Umbrella
The Travel Tech Powerhouse

Data Processing Agreement

concluded between

(hereinafter 'Customer')

and

Umbrella Organisation U & O AG
Binzstrasse 33
8620 Wetzikon
Switzerland

(hereinafter 'Umbrella')

Umbrella Organisation AG
Binzstrasse 33 | CH-8620 Wetzikon
phone/whatsapp: +41 (0)79 842 1687
Mail: helmut.pilz@umbrella.ch

1. Purpose of this Appendix

Customer (the "Data Controller") will use Umbrella Faces ("the Solution") provided by Umbrella (the "Data Processor") to process profile data of Customer. By providing the Services related to the Solution, Umbrella may process Personal Data (profile data) related to employees of its Customers. Such profile data may contain:

- Name
- Address
- Date of Birth
- Personnel Number
- ID-card
- Telephone Number
- Payment Information

Further details such as the scope of services and the use of data are set out in the Main Body of the Agreement.

2. Definitions

2.1. Terms and references which are not defined in this Appendix shall have the same meanings as those contained in the Agreement. In addition, Appendix unless the context otherwise requires:

2.2. "**Adequate Safeguards**"" means the measures provided for by Article 32 of the Regulation to compensate for the lack of protection, if a third country importing Personal Data does not ensure an adequate level of protection; such safeguards may in particular result from an international data transfer agreement incorporating the standard contractual clauses between the data exporting and the data importing party pursuant to Article 45 and 46 of the Regulation or any other adequate measure or alternative method that comply with the Directive such as for example Binding Corporate Rules (Article 47 of the Regulation).

2.3. "**Data Controller"** has the meaning set out in Article 4 (7) of the Regulation.

2.4. "**Data Processor**" has the meaning set out in Article 4 (8) of the Regulation.

2.5. "**Data Protection Laws and Regulations** "means laws and regulations regulating data privacy and/or the Processing of Personal Data, in particular laws and regulations implementing the Regulation; "Data Protection Law or Regulation" shall be construed accordingly.

2.6. "**Data Subject**" means an identified or identifiable natural person as set out in Art 4 (1) of the Regulation.

2.7. "**Regulation**" means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

2.8. "**Processing**" has the meaning set out in Article 4 (2) of the Regulation.

2.9. "**Relevant Transfer**" means a transfer of Personal Data to an entity which is in a country which (for the purposes of this Appendix) does not provide an adequate level of protection as required by the Data Protection Laws and Regulations.

3. General Information

3.1. Data Processor shall process the Personal Data within the territory of a Member State of the European Union, another signatory to the European Economic Area (EEA) or Switzerland.

3.2. If Data Processor needs to perform a Relevant Transfer in order to provide its services under the Agreement, Data Processor shall set up and observe and ensure that its Affiliates or Subcontractors carrying out any Relevant Transfer set up and observe Adequate Safeguards to carry out any Relevant

Transfer. Each act or omission of Umbrella or its Affiliates or Subcontractors in relation to the obligations set forth in the Adequate Safeguards shall be deemed to be an act or omission. Umbrella shall not make a Relevant Transfer before such Adequate Safeguards have been set up.

3.3. The Data Controller is entitled to issue directions to the Data Processor to the effect of amending the purpose, nature and scope of data Processing at any time. Direction means the written instruction, issued by Data Controller to Data Processor, and directing the same to perform a specific action with regard to Personal Data (including, but not limited to, anonymizing, blocking, deletion, making available). The Data Controller has the right to supplement its directions by any time respective to the processing of data. The Data Controller will set a reasonable time period to realize the direction. The Data Controller will bear any costs of Data Processor that are related to its direction.

4. Data Controller's Rights and Obligations

4.1. The Data Controller is responsible (within the meaning of Article 4 (7) of the Regulation) for the Data Processor's processing of data under the Main Body of the Agreement and it is incumbent on the Data Controller to determine whether, and the extent to which, data processing is admissible.

4.2. As the responsible party, the Data Controller must ensure that the rights of affected parties, which are to be exercised in relations with the Data Controller, are not violated. The Data Controller will issue (partial) orders in writing, and changes to the object of processing as well as procedural adjustments must be coordinated among the parties hereto.

