Raptim Humanitarian Travel

Data Processor

Binding Corporate Rules Customer Data

Content

Purpose and scope 3
Definitions 3
Articles 4
1. Notifying body, DPO and DPA 4
2. Description of the data flows and the purposes of Customer Data Processing 4
3. Binding nature of the BCR within Raptim 5
4. Binding nature of the BCR between the Data Controller and Data Processor 5
5. BCR Principles 5
6. National data protection legislation and the BCR 7
7. Publication duty 8
8. Cooperation duty 8
9. Data Protection Officer (DPO) 8
10. Training 8
11. Audits 9
12. Rights of the Data Subject 9
13. Complaint Procedures for the Data Subject 10
14. Third-Party Beneficiary Rights and liability 10
15. Mechanisms for reporting and recording changes 11
16. Governing national law 12
17. Entry into Force 12
APPENDIX 1: Raptim Entities 13
APPENDIX 2: Sub-Processors 14
APPENDIX 3: Overview of the Customer Data 15
APPENDIX 4: Role and tasks of the DPO 16

Purpose and scope

The headquarters of Raptim Humanitarian Travel are located within the EEA, namely Raptim Nederland B.V., having its registered office at Spoorlaan 306, 5038 CC Tilburg, The Netherlands, registered at the Dutch Chamber of Commerce (number 18011996). Raptim Humanitarian Travel has different entities within and outside the European Economic Area (EEA). Uniform and appropriate data protection standards need to be established regarding the Processing of Customer Data between these different entities. Therefore, these Binding Corporate Rules (BCR) have been drafted.

The BCR applies to the Processing of Customer Data by the different Raptim entities, in their role as Data Processors, within and outside the EEA, if the processing of such Customer Data is subject to EU law (for example, when it has been transferred from the EU). The Processing of Customer Data collected outside of the EEA by Raptim Entities outside of the EEA is carried out on the basis of the applicable national data protection law.

The BCR are aimed at creating an adequate level of data protection and provide for adequate data protection safeguards within the meaning of Articles 46 and 47 of the European Union Regulation 2016/679 of 27 April 2016 (the General Data Protection Regulation).

Definitions

In line with European Union Regulation 2016/679, the following definitions (both in plural and in singular) apply to the BCR:

1. **Appendix**: any annex attached to these BCR.
2. **Autoriteit Persoonsgegevens:** the Dutch Data Protection Authority, having its registered office at Bezuidenhoutseweg 30, 2594 AV The Hague (The Netherlands), registered at the Dutch Chamber of Commerce (number 27380834).
3. **Binding Corporate Rules (BCR)**: this document, which has been drafted to regulate the transfer of Customer Data within Raptim.
4. **Customer**: the organization making use of the Services of Raptim, in order to book travel, and (offer) related Services for the Data Subject.
5. **Customer Data**: any Personal Data of the Data Subject provided to Raptim by the Customer, in the course of the provision of Services to the Data Subject.
6. **Data Controller**: a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Customer Data.
7. **Data Processing Agreement**: the agreement concluded between the Data Controller and the Data Processor according to Article 28, section 3 of European Union Regulation 2016/679.
8. **Data Processor**: a natural or legal person, public authority, agency or other body which processes Customer Data on behalf of the Data Controller.
9. **Data Protection Authority (DPA)**: any independent public authority which has been established by a Member State of the European Union pursuant to Article 51 European Union Regulation 2016/679.
10. **Data Protection Officer (DPO)**: the person responsible for privacy issues (e.g. the monitoring, coordination, implementation and maintenance of the BCR) within Raptim and the first point of contact for the Data Protection Authorities.
11. **Data Subject:** an identified or identifiable natural person who uses the Services of Raptim via the Data Controller. An identifiable natural person is one who can be identified, directly or indirectly, in particular or by reference to an identifier such as a name, an identification

