PERSONAL DATA PROTECTION AGREEMENT

CLAUSE 1: Purpose

The Parties acknowledge that for the purposes of the Applicable Data Protection Law, the Client is the Data Controller and Easytrip SPA is the Data Processor in respect of any Personal Data.

The Data Processor has agreed to provide services to the Data Controller in accordance with the contract.

In the framework of their contractual relations referred to above, the Parties undertake to comply with Applicable Data Protection Law, including the provisions of EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 applicable as from 25 May 2018 (the "GDPR").

This Agreement sets out the contractual terms agreed by the Parties as required by Article 28(3) of the GDPR. Details of the data processing operations for any service(s) referred to in the contract are set out in Schedule 1.

This Agreement shall continue for no less than the terms of the contract.

CLAUSE 2: Definitions

For the purposes of the Clauses, the following terms shall have the meaning set forth below:

a) "**Affiliate**" shall mean any company from time to time directly or indirectly controlling, controlled by or under common control with a Party, where control shall mean the direct or indirect possession of more than half the voting securities of any company or the power effectively to direct or cause to be directed, the management and policies of a company through the ownership of voting securities or voting interest or otherwise;

b) "**Applicable Data Protection law"** means any law or regulation pertaining to data protection, privacy, and/or the processing of Personal Data, to the extent applicable in respect of a party's obligations under the contract and this Agreement, including the Data Protection Act 1998, the Data Protection Directive (95/46/EC) and any associated regulations or instruments and any other date protection laws, regulations and regulatory requirements applicable to each Party or any other legislation or regulations that transpose or supersede the above (including on and after 25 May 2018, the GDPR and laws implementing or supplementing the GDPR ;

c) "**Data Controller"** (or the "**Controller**") means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data, as set out in Article 4(7) of the GDPR;

d) "**Data Processor**" (or "the "**Processor**") means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller, as set out in Article 4(8) of the GDPR.

e) **"Data Subject"** means an individual who is the subject of Personal Data;

f) **"Personal Data"** means any information relating to an identified or identifiable natural person (a "Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an 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 that natural person , as set out in Article 4(1) of the GDPR;

g) “**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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

h) “**Technical and organizational security measures**“ means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

CLAUSE 3: Obligations of the Data Controller

The Data Controller undertakes to take all necessary measures pertaining to the compliance by itself and by its personnel with its obligations and especially, warrants and undertakes without limitation that:

- The processing, including the transfer itself, of the Personal Data has been and will continue to be carried out in accordance with the relevant provisions of the Applicable Data Protection Law (and where applicable, has been notified to the relevant authorities of the member state where the Data Controller is established) and does not violate the relevant provisions of that state;
- It has used reasonable efforts to determine that the Data Processor is able to satisfy its legal obligations under this Agreement;
- It has obtained any and all necessary permissions and authorizations necessary to permit the Processor, its Affiliates and sub-processors, to execute their rights or perform their obligations under this Agreement;
- It will communicate to the Processor only the Personal Data necessary for the processing carried out within the framework of the services rendered under the contract;
- It shall instruct the Data Processor to process the Personal Data in any manner that may reasonably be required in order for the Data Processor to carry out the processing in compliance with this Agreement and in compliance with Applicable Data Protection Law;
- It will provide the Data Subject with all the necessary information foreseen in Articles 13 and 14 of the GDPR to ensure fair and transparent processing in respect of the Data Subject;
- It will ensure that the Processor complies with security and data confidentiality measures throughout the processing period;
- It will ensure that the Processor provides sufficient guarantees as to the implementation of appropriate Technical and organizational measures so that the processing meets the requirements of the Applicable Data Protection Law and guarantees the protection of the rights of the Data Subject (Article 28 GDPR);
- It will supervise the processing and carry out audits if it considers it necessary.

CLAUSE 4: Obligations of the Processor

The Data Processor warrants and undertakes without limitation that:

- It will comply with all applicable law including Applicable Data Protection Law in its performance of this Agreement and the contract.
- It will process the Personal Data only for purposes described in Schedule 1 and in accordance with the documented instructions and authorizations received from the Data Controller.
- It will transfer Personal Data outside the European Union only in accordance with Clause 12.
- It will not disclose any Personal Data to a third party in any circumstances (whether free of charge or not) other than at the specific written request of the Data Controller, unless such disclosure is necessary in order to fulfil the obligations of the contract, or is required by applicable law.
- It will inform the Data Controller as soon as possible if, in his opinion, an instruction constitutes a violation of the regulations.

The Data Processor acknowledges and accepts that it may only act in accordance with this Agreement for the processing of the Data and files to which it may have access. The Processor shall maintain a record of the processing of Personal data carried out on behalf of the Controller, in accordance with the provisions of the GDPR. Data Processor will make the record available to the Data Controller upon written request sent by registered letter with acknowledgement of receipt.

