controller
Purpose(s) of the data transfer and further processing	Provision of the services described in the service agreement between the processor and the controller
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	Service provision Term (or as long as required under applicable laws).

C. COMPETENT SUPERVISORY AUTHORITY

Competent supervisory authority/ies in accordance with Clause 13	Authority of the EU Member State in which the data exporter is established.

TravelClick
an AMADEUS company

ANNEX B - TECHNICAL AND ORGANISATIONAL MEASURES*

Description of the technical and organisational security measures implemented by Amadeus:

1. Governance
    1. Corporate security department
    2. Dedicated security personnel
    3. Corporate security policy and procedures
    4. Corporate change management process
2. Infrastructure
    1. Network based IDS (intrusion detection systems)
    2. 3-tier architecture
    3. Centralized event logging
    4. Server hardening processes and build standards
    5. Anti-Virus infrastructure
3. Audit / Compliance
    1. PCI DSS yearly certification.
    2. Monthly vulnerability scans (Internet facing servers)
    3. Yearly penetration testing
    4. Internal audits (users, systems, security controls)
    5. Policy and procedure review annually
4. Vendor Management
    1. Current vendor support agreements

* This is a generic description for Amadeus and is subject to changes according to the specific service. To confirm product specific technical and organizational measures regarding a particular service please reach your account manager.