Data Processing Addendum

In accordance with Art. 28 para. 3 of the EU General Data Protection Regulation (GDPR)

1) In order to fulfil the contractually agreed business purposes, the collection, processing and use of the transferred personal data shall also be conducted in accordance with the relevant statutory provisions. Personal data is all data that is personally obtainable on the Contractual Partner (Customer), i.e. the name, postal address, email address, payment details, and ordered goods and services for instance.

2) The responsible body according to Art. 4 para. 7 of the GDPR is eventfactory GmbH, Grabenweg 71, 6020 Innsbruck, Austria.

3) According to Art. 6 para. 1 lit. f of the GDPR, eventfactory GmbH has a legitimate interest in storing the personal data transferred thereto over the period of the contract execution - which was collected for the purposes of contract execution - in order to have your contact information available for future orders.

4) The Contractual Partner (Customer) has the right to object and to provide justification therefor at any time against the processing of personal data, which is carried out on the basis of Art. 6 para. 1 lit. f of the GDPR.

   The objection can be made in any form and should ideally be sent via email to DE.Datenschutz@liberty-int.com (Data Protection Coordinator).

   If the Contractual Partner (Customer) objects, his/her personal data shall no longer be processed unless eventfactory GmbH can prove compelling and legitimate reasons for the processing which outweigh the interests, rights and freedoms of Contractual Partner (Customer) or the processing serves the assertion, exercise or defence of legal claims.

5) In addition, storage beyond the contractual period is required for tax purposes, for the assertion of warranty claims and thus corresponds to the fulfilment of a legal obligation on our part pursuant to Art. 6 para. 1 lit. c of the GDPR.

6) The person affected by the data processing has the right to information under Art. 15 of the GDPR, the right to rectification under Art. 16 of the GDPR, the right to erasure under Art. 17 of the GDPR, the right to restriction of processing under Art. 18 of the GDPR and the right to data portability under Art. 20 of the GDPR.

7) The personal data of Contractual Partner (Customer) shall not be disclosed to third parties; the sole exception within the scope of contract performance is the transfer to third parties who are involved in the execution of the contract (e.g. as part of third-party involvement in ticket distribution pursuant to Section 4.). The transfer of the data to third parties involved in the performance

of the contract shall also be carried out according to the legal regulations of the Federal Data Protection Act 2000 (DSG 2000) and the E-Commerce Act (ECA) as well as the General Data Protection Regulations (GDPR). The scope of the transfer is limited to the necessary minimum required for contract performance.

8) The Contractual Partner (Customer) has the option of changing or erasing the stored data about him/her at any time. There is no right to erasure of the stored data about him/her if its erasure conflicts with statutory or contractual retention periods, and especially if the data is necessary for the substantiation, content design or modification as well as the performance of the contractual relationship between him/her and the intermediary and must be stored for these purposes.

9) When the Contractual Partner (Customer) utilises services of eventfactory GmbH, information e-mails for similar services will be sent to them in the future. These e-mails are sent only after the conclusion of an order and with the aid of what is known as the 'double opt-in procedure'. This means that the information e-mails are only sent if the Contractual Partner (Customer) first confirms their registration through a confirmation e-mail sent via a link contained therein. The Contractual Partner (Customer) may ask to stop receiving such information e-mails at any time. To do so, please contact De.Datenschutz@liberty-int.com by e-mail or use the contact details given in the Legal Notice or click on the link at the end of the information e-mail.

PRIVACY POLICY NOTICE

For customers and prospective customers

eventfactory GmbH is aware of the importance of the personal information which you entrust to us. We are committed to ensuring the confidentiality of the data entrusted to us by our customers and prospective customers. The following information is intended to provide you with an overview of how we process your personal data and your data protection rights under the EU General Data Protection Regulation (GDPR) and the Federal Data Protection Act 2000 (DPA 2000). The details of the data which is processed and how the data collected is used depends largely on the services provided to you.

A. Responsible authority

The responsible authority within the meaning of the General Data Protection Regulation (GDPR) and the Federal Data Protection Act 2000 (DPA 2000) is:

eventfactory GmbH, Grabenweg 71, 6020 Innsbruck, Austria.

B. Data Protection Coordinator

You can reach our data protection coordinator:

Karin Salota

By e-mail: De.Datenschutz@liberty-int.com

C. Source of personal data

We process personal data from our customers and prospective customers as required in order to carry out our business operations. Furthermore, where the collection of data is necessary for the provision of our services, we shall process personal data only insofar as is necessary to further the legitimate business purposes stated having obtained such data from publicly available sources or in circumstances where the data has been provided to us by other companies within the Liberty International Tourism Group or by other third parties (such as information) the data in question has been transmitted for a legitimate purpose.

