

Data Processing Addendum

(to 'Software as a Service' Agreement)

Updated on: 11th April 2025

This Addendum is supplemental to the 'software as a service' agreement ("**Agreement**") applicable to the Services and Software Product(s). 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.

This Addendum does not apply to contact details exchanged by the Parties for the purpose of establishing contact for the purpose of demonstrating the Services and Software Product(s). Such contact details may include business emails and phone numbers. For avoidance of doubt, such contact details shall be considered "confidential information".

1. DEFINITIONS

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:

- (a) "**Addendum**" means the present document including all appendixes incorporated herein.
- (b) "**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**"), the Digital Personal Data Protection Act 2023 ("**DPDP Act**"), Regulation (EU) 2016/679 ("**GDPR**"), the UK Data Protection Act ("**UK DP Act**") 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.
- (c) "**Effective Date**" shall mean the date on which the Agreement or respective Order Form is signed by the Parties.
- (d) "**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.
 - "**Data Fiduciary**", "**Data Processor**", "**Data Principal**" and "**Data Protection Board**" used in the context and applicability of Indian laws shall have the meanings provided under the DPDP Act and relevant rules thereunder.
- (e) "**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.

- (f) **"Rakuten BCRs"** means Binding Corporate Rules implemented by the Licensor, as enforced by the Rakuten Group of companies, which latest version shall apply at all times.
- (g) **"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.
- (h) **"EEA"** means the European Economic Area.
- (i) **"Security Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.
- (j) **"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, the Licensor shall not be deemed a Controller of the Licensee's Personal Data.
- 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 for the purpose of performing its contractual obligations towards Licensee and complying with related legal obligations to which Licensor is subject. Such performance of contractual obligations shall be subject to appropriate notification to the Licensee, where reasonable.
- 2.4. The Parties agree that pursuant to clause 2.2, Licensor may Process Licensee's Personal Data for the following additional purposes: (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 nor shall Licensor sell or make available such Personal Data to third parties for monetary or other valuable consideration. Other than as detailed under this Addendum, the Licensor shall not Process Licensee's Personal Data for any other purpose.
- 2.5. The Licensee will ensure that the personal data it provides to the Licensor has a valid lawful basis for processing. The Licensor shall not be responsible for the determination of lawful basis or management of data subject consents.

3. LICENSEE'S INSTRUCTIONS

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

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

Licensor warrants and undertakes that:

- (a) 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 Error! Reference source not found. **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;
- (b) 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;
- (c) it will identify to Licensee a contact point within its organisation authorised to respond to enquiries concerning Processing of Licensee's Personal Data;
- (d) 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;
- (e) 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;
- (f) it will notify Licensee without undue delay if it becomes aware of:
 - 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;
 - any actual Security Breach concerning Licensee's Personal Data Processed by Licensor or a sub-Processor; or
 - 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;
- (g) upon discovery of any Security Breach, it shall:
 - take action without undue delay to prevent any further Security Breach; and
 - 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;
- (h) 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;

- (i) 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
- (j) 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

Licensee warrants and undertakes that:

- (a) Licensee's instructions comply with applicable Data Protection Laws;
- (b) it will, in its use of the Services, Process Personal Data in accordance with the requirements of applicable Data Protection Laws;
- (c) 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;
- (d) 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;
- (e) 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;
- (f) 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
- (g) 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

