DATA PROCESSING ADDENDUM

To

'Software as a Service' Agreement

Last Updated: 16th August 2022

This Addendum is supplemental to the 'software as a service' agreement ("**Agreement**") applicable to the Services and Software Product(s) provided to you ("**Licensee**") by Rakuten India Enterprise Private Limited ("**Licensor**").

This Addendum shall prevail in case of contradiction between this Addendum and the Agreement, the Order Form, or the Schedules to the Agreement. This Addendum shall be an integral part of the Agreement.

For purposes specific to this Addendum, the term "Licensee" shall refer to any and all participating affiliates, group companies, sister concerns, or any individual Users that the Licensee may permit to use the Services and Software Product(s). Each party will comply with all applicable Data Protection Laws with respect to its performance under this Addendum.

Further, this Addendum shall apply in all cases of any access to or use of the Services and/or Software Product(s), including but not limited to any trials, proof-of-concept demonstrations, pilot demonstrations, or pre-purchase customisation usage.

1. Definitions

1.1 Capitalized terms used but not defined in this Addendum will have the meanings provided in the Agreement. The following defined terms are used in this Addendum:

(i) "**Addendum**" means the present document including all appendixes incorporated herein.

(ii) "**Data Protection Law(s)**" means privacy or data protection laws that apply to Personal Data processed by Licensee under this Addendum, including, but not limited to, the Information Technology Act 2000 (**"IT Act"**), Regulation (EU) 2016/679 ("**GDPR**"), the California Consumer Privacy Act, as amended ("**CCPA**"), and the Act for the Protection of Personal Information of Japan ("**APPI**"), and any successor(s) thereto.

(iii) "**Effective Date**" shall mean the date on which the Agreement or respective Order Form is signed by the Parties.

(iv) "**Personal Data**", "**Process/Processing**", "**Controller**", "**Processor**", "**Data Subject**", **"Sensitive Data"** or **"Special Category Data"** and "**Supervisory Authority**" shall have the same meanings given to them in the GDPR (or where the same or similar terms are used under another applicable Data Protection Law, the meanings given to such terms under such Data Protection Law). For the sake of clarity, "**Process/Processing**" shall include, inter alia, collection, use, combination, and disclosure of Personal Data; Controller shall include business under CCPA; and Processor shall include service provider under CCPA.

(v) "**Rakuten Group**" means the international group of companies over which Rakuten Group Inc., a company incorporated in Japan with its place of business at 1-14-1 Tamagawa, Setagaya-ku, Tokyo 158-0094, Japan has control, by direct or indirect ownership or control of more than 50% of the voting interests of the subject company.

(vi) "**BCR**" means Binding Corporate Rules implemented by the Licensor, as enforced by the Rakuten Group of companies, which latest version shall apply at all times.

(vii) "**Standard Contractual Clauses**" means the Standard Contractual Clauses for the Transfer of Personal Data to Third Countries approved by EC Commission Decision of 4 June 2021 (Commission Implementing Decision (EU) 2021/914) or any successor thereto.

(viii) "**EEA**" means the European Economic Area.

(ix) "**Security Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

(x) "**Services**" shall broadly have the definition provided under the Agreement, however this Addendum shall be limited to those Services listed under Appendix C.

All other capitalised terms shall have the definitions provided under the Agreement (or its respective Schedules) or the Order Form.

2. Roles of the Parties

2.1 The Parties agree that regarding the Services and Software Product(s), Licensor is a Processor whenever Licensee is a Controller, and Licensor is a sub-Processor whenever Licensee is a Processor. For clarity, and subject to clauses 2.3 and 2.4 below, Licensor shall not be deemed a Controller.

2.2 Licensor will Process Licensee's Personal Data only: (i) on behalf of Licensee and in compliance with its lawful and documented instructions, within the scope and for the specific purpose of performing the Services, (ii) to perform its contractual obligations as described in clause 2.3 below**,** (iii) as required under applicable law or a valid and binding order of a law enforcement agency, subpoena or court order, in which case it shall notify Licensee as soon as that law permits and unless prohibited from doing so, and (iv) to fulfil Licensor's legitimate business interest as described in clause 2.4 below.

2.3 The Parties agree that pursuant to clause 2.2, Licensor may Process Licensee's account information as a Controller for the purpose of performing its contractual obligations towards Licensee and complying with related legal obligations to which Licensor is subject.

