# Data processing agreement

## Structure

This DPA is structured as follows:

| Section | Content |
|---|---|
| **Section A – Key terms** | The key variables that apply to the DPA are defined in Section A. |
| **Section B – Legal terms** | Sets out the general legal terms applicable to the processing. |
| **Section C – TOMs** | The applicable technical and organizational measures. |

# Section A – Key terms

| Variable | Value |
|---|---|
| **Controller(s)** | The entity or natural person subscribing to BeeTrip's services (hereinafter the “Customer”) |
| **Processor(s)** | BeeTrip, 1 rue de Rossan<br>Contact: Bruno Lapeyre (bruno@beetrip.pro)<br>(together with the Controller(s) the "**Parties**" and each a "**Party**") |
| **Processing Purpose** | Provision of the BeeTrip SaaS platform dedicated to travel agencies for customer relationship management (CRM), administration of booking records, and the centralization of travel projects. |
| **Duration of Processing** | Only as long as necessary for the Processing Purpose |
| **Categories of Data Subjects** | - Customers<br>- Employees<br>- Potential clients |
| **Categories of Personal Data** | - Birthday/age<br>- Contact data (email, phone)<br>- Home address<br>- IP address<br>- Name<br>- Nationality<br>- Passport/ID |
| **Place of storage & processing** | At the business address of the Processor and its approved Sub-processors as indicated in this data processing agreement |
| **On-premise audits** | No |
| **Sub-processors** | Amazon Web Services (AWS): Cloud infrastructure and secure storage. Data location: European Union (Ireland/Frankfurt Region).<br><br>Scaleway: Server hosting and database management. Data location: France (European Union).<br><br>Mailjet (Sinch): Transactional and marketing email services. Data |

| | |
|---|---|
| | location: France / European Union.<br><br>Consolto: Live chat and customer support solution. Data location: Israel (Country benefitting from an EU adequacy decision). |
| **Transfer outside of EU/EEA/Switzerland** | Only allowed to countries where the Processor or an approved Sub-processor is registered |

The variables defined in Section A serve as definitions in Section B and section C.

# Section B – General terms

## 1 Purpose and scope

The purpose of this data processing agreement (the "**DPA**") is to ensure compliance with Article 28(3) and (4) of the EU General Data Protection Regulation ("**GDPR**") and Article 9 of the Swiss Federal Act on Data Protection ("**FADP**"), with respect to each law only if and to the extent applicable to the respective processing activity.

This DPA applies with respect to the processing of personal data as specified in Section A.

## 2 Interpretation

Where this DPA uses the terms defined in the GDPR or the FADP, as applicable, those terms shall have the same meaning as in that law.

This DPA shall be read and interpreted in the light of the provisions of the GDPR and the FADP, as applicable.

These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in the GDPR or the FADP, as applicable, or prejudices the fundamental rights or freedoms of the data subjects.

## 3 Description of processing operations

The details of the processing operations, and in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the Controller, are specified in Section A.

## 4 Obligations of the Parties

### 4.1 General

The Processor shall process personal data only on documented instructions from the Controller, unless required to do so by Union, Member States or Swiss law to which the processor is subject. Such instructions are specified in Section A. In this case, the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the Controller throughout the duration of the processing of personal data. Such instructions shall always be documented.

The Processor shall immediately inform the Controller if instructions given by the Controller, in the opinion of the Processor, infringe applicable Union, Member States or Swiss data protection provisions.

## 4.2 Purpose limitation

The Processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Section A.

## 4.3 Erasure or return of data

Processing by the Processor shall only take place for the duration specified in Section A.

Upon termination of the provision of personal data processing services or termination pursuant to Clause 7, the Processor shall delete all personal data processed on behalf of the Controller and certify to the Controller that it has done so and delete existing copies unless Union, Member States or Swiss law requires storage of the personal data.

## 4.4 Security of processing

The Processor shall implement the technical and organizational measures specified in Section C to ensure the security of the personal data, including protection against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (personal data breach), in accordance with Article 5, Article 28(3)(c) and Article 32 GDPR and Article 8 FADP. In assessing the appropriate level of security, they shall in particular take due account of the risks involved in the processing, the nature of the personal data and the nature, scope, context and purposes of processing.

