The party of the first part,

Hotel
(hereinafter, *"the Data Controller"*)

AND

The party of the second part,

Tourisoft Sàrl, with registered address at Route de Champ -Colin 18, CH-1260 Nyon Switzerland and represented herein by Mr Marco Baurdoux (hereinafter, *"the Processor"*)

I. Object

The object of these clauses is to define the conditions under which the Processor undertakes to process the personal data defined below on behalf of the Data Controller.

As part of their contractual relationship, the parties hereby undertake to observe the regulations in effect applicable to personal data processing and, in particular, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, applicable as of 25 May 2018 (hereinafter, *"the European Data Protection Regulati ons"*).

II. Description of the Subcontracted Processing

The Processor is hereby authorised to process the personal data necessary on behalf of the Data Controller to provide the following service(s):

- Channel-Management Hotel-Spider
- Web-Booking-Engine Spider-Booking

The nature of the data processing shall be:

- Receipt
- Storage
- Transfer to the hotel software/hotel CRM
- Log files for the platform Hotel-Spider/Spider-Booking

The purpose of the processing shall be:

- Centralisation of the Data Controller's online hotel reservations
- Possible transfer to the Data Controller's internal hotel software
- Possible transfer to the Data Controller's CRM
- Traceability of transactions via the platform Hotel-Spider/Spider-Booking

The personal data processed shall be:

- The Data Controller's customers
  - Gender
  - Given name
  - Surname
  - House/building number
  - Street
  - Postal code
  - City
  - Region / Province / County / Department / District
  - Country
  - Telephone number
  - Mobile phone number
  - Fax number
  - Email address
  - Company name
  - IP address
  - Credit card details
- The Data Controller's employees
  - Company name
  - Gender
  - Given name
  - Surname
  - Position
  - Email:
  - Fixed/mobile telephone number
  - Language

The data subject categories are the Data Controller's customers and the Data Controller's or the Processor's employees.

In order to perform the service object of this contract, the Data Controller shall make the following necessary information available to the Processor:

- Written confirmation authorising the Processor to electronically recover hotel reservations sent to the Data Controller through hotel booking websites such as Booking.com, Expedia INC, etc.
- The recovery of reservations via in tegration in the Spider -Booking product on the Data Controller's website

III. Contract Term

This contract shall be effective as of 25 May 2018, for a term equal to the service agreement connecting the Data Controller to the Processor.

IV. Processor's Obligations towards the Data Controller

The Processor hereby undertakes to:

1. process the data **exclusively for the sole purpose(s)** of the subcontracted object.

2. process the data pursuant to the Data Controller's documented instructions established in the annex to this contract. If the Processor believes any of the instructions breaches European Data Protection Regulations or any other provision of EU or Member State law on data protection, it shall **immediately inform** the Data Controll er. Moreover, if the Processor is required to transfer data to a third country or an international organisation in virtue of EU or the Member law to which it is subject, it must inform the Data Controller of such legal obligation before processing unless t he law concerned prohibits such information for significant reasons of public interest.

3. guarantee the **confidentiality** of the personal data under the scope of this contract.

4. ensure the **people authorised to process the personal data** in virtue of thi s contract:

- undertake to respect the **confidentiality** or are subject to an appropriate legal confidentiality obligation;
- receive the necessary **training** on personal data protection.

5. considering the use of its tools, products, applications and services, observe the principles of **data protection by design** and **data protection by default** .

6. **Subcontracting**

The Processor may commission another Processor (hereinafter, ***"the Secondary Processor"***) to do specific processing tasks. In such case, it shall inform the Data Controller in advance and in writing of any change planned concerning the addition or replacement of other Processors. This information must clearly indicate the subcontracted processing tasks, the identity and contact details of the Processor and the subcontracting dates. The Data Controller shall have a minimum of **30 days** after receipt of such information to submit any objections. Such subcontracting may not be done unless the Data Controller files no objection before said deadline.

The Secondary Processor is required to respect the obligations under this contract on behalf of and according to the instructions issued by the Data Controller. The initia l Processor is required to ensure the Secondary Processor offers the same sufficie nt guarantees as concerns the implementation of the appropriate technical and organisational measures so the processing meets the requirements of European Data Protection Regulations. If the Secondary Processor does not fulfil its data protection obligations, the initial Processor will be fully liable towards the Data Controller for the performance by the other Processor of its obligations.

7. **Data Subjects' Rights**

Upon collecting any data, the Processor must provide data subjects with infor mation on the data processing to be performed. The wording and form of this information must be agreed upon with the Data Controller before any data collection.