- (a) Unless prohibited by law, Licensee agrees that the Licensor may transfer Licensee's Personal Data outside the country of origin to other geographic territories as necessary to provide the Services. In case of cross-border transfer of Licensee's Personal Data, the Licensor shall implement appropriate safeguards for the transfer to that territory in compliance with Data Protection Laws.
- (b) Where Licensor Processes Licensee's Personal Data within the Rakuten Group, Licensor represents and warrants that it will comply with the Rakuten BCRs to safeguard any international transfers to the extent required by applicable Data Protection Laws.
- (c) 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.
- (d) ***The following sub-clause is applicable only to cross-border transfer of Personal Data from the EEA:*** Licensor and Licensee agree that if the GDPR protects the transfer of Licensee's Personal Data, if the transfer is from the Licensee located within the EEA to the Licensor (outside of the EEA), and if the transfer is not governed by an adequacy decision made by the European Commission, then by entering into this Addendum, Licensee and Licensor are deemed to have signed the SCCs and their Annexes, which are incorporated by reference. Any such transfer of Personal Data is made pursuant to the SCCs, which are completed as follows:
- i. Module Two (Controller to Processor) of the SCCs apply when Licensee is a Controller and Licensor is processing Personal Data for the Licensee as a Processor.
 - ii. Module Three (Processor to Sub-Processor) of the SCCs apply when Licensee is a Processor and Licensor is processing Personal Data on behalf of Licensee as a Subprocessor.
 - iii. For each module, the following applies (when applicable):
 - The optional docking clause in Clause 7 does not apply;
 - In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of Subprocessor changes is 30 days;
 - In Clause 11, the optional language does not apply;
 - All square brackets in Clause 13 are removed;
 - In Clause 17 (Option 1), the SCCs will be governed by the laws of Governing Member State;
 - In Clause 18(b), disputes will be resolved in the courts of the Governing Member State; and
 - Appendix A of this Addendum contains the information required in Annex I, Annex II, and Annex III of the SCCs.
- (b) ***The following sub-clause is applicable only to cross-border transfer of Personal Data from the United Kingdom:*** Licensor and Licensee agree that if the UK DP Act protects the transfer of Licensee's Personal Data, if the transfer is from the Licensee located within the United Kingdom to the Licensor (outside of the United Kingdom), and if the transfer is not governed by an adequacy decision made by the United Kingdom Secretary of State, then by entering into this Addendum, Licensee and Licensor are deemed to have signed the international data transfer addendum to the EEA SCCs issued by the United Kingdom's Information Commissioner for Parties making Restricted Transfers under S119A(1) of the UK DP Act ("**UK Addendum**"), including any annexes thereto, which are incorporated by reference. Any such transfer of Personal Data is made pursuant to the UK Addendum, which are completed as follows:
- i. Clause 8(d) of this Addendum contains the information required in Table 2 of the UK Addendum.

- ii. Table 4 of the UK Addendum is modified as follows: Neither party may end the UK Addendum as set out in Section 19 of the UK Addendum; to the extent that the Information Commissioner's Office issues a revised Approved Addendum under Section 18 of the UK Addendum, the parties will work in good faith to revise this Addendum accordingly.
- iii. Appendix A of this Addendum contains the information required by Annex 1A, Annex 1B, Annex II, and Annex III of the UK Addendum.

9. AUDITS

- 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 Licensors 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. Licensors shall make available to Licensee and maintain at all times certification or standard documentation for Licensee to reasonably ascertain that Licensors are complying with its obligations as a Processor under this Addendum. This documentation is available on written request made by 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 audit for compliance with this Addendum, Licensee is entitled, on giving at least 90-day notice to Licensors 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 relevant equipment, documents and electronic data relating to the Processing of Licensee's Personal Data by Licensors, to audit that Licensors are complying with its obligations as a Processor under this Addendum.
- 9.4. Licensors 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 Licensors Process 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. Licensee agrees that Licensors may restrict access to data or information if Licensee's access to the information would negatively impact Licensors' intellectual property rights, confidentiality obligations, or other obligations under applicable law.
- 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 equipment, documents or data that are audited. Licensee shall reimburse the Licensors 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 Licensors.
- 9.6. Licensors shall allow and contribute to audits, at its own discretion, in English, Japanese and/or the official language of the relevant location of the 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 Licensors or its employees or sub-Processors.
- 10.2 Article 10.1 is without prejudice to the right of Data Subjects within the EEA and United Kingdom to seek compensation against one or more of the Parties. 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 article 10.1.

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

- (a) By executing or entering into the Agreement, Licensor and Licensee are deemed to have signed this Addendum. The term of this Addendum will start on the effective date of the Agreement and will continue until the Agreement expires or is terminated.
- (b) 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.
- (c) In the event that:
 - Licensor is in breach of its obligations under this Addendum, or the Agreement; or
 - 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.

- (d) Where Data Protection Laws (including the DPDP Act) mandate Personal Data retention and deletion timelines on the Data Controller or Data Fiduciary, the Licensee notify in writing such deletion timelines to the Licensor, with advance notice that is commercially and technologically reasonable to verify and/or certify Personal Data deletion in accordance with the relevant Data Protection Laws. Licensee acknowledges and agrees that Licensor will not be liable for any delay in such Personal Data deletion arising from the Licensee's failure to notify the Licensor in accordance with this sub-clause.
- (e) 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.
- (f) Licensor and Licensee will each remain subject to the obligations in this Addendum and Data Protection Laws until Licensee stops transferring Personal Data to Licensor, and Licensor stops processing Personal Data.

13. OBLIGATION AFTER THE TERMINATION OF PERSONAL DATA PROCESSING SERVICES OR THIS ADDENDUM

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:

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

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

14. GOVERNING LAW AND JURISDICTION

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, subject to jurisdiction enumerated under Data Protection Laws.

15. Modifications

Licensor may change or update this Addendum in the following instances: (a) where the change is required to comply with Data Protection Laws or any other applicable laws; or (b) where the change is required for Licensor's operational purposes, but does not impact Service provision or have a material impact on the Personal Data processing obligations of the Licensor, including any Data Subject rights.