CLAUSE 5: Safety and security

The Data Processor undertakes that:

- It shall implement all reasonable procedures to ensure the confidentiality and security of the Personal Data, which shall include the same degree of care that it uses to protect its own information of a similar nature, but in no event less than a reasonable degree of care;
- It will have in place appropriate Technical and organizational measures to protect the confidentiality of the Personal Data and to protect the Personal Data against accidental or unlawful destruction or accidental loss, distortion, alteration, unauthorized disclosure or access. The measures must be implemented with due regard to the current state of the art, costs of implementation and the nature, scope, context and purposes of the processing and the risk of varying likelihood and severity to the rights and freedoms of natural persons;
- The Processor shall implement the suitable Technical and organizational measures in such a manner that the processing by the Processor of Personal Data meets the requirements of the Applicable Data Protection Law;
- It shall ensure that the authorized persons to process Personal Data undertake to respect the obligation of confidentiality of the Personal Data and shall only process the data on the documented instructions of the Controller.
- Upon prior written request, the Data Processor will provide the Controller with details of the technical and organisational measures implemented.

CLAUSE 6: Upcoming data processor

The Data Controller expressly authorises the Data Processor to subcontractor to another data processor the processing of Personal Data on its behalf.

In this context, the Data Processor shall:

- conclude a written agreement with its subcontractor acting as data processor, imposing the same data protection obligations as those set out in this Agreement and the contract;
- impose on its data processor all obligations necessary to ensure that the confidentiality, security and integrity of the data are respected, and that such data may not be transferred or rented to a third party, whether free of charge or not, or used for purposes other than those defined herein;
- keep at the Data Controller's disposal a list of the Data Processor(s) involved in the Data processing and send at first written request.

In accordance with article 28 (2) of the GDPR, the appointment or replacement of subcontractor by the Data Processor will involve an information to the Data Controller by the Data Processor.

The Data Processor shall remain fully responsible for the execution by its subcontractor(s) of its/their obligations.

CLAUSE 7: Notifications

The Data Processor shall notify the Data Controller about:

(i) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorized access, and

(iii) any request received directly from the Data Subjects without responding to that request, unless it has been otherwise authorized to do so.

CLAUSE 8: Cooperation

The Processor shall to the necessary and reasonable extent assist the Controller in the performance of its obligations in the processing of the Personal Data covered by this Agreement, including in connection with:

- responses to Data subjects on exercise of their rights, especially Data Subject's rights laid down in Articles 15 to 23 of the GDPR;
- ensuring compliance with the obligations of the Controller pursuant to Articles 32 to 36 of the GDPR taking into account the nature of processing and the information available to the Processor;
- security breaches;
- impact assessments; and
- prior consultation of the supervisory authorities.

CLAUSE 9: Data Breach

Each Party shall notify other Party a Personal Data breach or a potential data breach as soon as possible but not later than forty-eight (48) hours after having become aware of the same, namely a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. The Data Processor will cooperate with the Data Controller in implementing any appropriate action concerning the breach or the potential breach as the case may be, including corrective actions.

This notification shall be sent to the person designated as Data Protection Officer, by telephone and email, and confirmed by registered letter with acknowledgment of receipt. It will describe, where possible, the nature and consequences of the personal data breach, and the measures already taken or proposed to be taken to address the personal data breach.

The Data Processor is committed to collaborate with the Data Controller to ensure that they are able to meet their regulatory and contractual obligations. It is the sole responsibility of the Data Controller to notify this data breach to the competent supervisory authority and, where applicable, to the Data Subjects.

Except as required by applicable laws, the notifying party will not make (or permit any third party to make) any statement concerning the security breach that directly or indirectly references the other party, unless the other party provides its explicit written authorization.

CLAUSE 10: Control

In the event of a control by a competent supervisory authority, the Data Controller and the Data Processor undertake to cooperate with each other, in particular by providing any information that may be necessary, and with the supervisory authority.

The Data Processor shall inform the Data Controller immediately in case of control carried out by a supervisory authority relating to the Data Controller's data processing.

The Data Processor shall abstain from making any commitment on his behalf.

CLAUSE 11: Data Subject Rights

The Data Processor shall, to the extent legally permitted, provide reasonable assistance to the Data Controller in ensuring compliance with Data Controller's obligation to provide Data Subjects with the ability to effectively exercise their rights under Applicable Data Protection Law, in particular:

- right of access,
- right of rectification,
- right of erasure, right to object

- right to restriction of processing
- right to Data portability
- right not to be the subject of an automated individual decision.

(the “Data Subject Rights”).