4.3. Prior to the commencement of data Processing and in regular intervals thereafter, the Data Controller must ascertain that the technical and organizational measures the Data Processor adopts to protect data are implemented as intended. For this purpose, the Data Processor must document results by a records of processing activities as stated in Art. 30 of the GDPR. The Data Controller will promptly notify the Data Processor if and when it detects errors or irregularities in connection with the Data Processor's processing of personal data

5. Data Processor's Obligations

5.1. The Data Processor processes personal data under effective agreements only, with the purpose, nature and scope of data processing being subject exclusively to the Data Controller's directions as set forth in the Main Body of the Agreement. The Data Processor may only transfer personal data to third parties to the extend necessary to provide its services and subject to the terms and conditions stipulated in this Appendix. Data Processor shall, upon Data Controller´s request and cost, provide to Data Controller all information on Data Controller´s personal data and information. In its processing of data, the Data Processor may deviate from such directions only to the extent that the Data Controller has consented thereto in writing.

5.2. The Data Processor will assist the Data Controller with the implementation as well as the full and swift completion of controls. Where Data Controller, based upon applicable data protection law, is obliged to inform an individual about the collection, processing or use of its personal data, Data Processor shall assist Data Controller in making this information.

5.3. The Data Controller shall retain title as to any carrier media provided to Data Processor as well as any copies or reproductions thereof. Data Processor shall store such media safely and protect them against unauthorized access by third parties. Documents and files containing personal data that are no longer needed must not be deleted (subject to applicable Regulation provisions) without the Data Controller's prior consent.

5.4. The Data Processor hereby confirms that it has appointed a data protection officer according to article 37ff GDPR.

5.5. For purposes of proper Personal Data Processing, the Data Processor represents and warrants that all agreed measures will be implemented as intended.

5.6. The Data Processor must ensure that its enterprise and the course of its operations are aligned with the objective of protecting the data Processed on the Data Controller's behalf as required – e.g., against unauthorized third-party access. The Data Processor will duly consult the Data Controller before implementing any changes to the system of processing the Data Controller's data, provided such changes lead to a lower data security level than it has been implemented on the effective date of this Agreement.

5.7. The Data Processor will promptly notify the Data Controller if and when it deems the latter's directions to be in violation of applicable law, and the Data Processor may put off following any such direction until it is confirmed or changed by the Data Controller.

5.8. The Data Processor is obligated to promptly inform the Data Controller of each violation of Regulation provisions, contractual terms and/or the Data Controller's directions that has occurred in the course of its own or a third party's Processing of data.

5.9. The Data Processor must adequately label the data it processes on the Data Controller's behalf. Insofar as data is processed for more than one purpose, the Data Processor must tag the data with the appropriate purpose.

5.10. The Data Processor must inform the Data Controller without delay in case of a control or measures of the Supervisory Authority which is related to Personal Data Processed on the behalf of Data Controller.

6. Subcontractor

6.1 The Data Processor may engage his own affiliated companies or other sub-contractors for the performance of the contract under the following conditions:

6.1.1 The Data Processor will select the subcontractor with care and must ensure, prior to the appointment that the subcontractor is capable of complying with the terms agreed between the Data Controller and the Data Processor.

6.1.2 Prior to any appointment and in regular intervals (for the duration of any subcontract) thereafter, the Data Processor must ascertain that the technical and organizational measures the subcontractor adopts to protect data are implemented.

6.1.3 The Data Processor must procure that the subcontractor is also bound by the provisions hereof as well as any additional Data Controller direction, and it will ensure compliance with any related duties on a regular basis.

6.1.4 In case the Data Processor appoints a Third Party as subcontractor, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

6.2 Subcontractor in the meaning of this Article 6 does not include ancillary services ordered by the Data Processor from third parties to assist in the performance of the commission. These may be e.g. telecommunications services, maintenance and user support, cleaning, auditing or the disposal of data media. To safeguard the protection and security of the Data Controller's data, even where ancillary services are taken from third parties, the Data Processor must however conclude adequate and lawful contractual agreements and undertake monitoring activities.

7. Monitoring rights of the data controller

7.1. The Data Controller is entitled to verify compliance with applicable privacy law and/or the terms of the parties' contractual arrangements and/or the Data Controller's directions (by the Data Processor) at any time and to the extent necessary. For such purpose, Controller may collect voluntary disclosures from Processor, have an expert provide a testimonial or expert´s opinion. If Data Controller has reasonable doubts that the provided testimonials are sufficient Data Controller shall inform Data Processor about its doubts in writing. If Data Processor does not provide Data Controller with sufficient testimonials after such written information in due time Data Controller shall be entitled to audit during regular business hours personally the Data Processor' place of business. When doing so, the Data Controller will ensure that the scope of its control is limited to the necessary extent so as to minimize its impact on the Data Processor's course of operations

7.2. The Data Processor is obliged to furnish the Data Controller with such information as may be required to facilitate controls within the meaning of § 6 number 1.