number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

12. **Data Sub-Processor**: a natural or legal person, public authority, agency or other body which processes Customer Data on behalf of the Data Processor, and ultimately on behalf of the Data Controller.
13. **Employee:** an identified or identifiable person who is currently employed by one of Raptim Entities.
14. **Personal Data**: any information relating to an identified or identifiable natural person as listed in Appendix 3.
15. **Processing**: any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
16. **Raptim Headquarters:** Raptim Nederland B.V., having its registered office at Spoorlaan 306, 5038 CC Tilburg, The Netherlands, registered at the Dutch Chamber of Commerce (number 18011996).
17. **Raptim:** all the Raptim Entities within Raptim Humanitarian Travel.
18. **Raptim Entities**: the entities within Raptim as enlisted in Appendix 1.
19. **Special categories of Personal Data**: Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data and biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
20. **Service Agreement**: the agreement concluded between the Data Controller and Data Processor regarding the use of the Services of Raptim for the Data Subjects.
21. **Services**: the humanitarian travel services offered by Raptim including but not limited to 24/7 emergency services, car rental, financial services, flight tickets, arranging group travel, hotel reservations, tickets for international ferry's, visa applications, consultation on passport and transit visas requirements, track & trace, technology solutions and travel insurance.

Articles

1. Notifying body, DPO and DPA

1.1 The notifying body of these BCR are the Raptim Headquarters. The Raptim Headquarters will adopt the BCR and will implement the BCR throughout Raptim.

1.2 The DPO is the first point of contact within Raptim for all questions concerning the BCR. Please send your questions to Privacy@raptim.org

1.3 The competent Data Protection Authority for these BCR and the first point of contact for all questions concerning the BCR is the Autoriteit Persoonsgegevens.

2. Description of the data flows and the purposes of Customer Data Processing

2.1 The BCR applies to all the different processes within the Services offered by Raptim in the course of which it may be necessary to transfer Customer Data between Raptim Entities.

2.2 The transfer of Customer Data may, additionally, *inter alia* be necessary for cross-border collaboration between Raptim Entities, fulfillment of any legal obligations and in order to

ensure the safety and other legitimate interests of the Customers, the Data Subjects as well as of the Raptim Entities.

3. Binding nature of the BCR within Raptim

3.1 The BCR shall apply to all Raptim Entities, including its entities in the EEA, North America, Switzerland and Africa.

3.2 All Raptim Entities and their Employees shall respect these BCR, the instructions regarding the Processing of Customer Data and the security and confidentiality measures as provided in the Service Agreement and/or Data Processing Agreement concluded between the Data Controller and the Data Processor.

3.3 Raptim shall adopt the BCR by way of formal training, labor contracts, policies and declarations which are binding upon the employees within the Raptim Entities and must be implemented and complied with.

3.4 The Raptim Entities shall provide appropriate measures for the implementation and enforcement of the BCR and ensure adherence by their Employees. The Employees are obliged to comply with the BCR and are informed about this, e.g. in the employment contract and via the Employee Computer Usage Policy. Any breach of the BCR by an Employee may give rise to disciplinary actions under employment law, including termination of employment.

4. Binding nature of the BCR between the Data Controller and Data Processor

4.1 The Data Controller and Data Processor will ensure that the BCR is part of the Service Agreement and/or Data Processing Agreement, or a reference will be made to it with a possibility of electronic access.

4.2 It is up to the Data Controller to apply the BCR to all Customer Data Processed for Processing activities that fall within the scope of the Service Agreement and/or Data Processing Agreement and to inform the Data Subjects about the BCR.

5. BCR Principles

5.1 The following principles shall apply to all members of the BCR:

Legal basis: Customer Data, including Sensitive Personal Data, shall only be Processed when there is a valid legal basis for this, such as permission, an agreement to which the Data Subject is a party, or legitimate interests of the Controller that outweigh the Data Subject's privacy interests. The Data Controller is responsible for this legal basis, including a valid legal basis for Processing Sensitive Personal Data.

Transparency and fairness: Data Processors and Data Sub-Processors shall help and assist the Data Controller to comply with the law (for instance, by being transparent about Data Sub-Processor activities in order to allow the Data Controller to correctly inform the Data Subject).