2.4 The Parties agree that pursuant to clause 2.2, Licensor may Process Licensee's Personal Data as a Controller for the following purposes, in furtherance of its legitimate business interests: (i) detecting security incidents, (ii) protecting Licensor, Licensee, and other users of the Services or Software Product(s) against fraudulent or illegal activity, (iii) exercising Licensor's legal rights, (iv) improving stability and performance of the Services or Software Product(s), (v) improving existing features or developing new features within or outside the scope of the Services or Software Product(s), provided that Licensor shall not use Licensee's Personal Data for profiling or advertising, combine it with any other data sourced from third parties except for a business purpose expressly permitted by applicable Data Protection Law, nor shall Licensor sell or make available such Personal Data to third parties for monetary or other valuable consideration. When acting as a Controller, Licensor shall not Process Licensee's Personal Data for any other purpose.

3. Licensee's Instructions

3.1 The Parties agree that the following instructions constitute Licensee's complete and final documented instructions: (i) the terms of the Agreement including this Addendum and any applicable Order Form, and (ii) Licensee's use or setting of, as well as actions within, the Services and/or Software Product(s). Any other instruction will be deemed as attempted instruction, and must be agreed on between the Parties, including an agreement on any additional fees payable by Licensee to Licensor for carrying out such

instructions.

4. Details of the Processing Activities

4.1 The details of the Processing activities to be carried out by Licensor on behalf of Licensee are specified in **Appendix A** to this Addendum.

5. Obligations of Licensor

5.1 Licensor warrants and undertakes that:

(i) it will have in place and will maintain appropriate technical and organisational security measures to protect Licensee's Personal Data which is transferred for the purpose of performing the works under the Agreement against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and in particular, where the Processing involves the transmission of data over a network, against all other unlawful forms of Processing, which technical and organisational security measures shall include at a minimum those listed in Appendix B. Having regard to the state of the art and cost of their implementation, Licensor agrees that such measures shall provide a level of security appropriate to the risk represented by the Processing and the nature of Licensee's Personal Data to be protected;

(ii) it will have in place procedures so that any third party it authorises, to the extent permitted by this Addendum, to have access to Licensee's Personal Data, including its sub-Processors, will respect and maintain the confidentiality and security of Licensee's Personal Data;

(iii) it will identify to Licensee a contact point within its organisation authorised to respond to enquiries concerning Processing of Licensee's Personal Data;

(iv) it will cooperate in good faith with Licensee concerning all enquiries from Licensee, Data Subjects or a Supervisory Authority regarding the Processing of Licensee's Personal Data within a reasonable time;

(v) it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from Licensee and its obligations under the Agreement and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by this Addendum, it will promptly notify the change to Licensee as soon as it is aware, in which case Licensee is entitled to suspend the transfer of data and/or terminate the Agreement regarding the relevant Services as per clause 12;

(vi) it will notify Licensee without undue delay if it becomes aware of:

(a) any legally binding request for disclosure of Licensee's Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(b) any actual Security Breach concerning Licensee’s Personal Data Processed by Licensor or a sub-Processor; or

(c) any complaint, communication or request received directly by Licensor or a sub-Processor from a Data Subject, in which case it shall provide Licensee with full co-operation and assistance in relation to any such complaint or request;

(vii) upon discovery of any Security Breach, it shall:

(a) take action without undue delay to prevent any further Security Breach; and

(b) provide Licensee with full and prompt cooperation and assistance in relation to any notifications that Licensee may be required to make as a result of the Security Breach;

(viii) it shall ensure all employees (and, to the extent permitted under this Addendum, agents or sub-Processors) are informed of the confidential nature of Licensee's Personal Data and are obliged to keep such Licensee's Personal Data confidential; have undertaken training relating to handling Personal Data; and are aware both of Licensor's duties and their personal duties and obligations under this Addendum;

(ix) it shall not disclose Licensee's Personal Data without prior instruction or the written consent of Licensee, except (i) to the extent required to provide the Services or any Associated Service, to those of its employees or sub-Processors who are engaged in the Processing of the Personal Data and are respectively subject to clause 5(h) above and clause 7 below, (ii) as strictly necessary to comply with the law or a valid and binding order of a governmental body, or (iii) as otherwise provided for in this Addendum; and

(x) it will provide Licensee with full and prompt cooperation and assistance in relation to any data protection impact assessment or regulatory consultation that Licensee is legally required to make in respect of Licensee's Personal Data.

