DATA PROCESSING ADDENDUM

1 GENERAL

1.1 This Data Processing Addendum sets out the terms that apply to the processing of Customer Personal Data by Keyloop in the provision of the Services. It forms part of the relevant Agreement between Keyloop and Customer.

1.2 The Privacy Hub provides further information regarding the way in which Keyloop processes Customer Personal Data.

2 DEFINITIONS AND INTERPRETATION

2.1 All capitalised terms in this Data Processing Addendum shall have the meaning given to them in the Agreement, unless otherwise defined below or in Appendix 1 to this Addendum.

2.2 The following words shall be given the following meanings in this Data Processing Addendum:

Agreement	the agreement between Customer and Keyloop for the provision of the Services, comprised of the Documentation;
Customer Personal Data	shall mean the personal data provided by Customer or Customer Affiliates to Keyloop, or which is otherwise processed by Keyloop on behalf of Customer or Customer Affiliates, pursuant to the Agreement;
Data Processing Particulars	the details regarding the processing of Customer Personal Data by Keyloop as shown in the Privacy Hub;
Data Protection Authority	a regulatory, administrative, supervisory authority or governmental agency, body or authority with jurisdiction over the personal data processing activities contemplated by this Data Processing Addendum;
Data Protection Legislation	means all applicable laws relating to the processing of personal data, in each case which are in force from time to time, such as (where relevant): (a) the EU GDPR; (b) the UK Data Protection Law;

(c) the German Data Protection Act 2018;

(d) the Portuguese data protection law comprising law no. 58/2019 of August 8, law no. 41/2004 of August 18;

(e) the Personal Information Protection and Electronic Documents Act (PIPEDA) and substantially similar Provincial laws;

(f) the Federal Law for the Protection of Personal Data in Possession of Private Parties in Mexico;

(g) the Personal Data Protection Act 2012 of Singapore;

(h) the Protection of Personal Information Act 4 of 2013 of South Africa

(i) the Federal Decree Law No. 45/2001 on the Protection of Personal Data in the United Arab Emirates;

(j) the Swiss Federal Act on Data Protection;

(k) the Personal Data Protection Act B.E. 2562 (A.D. 2019) and any regulation or announcement relating to the protection of personal data issued under such act in Thailand; and

(l) any further laws and statutory instruments relating to such regulations, data protection or privacy;

Data Recipient has the meaning given to it under clause 7.1;

EU GDPR the regulations on the protection of natural persons with regard to the processing of personal data and on the free movement of such data known as the General Data Protection Regulation (EU) 2016/679;

Privacy Hub means the Keyloop 'Privacy Hub' available at https://www.keyloop.com/legal-documentation;

Sub-Processor	any third party processor appointed by Keyloop, which may receive and/or have access to Customer Personal Data;
Transfer	shall mean the transfer, access or processing of Customer Personal Data to a Data Recipient;
UK Data Protection Law	comprises: (a) the EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 as modified by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019; (b) the UK Data Protection Act 2018; and (c) the Privacy and Electronic Communications Regulations 2003 as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 as modified by Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020.

2.3 Unless the context otherwise requires, the terms "**controller**", "**data subject**", "**personal data**", "**personal data breach**", "**processor**", "**processing**" and "**special categories of personal data**" are to be interpreted and construed by reference to Data Protection Legislation and "**process**" and "**processing**" shall have corresponding meanings.

3 DATA PROTECTION COMPLIANCE

3.1 The Parties acknowledge that, in relation to Customer Personal Data, Customer (or relevant Customer Affiliate) is a controller and Keyloop is a processor.

3.2 Keyloop shall process Customer Personal Data as set out in the Data Processing Particulars.

4 CUSTOMER OBLIGATIONS

4.1 Customer shall, and shall procure that Customer Affiliates shall:

4.1.1 ensure that it has, in accordance with Data Protection Legislation, (i) an appropriate lawful basis; (ii) obtained all necessary rights and consents from data subjects; and (iii) provided all appropriate notices in order to:

4.1.1.1 disclose Customer Personal Data to Keyloop; and

4.1.1.2 permit Keyloop to process Customer Personal Data as outlined in the Agreement, in accordance with Data Protection Legislation;

4.1.2 promptly provide assistance with responding to any enquiry made, investigation or assessment of processing under this Data Processing Addendum initiated by a Data Protection Authority;

4.1.3 provide Keyloop with documented written instructions as set out in the Agreement, regarding the processing of Customer Personal Data;

4.1.4 be responsible for responding to, and implementing appropriate measures to handle the exercise of data subject rights requests, and data subject access requests in line with Data Protection Legislation;

4.1.5 carry out all data protection impact assessments where required under Data Protection Legislation; and

4.1.6 at all times perform its obligations under this Data Processing Addendum in such a manner as to not cause Keyloop in any way to breach Data Protection Legislation.