Purpose limitation: Customer Data shall only be processed on behalf of the Data Controller and in compliance with its instructions. If a Data Processor or Data Sub-Processor cannot provide such compliance for whatever reasons, it shall promptly inform the Data Controller of its inability to comply, in which case the Data Controller is entitled to suspend the transfer

of data and/or terminate the Service Agreement and Data Processing Agreement. Upon the termination of the provision of Data Processing Agreement, the Data Processors and Data Sub-Processors shall, at the choice of the Data Controller, return all the Customer Data transferred and copies thereof to the Data Controller, or destroy all the Customer Data and certify to the Data Controller that they have done so, unless legislation imposed upon them prevents it from returning or destroying all or part of the Customer Data transferred. In that case, the Data Processors and the Data Sub-Processors will inform the Data Controller and warrant that they will guarantee the confidentiality of the Customer Data transferred and will not actively process the Customer Data transferred anymore.

Data minimization: Processing shall cover as little Customer Data as necessary for the purposes of Processing. Data Subjects shall not be asked to provide Customer Data which is unnecessary for the purposes of Processing. The Data Controller is responsible for this.

Data retention: Customer Data shall not be retained longer than necessary for the purposes of the Processing, unless there is a legal requirement to do so. The Data Controller is responsible for this, but the Data Processor and Data Sub-Processor shall assist by deleting or returning the data in a timely manner, as specified in the Service Agreement or Data Processing Agreement.

Privacy by design and by default: when designing a new product, service, project or process, this should infringe privacy as little as possible. The default settings of a service should be as privacy-friendly as possible, for example by making Customer Data available to a limited number of users. The Data Controller is responsible for this.

Data quality: Data Processors and Data Sub-Processors shall help and assist the Data Controller to comply with the law, in particular:

Data Processors and Data Sub-Processors will execute any necessary and reasonable measures when asked by the Data Controller, in order to have the Customer Data updated, corrected or deleted. Data Processor and Data Sub-Processors will inform each party and/or entity to whom the Customer Data has been disclosed of any rectification or deletion of the Customer Data.

On request of the Data Controller and from the moment the possibility of identification of the Data Subject is no longer required, Data Processors and Data Sub-Processors will execute any necessary and reasonable measures in order to delete or anonymize the personal data. The Data Processor and Data Sub-Processors will communicate to each entity and/or party to whom the Customer Data has been disclosed of any deletion or anonymization of the Customer Data.

Security: Data Processors and Data Sub-Processors must comply with security and organizational measures which at least meet the requirements of the European Union Regulation 2016/679 and any existing particular measures specified in the Service Agreement and/or Data Processing Agreement. Data Processors and Data Sub-Processors shall inform the Data Controller of any security breach regarding Customer Data as soon as possible. Raptim offers the following security measures:

- Firewalls are used;

- Logical access control using passwords and/or two-factor authentication;
- Organizational and physical measures in place for access security;
- Credit card is not accepted via e-mail in North America;
- Any credit card data stored on Raptim databases is encrypted;
- Employees are, via the Computer Usage Policy, bound to a duty of confidentiality, covering also Customer Data.

Data Subject rights: Data Processors and Data Sub-Processors will execute any necessary and reasonable measures when asked by the Data Controller, and communicate any useful information in order to help the Data Controller to comply with the duty to respect the rights of the Data Subjects. Data Processor and Data Sub-Processors will transmit to the Data Controller any Data Subject request. The Data Controller shall then further deal with the request itself. When a Data Processor or Data Sub-Processor assists the Data Controller in dealing with a Data Subject request, it is entitled to a reasonable compensation for this. No automated decision making (without any involvement of a human being) based on the Customer Data shall take place regarding the Data Subjects; the Data Controller is responsible for this.

