Data Processing Addendum

This Data Processing Addendum ("**Addendum**") to the Host Terms and Conditions (the "**Agreement**") is by and between Rakuten Group, Inc. ("**Rakuten**"), and Hosts under the Agreement ("**Host**"). Rakuten and Host are each a "Party" and collectively the "Parties".

1. Introduction.

This Addendum is an integral part of the Agreement and supersedes and replaces any existing data protection obligations contained in the Agreement. Any words or terms not otherwise defined in this Addendum have the same meaning as in the Agreement. In the event of a conflict between definitions or terms in the Agreement and this Addendum, the definitions and terms within this Addendum apply in relation to the Parties' data protection obligations only.

2. Definitions.

"**Business**" shall have the same meaning given to it in the California Consumer Privacy Act.

"**California Personal Information**" means any information that relates to, is capable of being associated with, or could be linked, directly or indirectly, with a particular California resident or household.

"**Data Protection Legislation**" means the Regulation, the e-Privacy Directive 2002/58/EC, any successors thereto, any national implementing laws, the California Consumer Privacy Act, the Act on Protection of the Personal Information in Japan ("**APPI**"), and any other applicable laws relating to data protection or privacy.

"**Data Subjects**" has the meaning given to it in the Regulation and for the purposes of this Addendum and the Agreement it also means employees, contractors and agents of Rakuten and End Users.

"**Personal Data,**" "**Personal Data Breach**". "**Process/Processing,**" "**Controller,**" "**Processor,**" "**Data Subject**" and "**Supervisory Authority**" shall have the same meanings given to them in the Regulation.

"**Regulation**" means Regulation (EU) 2016/679 of the European Parliament and the Council (General Data Protection Regulation).

"**SCC**" means the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 in accordance with Commission Implementing Decision (EU) 2021/914 of 4 June 2021; available from the European Commission via http://data.europa.eu/eli/dec_impl/2021/914/oj.

3. Role of the Parties.

In order to provide the Services under the Agreement, Rakuten discloses data, including Personal Data to Host for the purposes described in the Agreement (the "**Permitted Purposes**"). Rakuten is an independent Controller of the Personal Data

and a separate Business with respect to the California Personal Information it discloses to Host and that it collects from End Users. Pursuant to the Agreement, Host Processes the Personal Data as a separate and independent Controller for the Permitted Purposes. In no event will the Parties process the Personal Data as joint Controllers.

4. Obligations.

4.1. Each Party shall Process Personal Data and California Personal Information in accordance with applicable Data Protection Legislation, will not cause the other Party to breach its obligations under Data Protection Legislation and will individually and separately fulfill all obligations that apply to it as a Controller or a Business under the Data Protection Legislation.

4.2. In order to perform their obligations under the Agreement and in compliance with the Regulation, each Party's obligations include without limitation:

(a). identifying its independent legal bases for Processing Personal Data; and
(b). fulfilling transparency requirements regarding its use of and disclosure of Personal Data.

4.3. Rakuten warrants and undertakes that, where applicable, it has obtained and will obtain the necessary consent from Data Subjects to disclose Personal Data to Host pursuant to the Agreement for the Permitted Purposes (including, in particular, obtaining consent from End Users for Host to use Personal Data, cookies and other tracking technologies as part of the Software Services, as described in its appropriate privacy policy and, where applicable, cookie policy).

4.4. Rakuten further warrants that it will disclose accurate and up-to-date Personal Data to Host.

4.5. Each Party shall implement and maintain appropriate technical and organisational measures (including, but not limited to, encryption and password protection), when transferring and/or Processing Personal Data or California Personal Information, to preserve the confidentiality, integrity and availability of the Personal Data and California Personal Information and prevent any unlawful Processing or disclosure or damage, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of the Data Subjects;

4.6. In the event that either Party receives any correspondence, inquiry or complaint from a Data Subject or Supervisory Authority ("**Inquiry**") related to the Processing of Personal Data for the Permitted Purposes or the Processing of Personal Data by the other Party in connection with the Agreement, it will promptly inform the other Party and provide full details of the Inquiry. The Parties shall cooperate in good faith to timely respond to the Inquiry in accordance with requirements under the applicable Data Protection Legislation in its capacity as a independent Controllers.