8. **Exercise of Data Subjects' Rights**

To the extent possible, the Processor must assist the Data Controller with compliance with its obligation of responding to requests from data subjects to enforce their rights: rights of access, rectification, cancellation and opposition, the right to limit processing, the right of data portability, the ri ght not to be subject of automatic individual decisions (including profiling).

9. **Notification of Personal Data Breaches**

The Processor must notify the Data Controller of any personal data breach within a maximum of 72 hours after gaining knowledge by certified mail . This notification shall be accompanied by any useful documentation allowing the Data Controller, if necessary, to notify the competent control authority of such breach.

At the same time, the Processor must notify the competent control authority in the name and on behalf of the Data Controller of any personal data breaches as quickly as possible and, if possible, no later than 72 hours after gaining knowledge thereof unless the breach in question poses no risk to the ri ghts and liberties of private individuals.

At the very least, this notification must include:
- a description of the nature of the personal data breach including, if possible, the categories and approximate number of data subjects affected by the breach and the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or another contact person through which additional information may be obtained;
- a description of the likely consequences of the personal data breach;
- a description of the measures taken or those the Data Controller proposes taking to correct the personal data breach including, as necessary, any measures to mitigate any possible negative consequences.

If, to the extent where it is not possible to provide all of this information at the same time, the information may be communicated gradually without improper delay.
Upon agreement by the Data Controller, the Processor shall notify the data subject in the name and on behalf of the Data Controller of the personal data breach as quickly as possible when the breach in question may pose a risk to the rights and liberties of a private individual.
The communication to the data subject shall describe the nature of the personal data breach in clear and simple terms and at the very least include:
- a description of the nature of the personal data breach including, if possible, the categories and approximate number of data subjects affected by the breach and the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or another contact person through which additional information may be obtained;
- a description of the likely consequences of the personal data breach;
- a description of the measures taken or those the Data Controller proposes taking to correct the personal data breach including, as necessary, any measures to mitigate any possible negative consequences.

10. **Processor's Assistance with the Data Controller's Obligations**

The Processor shall assist the Data Controller with data protection impact analyses.
The Processor shall assist the Data Controller with data control authority preliminary queries.

11. **Security Measures**

The Processor hereby undertakes to implement the security measures described in the document entitled " Technical and Organisational Security Measures".

The Processor hereby undertakes to implement the security measures provided for by PCI-DSS.

12. Post-Processing

Upon termination of the provision of the services concerning the processing of these data, the Processor hereby undertakes to comply with the instructions listed in the document entitled " Technical and Organisational Security Measures" by:
destroying all personal data or forwarding the personal data to the Processor designated by the new Data Controller.
Any forwarding must be accompanied by the destruction of all existing copies in the Processor's information systems. Once destroyed, the Processor must prove such destruction in writing.

13. Data Protection Officer

The Processor must notify the Data Controller of the name and contact details of its Data Protection Officer , if one has been designated pursuant to article 37 of the European Data Protection Regulations.

14. Record of Processing Categories

The Processor hereby declares that it maintains a written record of all categories of processing performed on behalf of the Data Controller including:
- the name and contact details of the Data Controller on behalf of which it is acting, any Processors and, as applicable, the data protection officer;
- the categories of processing performed on behalf of the Data Controller;
- as applicable, any personal data transfers to a third country or an international organisation including the identification of the third country or international organisation and, for transfers provided for in article 49, paragraph 1, second sub-paragraph of the European Data Protection Regulations, the documents proving the existence of the appropriate guarantees;
- to the extent possible, a general description of the technical and organisational security measures including, as necessary:
  - o the pseudonymisation and encryption of personal data;
  - o measures to guarantee the constant confidentiality, integrity, availability and resilience of the processing systems and services;
  - o measures to re-establish the availability of personal data and access to them within the appropriate periods of time in the event of a physical or technical incident;
  - o a procedure aimed at regularly testing, analysing and evaluating the effectiveness of the technical and organisational measures to ensure processing security.

15. Documentation

The Processor shall make the necessary documentation to prove compliance with all of its obligations available to the Data Controller to conduct audits including inspections by the Data Controller or another auditor appointed by the latter and shall assist with any such audits.

V. Data Controller's Obligations towards the Processor

The Data Controller hereby undertakes to:
1. provide the Processor with the data indicated in clause II;

2. document all instructions in writing concerning the data processing to be done by the Processor;
3. ensure compliance with the obligations established in European Data Protection Regulations by the Processor before and throughout the duration of the processing;
4. supervise the processing including by conducting audits and inspections of the Processor.