Data Controller shall be responsible for any reasonable costs arising from Data Processor’s provision of Data Subject Rights assistance.

The Data Processor shall, as soon as possible, without exceeding a maximum of seventy-two (72) hours, notify the Data Controller of any request made by a Data Subject in relation to the exercise of his or her Data Subject Rights as detailed in paragraph above. Data Controller may, at its option, handle such requests and the Data Processor shall reasonably cooperate with and assist Data Controller in the execution and fulfillment of its obligations under Applicable Data Protection Law in relation to such requests. The Data Processor may only respond to the request of a Data Subject on the instructions of the Data Controller.

CLAUSE 12: Data Protection Officer (DPO)

The Data Processor has appointed a DPO to manage its compliance with the RGPD, which can be reached at:

- DPO .EASYTRIP@EASYTRIP.EU

The Data Controller has appointed a DPO to manage its compliance with the GDPR, which can be reached at:

- Email :
- Address :

Each Party undertakes to inform the other Party in the event of a change in the data of its DPO.

CLAUSE 13: Restitution and deletion of Data

At the end of the Agreement, the Data Processor shall, at the choice of Data Controller, delete or return all Personal Data and delete existing copies unless a mandatory rule resulting from Union law or Member State law applicable to the processing operations hereunder requires otherwise.

Data Processor has the right to keep the anonymized data for statistical processing purposes, including at the end of the contract.

If Union law or Member State law requires the storage of personal data, the Data Processor shall inform the Data Controller of this requirement.

The Data Processor shall provide the Data Controller, at first written request, proof of deletion of the Data.

CLAUSE 14: Data Location [Note: servers are located either in France, the Netherlands or Italy]

For the execution of the Agreement, no Data will be hosted outside France or the European Union. In this respect, in the event that all or part of the Data should be stored on servers located in countries outside the territory of the European Union; these countries must offer a sufficient and adequate level of protection, according to the GDPR.

The Data Processor shall inform the Data Controller of the location of Personal Data.

CLAUSE 15: Cross-border data flows

Data Processor shall comply with Data Controller's documented instructions concerning the transfer of Personal Data to a third country.

Data transfers outside the European Economic Area are authorized by the Data Controller if they comply with the following provisions:

- Any transfer of Data to a Data Processor office domiciled in a country outside the European Economic Area for which the European Commission has not determined by an adequacy decision that it provides an adequate level of protection ("Third Country") and any subsequent transfer in a Third Country must be governed by the Standard Contractual Clauses adopted by the European Commission on 5 February 2010 or by clauses having an equivalent content to these standard clauses.

CLAUSE 16: Audit

The Data Controller may, at his own expense, at no more than once every twelve (12) months, carry out an audit of the Technical and organizational security measures taken by the Data Processor.

This audit may be carried out by an internal audit structure of the Data Controller or by an independent external firm, provided that the latter does not itself also carry out an activity competing with the activity of the Data processor or has no legal link with a competitor.

If the Data processor provides objective reasons to consider that the audit firm chosen by the Data Controller does not offer sufficient guarantees of independence and impartiality, it will be entitled to refuse that the audit be carried out by this third party.

The Data Controller further acknowledges that his or the staff of the independent audit firm selected will adhere to and comply with the obligations and rules of security and confidentiality communicated by the Data Processor throughout the duration of the audit. The Data Controller shall ensure that the audit will not cause any disruption or discontinuity of Data Processor' activities.

A confidentiality agreement will have to be signed in advance between the Data Processor and the audit firm.

The Data Controller must inform the Data Processor in writing of his intention to have such an audit carried out and of the identity of the audit structure chosen in the case of an external firm and of the audit plan envisaged, subject to a thirty (30) calendar days' notice. Such notice may be shortened by mutual agreement between the Parties.

Prior to this audit, the Data Controller will communicate the proof of identity and title of his employees or experts seconded by the independent audit firm.

The audit carried out by the Data Controller will only concern the respect of the Data Processor contractual commitments in terms of Personal Data protection. The Data Processor undertakes, where applicable, to allow auditors access to the site assigned to the performance of the contract(s) concerned, to cooperate in good faith with them and to provide them with all necessary information. Nevertheless, the provisions of this article do not require the Data Processor to disclose to the Data Controller and/or its auditors any information of any kind previously disclosed or otherwise kept confidential by the Data Processor on its own behalf, that of any of its business partners or any other person in any capacity whatsoever. Consequently, the Data Processor may, at its sole discretion, deny the Data Controller and/or its auditors access to any information system (including databases and servers) and to any file, document, data or other information relating to the Protected Information. The Data Processor shall notify the Data Controller, in writing, scope of this refusal.