7.3. If and to the extent that data is processed in a private residence, access thereto is to be coordinated with the Data Processor in advance. The Data Processor represents and warrants that other residents, if any, are in agreement with this clause.

8. Data Secrecy

The Data Processor represents and warrants that it is aware of, and knows how to implement, applicable privacy rules. The Data Processor further represents and warrants that any staff involved in the performance of work contemplated herein will be instructed in such rules and held to the duty of data secrecy.

9. Technical/organizational measures

Without prejudice to the provisions of the Main Body of the Agreement on data protection, the Data Processor undertakes the technical and organizational measures set out in Schedule 1 to this Appendix to ensure compliance with applicable privacy rules.

10. Termination

10.1. Without prejudice to the provisions of the Main Body of the Agreement the Data Controller may terminate the Agreement without notice whenever the Data Processor (i) committed a material violation of applicable privacy rules or its obligations hereunder, (ii) is unable, or unwilling, to follow the Data Controller's directions or (iii) refuses entry to the Data Controller or the competent regulatory authorities in violation hereof.

10.2. Following the termination of this Agreement, the Data Processor must delete all documents and data in its possession, as well as any results of data processing or use, that are related to the relationship established by this Agreement unless needed by Data Processor to comply with its contractual or legal obligation to store this data. The Data Processor's media must then be physically deleted. This also applies to any back-up copies in the Data Processor's possession, and the act of such deletion is to be documented in a suitable manner. Rejected and test data is to be destroyed or physically deleted immediately.

Schedule 1

To Appendix 5

Description of Technical and Organizational Measures

a) Access control to premises and facilities

Measures restricting access to data-processing equipment employed to process or use personal data:

The Data Center is located in a separate Building. The access to this Building is secured by an electronic lock. All keys and electronic keys are registered. Access to the Data Center is only provided to those employees who are responsible for the operation of the Data Center. All other persons, who need access to the Data Center for specific reasons, have to register at the security office and only gain an access to the Data Center limited to the specific purpose and the duration of their visit. After finishing the visit, the limited access document has to be released to the security office. The Building is secured by an intrusion detection system as well as by motion detectors. The intrusion detection system is connected outside normal business hours with a security agency.

b) Access control to systems

Measures restricting access to data-processing systems:

The usage of the data processing systems requires a valid user account. User accounts are identifiable. Remote access to productive systems is secured by VPN connections (2-factor authorization). Security relevant activities are logged.

c) Access control to data

Employees only get access to data-processing systems subject to their official business tasks. Access privileges are in general related to business tasks and will be defined based on the job description and/or from tasks dedicated to a job area. Access privileges are defined by the applicable supervisor.

d) Distribution control

Data transmission will in general be encrypted using a state of the art encryption technology. The used technology is subject to the applicable application interface and will be agreed between sender and receiver. To avoid any misuse of no longer used storage media (e.g. CD, hard drives) as well as hardcopies, such media will be destroyed in-house by using a DIN-certificated shredder, or by authorization of a subcontractor specialized in file destruction and using closed containers for transport of such media.

e) Input control

Different user rights are defined. Each employee does only get access on an absolute need to know basis and subject to his business tasks. Processes for gaining access privileges for security relevant resources are transparent and will only requested and assigned by authorized persons. All security relevant administration activities are logged and the applicable log files will be analyzed.

f) Job control

Relevant employees are obliged to comply with the principal of data secret. Data Processor Agreements are signed with all subcontractors and their compliance is controlled on a regular basis. Jobs and processes are logged and controlled and analyzed at random.

g) Availability control

Scope of the services is a backup of applicable databases and their recovery in case of a loss of data. For this reason, an automatic database backup procedure following given standard procedures is in place. All systems are redundant. An active/active operation is secured by two locally separated data centers.

h) Segregation control

Identical services for comparable groups of customers are processed on jointly used systems. For that reason, System Administrators privileges are not assigned to one specific customer. Data will be logically separated and access is limited to authorized users. All data can be dedicated to a specific customer at all time. Test systems are logically separated from productive systems.