In the event of a personal data breach concerning data processed by the Processor, it shall notify the Controller without undue delay and at the latest within 48 hours after having become aware of the breach. Such notification shall contain the details of a contact point where more information concerning the personal data breach can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and data records concerned), its likely consequences and the measures taken or proposed to be taken to mitigate its possible adverse effects. Where, and insofar as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall be provided as it becomes available without undue delay.

The Processor shall cooperate in good faith with and assist the Controller in any way necessary to enable the Controller to notify, where relevant, the competent data protection authority and the affected data subjects, taking into account the nature of processing and the information available to the Processor.

The Processor shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. The Processor shall ensure that persons authorized to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (special categories of data), the Processor shall apply specific restrictions and/or additional safeguards as reasonably required by the Controller.

## 4.5 Documentation and compliance

The Parties shall be able to demonstrate compliance with this DPA.

The Processor shall deal promptly and properly with all reasonable inquiries from the Controller that relate to the processing under this DPA.

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations set out in this DPA and that are stemming directly from the GDPR or the FADP and at the Controller's request, allow for and contribute to reviews of data files and documentation or of audits of the processing activities covered by these Clauses, in particular if there are indications of non-compliance.

The Controller may choose to conduct the audit by itself, to mandate, at its own cost, an independent auditor or to rely on an independent audit mandated by the Processor. Where the Processor mandates an audit, it has to bear the costs of the independent auditor. The Controller's audit, access, and inspection rights under this Clause are limited to the Processor's records only (including inter-alia the registers of personal data processing activities, the registers of recipients of personal data) and does not apply to Processor's physical premises. Any audit and request for information shall be limited to information necessary for the purposes of this DPA and shall give due regard to the Processor's confidentiality obligations and legitimate interest to protect business secrets.

The Processor and Controller shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority on request if and to the extent required by the GDPR or the FADP, as applicable.

## 4.6 Use of Sub-processors

The Processor has the Controller's general authorization for the engagement of Sub-processors. The list of Sub-processors of the Processor can be found in Section A. The Processor shall inform in text form the Controller of any intended changes to that list through the addition or replacement of Sub-processors at least 30 days in advance, thereby giving the Controller the opportunity to object to such changes prior to the engagement of the concerned Sub-processors. Such objection shall not be unreasonably raised. The Parties shall keep the list up to date.

Where the Processor engages a Sub-processor for carrying out specific processing activities (on behalf of the Controller), it shall do so by way of a contract which imposes on the Sub-processor the same obligations as the ones imposed on the Processor under this DPA. The Processor shall ensure that the Sub-processor complies with the obligations to which the Processor is subject pursuant to this DPA, Article 28(2) to (4) GDPR and Article 9(3) FADP.

The Processor shall provide, at the Controller's request, a copy of such a Sub-processor agreement and subsequent amendments to the Controller.

The Processor shall remain fully responsible to the Controller for the performance of the Sub-processor's obligations under its contract with the Processor. The Processor shall notify the Controller of any failure by the Sub-processor to fulfil its obligations under that contract.

### 4.7 International transfers

Any transfer of data to a country outside of the EU/EEA and Switzerland (a "**Third Country**") or an international organization by the Processor shall be undertaken only if authorized in accordance with Section A and shall take place in compliance with Chapter V of the GDPR and Articles 16 to 18 of the FADP, as applicable.

The Controller agrees that where the Processor engages a Sub-processor in accordance with Clause 4.6 for carrying out specific processing activities on behalf of the Controller in a Third Country and those processing activities involve transfer of personal data within the meaning of the GDPR or the FADP, as applicable, the Processor and the Sub-processor may use standard contractual clauses adopted by the Commission on the basis of Article 46(2) GDPR in order to comply with the requirements of Chapter V of the GDPR, provided the conditions for the use of those clauses are met and provided that an internal assessment concluded that such transfer meets the level of data protection of the GDPR and the FADP.

## 5 Data subject rights

The Processor shall promptly notify the Controller about any request received directly from the data subject. It shall not respond to that request itself, unless and until it has been authorized to do so by the Controller.

