DATA TRANSFER AGREEMENT

THE PARTIES

Customer	**The customer entity as identified in the applicable Agreement** (hereinafter referred to as the **"TRANSFEROR"**.
THE HOTELS NETWORK S.L.P.	**THE HOTELS NETWORK (THN**), (acting herein on its behalf), with registered office at Avda. Diagonal, 439, 3º-1ª, 08036, Barcelona, (Spain), with tax identification number B-65542714, and herein represented by Mr. Juan José Rodríguez, as authorized signatory (hereinafter referred to as **"ASSIGNEE" or THN**).

(hereinafter collectively referred to as **the "Parties"**)

Acknowledging their sufficient legal capacity to execute this agreement (hereinafter, the "**Agreement**")

BACKGROUND

The Parties acknowledge that both ASSIGNEE and TRANSFEROR act as independent controllers of the personal data transferred under this Agreement, in accordance with Regulation (EU) 2016/679, of April 27, 2016 (GDPR), and Organic Law 3/2018, of December 5 (LOPDGDD).

As independent controllers, the Parties will process personal data according to their own purposes.

The Transferor wishes to contract the SafeDirect service offered by the Assignee. This service consists of providing a travel assistance service that may include issuing a travel assistance or cancellation certificate to customers making room reservations (hereinafter, "Services"). The holder of the travel assistance service will be the Assignee. To this end, the Transferor authorizes the Assignee to enter into a collaboration agreement with a Travel Assistance entity. The agreement between the Assignee and the collaborator must meet the same requirements and obligations set forth in this agreement.

To fulfill such Services, the Assignee must process personal data provided by the Transferor. Therefore, the parties enter into this data transfer agreement (hereinafter, "Agreement").

The Transferor declares that it has informed website users and has a legal basis to process and transfer personal data to third parties.

The purpose of this Agreement is to ensure adequate protection of the processing and transfer of personal data in compliance with applicable data protection regulations.

1. Definitions

For the purposes of this Agreement, the capitalized terms used herein but not otherwise defined will have the following meanings:

"Personal Data": any information related to an identified or identifiable natural person.

"Data Subject": the identified or identifiable natural person to whom the Personal Data pertains.

"Processing": any operation performed on Personal Data, such as collection, storage, use, disclosure, and transfer.

"Travel Assistance Entity": any travel assistance company that has entered into a Services Agreement with the Assignee.

2. Independent Data Controllers

2.1. The Parties acknowledge that both the Transferor and the Assignee act as independent controllers of the personal data transferred under this Agreement, in compliance with applicable privacy laws.

2.2. As independent controllers, the Parties will process personal data in accordance with their respective purposes.

2.3. The Parties commit to fulfilling their respective obligations under the GDPR and other applicable personal data protection regulations. In particular, each Party is responsible for informing Data Subjects as per Articles 13 and 14 of the GDPR.

2.4. Furthermore, the Parties will cooperate to ensure compliance with applicable data protection regulations.

3. Categories of Personal Data and Data Subjects

3.1. The categories of personal data subject to transfer are as follows:

- Contact information, including users' full names and email addresses
- Device identification data and traffic data: IP addresses, MAC addresses, backend HASH.

(hereinafter referred to as **"Reservation Data"**)

3.2. The categories of Data Subjects are as follows: Customers of the Transferor

3.3. Authorized Processing operations are as follows: Consultation, use, interconnection, and deletion or destruction.

4. Authorized Personnel

4.1. The Assignee ensures that personnel authorized to process data have expressly and in writing committed to data confidentiality or are subject to a legal obligation of confidentiality.

4.2. The Assignee ensures that authorized personnel have received the necessary training to uphold the protection of personal data.