4.7. Each Party shall notify the other Party without undue delay and in any event within 24 hours of becoming aware of a Personal Data Breach notifiable to the Supervisory Authorities under applicable Data Protection Legislation affecting

Personal Data and/or California Personal Information Processed by either Party in connection with the Agreement. Each Party agrees to keep the other Party regularly updated as to the handling of such Personal Data Breach and bear their own costs in complying with their obligations under this clause.

4.8. Each Party shall provide all such co-operation and information as the other Party may reasonably require in order to enable that Party to comply with its obligations under Data Protection Legislation. Each Party will bear its own costs in complying with its respective obligations under Data Protection Legislation.

5. International Data Transfers.

5.1. The Parties acknowledge that in carrying out their obligations under the Agreement, Personal Data may be transferred internationally including from the European Union ("**EU**"), European Economic Area ("**EEA**") or the United Kingdom to the United States, Japan, or other territory(ies) whose level of protection for Personal Data differs from that of the EU and EEA. In all cases where Personal Data is transferred internationally to territories not providing adequate Personal Data protection in accordance with the Regulation, the Parties will ensure that Standard Contractual Clauses as set out in Exhibit A are put in place.

5.2. Notwithstanding clause 5.1 above, if Personal Data will be transferred from Japan to countries or territories outside of Japan, excluding the countries in the EEA, the Parties must first execute an appropriate data transfer agreement similar to Exhibit B attached hereto to ensure lawful transfer of Personal Data under the APPI unless appropriate consent from the Data Subject is first obtained for this international transfer or unless the transfer is otherwise permitted by the APPI.

5.3. For the purposes of the Standard Contractual Clauses the following additional provisions shall apply:

(a). Rakuten shall be regarded as the data exporter and the Host shall be regarded as the data importer;

(b). The data exporter and the data importer agree to observe the terms of the Standard Contractual Clauses without modification; and

(c). In the event of any conflict between the provisions of the Standard Contractual Clauses, the remaining terms of this Addendum and the Agreement, the Standard Contractual Clauses or any replacement thereof shall take precedence. The terms of this Addendum and of the Agreement shall not vary the Standard Contractual Clauses in any way.

6. Survival.

This Addendum shall survive termination or expiration of the Agreement. Upon termination or expiration of the Agreement, Host may continue to process Personal Data received from Host provided that such use complies with the requirements of this Addendum and under the Regulation.

[Exhibit A to the Data Processing Addendum]

(Standard Contract Clauses)

In this Addendum, Module 1 of the SCC shall apply. The SCC shall be deemed to be completed as follows:

Clause 7: the optional docking clause does not apply;

Clause 11: the optional language does not apply;

Clause 17: Option 2 does apply. Where the respective EU member state does not allow for third-party beneficiary rights, the law of Luxembourg shall apply;

Clause 18(b): disputes shall be resolved before the courts of Luxembourg;

Annex I A (List of Parties) shall be deemed completed with the information of the Parties of this Addendum;

Annex I B (Description of Transfer) shall be deemed completed with the information set out in Annex B to this Addendum;

Annex I C: The competent supervisory authority shall be the National Commission for Data Protection of the Grand-Duchy of Luxembourg (“CNPD”);

Annex III shall be deemed completed with the information set out in Annex C to this Addendum.

ANNEX A

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal Data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal Data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause 2.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.

8. Automated decisions: For purposes hereof “automated decision” shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

   8.1. i. such decisions are made by the data importer in entering into or performing a contract with the data subject, and

   ii. the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

   or

   8.2. where otherwise provided by the law of the data exporter.

ANNEX B

DESCRIPTION OF THE TRANSFER

(To be completed by the parties)

Data subjects

The personal data transferred concern the following categories of data subjects:
the users of Rakuten Travel Experience

Purposes of the transfer(s)

The transfer is made for the following purposes:
For the purpose of sharing user information necessary for hosts to provide services to users under Host Terms and Conditions.

Categories of data

The personal data transferred concern the following categories of data:
Following user information:
name, email address, phone number, SNS account, country of residence, nationality, passport information, age, date of birth, gender, accommodation information (name, address), driver's license copy, physical information required for the experience,, other hosts usage information (name, email address, phone number, and person in charge of travel experience providers), proof of travel cancellation(in case of disaster cancellation), vaccination certificate, certificate of negative test for covid-19.

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients:
The Data Importer and such other third parties as the Data Importer may transfer the personal data to in accordance with these clauses.