6. Obligations of Licensee

6.1 Licensee warrants and undertakes that:

(i) Licensee's instructions comply with applicable Data Protection Laws;

(ii) it will, in its use of the Services, Process Personal Data in accordance with the requirements of applicable Data Protection Laws;

(iii) it will, to the extent required by applicable Data Protection Laws, provide notice and disclose to Data Subjects or Controllers of the use of Licensor as a Processor or sub-Processor;

(iv) it will, to the extent required by applicable Data Protection Laws, provide notice to Data Subjects of the Processing activities carried out by Licensor in its capacity of Controller for the purposes described in clauses 2.3 and 2.4;

(v) it will notify Licensor without undue delay if it becomes aware of any complaint, communication or request received directly or indirectly by Licensee from a Data Subject regarding Processing activities carried out by Licensor in its capacity of Controller for the purposes described in clauses 2.3 and 2.4, and will direct said Data Subject to Licensor without adding further to that response;

(vi) it will identify to Licensor a contact point within its organisation authorised to receive and follow up on notifications concerning Processing of Licensee's Personal Data; and

(vii) in any instance where Licensee acts as a Processor, Licensee's instructions, including appointment of Licensor as sub-Processor, have been duly authorized by the relevant Controller.

7. Subcontracting to Sub-Processors

7.1. Licensee grants Licensor a general authorization to use sub-Processors to fulfil its obligations under this Addendum. Licensor maintains at all times a current list of sub-Processors that are engaged by Licensor to Process Licensee's Personal Data on behalf of Licensee regarding the Services. Licensor shall make this list available upon request from Licensee via the Service, or to any other address as duly notified to Licensee.

7.2. To the extent reasonable, where Licensor subcontracts its obligations under this Addendum regarding Processing of Licensee's Personal Data, it shall do so only by way of a written agreement with the sub-

Processor, which imposes the same obligations on the sub-Processor as are imposed on Licensor under this Addendum, including but not limited to the present clause.

7.3. Where required under applicable Data Protection Law, Licensor shall provide a copy of such a sub-Processor agreement and any subsequent amendments to Licensee at Licensee's request. To the extent necessary to protect business secret or other confidential information, including Personal Data, Licensor may redact the text of the agreement prior to sharing the copy.

8. International Data Transfers

8.1 Licensor maintains at all times a current list of countries where Licensee's Personal Data are Processed. Licensor shall make this list available upon request from Licensee via the Service, or to any other address as duly notified to Licensee.

8.2 Where Licensor Processes Licensee's Personal Data within the Rakuten Group, Licensor represents and warrants that it will comply with the BCR to safeguard any international transfers to the extent required by applicable Data Protection Laws.

8.3 Where Licensor entrusts a sub-Processor with Licensee's Personal Data outside of the Rakuten Group, Licensor represents and warrants that Licensor and sub-Processor will implement appropriate safeguards to ensure a level of data protection of Licensee's Personal Data essentially similar to that provided under applicable Data Protection Laws (including, inter alia, by entering into the Standard Contractual Clauses) or this Addendum, whichever level of data protection is higher.

8.4 Where applicable, the Licensor agrees to abide by and process Personal Data originating from (i) the EU/EEA; and (ii) the United Kingdom, in accordance with the Standard Contractual Clauses. For clarity, the Standard Contractual Clauses shall apply as follows:

(i) The Licensee is the "data exporter" and the Licensor is the "data importer".

(ii) The applicable and governing Data Protection Law(s) shall be where the data exporter is established;

(iii) Appendix A of this Addendum shall be incorporated fit the information required under Appendix 1 to the Standard Contractual Clauses;

(iv) Appendix B of this Addendum shall be incorporated to fit the information required under Appendix 2 to the Standard Contractual Clauses.

8.5 In the event that the Standard Contractual Clauses no longer apply or are no longer accepted as a valid mechanism for international transfer, the Parties shall ensure that any further transfer of Personal Data from the data exporter shall be performed in accordance with Data Protection Law(s).