5. Transmission of Personal Data to Third Parties

5.1. **EU Standard Contractual Clauses**: To the extent Personal Data includes information about individuals located in the European Economic Area ("EEA"), United Kingdom, and/or Switzerland, and the Parties or their subcontractors transfer, store, or otherwise access such Personal Data outside these areas ("Third

Countries"), the Parties agree to include the standard contractual clauses (hereinafter “SCC”) (as defined in Annexes I-III) or any modifications thereof, as an adequate transfer mechanism for such data. The SCC will be deemed incorporated and form part of this Data Protection Annex, as set forth in Annexes I-III of this Annex, which define the roles of the Parties and the description of the transfers.

5.2. To the extent Reservation Data includes information about any natural person residing in the state of California, USA, all terms defined by the California Consumer Privacy Act ("CCPA"), CAL. CIV. CODE Title 1.81.5 § 1798.100 et seq., as amended by the California Privacy Rights Act ("CPRA") (collectively, "California Privacy Law") shall apply.

6. Technical and Organizational Measures

6.1. Both parties acknowledge their obligations to establish security measures for the various categories of data and processes established in the GDPR and applicable regulations.

6.2. Each Party commits to adopting appropriate technical and organizational measures to protect personal data against unauthorized or unlawful processing and accidental loss, destruction, or damage, taking into account the level of harm that could result for the data subject whose personal data is affected.

6.3. Additionally, the Assignee shall implement security procedures and programs specifically addressing the nature of any special categories of personal data, such as:

- Pseudonymization and encryption of personal data;
- Ensuring the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
- Ensuring the ability to restore data access in a timely manner in the event of a technical or physical incident;
- Procedures for periodic testing, assessment, and evaluation of the effectiveness of technical and organizational measures.

7. Data Breaches

7.1. Data breaches known to the Assignee affecting data transferred under this Agreement must be reported without undue delay and, in any case, within 24 hours of awareness, to the Transferor for necessary mitigation measures. Notification is not required when the breach is unlikely to pose a risk to individuals’ rights and freedoms.

7.2. The breach notification between the Parties will include, at a minimum:

- Description of the nature of the breach;
- Categories and approximate number of affected Data Subjects;
- Categories and approximate number of affected data records;

- Possible consequences;
- Measures taken or proposed to mitigate effects;
- Contact details for further information.

8. Data Subject Rights

Each Party is responsible for managing Data Subjects' rights requests. Data Subjects or their legal representatives may exercise their rights (access, rectification, erasure, objection, restriction of processing, data portability, and the right not to be subject to automated individual decisions) via the following emails:

- ASSIGNEE's Email: privacy@thehotelsnetwork.com
- TRANSFEROR's Email: As specified in the applicable Agreement.

9. Duty of Confidentiality

Each Party shall maintain the confidentiality of personal data accessed under this Agreement, even after its termination.

10. Liability

Both Parties, as controllers, will be liable for damages caused by non-compliance with this Agreement.

11. Termination of Service Provision

Upon termination of the service provision under this Agreement, both parties must return or delete data as requested unless subject to implicit legal obligations.

THE HOTELS NETWORK, S.L.P.

Full Name: Juan José Rodríguez

Title: CEO

ANNEX I

A. LIST OF PARTIES

Transferor of data in Transfer A and Assignee of data in Transfer B:

Company Name and address	**The customer entity identified in the applicable Agreement**
Full Name, title and contact details	*As identified in the applicable Agreement*
Activities related to the data transferred under these clauses: As provided in the Agreement.	*As provided in the Agreement.*
Signature and date	*As provided in the Agreement.*
Role (Controller/Processor)	*Controller*

Importer of data in Transfer A and Exporter of data in Transfer B:

Company Name and address	*The Hotels Network, S.L.P.*
Full Name, title and contact details	*Juan José Rodríguez* *jro@thehotelsnetwork.com*
Activities related to the data transferred under these clauses: As provided in the Agreement.	*As provided in the Agreement.*
Signature and date	*As provided in the Agreement.*
Role (Controller/Processor)	*Controller*