Sensitive data (if appropriate)

The personal data transferred concern the following categories of sensitive data:
N/A

Data protection registration information of data exporter (where applicable)

N/A

Additional useful information (storage limits and other relevant information)

N/A

Contact points for data protection enquiries

Data importer

Contact point notified from Hosts to Rakuten

Data exporter

inquiry form

ANNEX C

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

This Annex B summarizes the technical, organisational and physical security measures implemented by the Parties in accordance with clause 8.5(a) of the SCC:

Each party shall comply with the following:

Each party undertakes to implement, maintain, and continuously control and update, appropriate technical and organizational security measures to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected. This includes:

1. Preventing unauthorised persons from gaining access to data processing systems with which Personal Data are processed or used (physical access control); in particular, by taking the following measures:
    1.1. Controlled access for critical or sensitive areas
    1.2. Video monitoring in critical areas
    1.3. Incident logs
    1.4. Implementation of single entry access control systems
    1.5. Automated systems of access control
    1.6. Permanent door and windows locking mechanisms
    1.7. Key management
    1.8. Locked doors (key, code, badge or other similar mechanism)
    1.9. Monitoring facilities (e.g. alarm device, video surveillance)
    1.10. Logging of visitors
    1.11. Compulsory wearing of ID cards
    1.12. Security awareness training.
2. Preventing data processing systems from being used without authorisation (logical access control); in particular, by taking the following measures:
    2.1. Network devices such as intrusion detection systems, routers and firewalls
    2.2. Secure log-in with unique user-ID/password
    2.3. Policy mandates locking of unattended workstations. Screensaver password is implemented such that if user forgets to lock the workstation, automatic locking is ensured.

2.4. Logging and analysis of system usage

2.5. Role-based access for critical systems containing personal data

2.6. Process for routine system updates for known vulnerabilities

2.7. Encryption of laptop hard drives

2.8. Monitoring for security vulnerabilities on critical systems

2.9. Deployment and updating of antivirus software

2.10. Individual allocation of user rights, authentication by password and username, use of smartcards for log in, minimum requirements for passwords, password management, password request after inactivity, password protection for BIOS, management of access to external ports (such as USB ports), encryption of data, virus protection and use of firewalls, intrusion detection systems.

3. Ensuring that persons entitled to use a data processing system can gain access only to the data to which they have a right of access, and that, in the course of processing or use and after storage, personal data cannot be read, copied, modified or deleted without authorisation (access control to data); in particular, by taking the following measures:

   3.1. Network devices such as intrusion detection systems, routers and firewalls

   3.2. Secure log-in with unique user-ID/password

   3.3. Logging and analysis of system usage

   3.4. Role based access for critical systems containing personal data

   3.5. Encryption of laptop hard drives

   3.6. Deployment and updating of antivirus software

   3.7. For the processing of credit card information: Compliance with Payment Card Industry Data Security Standard (PCI-DSS)

   3.8. Definition and management of role based authorization concept, access to Personal Data only on a need-to-know basis, general access rights only for a limited number of admins, access logging and controls, encryption of data, intrusion detection systems, secured storage of data carriers, secure data lines, distribution boxes and sockets.

4. Ensuring that Personal Data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage and that it is possible to verify and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged (data transfer control); in particular, by taking the following measures:

   4.1. Encryption of communication, tunnelling (VPN = Virtual Private Network), firewall, secure transport containers in case of physical transport, encryption of laptops

5. Ensuring that it is possible retrospectively to examine and establish whether and by whom personal data have been inserted into data processing systems, modified or removed (entry control); in particular, by taking the following measures:

    5.1. Logging and analysis of system usage

    5.2. Role based access for critical systems containing personal data

    5.3. Logging and reporting systems, individual allocation of user rights to enter, modify or remove based on role based authorization concept.

6. Ensuring that Personal Data processed on the basis of a commissioned processing of Personal Data are processed solely in accordance with the directions of the Data Exporter (job control); in particular, by taking the following measures:

    6.1. Mandatory security and privacy awareness training for all employees involved with processing personal data

    6.2. Employee hiring procedures which require the completion of a detailed application form for key employees with access to significant Personal Data and, where allowed by local law

    6.3. Periodic audits are conducted

    6.4. Implementation of processes that ensure that Personal Data is only processed as instructed by the Data Exporter, covering any sub-processors, including diligently selecting appropriate personnel and service providers and monitoring of contract performance, entering into appropriate data processing agreements with sub-processors, which include appropriate technical and organizational security measures.