The Processor shall assist the Controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights in accordance with Chapter III of the GDPR and Chapter 4 of the FADP, namely:

- the right to be informed when personal data are collected from the data subject;
- the right to be informed when personal data have not been obtained from the data subject;
- the right of access by the data subject;

- the right to rectification;
- the right to erasure ('the right to be forgotten');
- the right to restriction of processing;
- the notification obligation of rectification or erasure of personal data or restriction of processing;
- the right to data portability;
- the right to object;
- the right not to be subject to a decision based solely on automated processing, including profiling; and
- the right to withdraw consent.

The Processor shall assist the Controller in case a data subject has lodged a complaint to the competent supervisory authority that concerns data processed on the basis of this DPA.

In addition to the Processor's obligation to assist the Controller pursuant to Clause 50, the Processor shall furthermore assist the Controller in ensuring compliance with the following obligations, taking into account the nature of the processing and the information available to the Processor:

- The obligation to notify a personal data breach to the competent supervisory authority without undue delay after having become aware of it, (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons), in accordance with Article 33 GDPR and Article 24(1) to (3) FADP;
- the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, in accordance with Article 34 GDPR and Article 24(4) FADP;
- the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, in accordance with Article 35 GDPR and Article 22 FADP;
- the obligation to consult the competent supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk, in accordance with Article 36 GDPR and Article 23 FADP.

The Parties shall set out in Section C the appropriate technical and organizational measures by which the Processor is required to assist the Controller in the application of this Clause as well as the scope and the extent of the assistance required.

## 6 Notification of personal data breaches

In the event of a personal data breach, the Processor shall cooperate in good faith with and assist the Controller in any way necessary for the Controller to comply with its obligations under Articles 33 and 34 of the GDPR and Article 24 of the FADP, as applicable, taking into account the nature of processing and the information available to the Processor.

The Processor shall assist the Controller in notifying the personal data breach to the competent supervisory authority, where relevant. The Processor shall be required to assist in obtaining in particular the following information which, pursuant to Article 33(3) GDPR or Article 24(2) FADP, as applicable, shall be stated in the Controller's notification:

- The nature of the personal data including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
- the likely consequences of the personal data breach;
- the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

## 7 Termination

Without prejudice to any provisions of the GDPR or the FADP, as applicable, in the event that the Processor is in breach of its obligations under this DPA, the Controller may instruct the Processor to temporarily suspend the processing of personal data until the latter complies with this DPA or the contract is terminated. The Processor shall promptly inform the Controller in case it is unable to comply with this DPA, for whatever reason.

The Controller may terminate this DPA where:

- the processing of personal data by the Processor has been temporarily suspended by the Controller pursuant to point (a), Processor's breach is material, and compliance with this DPA is not restored within a reasonable time and in any event within one month;
- the Processor is in substantial or persistent breach of this DPA or its obligations under the GDPR or the FADP, as applicable, and such breach cannot be reasonably expected to be remedied;
- the Processor fails to comply with a binding decision of a competent court or the competent supervisory authority regarding its obligations under this DPA or under the GDPR or the FADP, as applicable.

# 8 Miscellaneous

**Confidentiality:** The Parties agree to keep the terms and existence of this Agreement as well as any information exchanged under this Agreement confidential unless agreed otherwise between the Parties.

**Entire agreement:** This DPA is the entire agreement, and supersedes all prior agreements, between the Parties relating to the scope of this DPA.

**Amendments:** All amendments and supplements to this DPA must be made in writing (incl. non-qualified e-signature solutions).

**Notices:** Any notice 'in writing' needs to be delivered with physical mail, any notice 'in text form' includes any electronic message, each to the last communicated or available address. If the form is not stated, text form is sufficient.

**No assignment:** Neither Party may assign any of its rights, obligations or claims under this Agreement unless agreed otherwise.

**Severability:** If any provision of this DPA (in whole or part) is held to be illegal, invalid or otherwise unenforceable, the other provisions will remain mutatis mutandis in full force and effect.

**Governing law & jurisdiction:** As per the Base Agreement.

# Section C – TOMs

Description of the technical and organizational security measures implemented by the Processor(s):

## 1 Organizational security measures

### 1.1 Security management

Security policy and procedures: The Processor has a documented security policy with regard to the processing of personal data.