5 KEYLOOP OBLIGATIONS

5.1 Keyloop shall:

5.1.1 and shall take reasonable steps to ensure that its Personnel shall process Customer Personal Data only for the limited purposes of carrying out the Agreement and on the documented written instructions of Customer as set out in the Agreement unless required to do otherwise by Applicable Law. In this case, Keyloop shall inform Customer of that legal requirement before processing, unless it is prohibited from doing so by Applicable Law. If Keyloop is aware that, or is of the opinion that, any instruction given by Customer breaches Data Protection Legislation, Keyloop shall inform Customer without undue delay where permitted to do so by Applicable Law;

5.1.2 ensure that Personnel who are authorised to process Customer Personal Data are under obligations of confidentiality that are enforceable by Keyloop or the relevant Sub-Processor;

5.1.3 taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for data subjects, implement appropriate technical and organisational measures to ensure a level of security appropriate to protect Customer Personal Data, including from accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access. The appropriate and technical, physical organisational measures implemented by Keyloop are listed in the Privacy Hub;

5.1.4 to the extent not possible through the functionality of the Products and in a manner consistent with Keyloop's role as a processor, assist Customer with responding to data subjects' rights requests, complying with Customer's obligations in relation to security, notification of breaches to data subjects and the Data Protection Authority, data protection impact assessments and any consultation with or request from the Data Protection Authority. In addition, Keyloop shall promptly inform Customer:

5.1.4.1 if it receives any data subject access request, or request by a data subject to transfer, rectify, erase, destroy or restrict Customer Personal Data; and

5.1.4.2 of any request for the disclosure of Customer Personal Data from a third party which Keyloop receives directly, and provide a copy of such request.

Keyloop shall not disclose or release any Customer Personal Data other than to Customer, except where required or permitted by Applicable Law;

5.1.5 upon request of Customer, return Customer Personal Data to Customer in a format which retains the integrity of Customer Personal Data or securely destroy or anonymise Customer Personal Data (including all copies of it) unless any Applicable Law requires Keyloop to continue to store Customer Personal Data, in which case Keyloop shall process such Customer Personal Data as Controller. On termination of the Agreement Customer and Keyloop shall remove and delete data as set out in clause 15.2 of the Master Terms;

5.1.6 upon request (but no more than once per year) provide Customer with a copy of an audit of Keyloop's compliance with this Data Processing Addendum. Where Customer determines, acting reasonably that such report is insufficient to evidence Keyloop's compliance, where it is reasonably practicable to do so Keyloop shall allow Customer (or its authorised representatives) reasonable access during normal Keyloop working hours at an agreed time to any relevant

premises and documents to inspect the procedures and measures referred to in this Data Processing Addendum. Customer shall not disrupt Keyloop's business as usual activities, Customer may only access resources that relate specifically to Customer Personal Data and Customer (or its representative) must sign a non-disclosure agreement before being permitted any access; and

5.1.7 use reasonable endeavours to notify Customer within 24 hours, and in any event without undue delay, after becoming aware of a personal data breach with respect to Customer Personal Data that is processed by, or on behalf of, Keyloop in connection with the Agreement.

5.2 Keyloop reserves the right to apply additional charges calculated at Standard Rates to provide the assistance and information described in clauses 5.1.6.

6 APPOINTMENT OF SUB-PROCESSORS

6.1 By entering into the Agreement, Customer authorises Keyloop's appointment of the Sub-Processors listed in the Privacy Hub.

6.2 Customer consents to Keyloop's alteration of Sub-Processors where the conditions under clause 6.3 to 6.5 have been satisfied.