9. Audit

9.1 Without prejudice to the rights and obligations laid down in the Standard Contractual Clauses (as applicable), and any other prerogatives of a Supervisory Authority under applicable Data Protection Law, Licensee instructs Licensor to carry out audits as described in clauses 9.2 to 9.6, provided such audit is required or mandated under applicable Data Protection Law(s).

9.2 Licensor shall make available to Licensee and maintain at all times a standard documentation for Licensee to reasonably ascertain that Licensor is complying with its obligations as a Processor under this Addendum. This documentation is available on request from Licensee via the Service, or any other address as duly notified to Licensee. Licensee understands that some of the requested documentation may only be provided pursuant to Licensee signing a non-disclosure agreement specific to this request.

9.3 If, following a full review of the documentation provided under clause 9.2, Licensee wishes to conduct an in-person and on-site audit, Licensee is entitled, on giving at least 60-day notice to Licensor and subject to signing a non-disclosure agreement, to appoint representatives composed of Licensee employees that have an appropriate level of expertise and qualification in the subject matter to perform the audit, and/or independent members in possession of the required professional qualifications bound by a duty of confidentiality, to inspect all facilities, equipment, documents and electronic data relating to the Processing of Licensee's Personal Data by Licensor, to audit that Licensor is complying with its obligations as a Processor under this Addendum.

9.4 Licensor shall under no circumstances provide Licensee with the ability to audit any portion of the Services which would (i) be reasonably expected to compromise the confidentiality or security of the Personal Data that the Licensor Processes for its other licensees; or (ii) impact the services in any manner, including those rendered to the Licensee; or (iii) be digitally or physically impossible to conduct, or requires more than reasonable effort or time to conduct.

9.5 Licensee may exercise its audit right at reasonable intervals and no more than once per calendar year, or if there are indications of non-compliance with this Addendum, and only during business days and hours of the relevant location of the facilities, equipment, documents or data that are audited. Licensee shall reimburse the Licensor for its time and efforts expended in connection with an audit based on market rates for similar services, which shall be made available to Licensee upon request and shall be reasonable taking into account the time and effort required by Licensor.

9.6 Licensor shall allow and contribute to audits, at its own discretion, in English, Japanese and/or the official language of the relevant location of the facilities, equipment, documents or data that are audited.

10. Limitation of Liability

10.1 The Parties acknowledge that, to the extent permissible by law, any limitation of liability in the Agreement shall also apply to any liabilities arising out of any breach of this Addendum or any failure to comply with any of the obligations under this Addendum by Licensor or its employees or sub-Processors.

10.2 Clause 10.1 is without prejudice to the right of Data Subjects to seek compensation against one or more of the Parties under the Standard Contractual Clauses. If one Party is held liable under this clause, it shall be entitled to claim back from the other Party that part of the compensation corresponding to its responsibility for the damage and within the limits set in clause10.1.

11. Allocation of Costs

11.1 Excluding clause 9, each Party shall perform its obligations under this Addendum at its own cost.

12. Term, Suspension and Termination

12.1 This Addendum shall be effective from the Effective Date and as long as the Services are used.

12.2 In the event that the Agreement terminate for any reason, this Addendum shall be immediately terminated, except as to those provisions of this Addendum that survive termination.

12.3 In the event that:

(i) Licensor is in breach of its obligations under this Addendum, or the Agreement; or

(ii) Licensee receives a notification from Licensor that compliance by Licensor with this Addendum would put it in breach of its legal or regulatory obligations in one of the countries where Licensor operates;

then Licensee may temporarily suspend the transfer of Licensee's Personal Data to Licensor until the breach is cured.

12.4 In the event that the Licensor is in substantial or persistent breach of any warranties or undertakings given by it under this Addendum, then the Licensee, without prejudice to any other rights which it may have against LLicensor, shall be entitled to terminate the Agreement regarding the relevant Services.

