

Data Protection Notice

Document Control

Classification: Public

Last Update: 24 Jun 2021

Revision: 8e7dfa

GENERAL INFORMATION

Simard OÜ – (“Company”) acts as the controller of personal data and is responsible for the protection of personal data, as it processes information in connection with third parties, contact persons of its business partners that work with the Company, and other individuals, such as passengers (collectively: “individuals”). This information qualifies as “personal data” as defined in of Article 4 (1) of the General Data Protection Regulation 2016/679 of the EU (“GDPR”).

This data protection notice (“Notice”) provides information regarding the processing of this personal data and the rights and remedies of the individuals with regards to said data processing.

Contact details of the Company:

- Registered seat of the Company: Harju maakond, Tallinn, Kesklinna linnaosa, Tartu mnt 67/1-13b, 10115, Tallinn, Estonia
- Registration number of the Company: 14905495
- E-mail address of the Company: contact@simard.io
- Website of the Company: <https://simard.io>
- Data Protection Officer of the Company and his / her contact details: Pedro Anderson (pedro@simard.io)

UPDATES AND AVAILABILITY

The Company reserves the right to unilaterally modify this Notice with immediate effect, subject to the limitations provided by law and the requirements of advance notification to the individuals in due time, if necessary. The Company may modify this Notice, particularly when it is required as a result of changes in the laws, the practice of the data protection authority, business needs or employees’ needs, any new activity involving personal data processing or any newly revealed security exposures, or if it is deemed necessary because of individuals’ feedback. When communicating in relation to this Notice or privacy issues, or otherwise keeping in contact with individuals, the Company may use the contact details of individuals available to the Company in order to get or keep in contact with individuals. Upon the request of an individual, the Company will, for example, send a copy of the latest updated version of this Notice to individuals or certify that a certain individual has read the Notice.

SPECIFIC DATA PROTECTION TERMS

In certain cases, specific privacy-related terms and conditions may also be applicable to certain individuals; said individuals will be duly notified thereof. Such specific terms and conditions are provided for in connection with the cookies that are used on the website of the Company.

In each case, individuals shall make the relevant personal data available to the Company in accordance with the applicable laws. Individuals shall give an adequate and informed consent or any other appropriate legal basis must exist for making personal data available to the Company. If the Company becomes aware that any personal data of a data subject was disclosed without his/her consent or any other appropriate legal basis, then the Company shall immediately delete such personal data, and the data subject is also entitled to exercise the rights and remedies set forth in this Notice. The Company will not be liable for any loss or harm which may arise from any breach of the above undertaking and representation of any individual.

SCOPE OF THE DATA AND THE PURPOSE OF ITS PROCESSING

The list below describes the scope of the processed personal data, the purposes, the legal basis, the duration of the processing and the scope of the persons authorised to have access to the data. Where a purpose of processing is required for pursuing a legitimate interest of the Company or any third party, then the Company will perform a balancing test of the underlying interests, which is available upon a request submitted to the Company by means of the contact details listed hereinabove.

The Company expressly wishes to draw the attention of the individuals to their right of objection to the processing of their personal data on grounds relating to their particular situation at any time where the processing is based on a legitimate interest, including cases where the processing takes the form of profiling. In such cases, the Company shall cease to process the personal data unless it can prove that the processing has to be continued due to compelling legitimate reasons which override the interests, rights and freedoms of the individuals, or which relate to the submission, the enforcement or the protection of legal claims. If personal data is processed for the purpose of direct marketing, individuals may at any time object to the processing of their personal data for that purpose. Said grounds for objection include profiling if it is connected to direct marketing.

The Company process personal data for the following purposes:

- (P1) Creating and managing a booking (flight, hotel) with a travel supplier
- (P2) Preventing fraud in relation to the payment
- (P3) Monitoring the performance of the services
- (P4) Sending marketing messages, offers and services via email
- (P5) Responding to legal requests
- (P6) Processing the personal data of contact persons of contracting partners and/or persons involved in contract performance / verification of performance for the day-to-day implementation of contracts
- (P7) Processing the personal data of contact persons of contracting partners and/or persons involved in contract performance and verification of performance in connection with compliance issues or any other activity needed to implement the contract including seeking remedies in order to enforce the rights arising from the contracts
- (P8) Handling customer and other inquiries received by the Company

P1: Creating and managing a booking (flight, hotel) with a travel supplier

This shall include:

- Processing payment for the services provided.
- Support on the bookings created. For example, fulfilment of requests from travel sponsors (i.e. the person making the booking, such as an employer, assistant, family member, passenger), sending notifications in case of cancellations or disruptions, responding to user inquiries (i.e. anyone who is involved in the booking, such as travel sponsors or passengers).
- Performance of "Duty of Care" obligations. For example, if a passenger is stranded in a country with

an unexpected event (volcano eruption, civil war) or with a missed connection, her/his employer or travel agent has a duty of care to help. The Company will contact the relevant individuals and find alternative options for the travelling.