Data Sub-Processing within Raptim: Customer Data may be (sub-) Processed by other members of the BCR only with prior information to the Data Controller and its prior written consent. The Service Agreement and/or Data Processing Agreement will specify if a general prior consent given at the beginning of the Service Agreement and/or Data Processing Agreement. The Data Controller shall be informed on any intended changes concerning the addition or replacement of Data Sub-Processors in a timely fashion giving the Data Controller the opportunity to object to the change or to terminate the Service Agreement and/or Data Processing Agreement before the Customer Data is communicated to the new Raptim Entity

Onward transfers of Customer Data to external Sub-Processors: Customer Data may be Sub-Processed by non-members of the BCR but only with prior information to the Data Controller and its prior written consent. Within the Service Agreement and/or Data Processing Agreement it will be specified whether this required prior written consent has to be obtained during the duration of the Service Agreement and/or Data Processing Agreement, or whether it has already been provided at the beginning of the Service Agreement and/or Data Processing Agreement. The Data Controller should be informed of any intended changes concerning the addition or replacement of Data Sub-Processors in a timely fashion to allow the Data Controller the ability to object to the change or to terminate the Service Agreement and/or Data Processing Agreement before the Customer Data is communicated to the new Data Sub-Processor. If the member of BCR subcontracts its obligations under the Service Agreement and/or Data Processing Agreement, and with the consent of the Data Controller, it shall do so with a written agreement with the Data Sub-Processor which provides that adequate protection is provided, and which ensures that the external Data Sub-Processor is required to respect the same obligations regarding the Processing of Customer Data as are imposed on the members of the BCR according to the Service Agreement, Data Processing Agreement and the BCR.

6. National data protection legislation and the BCR

6.1 Where a member of the BCR has reasons to believe that existing or future legislation applicable to it may prevent it from fulfilling the instructions received from the Data

Controller or its data protection obligations under the BCR, Data Processing Agreement and/or Service Agreement, it will promptly notify the Data Controller (which is entitled to suspend the transfer of Customer Data and/or terminate the Service Agreement), to the Raptim Headquarters, but also to the DPA competent for the Controller.

6.2 Any legally binding request for disclosure of the Customer Data by a law enforcement authority shall be communicated to the Data Controller unless otherwise prohibited, such as a prohibition under criminal law which is meant to preserve the confidentiality of a law enforcement investigation. The request for disclosure should be put on hold and the DPA competent for the Data Controller and the lead DPA (the Dutch DPA: the 'Autoriteit Persoonsgegevens') for the BCR should be clearly informed about it.

6.3 Where local legislation, for instance EEA legislation, requires a higher level of protection for Customer Data, it will take precedence over the BCR. In any event the Customer Data shall be processed in accordance with European Union Regulation 2016/679.

7. Publication duty

7.1 The BCR shall be published on the website of Raptim in a way easily accessible to Data Subjects.

8. Cooperation duty

8.1 All members of the BCR shall cooperate with, and could be audited by the DPA competent for the relevant Data Controller and comply with the advice of the DPA on any issues related to the BCR.

8.2 Any Data Processor or Data Sub-Processor shall cooperate and assist the Data Controller to comply with European Union Regulation 2016/679, within a reasonable period of time and to the extent reasonably possible.

9. Data Protection Officer (DPO)

9.1 Raptim shall appoint a DPO with top management support to oversee and ensure compliance with data protection rules, to advise the Raptim Entities, answer questions on behalf of the Raptim Entities, deal with DPA investigations, annually report on compliance, and ensure compliance at a global level.

9.2 The DPO shall have a sufficient level of independence when exercising this responsibility. The rights and responsibilities will be defined in the letter appointing the DPO and shall be guaranteed by the signature of the managing director of the Raptim Headquarters. Roles and responsibilities are more particularly described in Appendix 4.

10. Training

10.1 Raptim Entities will ensure the implementation of and compliance with the BCR by their Employees by way of appropriate training measures. Appropriate training on the BCR will be provided to Employees who have permanent or regular access to Customer Data, and are involved in the collection of Customer Data or in the development of tools used to Process Customer Data.