D. Categories of personal data being processed

We shall process the following categories of personal data:

- Master data (e.g. name, address and date of birth),
- Contact details (e.g. telephone number, email address),
- Data for the fulfilment of our contractual obligations (e.g. sales data),
- Information about your credit rating,
- Correspondence (e.g. correspondence with you),
- Advertising and sales data (e.g. regarding products which may be of interest to you)
- As well as any other such data comparable with the above-mentioned categories.

E. PURPOSES FOR WHICH YOUR PERSONAL DATA SHALL BE PROCESSED AND LEGAL BASIS ON WHICH YOUR DATA IS PROCESSED

We shall process all personal data in accordance with the provisions of the EU General Data Protection Regulation (GDPR) and the Federal Data Protection Act 2000 (DPA 2000):

1. based on your consent (Art. 6 para. 1 lit. a GDPR)

Where you have provided us with consent to process personal data for a specific purpose (e.g. transmission of newsletters, forwarding of data, analysis of payment transaction data for marketing purposes, photographic content in the context of events) such consent shall form the legal basis upon which your data is processed. Your consent to such processing can be revoked at any time. This also applies to the revocation of consent forms, which were issued to us before the introduction of the GDPR, i.e. prior to 25th May 2018. The withdrawal of consent is only effective from the date of receipt and does not affect the legal basis of the data processed until such withdrawal of consent is processed.

2. the fulfilment of contractual obligations (Art. 6 para. 1 lit. b GDPR)

The processing of data is carried out in order to provide services in the context of the execution of our contracts with our customers or to carry out pre-contractual measures, which are completed upon request. The purpose for the data processing is based primarily on the specific contractual relationship in question (e.g. event planning, agency). Further details concerning the data processing purposes can be found in the individual contracts and terms and conditions.

3. due to legal obligations (Art. 6 para 1 lit. c GDPR) or in the public interest (Art. 6 para. 1 lit. e GDPR)

eventfactory GmbH is subject to a number of different legal obligations, which includes legal requirements. The purpose for processing your data shall include, but is not limited to, compliance with tax regulations including reporting obligations as well as conducting risk assessments and for the purpose of ensuring the proper management of the Company and the Group.

4. in the context of balancing legitimate interests (Art. 6 para. 1 lit. f GDPR)

Where necessary, we shall process your data beyond the actual fulfilment of the contract where it is necessary to do so for the protection of our legitimate interests or those of third parties. Exempels:

- Examination and optimization of requirement analysis procedures for direct customer approaches,
- Advertising or market and opinion research as long as you have not objected to the use of your data for such purpose,
- Asserting legal claims and preparation of defenses in legal disputes,
- Ensuring IT security and general IT operations,
- Measures for maintaining building and system security (e.g. access control),
- Measures to ensure the domiciliary right,
- Measures for the purpose of business management and/or the further development of services and products
- Consultation and data exchange with credit reference agencies for the identification and assessment of credit risks.

F. Disclosure of data

Information about our customers and prospective customers is important to us and helps us to optimise our offering. However, it is not part of our business operations to sell this customer information. Within our company only those entities that need access to such data in order to fulfil contractual and legal obligations are entitled to access sad data.

eventfactory GmbH also permits the foregoing processes and services to be performed by carefully selected and data protection compliant service providers based in the EU or in a third country, depending on their location. These are companies who eventfactory GmbH has selected as a trusted partner who provides any of the following: IT, payment, billing and consultancy services including sales and marketing services as well as service providers, which we use in the context of order processing. With respect to the disclosure of data to other recipients, we shall only disclose information about you if required to do so by law, or where you have consented, or we are authorised to disclose your data. If the conditions are met, recipients of your personal data may be:

- Public bodies and institutions (e.g. tax authorities) where there is a legal or regulatory obligation.
- Other companies or similar entities to which we provide personal information (e.g. hotels, transport companies, restaurants, etc.) in order to progress our business relationship with you.
- Other companies within the Group.

In addition, other entities may become data recipients provided that you have given us your consent to the transmission of your data.

G. Duration of data storage

We shall process and store your personal data for such time as is necessary for the fulfilment of our contractual and legal obligations.

If the data is no longer required for the fulfilment of our contractual or legal obligations such data shall be deleted, unless their temporary processing is necessary for any of the following purposes:

- Fulfilment of business and tax-related obligations which may arise. The periods for storage of such documentation is between two and ten years.
- Preservation of evidence in the context of the statutory statute of limitations**.**

H. Rights of the Person Affected (the Data Subject)

Every person has the right to receive information under Art. 15 GDPR, the right to correct said data under Art. 16 GDPR, the right to remove inaccurate data under Art. 17 GDPR, the right to limit data processing in accordance with Art. 18 GDPR, the right to object to data under Art. 21 GDPR and the right to data portability under Art. 20 GDPR. In addition, there is a right of appeal to a competent data protection supervisory authority (Art. 77 GDPR).

