
# Raptim Humanitarian Travel

# Data Processor

## Data Processing Agreement

# Data Processing Agreement

This Data Processing Agreement applies to all forms of personal data which are being processed by **Raptim Nederland B.V.**, a legal entity in accordance with Dutch public law organised and existing pursuant to the laws of The Netherlands and having its principle office at Tilburg (The Netherlands) (hereinafter referred to as "**Data Processor**"), on behalf of customer (hereinafter referred to as "**Data Controller**") to whom the travelling services are delivered by Data Processor.

Data Controller and Data Processor, each a "**Party**" and together referred to as the **"Parties"**.

**CONSIDERATIONS**

**A.** Data Controller has access to the personal data of various travellers (hereinafter: 'Data subjects');
**B.** Data Controller wants Data Processor to execute certain types of processing in accordance with the Agreement.

## 1. DEFINITIONS

The following terms as used in this Data Processing Agreement shall, unless the context clearly indicates to the contrary, have the meanings set forth in this Clause:

| | |
|---|---|
| "**Agreement**" | means the Data Processing Agreement, including any changes thereto and any further agreement agreed to between the Parties that refers to this Data Processing Agreement; |
| "**Applicable Data Protection Law**" | means all data protection laws applicable to the Processing (including transfer) and use of Personal Data in the context of activities carried out pursuant to the Agreement, including the GDPR and the Swiss Federal Act on Data Protection (FADP); |
| **"Data Processing Agreement"** | means the present data processing agreement including the annexes hereto; |
| **"FADP"** | means the Swiss Federal Act on Data Protection of 19 June 1992; |
| **"GDPR"** | means the General Data Protection Regulation (EU) 2016/679 |
| "**Personal Data**" | means any information relating to an identified or identifiable natural person ("**Data Subject**"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity that will be processed by the Data Processor in the context of the Agreement as set out in **Annex 1**; |

| | |
|---|---|
| "**Processing" or "Process**" | means any operation or set of operations which is performed on Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction; |
| "**Security Breach**" | means any breach of security leading to or that may have led to accidental or unlawful destruction, loss, alteration, compromise, disclosure of, or access to Personal Data, stored, transmitted or otherwise processed in the context of the Agreement; |
| "**Sensitive Personal Data**" | means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person and data concerning health or sex life or sexual orientation; |
| "**Sub Processor**" | means any processor, as defined in the GDPR and the FADP, engaged by the Data Processor who agrees to Process Personal Data on behalf of the Data Controller; |
| "**Technical and Organizational Measures**" | means the technical and organizational measures as defined in the GDPR and the FADP. |

## 2. OBLIGATIONS OF THE PARTIES

2.1. The Data Processor will:

a. process Personal Data on behalf of the Data Controller, and for fulfilment of the Agreement, as set out in **Annex 1**;

b. not Process any Personal Data other than in accordance with the Data Controller's instructions;

c. only store the Personal Data for as long as this is necessary for performance of the Agreement and as the Data Controller requires and correct, anonymize, block or delete the relevant Personal Data at the Data Controller's reasonable instructions. In case it is not possible for the Data Processor to follow up any of these instructions, for example because of technical limitations or requirements of third parties for fulfilment of the Agreement, the Data Processor will inform Data Controller thereof as soon as possible;

d. ensure that the only persons able to process or access any particular Personal Data in Data Processor's or Sub Processor's possession, custody or control in the performance of the Agreement are the Data Processor's or Sub Processor's employees who need to process or access such Personal Data in order to carry out their duties in connection with the Agreement;

e. taking into account the nature of the processing, assist the Data Controller by appropriate Technical and Organizational Measures, insofar as this is possible and reasonable, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the Data Subject's rights laid down in Chapter III of the GDPR, for which the Data Processor may charge reasonable costs; and

f. process Personal Data in compliance with the Applicable Data Protection Law.

2.2. The Data Controller will:

a. be responsible for other Processing of Personal Data, including but not limited to, its collection of Personal Data, Processing for purposes that are not reported to the Data Processor, and Processing by third parties and/or for any other purposes.

b. represent and warrant that it has a legal basis to Process the relevant Personal Data, and has notified any supervisory authority of its processing activities, including in particular the processing activities performed by the Processor for the Data Controller under the present Agreement, to the extent required under Applicable Data Protection Law. Furthermore, the Data Controller will represent and warrant that the content is not unlawful and does not infringe any rights of a third party. In this context, the Data Controller will indemnify the Data Processor of all claims and actions of third parties related to the Processing of Personal Data under this Data Processing Agreement.

## 3. TECHNICAL AND ORGANIZATIONAL MEASURES

3.1. The Data Processor will:

a. adopt and maintain Technical and Organizational Measures as set out in **Annex 2**; and

b. take into account the nature of the processing as well as with all the means at its disposal and as far as this is reasonable provide the Data Controller assistance in ensuring compliance with regard to the obligations arising from articles 32 up to and including 35 of the GDPR when applicable and from articles 4 up to and including 15 of the FADP. The Data Processor may charge reasonable costs for this assistance.