10.2 A training program shall be provided by Raptim in the form of a web-based training module. The training program shall enable the Employees to ensure the implementation of and compliance with the BCR. The measures comprise the following components:

- web-based training that will include the background, overview, key components and applicable fines for non-compliance;

11. Audits

11.1 Raptim shall carry out data protection audits on a regular basis (at least once a year) (by either internal or external accredited auditors), or upon a specific request from the DPO.

11.2 Such audits shall cover all aspects of the BCR, including methods of ensuring that corrective actions will take place when a breach of the BCR has been detected. The result of an audit will be communicated to the DPO and to the Raptim Headquarters, but also made accessible to the Data Controller.

11.3 The DPA competent for the Data Controller can have access to the results of the audit upon request, and shall have the authority to carry out a data protection audit itself if required and legally possible.

11.4 Any Data Processor or Data Sub-Processor handling the Customer Data of a particular Data Controller will accept, at the request of that Data Controller, to submit their Customer Data Processing facilities for audit of the processing activities relating to that Data Controller, which shall be carried out by the Data controller or an inspection body composed of independent members who are in possession of the required professional qualifications and bound by a duty of confidentiality, selected by the Data Controller.

Moreover, a third party scans the firewalls used by Raptim for PCI compliance.

12. Rights of the Data Subject

The Controller shall grant Data Subjects the rights listed below. The Data Subjects' rights to information and disclosure can be restricted only in the individual case and only if one of the exceptions under Regulation 2016/679 applies. The Processor shall assist the controller in handling requests by Data Subjects regarding their Customer Data, under the conditions specified in the BCR, the Service Agreement and the Data Processing Agreement.

a. A Data Subject may demand information from the Data Controller in an intelligible form about the Customer Data stored about himself as well as about its origin and the purpose for which the said data was collected.
b. A Data Subject may obtain information from the Data Controller about the recipients or the categories of recipients, to whom his/her Customer Data has been or will be transferred.
c. In the case of automated decisions, the Data Subject may request information about the processes involved in the automated Processing.
d. A Data Subject may - at appropriate intervals - obtain a copy of all Customer Data relating to him/her and which are the subject matter of Processing. This shall be provided at no cost, however, reasonable costs may be charged when multiple copies of the Customer Data are requested in one request. The costs may not be used to deter the exercise of Data Subject rights. A request shall, in principle, be dealt with within four weeks, unless it is excessive or manifestly unfounded.
e. A Data Subject may require his/her Customer Data to be blocked, deleted or corrected if:
    - it is incorrect or incomplete;
    - there are reasonable grounds for believing that said Customer Data has been collected or processed contrary to applicable data protection legislation or contrary to the Raptim BCR;

- if it is established that under applicable data protection law or the Raptim BCR it is no longer lawful to process the said Customer Data.

f. A Data Subject may object - free of charge - against the Processing of his/her Customer Data for the purposes of direct marketing.

g. A Data Subject may object against the Processing of his/her Customer Data for reasons associated with his/her personal situation provided that the Processing is not:
   - necessary to fulfil a contract to which the Data Subject is a contracting party, or necessary to implement pre-contractual measures taken upon the Data Subject's request;
   - necessary to fulfil a legal obligation to which the Data Controller is subject; or
   - necessary for safeguarding vital interests of the Data Subject. If the protest is well-founded, any further Processing shall be ceased.

13. Complaint Procedures for the Data Subject

13.1 Raptim shall create a contact point for Data Subjects.

13.2 All members of the BCR have the duty to communicate a claim or request made by a Data Subject without delay to the Data Controller, without obligation to handle it (except when agreed otherwise with the Data Controller).

13.3 The Data Processor shall handle complaints when the Data Controller has disappeared factually, ceased to exist in law or become insolvent.

13.4 In all cases where the Data Processor handles complaints, these shall be dealt with the DPO.

13.5 The Data Subject can complain with Raptim Netherlands BV at the e-mail address: Privacy@raptim.org. A complaint shall, in principle, be dealt with within four weeks, unless it is manifestly unfounded. If the complaint is considered justified, the Raptim entity shall modify or cease the Processing of the Customer Data of the Data Subject concerned.