13. Obligations after the Termination of Personal Data Processing Services and/or this Addendum

13.1 Except for Processing activities and purposes described in clause 2, the Parties agree that upon termination of this Addendum, upon written request of the Licensee:

(i) the Licensor and its sub-Processors shall cease Processing the Licensee‘s Personal Data and, Licensee shall instruct Licensor within 90 days to either (i) return all Licensee's Personal Data and the copies thereof, even if the data is anonymized, to Licensee, or (ii) securely delete all Licensee‘s Personal Data. In any event, and unless specifically agreed otherwise between the Parties in a written agreement, Licensee's Personal Data shall be securely and irretrievably deleted at the end of the 90-day period;

(ii) when Data Protection Laws or any other laws applicable to Licensee's Personal Data or other laws imposed on Licensor and its sub-Processors prevents them from returning or deleting all or part of Licensee's Personal Data, Licensor warrants that it will guarantee the confidentiality of Licensee's Personal Data, and will not actively Process Licensee's Personal Data transferred anymore; and

(iii) upon request, Licensor shall confirm to Licensee that it has complied with the instructions set forth in this clause 13.

13.2 The provisions of this Addendum shall survive termination until Licensee's Personal Data are deleted or returned.

14. Governing Law and Jurisdiction

14.1 This Addendum shall be governed by the law of and submitted to the exclusive jurisdiction of the courts of the country provided in the Agreement.

Appendix A | Details of the Processing

The subject-matter of the processing: Personal Data Processed by the Licensor under this Addendum, for the provision of Services under the Agreement.

The duration of the processing: For the period that the Agreement is in force.

The nature and purpose of the processing: The provision of the Services by Licensor to the Licensee, as detailed in the Agreement. These Services may include the processing of Personal Data by the Licensor, as determined by the Licensee in its use of the Services.

The types of personal data: Personal Data that is submitted to the Services by the Licensee, which may include authorised Users full names, login details (username and password), registered e-mail addresses, IP addresses, contact number, and any other types of identifiable data that is configured by the Licensee in its use of the Services.

Special categories of personal data: No special categories of personal data.

The categories of data subjects: Authorised Users of the Services, and any data subjects that interact with the Services, the Software Product(s) or any other products and services offered by the Licensor.

Appendix B | Technical, Physical and Organisational Security Measures

This Appendix B summarizes the technical, organisational and physical security measures implemented by the parties in accordance with clause 5(a).

In addition to any data security requirements set forth in the Agreement, Licensor shall comply with the following:

Licensor 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:*
    - Controlled access for critical or sensitive areas
    - Video monitoring in critical areas
    - Incident logs
    - Implementation of access control systems
    - Monitoring facilities (e.g. alarm device, video surveillance)
    - Logging of visitors
    - Security awareness training
2. *Preventing data processing systems from being used without authorisation (logical access control); in particular, by taking the following measures:*
    - Network devices such as intrusion detection systems, routers and firewalls
    - Secure log-in with unique user-ID/password
    - Logging and analysis of system usage
    - Role-based access for critical systems containing personal data
    - Process for routine system updates for known vulnerabilities
    - Hardening of devices
    - Monitoring for security vulnerabilities on critical systems
    - Deployment and updating of antivirus software
    - Individual allocation of user rights, authentication by password and username, use of smartcards for access premises, minimum requirements for passwords, password management, blocking of external ports (such as USB ports), encryption of critical data, virus protection and use of firewalls, and 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:*
    - Network devices such as intrusion detection systems, routers and firewalls
    - Secure log-in with unique user-ID/password
    - Logging and analysis of system usage
    - Role based access for critical systems containing personal data
    - Hardening of devices
    - Deployment and updating of antivirus software
    - Definition and management of role-based authorization, 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 critical data, secured data transfers and intrusion detection systems.
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:*
    - Encryption or securing of communication, implementation of virtual private networks, firewall, hardening of devices.
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:*
    - Logging and analysis of system usage
    - Role based access for critical systems containing personal data
    - 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:*
    - Mandatory security and privacy awareness training for all employees

- Employee hiring procedures which require the completion of a detailed application form for key employees with access to significant personal data and, where necessary under local laws
- Periodic audits are conducted
- 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 peformance, 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:*
    - Backup procedures and recovery systems, business continuity plans, 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:*
    - Internal client concept and technical logical client data segregation, development of a role based authorization concept, separation of test data and live data.

Appendix C | List of Services

This Appendix C lists the services to which the Addendum applies:

- Rakuten SixthSense Observability
- Test Acceleration Platform (TAP)
- Incident Management (Buzzr)

The applicability of this Addendum shall extend to any and all cases of access to or use of the Services listed above, including but not limited to any trials, proof-of-concept demonstrations, pilot demonstrations, or pre-purchase customisation usage.