You may revoke your consent to the processing of personal data at any time. This also applies to the revocation of consent forms, which were issued to us before the introduction of the GDPR, i.e. prior to 25th May 2018. Please note that such revocation only applies from the point upon which the revocation has been received and duly processed. Processing that occurred before the revocation is not affected.

I. Obligations of the Person Affect (the Data Subject)

As part of our business relationship, you must provide all personal information necessary to initiate, conduct and terminate a business relationship and to carry out all related contractual obligations, or any other data as we are required to collect by law. Without this data, we will be unable to conclude, execute or terminate a contract with you.

J. Pass an automated decision including profiling

In principle, we do not use automatic decision-making pursuant to Art. 22 of the GDPR to justify and implement the business relationship. If we use these procedures in individual cases, we will inform you about this separately, if this is required by law. We sometimes process your data automatically with the aim of evaluating certain personal aspects (profiling). We use profiling as part of the assessment of your solvency and to improve our sales activities in order to address you more needs and more targeted.

K. Intention to transfer the personal data to a third country or international organisation

An active transfer of personal data to a third country or to an international organisation takes place if necessary in the context of the performance of the contract.

RIGHT TO OBJECT

Information about your right of objection under Article 21 General Data Protection Regulation (GDPR)

1. INDIVIDUAL RIGHT OF CONFLICT

You have the right at any time, for reasons arising out of your particular situation, to prevent the processing of personal data concerning you pursuant to Art. 6 para. 1 lit. e of the GDPR (Data Processing in the Public Interest) and Art. 6 para. 1 lit. f GDPR (Data processing on the basis of a balance of interests) takes place, objecting; this also applies to a profiling based on this provision within the meaning of Art. 4 No. 4 GDPR. If you object, we will no longer process your personal information unless we can establish compelling legitimate grounds for processing that outweigh your interests, rights and freedoms, or the processing is for the purposes of asserting, exercising or defending legal claims.

2. OPPOSITE RIGHT AGAINST PROCESSING OF DATA FOR PURPOSES OF DIRECT ADVERTISING

In individual cases, we process your personal data in order to operate direct mail. You have the right to object at any time to the processing of personal data concerning you for the purposes of such advertising; this also applies to profiling insofar as it is associated with such direct mail.

If you object to the processing for direct marketing purposes, we will no longer process your personal data for these purposes.

The objection can be free of form and should be directed as far as possible to:

Karin Salota

De.datenschutz@liberty-int.com

Technical and Organisational Measures (TOM)

Under the provisions of Art. 32 of the General Data Protection Regulation (GDPR)

The Organisation: eventfactory GmbH

Organisations which collect, process or use personal data, whether on their own behalf or by order of a third party, must implement technical and organisational measures necessary to ensure compliance with the provisions of the data protection regulations. Measures are deemed necessary only to the extent that the cost of their implementation is in appropriate relation to the targeted protection purpose.

The aforementioned organisation meets this requirement with the following measures:

I. Confidentiality

a) Physical Access Control

- Facilities are accessed with a chip card, an access code or by manual access.
- Access to the facilities by guests takes place within office hours and under supervision.
- A list of all people (employees, clients, partners, suppliers) with access to the facilities is being kept („Key List“).
- Diligence in selecting cleaning personnel

b) Data Access Control

- IT systems are in principle accessed only with a valid user name and password.
- Passwords meet the highest security criteria and are regularly changed.
- Passwords are not documented on paper.
- User accounts have no local admin rights. For cases of emergency, a local admin account is in existence, known only to specific people.
- Admin passwords are documented via a web-based password manager online service.
- Administrative access to IT systems is carried out through personalised user accounts, via a multi-factor authentication insofar as supported by the systems.
- The fade-out process of employees is documented and access to facilities and IT systems disabled accordingly.
- A separate guest access exists in addition to an internal Wi-Fi network.
- The Internal Wi-Fi network as well as the guest access is protected with a password.
- The internal network is protected against threats from the Internet via a firewall.
- PCs and laptops are safeguarded by an always up-to-date virus protection.
- PCs and laptops are automatically provided with security relevant updates.
- Monitors of PCs and laptops are automatically locked after 10 minutes.
- Allocation of authorisations is carried out on a personalised level.
- The necessity of authorisations is being strictly verified.