In case of a rejection of the complaint, Raptim shall explain this. If the Data Subject does not agree, he/she can lodge a complaint with the Autoriteit Persoonsgegevens, or before the competent court.

13.6 The Data Subject shall be informed both by the Data Controller and Raptim about the points listed in Article 13.5.

14. Third-Party Beneficiary Rights and liability

14.1 A Data Subject shall have the right to enforce the BCR as a third-party beneficiary in case the Data Subject is not able to bring a claim against the Data Controller because the Data Controller has factually disappeared, ceased to exist in law or become insolvent; unless any successor entity has assumed the entire legal obligations of the Data Controller by contract or by operation of law, in which case the Data Subject can enforce his/her rights against such entity. This Data Subject right shall cover the judicial remedies for any breach of the rights guaranteed in these BCR and the right to receive compensation for any damage resulting from such breach. The third party beneficiary right shall cover the following articles of the BCR: 2.1, 2.2, 3.2, 5, 6.1, 8.1, 8.2, 14.1, 14.4, 14.6.

14.2 Data Subjects shall be entitled to lodge a complaint before the DPA or Courts competent for the Data Controller. If this is not possible for the reasons stated under Article 14.1, the Data Subject may take action before the DPA or the court competent for the Raptim

Headquarters. If those situations are not applicable, the Data Subject shall be entitled to lodge a complaint with the court of his place of residence. If more favorable solutions for the Data Subject exist according to national law, these shall be applicable.

14.3 The BCR shall be made binding toward the Data Controller through a specific reference to it in the Service Agreement and/or Data Processing Agreement. The Data Controller shall have the right to enforce the BCR against any of the Raptim Entities for breaches of privacy rules caused by these entities, including judicial remedies and the right to receive compensation.

14.4 The Raptim Headquarters shall accept responsibility for and take the necessary action to remedy the acts of other members of the BCR established outside of the EEA or breaches caused by external Sub-Processors established outside the EEA, and to pay compensation for any damages resulting from the violation of the BCR. The Raptim Headquarters will accept liability as if the violation had taken place by it in the Member State in which it is based.

14.5 The Raptim Headquarters may not rely on a breach by a Sub-Processor (internal or external of Raptim) of its obligations in order to avoid its own liabilities.

14.6 Where Data Subjects or the Data Controller can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of a breach of the BCR by one of the Raptim Entities, it will be for the Raptim Headquarters to prove that the Raptim Entity outside the EEA or the external Sub-Processor was not responsible for the breach of the BCR giving rise to those damages or that no such breach took place. If the Raptim Headquarters can prove that the Raptim Entity outside the EEA or the external Sub-Processor is not responsible for the act, it may discharge itself of any responsibility.

15. Mechanisms for reporting and recording changes

15.1 The BCR can be modified by the Raptim Headquarters (for instance, to take into account modifications of the regulatory environment or the company structure), but changes shall be reported to all the Raptim Entities, to the competent DPA and to the Data Controller.

15.2 Updates to the BCR or to the list of the members of the BCR are possible, provided that:

a. the DPO keeps a fully updated list of the Raptim Entities and of the Data Sub-Processors involved in the Processing activities for the Data Controller, which shall be made accessible to the Data Controller, Data Subjects and DPA;
b. the DPO keeps track of and record any updates to the BCR and provide the necessary information systematically to the Data Controller and upon request to DPAs;
c. no transfer is made to a new Raptim Entity until the new Raptim Entity is effectively bound by the BCR and can deliver compliance;
d. any substantial changes to the BCR or to the list of Raptim Entities shall be reported once a year to the Autoriteit Persoonsgegevens, with a brief explanation of the reasons justifying the update.

15.3 Where a change affects the Processing conditions, the information shall be given to the Data Controller in a timely fashion allowing the Data Controller to object to the change or to terminate the Service Agreement and/or Data Processing Agreement before the modification is made (for instance, on any intended changes concerning the addition or replacement of Data Sub-Processors, before the Customer Data is communicated to the new Data Sub-Processor).