APPENDIX A

DETAILS OF THE PROCESSING

A. Parties

Data Exporter:

Name: Licensee

Address: Address provided by Licensee in Agreement.

Contact person's name, position, and contact details: Contact details provided by Licensee in Agreement.

Activities relevant to the data transferred under these Clauses: Processing of Personal Data to provide Services under the Agreement.

Signature and date: In accordance with clause 12(a) of this Addendum.

Role: Controller or Processor.

Data Importer:

Name: Rakuten India Enterprise Private Limited

Address: Address provided by Licensor in Agreement.

Contact person's name, position, and contact details: Contact details provided by Licensor in Agreement.

Activities relevant to the data transferred under these Clauses: Processing of Personal Data to provide Services under the Agreement.

Signature and date: In accordance with clause 12(a) of this Addendum.

Role: Processor or Subprocessor.

B. Transfer description

Categories of data subjects whose personal data is transferred: Authorised Users of the Services, and Licensee's employees, customers, vendors and end-users that interact with the Services, the Software Product(s) or any other products and services offered by the Licensor.

Categories of personal data transferred:

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.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: No sensitive or special categories of personal data are transferred. The nature of the Services does not require the collection or processing of any Special Categories of Personal Data, and the Licensor does not collect or otherwise require the Licensee to transfer such data. In the event that Special Categories of Personal Data are transferred or needed for processing under the Agreement, the Licensor will notify the Licensee of the processing and apply all necessary restrictions and safeguards that fully take into consideration the nature of the data and risks involved, including restrictions on onward transfers or additional security measures.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Continuous basis.

Nature of the processing: The Services as described in the Agreement and any ancillary activities to fulfil performance of the Agreement.

Purpose(s) of the data transfer and further processing: The provision of the Services by Licensor to the Licensee, as detailed in the Agreement. These Services may include the provision of support and maintenance, and improvements or updates to the Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: For the period that the Agreement and this Addendum are in force, and for the additional retention period detailed in clause 13 of this Addendum.

For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing: Licensee's Personal Data may be transferred to subprocessors to provide support services as required for the Services to be fulfilled.

C. Competant Supervisory Authority

Determined in accordance with Data Protection Laws.

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).

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:

Access control measures:

- Tenant-level access restrictions on processing systems.
- Restriction of access to Personal Data to employees with a defined role requiring the access on a need-to-know basis.
- Periodic provisioning and de-provisioning of accounts.
- Industry-standard employee authentication measures and password management.
- Secure login and account management by Licensee's users.

Data Security:

- Network devices such as intrusion detection systems, routers and firewalls.
- Process for routine system updates for known vulnerabilities.
- Hardening of devices and endpoint security management.
- Monitoring for security vulnerabilities on critical systems.
- Deployment and updating of antivirus software.
- Mandatory security and privacy awareness training for all employees.
- Supplementary measures where Personal Data is processed by any subprocessors, including monitoring of contract performance, entering into appropriate data processing agreements with sub-processors, and implementing appropriate technical and organizational security measures.

Cryptography:

- Encryption or securing of communication between public networks.
- Implementation of virtual privacy networks where necessary.
- Encryption controls for both 'data in transit' & 'data at rest'.

Security Testing and Audits

- Maintenance of SSAE 18 SOC 2 Type II or comparable certification for the Services.
- Maintenance of ISO/IEC 27001:2022 certification for the organization.
- Periodic penetration testing of Services and underlying infrastructure and timely resolution of vulnerabilities in accordance with internal vulnerability management policies.
- Periodic network vulnerability scans and redressal of findings based on criticality level.
- Periodic internal audits conducted in accordance with ISO/IEC 27001:2022 requirements.

Environment and Change Management

- Development, testing and production environments are segregated.
- Internal client concept and technical logical client data segregation.
- Processes for changes or updates to the Services and adhere with quality management standards.

Business Continuity for protection of Personal Data against accidental destruction or loss.

- Periodically tested backup procedures and recovery systems.
- Business continuity impact assessment and detailed plans for operational uptime.
- Anti-virus/firewall systems and malware protection
- Disaster recovery and emergency plans for systems and premises.

Corporate Security and Administrative Controls

- Implementation of access control systems across premises.
- Monitoring of facilities, including video surveillance and alarms.
- Logging of visitors and vendor personnel.
- Secure employee hiring procedures and disciplinary policies.

Risk Management

- Information Security Management Systems (ISMS) program reviewed periodically for compliance.
- Risk management programs and treatment plans reviewed based on risk severity, regulatory requirements, and impact to business.

Appendix C

List of Services

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

- SixthSense Observability
- SixthSense Data Observability
- SixthSense API Security
- SixthSense GenEYE
- SixthSense AIOps
- SixthSense Test Acceleration Platform