Without the personal data, the Company is unable to create and manage the booking.

P1: Legal basis of the processing

It depends on whether a contract is concluded with the individual (the passenger) or with an organisation.

There are three possible scenarios:

1. The booking is done on the glider.travel booking portal operated by Simard - in such case the contracting partner is an individual.
2. The booking is done on a corporate booking tool using Simard services - in such case the contracting partner is the employer of the passenger.
3. The booking is done on a third-party travel agency using Simard services - in such case the contracting partner is a company, but the passenger is not an employee of the partner company.

The legal basis of the data processing is Article 6(1)(b) of the GDPR – the purpose is directly the performance (implementation) of the contract with the contracting party, i.e. the individual or company making the booking.

P1: Scope of processed data

Passenger data: name of the passenger, date of birth, passport or government identification number, contact data, airline or hotel loyalty card numbers.

In the case of corporate travellers: name of the company and other company specific identifiers: Cost Centre, Project Code, Employee ID).

Payment data: instrument reference (such as a credit card number), cardholder name, expiration date and the security code associated with the payment instrument.

Contact data: phone number and email address of the passenger and company making the booking, if applicable.

Administrative information related to the booking: booking number, travel information.

P1: Data retention and data transfers

Personal data may be processed during the course of the contractual relationship and retained up to 3 years after the provision of service by the Company has ended, unless the data is required for record-keeping purposes, e.g. tax, accounting, where the data retention period can be longer – up to 7 years.

The Company is sharing the passenger data and the contact data with travel suppliers (e.g.: an airline, an hotel chain or other travel aggregators). The list of these travel suppliers is set out in Schedule 1 .

P2: Preventing fraud in relation to the payment

For example: checking the card number against a list of stolen cards, checking cases of multiple attempts with the same card for unrelated bookings, checking the card issuing country against a list of high risk countries.

Actions taken as the result of the fraud prevention: For example, in case of fraud, a payment institution can request Simard to cancel some orders based on the card number.

P2: Legal basis of the processing

The legal basis of the data processing is Article 6(1)(f) of the GDPR – pursuing the legitimate interests of both the Company and the contracting partner: combatting financial fraud or other fraudulent use of services, ensuring that companies and passengers will not misuse the booking service (or will not be able to obtain services without payment).

P2: Scope of Processed Data

The personal data listed in the previous heading titled “Creating and managing a booking (flight, hotel) with a travel supplier”.

Passenger data and device/location data might also be used for fraud screening purpose.

P2: Data retention and data transfers

Data may be processed during the course of the contractual relationship and retained up to 3 years after the provision of service by the Company has ended

P3: Monitoring the performance of the services

The Company is using the aggregated data to detect trends on a specific setup, for example if 100% of requests from MacOS are failing but they are all working fine for Windows and Linux users, then the Company can engage an engineer try to identify if this is correlated to an issue in the software in conjunction with this specific operating system.

P3: Legal basis of the processing

The legal basis of the data processing is Article 6(1)(f) of the GDPR (processing of the data is needed for pursuing the legitimate interests of the Company).

The legitimate interest: to improve the performance of the Company’s services.

P3: Scope of Processed Data

- Device data: information about the computer, phone, tablet or other device which is automatically sent or provided by the device when interacting with the Company, e.g. IP Address, Browser Version, Operating System, Screen Resolution, Language.
- Location data: (not accurate) data derived from IP address to identify country and region.

P3: Data retention and data transfers

Data may be processed during the course of the contractual relationship and retained up to 3 years after the provision of service by the Company has ended.

P4: Sending marketing messages, offers and services via email

P4: Legal basis of the processing

The legal basis of the data processing is Article 6(1)(a) of the GDPR – voluntary consent of the individual or the contracting partner.