7. Ensuring that Personal Data are protected against accidental destruction or loss (availability control); in particular, by taking the following measures:

    7.1. Backup procedures and recovery systems, redundant servers in separate location, mirroring of hard disks, uninterruptible power supply and auxiliary power unit, remote storage, climate monitoring and control for servers, fire resistant doors, fire and smoke detection, fire extinguising system, anti-virus/firewall systems, malware protection, disaster recovery and emergency plan.

8. Ensuring that data collected for different purposes or different principals can be processed separately (separation control); in particular, by taking the following measures:

    8.1. Internal client concept and technical logical client data segregation, development of a role based authorization concept, separation of test data and live data.

Additional provisions applicable to Sensitive Data or Special Category of Data:

N/A

[Exhibit B to the Data Processing Addendum]

Data Transfer Agreement

THIS DATA TRANSFER AGREEMENT ("**DTA**") is made by and between *Rakuten Group, Inc.*, a private company incorporated in *Japan* with its office located at *1-14-1 Tamagawa, Setagaya-ku, Tokyo, 158-0094* (the "**Data Exporter**") and *Host of travel-related products or services* in connection with the provision by the Data Exporter of the personal information (the "**Personal Information**") to the Data Importers, which are needed for implementing the business of Data Importers and/or Data Exporter.

1. Purpose of DTA

The purpose of DTA is to set forth the minimum requirements in order to comply with Article 24 of the Japanese Act on the Protection of Personal Information (the "**APPI**") regarding the transfer of "Personal Information" from Japan to a foreign country, excluding countries in the European Economic Area ("**EEA**"). Thus, the parties are separately required to abide by any other applicable laws in their jurisdictions, as necessary. In addition, the parties are required to comply with the terms and conditions of the *Host Terms and Conditions* Agreement and any other business agreements if they are executed between the parties. Where there are any discrepancies between such business agreements and DTA, in relation to the handling of the Personal Information, DTA shall prevail. No part of DTA shall be construed so as to obligate the Data Exporter to provide any personal information to the Data Importer.

2. Personal Information

Personal Information shall mean information about a living individual ("**Data Subject**") which can identify the specific individual by name, date of birth or other description contained in such information (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual). The Personal Information shall include, but not be limited to, the information which may be categorized in the items as listed in Schedule A attached hereto.

3. Obligations of the Data Exporter

The Data Exporter warrants and undertakes the following in accordance with the APPI.

3.1. It shall obtain or collect the Personal Information in an appropriate manner.

3.2. It shall promptly inform the Data Subject, or disclose to the public, the purposes of use of the Personal Information set out in the attached Schedule B (each a "**Purpose of Use**") and any other necessary information pursuant to the APPI. Where it is required under the APPI, it shall inform the same to the Data Subject before obtaining his/her Personal Information.

3.3. It shall disclose, correct, add to or delete the Personal Information at the request of the Data Subject in accordance with the APPI.

4. Obligations of the Data Importer

The Data Importer warrants and undertakes the following.

4.1. The Data Importer shall not use the Personal Information beyond the scope of the Purposes of Use and shall use the Personal Information only to the extent necessary to implement the Purposes of Use, without the prior written consent of the Data Exporter.

4.2. The Data Importer shall keep the Personal Information accurate and up-to-date within the scope necessary to achieve the Purpose of Use, and shall delete any Personal Information that no longer needs to be retained. For the avoidance of doubt, it is not necessary to delete Personal Information where the applicable law requires the Data Importer to keep it.

4.3. The Data Importer shall (i) establish basic policy and rules to the extent necessary for securing proper handling of Personal Information and (ii) have in place appropriate systematic, human, physical, and/or technical measures, to protect the Personal Information against accidental or unlawful destruction or accidental loss, alteration, and unauthorized disclosure or access, that provide a level of security appropriate to the risk represented by the processing and the nature of the Personal Information to be protected. In order to ensure implementation of DTA, it shall appoint an appropriately positioned person who can control the handling of the Personal Information, and shall inform the Data Exporter of the name, title and contact information of such person.