3.2. The Data Processor shall take Technical and Organizational Measures that are appropriate, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of persons. In this regard the Data Processor has taken the security measures as described in **Annex 2**.

## 4. TRANSFER OF PERSONAL DATA

4.1. The Data Processor is allowed to Process the Personal Data within Switzerland and within the European Economic Area (**"EEA"**). In addition, the Data Controller hereby grants the Data Processor permission to Process the Personal Data outside Switzerland and the EEA in compliance with the Applicable Data Protection Law.

4.2. In case Personal Data is transferred to a Sub Processor located in a country outside the EEA and Switzerland and there are no European Commission (**"EC"**) Model Clauses available that regulates the transfer between two processors, the Data Controller instructs and authorizes the

Data Processor to instruct the Sub Processor in Data Controller's name and vis-à-vis the Sub Processor's to conclude EC Model Clauses.

## 5. AUDITS

5.1. The Data Controller is at any given moment entitled to audit Data Processor's compliance with this Data Processing Agreement and more specific with respect to the Technical and Organizational Measures by an independent third party who shall be bound to confidentiality. The audit will no earlier be undertaken than two (2) weeks after the Data Controller has provided written notice to the Data Processor. Thereby, any such audit will follow the Data Processor's reasonable security requirements, and will not interfere unreasonably with the Data Processor's business activities.

5.2. The Data Processor shall provide the Data Controller and its certified independent auditor, which does not provide competing services to the Data Processor, with all reasonable cooperation, access to its Processing facilities and assistance in relation to each audit.

5.3. The costs of the audit will be borne by the Data Controller. In the event that it appears that the Data Processor breaches the Data Processing Agreement, the costs of the audit will be borne by the Data Processor.

5.4. The findings in respect of the performed audit will be discussed and evaluated by the Parties and, where applicable, implemented by one of the Parties or by both Parties jointly.

## 6. USE OF SUB PROCESSORS

6.1. The Data Controller, hereby, grants the Data Processor its approval to engage Sub Contractors for the Processing of Personal Data for fulfilment of the Agreement, considering the Applicable Data Protection Law. The Data Processor may not engage a Sub Processor, unless the Data Processor:

a. enters into sub processing agreements with the relevant Sub Processors, requiring the Sub Processor to abide by the same obligations as the Data Processor under this Data Processing Agreement.

6.2. In relation to the Data Controller, the Data Processor is fully responsible for the fulfilling of the obligations of the Data Processing Agreement between the Data Processor and the Sub Processor(s), subject to clause 8 below.

6.3. The Data Controller retains the right to object, based on reasonable grounds, to any Sub Processor engaged by Data Processor. As a result, the Data Processor might no longer be able to offer its services to the Data Controller.

## 7. CONFIDENTIALLITY

7.1. The Data Processor keeps all Personal Data strictly confidential [in accordance with the Agreement] and ensures, prior to the disclosure of Personal Data to its employees, subcontractors or employees of subcontractors, that these persons are bound by the same conditions of confidentiality.

7.2. This duty of confidentiality will not apply in the event that the Data Controller (i) has expressly authorised the furnishing of such information to third parties, (ii) where the furnishing of the information to third parties is reasonably necessary with a view on the nature of the instructions and the implementation of this Data Processing Agreement, or (iii) if there is a legal obligation to make the information available to a third party.

7.3. In addition, the commitments set forth in Clause 7.1 above do not apply to Personal Data that the Data Processor is able to prove:

- already was in the Data Processor's possession, without any limitation regarding its disclosure at the time it was transmitted to the Data Processor; or
- was obtained in good faith and without any commitment relating to confidentiality from a third party entitled to disclose it; or
- has to be disclosed to comply with the applicable law or with a court order or the decision of a competent authority. In such case, the Data Processor shall first inform the Data Controller of its obligation to disclose such Personal Data.

7.4. The obligation of confidentiality shall also apply after termination of this Data Processing Agreement.

## 8. LIABILITY

8.1. The Data Processor is liable for (i) damages; and (ii) fines imposed by regulators, which directly arise from intentional misconduct or wilful recklessness, or an attributable breach of the Agreement by the Data Processor. This liability is limited in relation to a single event (a series of events is registered as one event). In no event, the total compensation for direct damages will be more than the fee paid by the Data Controller to the Data Processor to book travels of Data Subjects over the last six (6) months. This limitation will not apply in the event damage was a direct consequence of wilful intent or gross negligence.

8.2. A notice of default will be served in writing by the Data Controller, and the Data Processor will be given a reasonable period in which to meet its obligations. The notice of default shall describe the attributable breach of the Agreement in full, allowing the Data Processor to fulfil its obligations adequately.