B. DESCRIPTION OF THE TRANSFER

	TRANSFER A (FROM TRANSFEROR TO ASSIGNEE)	**TRANSFER B (FROM ASSIGNEE TO TRANSFEROR)**
Categories of data subjects whose personal data are transferred	Customers	
Categories of personal data transferred	- Contact information, including users' full name and email address. - Device identification data and traffic data: IP addresses, MAC addresses, backend HASH.	
Sensitive Data	Not applicable Sensitive data may only be transferred if safeguards or restrictions are applied that fully account for the nature of the data and the associated risks, such as strict purpose limitation, access restrictions (including access only for personnel with specialized training), maintenance of an access log, restrictions on onward transfers, or additional security measures.	
Frequency of transfer	Regular processing	
Nature of processing	Consultation, utilization, interconnection, and deletion or destruction.	
Purpose(s) of the transfer and subsequent data processing	Provision of services and as necessary for fulfilling obligations arising from the Agreement.	
Retention period for personal data	As necessary to fulfill the obligations arising from the Agreement and to comply with any applicable legal obligations.	
For transfers to (sub)processors, specify also the purpose, nature,	To the extent the Transferor may share Data with third parties, it shall apply the requirements of this Data Protection Annex.	

and duration of the processing	

ANNEX II

TECHNICAL AND ORGANIZATIONAL MEASURES, INCLUDING MEASURES TO ENSURE DATA SECURITY

To the extent that the Assignee or its third parties access Customer and/or Booking Data in relation to this Agreement, the Assignee will implement an Information Security Program that includes administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of the Customer and/or Booking Data and to protect it from unauthorized access, use, disclosure, alteration, or destruction. Specifically, the Information Security Program of the Importer will include, but not be limited to, the following safeguards, as appropriate or necessary to ensure the protection of Customer and/or Booking Data:

(i) Access Controls

Policies, procedures, and physical and technical controls to:
a. Limit physical access to information systems and facilities to authorized individuals.
b. Ensure that all staff members requiring access to Customer and/or Booking Data have controlled access and to prevent unauthorized personnel from gaining access.
c. Authenticate and permit access only to authorized individuals and prevent staff members from providing Customer and/or Booking Data or related information to unauthorized persons.
d. Encrypt and decrypt Customer and/or Booking Data as applicable.

(ii) Security Awareness and Training

A security awareness and training program for all staff members (including management) that includes training on the application and compliance with its Information Security Program.

(iii) Security Incident Procedures

Policies and procedures to detect, respond to, and otherwise address security incidents, including:
a. Monitoring systems to detect actual or attempted attacks or intrusions into Customer and/or Booking Data or related information systems.
b. Procedures to identify and respond to known or suspected security incidents, mitigate the harmful effects of such incidents, and document incidents and their outcomes.

(iv) Contingency Planning

Policies and procedures to respond to emergencies or other events (e.g., fire, vandalism, system failure, or natural disaster) that damage Customer and/or Booking Data or the systems containing it, including a data backup plan and disaster recovery plan.

(v) Device and Media Controls

Policies and procedures governing the receipt and removal of hardware and electronic media containing Customer and/or Booking Data within and outside an Importer's facilities, including procedures to ensure secure disposal or re-use of such media.

(vi) Audit Controls

Hardware, software, and/or procedural mechanisms that log and examine activity in information systems containing or using electronic information, including appropriate records and reports relating to these security requirements and their compliance.

(vii) Data Integrity

Policies and procedures to ensure the confidentiality, integrity, and availability of Customer and/or Booking Data and protect it from improper disclosure, alteration, or destruction.

(viii) Storage and Transmission Security

Technical measures to prevent unauthorized access to Customer and/or Booking Data transmitted over an electronic communications network, including encryption as needed during transmission or storage in systems accessible to unauthorized persons.

(ix) Secure Deletion

Policies and procedures for the secure deletion of Customer and/or Booking Data, considering available technology to ensure it cannot be feasibly reconstructed.

(x) Assigned Security Responsibility

The Assignee will designate a security officer responsible for developing, implementing, and maintaining its Information Security Program.