A copy of the audit report will be provided to the Data Processor as soon as possible. The report will then be subject to an adversarial review. In the event that the audit report reveals breaches by the Data Processor of its obligations under this Agreement, the Data processor undertakes to implement, at its own expense, the necessary corrective measures as soon as possible. If the audit conclusions contain recommendations, their implementation conditions will be examined contradictorily as soon as possible.

CLAUSE 17: Variation

The Parties may not modify this Agreement except to update any information in Schedule 1, in which case they will inform the DPO where required. This does not preclude the Parties from adding additional commercial clauses where required and does not affect the contract between the Data Controller and the Data Processor. In cases where any conflict arises in the interpretation of these agreements, this Agreement shall take precedence.

CLAUSE 18: Governing law

This Agreement shall in all respects be governed by and interpreted in accordance with the laws applicable to the contract. The parties hereto hereby submit to the jurisdiction of the courts as provided for in the contract.

Date:
Signature and company stamp of the Client

Read, approved and undersigned

Place of residency ______________________
Signature _____________________

Schedule 1: Description and purposes of the processing of personal data

The Data Processor may be required to process personal data in the context of the processing operations described in the table below:
The processing operations relate to any service as referred to in the contract.

Service	Nature and purpose	Type of Personal Data	Sensitive Data category	Categories of data subjects	Transfer outside UE	Recipients
Connect	Provide a service for fleet management optimization	Civil data, identity, identifying information, financial data, glocalization data	Individual national data	Client's employees	No	Fleet managers Easytrip Employees Subcontractors
VAT	to Collect VAT / Excise amount	Civil data, email address identifying information	Individual national identification number	Client's employees	No	Clients Easytrip Employees
Booking	to book a place in a Ferry, a train or to buy a vignette for trucks of our customers	Civil data, e mail, address identifying information	Individual national identification number	Client's employees	Turkey Morocco Tunisia Israel	Easytrip Employees Providers
Easyrep FR	designate a Legal representative in France and provides detailed data of the Drivers that load and/or unload in France	Civil data, identifying information Professional life Economic and financial information	Individual national identification number	Client's employees	no	Easytrip Employees Local Authorities
Easyrep IT	designate a Legal representative in Italy and provides detailed data of the Drivers that load and/or unload in Italy	Civil data identifying information Professional life Economic and financial information	Individual national identification number	Client's employees	no	Easytrip Employees Local Authorities
Toll	Opening of Tolls account at (Provider)	Civil data, email, identifying information	N/A	Client's employees	no	Easytrip Employees Providers
Communication	Inform the client database about the existing portfolio's services and new opportunities	civil data; identifying information	N/A	Client's employees	N/A	Clients Easytrip Employees

Duration: the duration of the processing carried out by the Data Processor is limited to the duration of performance of the services provided for in the contract and cannot in any event exceed the duration of the contract plus the applicable statutory limitation periods.

Schedule 2: Technical and organizational security measures taken by the Data Processor:

The means used by the Data Processor to ensure the security and confidentiality of the data are described below:

- physical security:

- Data center access is protected. An internal procedure and material means are put in place to ensure that no outsider or unauthorized person can access this room.

Physical access to Data Processor's premises is protected

- logical security:

- Data Processor guarantees that it has taken into account the computer security requirements and undertakes to implement all technical means in accordance with the state of the art, necessary to ensure the logical security of access to computer applications and hosted data and prevent any intrusion by unauthorized persons, whatever the nature or technique used.
- All critical systems, i.e. systems hosting critical functions, are redundant.
- A data backup plan is defined, implemented and monitored.
- A major disaster recovery plan is defined.
- All flows are traced. These traces contain the time stamp of the flow, its sender and recipient, and the functional nature of the exchange.
- Application access rights are assigned to the actors as strictly necessary and are based on role and user profile management.

All workstations are protected by regularly and automatically updated anti-virus software.

- organizational security:

- The employment contracts of Data Processor's employees include confidentiality and workstation usage clauses.
- The subcontracting contracts with companies in charge of the hosting, supervision and maintenance of the systems include clauses relating to security and confidentiality.

The Data Processor may change the means used to ensure the security and confidentiality of data and files. In this case, the Data Processor undertakes to replace them by means that are at least equivalent.

The Data Controller may also require amendments to the security and confidentiality measures, if required by law, authorities or internal auditors.

In case of a data protection audit conducted by the Data Controller itself at Data Processor's premises, any change of any means used to ensure data security and confidentiality may be raised. The Data Controller undertakes to specify the special security measures that it considers necessary in relation to the nature and risks associated with the treatment. The implementation of these special security measures by the Data Processor will result in an analysis, especially in terms of technical compatibility and feasibility, and, if appropriate, a quotation.