Consent may be withdrawn at any time, without limitation and reasoning, free of charge. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Without consent, the Company is not permitted to send out advertisements and newsletters by email.

P4: Scope of Processed Data

Name and email address of the recipients.

P4: Data retention and data transfers

If the recipient withdraws consent, then personal data must be deleted.

P5: Responding to legal requests

For example, to legal request in relation to preventing human trafficking, preventing children from traveling alone, supporting the police in investigations for terrorism, fulfilment of anti-money laundering obligations, fulfilment of obligations in relation to countries under embargoes.

P5: Legal basis of the processing

The legal basis of the data processing is Article 6(1)(c) of the GDPR – the data processing is necessary for compliance with a legal obligation to which the Company is subject.

P5: Scope of Processed Data

Name and email address of the individual, together with the passenger data, contact data, payment data and travel information, as applicable.

P5: Data retention and data transfers

Data may be processed during the course of the contractual relationship and retained up to 3 years after the provision of service by the Company has ended. Data may be retained longer, if the Company has a legitimate interest for retaining such data, e.g. if the data is necessary for ongoing legal proceedings.

The Company may share the relevant data with the competent authorities and courts. For example, the competent court or police might order to disclose the booking data as part of anti-terrorism measures or to disclose the payment data to comply with anti-money laundering regulations.

P6: Processing the personal data of contact persons of contracting partners and/or persons involved in contract performance / verification of performance for the day-to-day implementation of contracts

This includes sending official notifications with the use of the contact details and information regarding contractual obligations to be fulfilled.

P6: Legal basis of the processing

The legal basis of the data processing is Article 6 (1) (b) of the GDPR – the purpose is directly the performance (implementation) of the contract with the contracting party, i.e. the individual or company making the booking.

The exchange of personal data is required under the contract; without that, the Company is unable to conclude the contract and/or implement it.

P6: Scope of Processed Data

The contact details (i.e. e-mail addresses, telephone numbers, mobile phone numbers, telefax numbers) of the contact persons of the contracting partners and/or persons involved in contract performance and verification of performance, and any other activity or communication which includes any kind of personal data (e.g. communication received from a contact person or any other person acting on behalf of a contracting partner) in connection with the contract.

The personal data is either provided to the Company by the contracting partner, or by the individuals themselves.

P6: Data retention and data transfers

Data may be processed during the course of the contractual relationship and retained up to 3 years after the provision of service by the Company has ended.

P7: Processing the personal data of contact persons of contracting partners and/or persons involved in contract performance and verification of performance in connection with compliance issues or any other activity needed to implement the contract including seeking remedies in order to enforce the rights arising from the contracts

P7: Legal basis of the processing

The legal basis of processing data is the legitimate interest of the Company (Article 6 (1) (f) of the GDPR). The legitimate interest: handling compliance issues or any other activity needed to implement the contract including seeking remedies in order to enforce the rights arising from the contracts.

P7: Scope of Processed Data

The contact details (i.e. names, e-mail addresses, telephone numbers, mobile phone numbers, telefax numbers) of the contact persons of the contracting partners and/or persons involved in contract performance and verification of performance, and any other activity or communication which includes any kind of personal data (e.g. any communication received from a contact person or any other person acting on behalf of a contracting partner) in connection with the contract.

The personal data is provided to the Company either by the contracting partner or the individuals themselves.

P7: Data retention and data transfers

Data may be processed during the course of the contractual relationship and retained up to 3 years after the provision of service by the Company has ended. Data may be retained longer, if the Company has a legitimate interest for retaining such data, e.g. if the data is necessary for ongoing legal proceedings.

P8: Handling customer and other inquiries received by the Company

P8: Legal basis of the processing

The legal basis of the data processing is Article 6 (1) (b) of the GDPR – the purpose is directly the performance (implementation) of the contract with the contracting party, i.e. the individual or company making the booking

P8: Scope of Processed Data

The personal data affected by the customer and other inquiries that are received by the Company, the contact data of the customers and other private individuals (i.e. name, address, e-mail address, telephone number) and the records of the actions taken in relation to the inquiry.

P8: Data retention and data transfers

Data may be processed during the course of the contractual relationship and retained up to 3 years after the provision of service by the Company has ended.

DATA PROCESSORS

The Company engages the following contractual partners for carrying out tasks related to data processing operations in addition to the ones listed above. Such contracting parties act as so-called “data processors” (i.e. they process the personal data defined in this Notice on behalf of the Company).