- A concept for the allocation of user authorisations exists.
- Remote access to PCs and laptops is allowed via TeamViewer for maintenance/support purposes.
- Data carriers are encrypted with BitLocker (Windows) or FileVault (Apple) accordingly.
- Provisions are in place for the private use of company devices.
- There are provisions in place for locking the PCs (manual and automatic).
- Mobile devices (smartphones) are protected with a PIN.
- Mobile devices are being locked/disabled after a PIN has been incorrectly entered 5 times.
- There are provisions for the handling of devices (smartphones).
- There are provisions for the orderly handling of documents in the workspace.

c) Safeguard against Unauthorised Access

- Analogue data is stored in lockable cabinets.
- An authorisation /services agreement exists.
- The number of administrators is minimised.
- Authorised people carry out the administration of user rights.
- Extraction/erasure of hard drives prior to professional disposal of all data carriers

d) Data Carrier Control

- Deployed computers are protected with BitLocker for Windows machines and with FileVault for Apple machines respectively.
- The use of external USB sticks on company computers is prohibited.

e) Separation Control

- With completion of the services agreement, all personal data processed in the course of the performance of services will be erased from the systems of the data controller insofar that there are no reasons for further storing the data.
- Separation of productive and test environment

f) Pseudonymisation

- Insofar as possible, datasets will be pseudonymised in the process of data transmission.

II. Integrity

a) Transmission Control

- Transmission of personal data is carried out only over encrypted channels.
- Data recipients as well as intended duration of data storage and deadlines for deletion are all documented.
- Overview of frequent data retrieval and transmission processes
- If possible, transmission takes place in an anonymous or pseudonymised form.
- Personal transmission is only carried out with a protocol.
- For support purposes personal data is transmitted only to the extent to which it is necessary for solving problems. The transmission is carried out via e-mail or on the designated support platform of the affected systems respectively.
- Passwords of clients are not transmitted electronically.

b) Data Entry Control

- Entry, modification and deletion of data will be logged via technical protocol.
- Only authorised personnel carry out the entry, modification or deletion of personal data in the systems.
- Entry, modification or deletion of personal data in the systems is being documented.
- Access to the documentation is reserved for authorised personnel only.
- There are clear rules for the responsibilities with regards to data deletion.

c) User Control

- PCs and laptops are provided with an automatic lock screen that activates itself after 10 minutes.
- Employees lock the computers and laptops in usage when leaving the workspace.
- Deployed smartphones are protected with a PIN.

III. Availability and Resilience – criteria with a Cloud infrastructure

- Computers in usage are equipped with an up-to-date virus protection that is regularly and automatically updated (security updates).
- In case an employee leaves the company or an agreement with a sub-contractor is terminated, access to the systems will be deleted promptly.
- Only Cloud services of renowned manufacturers, i.e. Microsoft, are deployed.
- A concept for backing up and restoring data exists.
- Successful saving of data is controlled.
- An emergency plan exists.
- Data is being saved as follows
    - file data
    - mail data
    - application data
- There are maintenance agreements in place with systems suppliers and/or external IT firms respectively.

IV. Processes for Regular Testing, Assessment and Evaluation

a) Data Protection Management

- Employees are regularly trained in GDPR conform handling of personal data and IT security.
- Employees and sub-contractors respectively are provided with provisions for the handling of personal data.
- Employees are obligated to confidentiality and discretion, confirmed in writing in employee data privacy statements.
- A centralised documentation of all processes and provisions for data protection is available to employees.
- The effectiveness of technical security measures is being reviewed 1 x year.
- There is an internal data protection coordinator.
- The organisation complies with the obligations to inform data subjects according to Art. 13 and 14 of the GDPR.
- There is a specified process in place for handling requests for disclosure from data subjects.

b) Support of the Reaction to Security Violations

- There is a documented process for the detection and notification of security incidents/data breaches, and regarding the obligation to report to the supervisory authority.
- There are documented procedures for handling security incidents.
- Security incidents or data breaches are documented.
- There is a formal process as well as responsibilities for post-processing security incidents or data breaches.

c) Data Protection By Default

- Insofar as supported by the systems, data protection by default will be ensured, for example through a multi-factor authentication for administrative users. Complex passwords and BitLocker encryption will be implemented as well.
- Only relevant personal data is processed to the extent that it is necessary for the respective purpose.

d) Processor Control

- Data processing is carried out under the principles of Art. 28 GDPR and on documented instruction from the controller. Such instructions are either noted in the services agreement, and in individual cases or for specific projects otherwise provided in written form. In the course of regular meetings, the status as well as required measures are being discussed and improvements suggested.
- The organisation exercises its control rights towards suppliers accordingly.
- Established security measures (TOMs) and their documentation are being reviewed.
- Suppliers are selected based on aspects of due diligence.
- Insofar as if necessary, respective agreements have been concluded (Confidentiality, Processor Agreement, EU Standard Contract Clauses).