16. Governing national law

The BCR are governed by the law of the EEA member state in which the Raptim Entity has its registered office, otherwise by Dutch law.

17. Entry into Force

The BCR enter into force upon adoption by the Raptim Headquarters.

Receipt & Acknowledgement

I understand that my signature below indicates that I have read and understand the above statements and have received a copy of Raptim's Binding Corporate Rules (BCR).

_____

Printed Name

_____ _____

Signature Date

APPENDIX 1: Raptim Entities

Raptim Entities EEA:

The Netherlands	**Raptim Nederland B.V**., having its registered office at Spoorlaan 306, 5038 CC Tilburg, The Netherlands, registered at the Dutch Chamber of Commerce (number 18011996)
	Multatuli Travel B.V., having its registered office at Plantage Middenlaan 16, 1018 DD Amsterdam, The Netherlands, registered at the Dutch Chamber of Commerce (number 33253131)
	Climate Neutral Group B.V., having its registered office at Arthur van Schendelstraat 650, 3511 MJ Utrecht, The Netherlands, registered at the Dutch Chamber of Commerce (number 30180751)
Denmark	**Raptim Humanitarian Travel**, Glarmestervej 20A, DK 8600 Silkeborg, Denmark
France	**Raptim France S.A.S.U**., 26, Rue de Martignac, 75007 Paris, France
Italy	**Raptim S.r.l.**, Via del Falco 9, 0193 Roma, Italy
	LDV S.r.l., Piazza San Zeno 12 37123 Verona, Italy
	Inn Town S.r.l., Galleria Hoepli 3D, 20121 Milano, Italy

Raptim Entities EX-EEA:

Africa	**Jet Travel Ltd.**, Waiyaki Way (Outer Road) – Westlands, P.O. Box 58805 Nairobi 00200, Kenya
USA	**Raptim International Travel Inc.**, 6420 Inducon Drive West - Suite A Sanborn, NY 14132, USA
	Raptim Humanitarian Travel, 116 Lake Street, Ephrata, PA 17522
	Raptim Humanitarian Travel, 1061 Texan Trail, Suite 550, Grapevine, TX, 76051
Canada	**Raptim Canada Inc**., 1515 Rebecca Street, 3rd Floor, Suite 300, South Oakville Centre, Oakville, ON L6L 5G8, Canada
	McTavish Holdings Inc., Oakville
	McTavish Travel Centre Ltd., Oakville
Switzerland	**Raptim S.A**., Route de Ferney 150, 1218 Le Grand-Saconnex, Switzerland

APPENDIX 2: Sub-Processors

Sub-Processors EEA:

Amadeus Hospitality Netherlands B.V.
Airplus
Hotels, car rental agencies, airlines, trains, tour operators

Sub-Processors EX-EEA:

TravelEx Booksmart (travel insurance provider)
Mimecast (cloud based spam filter and e-mail archive)
NuTravel
Cvent
Booking Builder
Grasp Technologies, Inc.
GoDaddy Operating Company, LLC
TravelCase
Core
Manulife (CA)
TRAMS
Hotels, car rental agencies, airlines, trains, tour operators

APPENDIX 3: Overview of the Customer Data

Raptim processes the following Customer Data:

Personal Data	Name
	Address
	E-mail address
	Phone number
	Date of birth
	Gender
Sensitive Personal Data	Passport number, expiration date, issuing country
	Citizenship
	Dietary requirements
	Credit Card (card number, expiration date, security code)

APPENDIX 4: Role and tasks of the DPO

The DPO is responsible for implementation and enforcement of data privacy standards within Raptim. The DPO will:

• Coordinate and monitor suitable measures for data privacy.

• Monitor compliance with data protection rules.

• Assess initiatives and projects for which Customer Data is processed.

• Provide training on data privacy for Raptim employees.

The DPO shall have a sufficient level of knowledge and independence when exercising this duty, and report directly to the management of the Raptim Headquarters.