The Company shall only use data processors that provide sufficient safeguards, in particular in terms of expertise, reliability and resources, for the implementation of technical and organisational measures which ensure that the requirements of the GDPR are met. Said safeguards include the security of processing. The particular tasks and liabilities of the data processor are provided for in the data processing agreement made between the Company and the data processor. After the completion of the processing on behalf of the Company, the processor shall, at the choice of the Company, return or delete the personal data, unless there is a requirement to store the personal data under applicable law.

Stripe

- Legal Name: Stripe Payments Europe Ltd. ("Stripe")
- Address: C/O A&L Goodbody, Ifsc, North Wall Quay, Dublin 1, Ireland
- Privacy Notice: <https://stripe.com/en-ee/privacy>
- Purpose: Payment processing

American Express

- Legal name: American Express Europe S.A ("American Express")
- Address: Avenida Partenón 12-14, 28042 Madrid, Spain
- Privacy Notice: <https://www.americanexpress.com/us/privacy-center/>
- Purpose: Payment processing

Wise

- Legal name: Wise Europe SA ("Wise")
- Address: Avenue Louise 54, Room s52, 1050 Brussels, Belgium

- Privacy Notice: <https://wise.com/terms-and-conditions>
- Purpose: Payment processing

Amazon Web Services

- Legal Name: Amazon Web Services EMEA SARL, ("AWS Europe")
- Address: Avenue John F. Kennedy 38, 1855, Luxembourg, Luxembourg
- Privacy Notice: <https://aws.amazon.com/privacy/>
- Purpose: Providing the infrastructure to operate the services, monitoring the performance of the services

Note: The Amazon Web Services datacenter is located in Europe.

Finance Management OÜ

- Legal Name: Finance Management OÜ
- Address: Mustamäe tee 62, 12916 Tallinn, Estonia
- Privacy Notice: info@five.ee
- Purpose: Accounting Services

TECHNICAL AND ORGANISATIONAL DATA SECURITY MEASURES

The Company protects the personal data it processes primarily by restricting the access to the information and by clearly specifying individuals' rights. Only the persons who require access in order to fulfil the above-mentioned purposes and/or are authorised to have access are entitled to access the systems and instruments used for processing the personal data referred to in this Notice. These persons include, e.g., designated team members or departments (e.g. in respect of user data that are required for the use of the Company's IT systems, the IT Department).

The Company ensures the safe and legitimate use of the devices which it makes available (including Company-owned computers, notebooks and mobile phones), the e-mail accounts and the Internet, and the desired level of awareness of the employees related to such use by applying the following measures:

- The Company requires that the devices that it made available and that have access to the Internet as well as the e-mail accounts are used by the employees with specific user names and passwords which are adequately complex and up-dated at regular intervals.
- The Company protects all its systems and devices by fire wall, antivirus software and spam filters. In addition, the Company operates an intrusion protection system (so-called IPS) which enables the detection, blocking and logging of illegitimate attempts of intrusion into the computer systems of the Company.
- The Company makes safe wired and wireless network access available for all company devices provided by the Company.
- Remote access to the systems and software of the Company from any device is possible only through safe connection (VPN) by using specific user names and passwords, with mitigation of chances of accidental access (including illegitimate access by the use of stolen or lost devices).
- The IT Department of the Company carries out regular software and system up-dates and back-up saves of data in accordance with its own internal regulations.

As regards the physical protection of data and electronic documents, the Company owns locked server rooms and ensures that access to a particular document is reserved to adequately authorised persons only (e.g. access to HR documents is reserved to the HR Department, access to payroll data is reserved to the Financial Department and the data processor engaged for payroll accounting).

DATA PROTECTION RIGHTS AND REMEDIES

Data protection rights and remedies

The detailed rights and remedies of the individuals are set forth in the applicable provisions of the GDPR (especially in Articles 15, 16, 17, 18, 19, 20, 21, 22, 77, 78, 79, 80, and 82 of the GDPR). The summary set out below describes the most important provisions and the Company provides information for the individuals in accordance with their rights and remedies related to the processing of personal data. If the individual wishes to exercise their rights described herein, they should contact the Company via the contact information specified in clause 1 of this Notice.

The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the individual, information may also be provided orally, provided that the identity of the individual is verified by other means.