**Roles and responsibilities :**

- Roles and responsibilities related to the processing of personal data is clearly defined and allocated in accordance with the security policy.
- During internal re-organizations or terminations and change of employment, revocation of rights and responsibilities with respective hand-over procedures is clearly defined.

**Access Control Policy:** Specific access control rights are allocated to each role involved in the processing of personal data, following the need-to-know principle.

**Resource/asset management:** The Processor has a register of the IT resources used for the processing of personal data (hardware, software, and network). A specific person is assigned the task of maintaining and updating the register (e.g. IT officer).

**Change management:** The Processor makes sure that all changes to the IT system are registered and monitored by a specific person (e.g. IT or security officer). Regular monitoring of this process takes place.

### 1.2 Incident response and business continuity

**Incidents handling / Personal data breaches:**

- An incident response plan with detailed procedures is defined to ensure effective and orderly response to incidents pertaining personal data.
- The Processor will report without undue delay to the controller any security incident that has resulted in a loss, misuse or unauthorized acquisition of any personal data.

**Business continuity:** The Processor has established the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system processing personal data (in the event of an incident/personal data breach).

### 1.3 Human resources

**Confidentiality of personnel:** The Processor ensures that all employees understand their responsibilities and obligations related to the processing of personal data. Roles and responsibilities are clearly communicated during the pre-employment and/or induction process.

**Training:** The Processor ensures that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the processing of personal data are also properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.

## 2 Technical security measures

### 2.1 Access control and authentication

An access control system applicable to all users accessing the IT system is implemented. The system allows creating, approving, reviewing, and deleting user accounts.

The use of common user accounts is avoided. In cases where this is necessary, it is ensured that all users of the common account have the same roles and responsibilities.

When granting access or assigning user roles, the 'need-to-know principle' shall be observed in order to limit the number of users having access to personal data only to those who require it for achieving the Processor's processing purposes.

Where authentication mechanisms are based on passwords, the Processor requires the password to be at least eight characters long and conform to very strong password control parameters including length, character complexity, and non-repeatability.

The authentication credentials (such as user ID and password) shall never be transmitted unprotected over the network.

### 2.2 Logging and monitoring

Infrastructure-level logging is maintained by the hosting providers (AWS and Scaleway) for security monitoring and server authentication purposes.

### 2.3 Security of data at rest

**Server/Database security:**

- Database and applications servers are configured to run using a separate account, with minimum OS privileges to function correctly.

- Database and applications servers only process the personal data that are actually needed to process in order to achieve its processing purposes.

**Workstation security:**

- Users are not able to deactivate or bypass security settings.
- Anti-virus applications and detection signatures is configured on a regular basis.
- Users don't have privileges to install or deactivate unauthorized software applications.
- The system has session time-outs when the user has not been active for a certain time period.
- Critical security updates released by the operating system developer is installed regularly.

## 2.4 Network/Communication security

Whenever access is performed through the Internet, communication is encrypted through cryptographic protocols.

Traffic to and from the IT system is monitored and controlled through firewalls and intrusion detection systems.

## 2.5 Back-ups

Backup and data restore procedures are defined, documented, and clearly linked to roles and responsibilities.

Backups are given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.

Execution of backups is monitored to ensure completeness.

## 2.6 Mobile/Portable devices

Mobile and portable device management procedures are defined and documented establishing clear rules for their proper use.

Mobile devices that are allowed to access the information system are pre-registered and pre-authorized.

## 2.7 Application lifecycle security

During the development lifecycle, best practice, state of the art and well acknowledged secure development practices or standards are followed.

## 2.8 Data deletion/disposal

Software-based overwriting will be performed on media prior to their disposal. In cases where this is not possible (CDs, DVDs, etc.) physical destruction will be performed.

Shredding of paper and portable media used to store personal data is carried out.

## 2.9 Physical security

The physical perimeter of the IT system infrastructure is not accessible by non-authorized personnel. Appropriate technical measures (e.g. intrusion detection system, chip-card operated turnstile, single-person security entry system, locking system) or organizational measures (e.g. security guard) shall be set in place to protect security areas and their access points against entry by unauthorized persons.