8.3. Any explicit notification by the Data Controller to the Data Processor of a claim for damages which is insufficiently specified to allow the Data Processor to fulfil its obligations adequately will lapse twelve (12) months from the time of the event giving rise to liability.

8.4. The Data Processor shall ensure that it has in force and maintain the following insurances: general liability insurance, professional liability insurance and crime insurance (including coverage for employee fraud).

## 9. NOTIFICATION

9.1. As part of the obligations incumbent on the Data Processor with regard to the security of personal data, the Data Processor shall establish and maintain procedures designed to

reasonably detect Data Breaches and then implement the correct measures, including recovery measures.

9.2. The Data Processor will promptly, and in any case within 48 hours after discovery, notify the Data Controller, as set out in Clause 9.3, about a Data Breach, after which the Data Controller shall determine whether or not to inform the relevant regulatory authority(ies) and/or the Data Subjects. The Data Controller is responsible for fulfilment of any legal notification obligations.

9.3. The Data Processor will notify Data Controller of an event as set out in Clause 9.2, and shall provide the Data Controller, for as far as known by the Data Processor, with the following information:

a. the time, date and location of such event;

b. a detailed account of such event, including a characterization of affected and potentially affected Personal Data;

c. the likely consequences of such event, including the consequences for the Data Subject;

d. the expected recovery time;

e. measures taken or to be taken to mitigate the consequences of the Security Breach; and

f. any other information requested by the Data Controller in order to notify the Security Breach in compliance with the Applicable Data Protection Law.

9.4. The Data Processor will subsequently keep the Data Controller fully informed about any progress of the recovery or other relevant developments with respect to the Data Breach.

9.5. The Data Processor will promptly, without undue delay, take all reasonable measures to recover and/or mitigate the consequences of the Data Breach. The Data Processor is required to inform the Data Controller of these measures.

## 10. REQUESTS BY DATA SUBJECTS

10.1. The Data Processor will provide all reasonable assistance to ensure that the Data Controller is able to fulfil its legal obligations when a Data Subject exercises his or her rights under the Applicable Data Protection Law.

10.2. As soon as the Data Processor receives a request as mentioned in paragraph 10.1, the Data Processer shall promptly inform the Data Controller and forward this request to the Data Controller. The Data Controller will then deal with this request. The Data Processor shall not respond to the request without the consent of the Data Controller, unless Applicable Data Protection Law specifically would specifically require otherwise.

10.3. On the instruction of the Data Controller, the Data Processor shall, without undue delay, correct, erase or otherwise adjust or process the Personal Data.

## 11. TERM AND TERMINATION

11.1. This Data Processing Agreement is concluded on the moment the Parties signed the same and is effective until termination of the agreement referring to this Data Processing Agreement.

11.2. Parties agree that on the day of termination of this Data Processing Agreement, the Data Processor shall, at the choice of the Data Processor return or destroy all Personal Data and the copies thereof, by means of the Data Controllers choice, to the Data Controller or a third party designated by the Data Controller. The Data Processor may charge reasonable costs for return of the Personal Data. The obligations of the Parties under this Data Processing Agreement will remain in force until the Processor has returned or destroyed all Personal Data.

11.3. On request of the Data Controller, the Data Processor will confirm to the Data Controller in writing that it has destroyed the Personal Data.

## 12. MISCELLANEOUS

12.1. This Data Processing Agreement shall be governed by, and construed in accordance with, the laws of Switzerland.

12.2. No term of this Data Processing Agreement shall be amended or modified, unless such amendments or modifications are made in writing with express reference to this Data Processing Agreement and signed by both Parties.

12.3. Both Parties shall provide their full cooperation for modification of this Data Processing Agreement for the purpose of compliance with the Applicable Data Protection Law.

## Annex 1

## *DESCRIPTION OF PROCESSING OPERATIONS*

**Categories of personal data**

The Personal Data transferred concern the following categories of data:

- names;
- addresses;
- e-mail addresses;
- phone numbers;
- date of births;
- gender;
- citizenship;
- payment information (i.e. credit card information and bank account numbers);
- passport number;
- passport expiration date;
- issuing country of passport;
- place of birth.

**Categories of Data Subjects**

The Personal Data relates to the following categories of Data Subjects:

- Employees of Data Controller (end travellers);

**Annex 2**

***DESCRIPTION OF TECHNICAL AND ORGANIZATIONAL MEASURES***

This Annex describes the technical and organizational security measures and procedures that the Data Processor shall maintain to protect the security of Personal Data. The Data Processor has taken the following security measures:

- Firewalls;
- No acceptance of credit cards via e-mail in North America;
- Encryption of any credit card data;
- Logical access control using passwords;
- Organizational and physical measures for access security;
- Security of network connections via Secure Socket Layer (SSL) or Transport Layer Security (TLS) technology.