The Company will respond without unreasonable delay to the request of an individual in which such person exercises his/her rights about the measures taken upon such request (see Articles 15-22 of the GDPR), with said response by no means to occur later than one month after receipt thereof. This period may, if needed, be extended for a further two months in light of the complexity of the request and the number of requests to be processed. The Company shall notify the individual about the extension and also indicate its grounds therefor within one month of the receipt of the request. Where the request has been submitted by electronic means, the response should likewise be sent electronically, unless the individual requests otherwise.

If the Company does not take any measure upon the individual's request, it shall so notify the individual without delay, but by no means later than one month after receipt thereof, stating why no measures will be taken. Additionally, the Company shall inform the individual about the individual's right to lodge a complaint with the data protection authority and to file an action for remedy with the courts.

The individual's right of access

- The individual has the right to obtain confirmation from the Company with regards to whether or not personal data concerning them is being processed. In such a case, the individual is entitled to have access to the relevant personal data and to the following information:
 - the purposes of the processing;
 - the categories of personal data concerned;
 - the recipients or categories of recipient to whom the personal data has been or will be disclosed, including recipients in third countries and/or international organisations;
 - where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
 - the right of the individual to request from the Company rectification or erasure of personal data, or restriction of processing of personal data concerning the individual, or to object to such processing;
 - the right to lodge a complaint with a supervisory authority;
 - where the personal data is not collected from the individual, any available information as to its source.

- Where personal data is forwarded to a third country, the individual is entitled to obtain information concerning the adequate safeguards of the data transfer.
- The Company provides a copy of the personal data undergoing processing to the individual. The Company may charge a reasonable fee based on administrative costs for requested further copies thereof. Where the individual submitted their request by electronic means, the information will be provided to them in a commonly used electronic form unless otherwise requested by the data subject.

Right to rectification

The individual has the right to request that the Company rectify inaccurate personal data which concerns them without undue delay. In addition, the individual is also entitled to have incomplete personal data completed e.g. by a supplementary statement or otherwise.

Right to erasure ('right to be forgotten')

- (1) The individual has the right to request that the Company erase the personal data concerning them without delay where one of the following grounds applies:
 - the personal data is no longer required for the purposes for which it was collected or otherwise processed by the Company;
 - the individual withdraws consent on which the processing is based, and there are no other legal grounds for the processing;
 - the individual objects to the processing and there are no overriding legitimate grounds for the processing;
 - the personal data has been unlawfully processed;
 - the personal data has to be erased for compliance with a legal obligation in Union or Member State law to which the Company is subject.
- (2) If the Company has made the personal data public and it is later obliged to delete it as a result of the above stated grounds, it will take reasonable steps to delete it, taking into account the available technology and the costs of implementation. These reasonable steps include technical steps in order to inform processors who carry out processing that the individual has initiated a request for the links leading to the relevant personal data, or the copies or reproductions thereof, be deleted.
- (3) Paragraphs (1) and (2) shall not apply to the extent that processing is necessary, among other things, for:
 - compliance with a legal obligation which requires processing by European Union or Member State law to which the Company is subject;
 - archiving purposes in the public interest, scientific or historical research purposes or statistical purposes insofar as the right referred to in paragraph (1) is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
 - the establishment, exercise, or defence of legal claims.

Right to restriction of processing

- (1) The individual has the right to obtain from the Company restriction of processing where one of the following applies:
 - the accuracy of the data is contested by the individual, for a period enabling the Company to verify the accuracy of the personal data;
 - the processing is unlawful, and the individual opposes the erasure of the personal data

- and requests the restriction of its use instead;
 - the Company no longer needs the personal data for the purposes of the processing, but the individual requires it for the establishment, exercise or defence of legal claims;
 - the individual has objected to processing pending the verification of whether the legitimate grounds of the Company override those of the individual.
- (2) Where processing has been restricted under paragraph (1), such personal data shall, with the exception of storage, only be processed with consent of the individual or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.
 - (3) The Company informs the individual whose request has served as grounds for the restriction based on the aforesaid, before the restriction of processing is lifted.

Notification obligation regarding rectification or erasure of personal data or restriction of processing

The Company will communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort. The Company shall inform the individual about those recipients if they so request.