(xi) Testing

The Assignee shall regularly test (at least annually) the controls, systems, and procedures of its Information Security Program to ensure proper implementation and effectiveness. Tests shall be conducted or reviewed by independent third parties or personnel separate from those who develop or maintain the security programs.

(xii) Program Adjustment

The Assignee will monitor, evaluate, and adjust the Information Security Program as appropriate in light of technological changes, industry security standards, the sensitivity of Customer and/or Booking Data, and evolving internal or external threats.

ANNEX III

STANDARD CONTRACTUAL CLAUSES FOR THE EEA, SWITZERLAND AND THE UNITED KINGDOM

For data transfers between the Exporter and the Importer, the following SCCs are incorporated:

- C-to-C Transfer Clauses of the SCC: This refers to the Standard Contractual Clauses for the Transfer of Booking Data to Third Countries (Controller-to-Controller module) as described in Article 46 of the GDPR and adopted by the European Commission's Implementing Decision (EU) 2021/914 of June 4, 2021, available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj, as applicable to Module One (Controller-to-Controller), completed as outlined herein;
- Swiss SCCs, meaning the standard data protection clauses issued, approved, or recognized by the Swiss Federal Data Protection and Information Commissioner, and completed below.
- UK Addendum, meaning the applicable standard data protection clauses adopted in accordance with Article 46(2)(c) or (d) of the UK GDPR, including the standard data protection clauses issued by the Commissioner under Section 119A(1) of the UK Data Protection Act 2018 (DPA), also available at link, as amended from time to time and completed below

Together referred to as the "SCCs."

EUROPEAN UNION

Data Exporter	As specified in Annex I.
Data Importer	As specified in Annex I.
Clause 7 of the EU SCCs	Applies
Clause 11 of the EU SCCs:	The optional language does not apply.
Clause 13(a) of the EU SCCs:	Spanish Supervisory Authority.
Clause 12 of the EU SCCs:	The liability of the Data Exporter under Clause 12 of the C-to-C Transfer Clauses of the SCCs and this Data Protection Annex shall be subject to the limits of the main Agreement.
Clause 18 of the EU SCCs:	Spanish Courts

Annexes I and II of the EU SCCs:	As specified in Annexes I and II.

UNITED KINGDOM
Regarding transfers of Reservation Data protected by UK privacy laws, the UK Addendum applies to such transfers subject to the following:

Parties (Table 1)	As specified in Annex I
SCCs, Modules, and Selected Clauses (Table 2):	Refer to the selected modules and clauses of the C-to-C Transfer Clauses of the SCCs as specified above.
Appendix Information (Table 3):	Refer to the relevant information in Annexes I and II.
Termination of this Addendum when the approved Addendum changes (Table 4):	Both Parties may terminate the UK Addendum in accordance with its terms.

SWITZERLAND

Regarding transfers of Reservation Data protected by Swiss privacy laws, subject to the following:

a) Any reference in the C-to-C Transfer Clauses of the SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as a reference to the Swiss Data Protection Act (DPA).

b) All references to "EU," "Union," and "Member State law" shall be interpreted as references to Swiss law.

c) Any reference to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the relevant Swiss data protection authority and courts.

Unless the C-to-C Transfer Clauses of the SCCs, as applied herein, cannot be used to legally transfer such Customer and/or Reservation Data in accordance with Swiss privacy law, in which case the Swiss SCCs will be incorporated by reference and will apply to such transfers. In that case, the relevant annexes or appendices of the Swiss SCCs will be completed with the information contained in Annexes I and II of this Data Protection Statement.

Nothing in this Data Protection Annex is intended to modify or contradict the SCCs, except for Clauses 7, 11, 12, 13, and 18, which are additional commercial clauses relating to the C-to-C Transfer Clauses of the SCCs, as permitted by Clause 2(a) of the C-to-C Transfer Clauses of the SCCs, the UK Addendum, and the Swiss SCCs.