4.4. The Data Importer shall exercise the necessary and appropriate control and supervision over its officers and employees to ensure the safety of the Personal Information, as stated in Section 4.3 above. Where an officer or employee resigns from its position or upon request of the Data Exporter, it shall have such officer or employee execute a covenant to comply with all obligations of DTA (including but not limited to confidential obligations under Article 6), and shall take any additional necessary and appropriate measures to ensure compliance with DTA.

4.5. In the case where Data Importer entrust the handling of the Personal Information to a third party pursuant to this section, they shall exercise necessary and appropriate control and supervision over the entrustees to ensure the safety of such Personal Information, as stated in Section 4.3 above, and they shall require the entrustees comply with obligations equivalent to the obligations of the Data Importer under DTA, including the obligations in this section. The Data Importer shall be responsible for any breach by the entrustees (and any subsequent entrustee) of the obligations above. For clarity, this Section 4.5 shall apply to all third party entrustees and subsequent third party entrustees.

4.6. Except as permitted in Section 4.5 above, the Data Importer shall not transfer or disclose all or part of the Personal Information to a third party without the prior written consent of a relevant data subject.

4.7. To the extent required by the APPI, upon request of the Data Subject, the Data Importer shall disclose the information on the Personal Information stipulated under the APPI, including (i) the contents of the retained Personal Information; (ii)

the name of the Data Importer; (iii) the purpose of use of the Personal Information; (iv) the procedures for responding to a request for the Personal Information; and (v) the contact information Data Subjects should use to make claims regarding the handling of the Personal Information. The Data Importer shall promptly inform the Data Subject if it has determined it does not have to provide requested information on the contents and/or the purpose of use of the Personal Information.

4.8. To the extent required by the APPI, upon request of the Data Subject, the Data Importer shall correct, add, or delete certain Personal Information if the Data Subject can show the contents of the Personal Information are incorrect. The Data Importer shall promptly inform the Data Subject if it has corrected, added, or deleted Personal Information, or if it has determined it does not have to do so.

4.9. To the extent required by the APPI, the Data Importer shall delete or stop utilizing the Personal Information if the Data Subject can show that the Data Importer is using or has used such Personal Information outside of the designated Purpose of Use or if was acquired by improper means; provided, however, that it is not required where it would be unreasonably expensive or unreasonably difficult to do so and where alternative action which would protect the Data Subject's interests can be taken. The Data Importer shall promptly inform the Data Subject if it has deleted or stopped utilizing the Personal Information, or if it has determined it does not have to do so.

4.10. To the extent required by the APPI, the Data Importer shall stop providing Personal Information to a third party, if the Data Importer has provided it to a third party in violation of the restrictions related to the provisions of the Personal Information to a third party under the APPI; provided, however, that it is not required where would be unreasonably expensive or unreasonably difficult to do so and where alternative action which would protect the Data Subject's interests can be taken. The Data Importer shall promptly inform the Data Subject if it has stopped providing the Personal Information, or if it has determined it does not have to do so.

5. Data Breach and Unjust Use

If the Data Importer know or should know that the Personal Information has been or is likely to be leaked, disclosed, accessed, destroyed, altered, lost, used without authorization, or otherwise handled in any way not permitted under DTA, regardless of whether or not the Data Importer is liable for such incidents, the Data Importer shall immediately inform the Data Exporter of the same in writing, and shall take any appropriate measures to prevent such incident from occurring, expanding, and recurring.

6. Governing Law and Venue

DTA, and any disputes arising out of DTA, shall be governed by the laws of Japan. Both parties shall submit to the exclusive jurisdiction of the Tokyo District Court in the first instance in relation to any dispute arising out of or in connection with DTA or its subject matter, although the Data Exporter is also entitled to apply to any court worldwide for injunctive or other remedies.

Schedule A

The Personal Information shall include, but not be limited to, information which may be categorized as listed below.

Following user information:

name, email address, phone number, SNS account, credit card brand name, IP address, country of residence, nationality, passport information, age, date of birth, gender, accommodation information (name, address), driver's license copy, physical information required for the experience, height & weight, other hosts usage information (name, email address, phone number, and person in charge of travel experience providers), proof of travel cancellation(in case of disaster cancellation), vaccination certificate, certificate of negative test for covid-19.

Schedule B

The Purposes of Use of the Personal Information are as follows.

For the purpose of sharing user information necessary for hosts to provide services to users under Host Terms and Conditions.