Right to data portability

- (1) The individual has the right to receive the personal data concerning them, which they have provided to the Company in a structured, commonly used, and machine-readable format and have the right to transmit that data to another controller without hindrance from the Company, where:
 - the processing is based on consent or on a contract; and
 - the processing is carried out by automated means.
- (2) In exercising the right to data portability pursuant to paragraph (1), the individual shall have the right to have the personal data transmitted directly from one controller to another (thus from the Company to another controller), where technically feasible.
- (3) Exercising the aforesaid right shall be without prejudice to provisions concerning the right to erasure ('right to be forgotten') and, further, this right shall not adversely affect the rights and freedoms of others.

Right to object

- (1) The individual has the right to object, on grounds relating to his/her particular situation, at any time to the processing of personal data concerning them for the purposes of legitimate interests. In such a case, the Company will no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the individual, or for the establishment, exercise or defence of legal claims.
- (2) Where the processing of personal data serves direct marketing purposes the individual is entitled to object to the processing of personal data regarding them for such purposes, including profiling, in so far as the latter relates to direct marketing.
- (3) If the individual objects to the processing of personal data with the aim of direct marketing, then the personal data can no longer be processed for this purpose.

- (4) In connection with the use of services related to information society, the individual may resort to their right of objection, with deviation from Directive No 2002/58/EC, by means of automated devices based on technical requirements.
- (5) Where personal data is processed for scientific or historical research purposes or statistical purposes, the individual, on grounds relating to their particular situation, has the right to object to the processing of personal data concerning them, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Right to lodge a complaint with a supervisory authority

The individual has the right to lodge a complaint with a supervisory authority, in particular in the Member State of their habitual residence, place of work, or place of the alleged infringement if they consider that the processing of personal data relating to them infringes the GDPR.

Right to an effective judicial remedy against the Company or the processor

- (1) Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, any individual has the right to an effective judicial remedy where they consider that their rights under the GDPR have been infringed as a result of the processing of their personal data in non-compliance with the GDPR.
- (2) Proceedings against the Company or a processor shall be brought before the courts of the Member State where the Company or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the individual has habitual residence.

Schedule 1: Travel Suppliers

The Company transfers personal data to the following companies listed in the table below in addition to the ones listed above.

These companies act as independent data controllers which means that they may determine the purpose of data processing independently or jointly with others, make decisions and implement them, or have them implemented by a data processor engaged for that purpose. The recipients of data transfers act as independent data controllers in accordance with their own terms and conditions of data processing; the Company has no control over this. The Company may obtain more detailed information from these companies about the data processing they carry out.

Recipient: American Airlines

- Legal name: American Airlines, Inc.
- Legal Address: 1 Skyview Drive, MD 8B503, Fort Worth, TX 76155, USA
- Privacy Policy: <https://www.aa.com/i18n/customer-service/support/privacy-policy.jsp>

American Airlines is a US-based carriers that will process process personal data whenever a booking is created for this carrier or its interline partners.

Recipient: United Airlines

- Legal name: United Airlines, Inc.
- Legal Address: 233 S. Wacker Drive, Chicago, Illinois 60606, USA

- Privacy Policy: <https://www.united.com/ual/en/us/fly/privacy.html>

United Airlines is a US-based carriers that will process process personal data whenever a booking is created for this carrier or its interline partners.

Recipient: ATPCO

- Legal name: Airline Tariff Publishing Company ("ATPCO")
- Legal Address: 45005 Aviation Drive, Dulles, Virginia 20166, USA
- Privacy Policy: <https://www.atpco.net/privacy>

ATPCO processes travel bookings for multiple airlines, and therefore will process personal data whenever a booking is created for one of the created for one of the airlines available on their platform.

Recipient: Amadeus

- Legal name: Amadeus IT Group S.A. ("Amadeus")
- Legal Address: Salvador de Madariaga 1, 28027 Madrid, Spain
- Privacy Policy: <https://amadeus.com/en/policies/privacy-policy>

Amadeus processes travel bookings for multiple airlines and Hotels, and therefore will process personal data whenever a booking is created for one of the travel suppliers available on their platform.

Recipient: eRevMax

- Legal names: eRevMax Ltd.
- Legal Address: 2 Red Lion Point, Leman St, London, E1 8FA, England
- Privacy Policy: <https://www.erevmax.com/ratetiger/privacy-policy-terms-use.html>

eRevMax processes travel bookings for Hotels, Hotel Chains and other accomodation providers, and therefore will process personal data whenever a booking is created for one of the accomodation service provider available on their platform.