6.3 Keyloop shall update the Privacy Hub to reflect the details of each Sub-Processor at least 30 days prior to such Sub-Processor's processing of Customer Personal Data. Customer may object to such change within the above mentioned time period where Customer believes, acting reasonably, that the Sub-Processor does not have technical and organisational measures or appropriate safeguards as required by this Data Processing Addendum or that the appointment of the Sub-Processor shall result in a failure to deliver the Services.

6.4 Keyloop shall inform Customer if the Privacy Hub is updated pursuant to clause 6.3.

6.5 Keyloop shall put in place with any Sub-Processor, written contractual obligations which are: (a) at least equivalent to the obligations imposed on Keyloop pursuant to this Data Processing Addendum; and (b) compliant with Data Protection Legislation. Subject to any applicable confidentiality obligations, on written request from Customer Keyloop shall provide written excerpts of Sub-Processor contractual obligations.

6.6 As between Keyloop and Customer, Keyloop shall remain liable for any Sub-Processor's failure to comply with such equivalent data protection obligations.

7 CROSS-BORDER TRANSFERS

7.1 Subject to compliance with clause 7.2, Keyloop (and its Sub-Processors) may Transfer Customer Personal Data to recipients based inside or outside of the Territory, including inside or outside of the European Economic Area (EEA), United Kingdom (UK), Switzerland or any territory deemed to be adequate by the European Commission, the UK or Swiss Governments (as the case may be).

7.2 Keyloop shall carry out the Transfer in accordance with Data Protection Legislation. Such safeguards may include reliance on an adequacy decision made by a Data Protection Authority or under a contract that includes model clauses obliging the Sub-Processor in the relevant territory to implement the provisions, measures, controls and requirements set out in the relevant Data Protection Legislation and/or the completion of a data transfer assessment as required by Data Protection Legislation.

8 CONTACT DETAILS

Customer may contact Keyloop relating to any data protection queries at DPO@keyloop.com.

APPENDIX 1

Territory Specific Terms

1. South Africa

1.1. Any reference to 'controller' in the Data Processing Addendum shall include within its ambit the term 'responsible party' and each reference to a 'processor' shall include within its ambit the term 'operator' and reference to the term 'personal data' shall include within its ambit the term 'personal information' as such terms are defined as follows:

1.1.1. ''responsible party" means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

1.1.2. "operator" means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party; and

1.1.3. "personal information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.

2. Kingdom of Saudi Arabia

2.1. For the purposes of this paragraph, Keyloop is referred to as the 'Personal Data Importer' and Customer is referred to as the 'Personal Data Exporter'. In the event of any discrepancy between this paragraph and any other provision in the relevant Agreement between Keyloop and Customer, to the extent that the discrepancy relates to the international transfer of personal data collected from the Kingdom of Saudi Arabia, the terms of this paragraph shall take precedence

2.2. The following terms shall have the meanings assigned to each of them below:

Implementing Regulations	the Implementing Regulations of the Law "Includes both of the implementing Regulations and the implementing Regulation for Personal Data Transfer outside the Kingdom";
Technical and Organisational Measures Document	The document with the same name shown which is available in the Privacy Hub;

The Kingdom	The Kingdom of Saudi Arabia (KSA);
The Law	The Personal Data Protection Law (PDPL) issued by Royal Decree No. (M/19) dated 9/2/1443 AH and amended by Royal Decree No. (M/148) dated 5/9/1444 AH;
The Competent Authority	Saudi Data & AI Authority (SDAIA);
Appropriate Safeguards	The requirements imposed by the competent authority on controllers, which include adherence to the Law and Regulations when transferring or disclosing personal data to entities outside the Kingdom. This applies in cases where exemptions are granted from the conditions for providing an appropriate or minimum level of personal data protection, to ensure appropriate level of protection when transferring personal data outside the Kingdom that meets at least the standards prescribed by the Law and Regulations;
Transfer of Personal Data	Transfer, disclosure (or granting of access) of Personal Data from the Kingdom of Saudi Arabia to Controllers, Processors, or other recipients in countries or international organizations other than the Kingdom of Saudi Arabia where neither the Personal Data Exporter nor the Importer of the Personal Data.

2.3. Processing Instructions. The Personal Data Importer shall only process the transferred Personal Data based on written instructions from the Personal Data Exporter. Accordingly, if the Personal Data Importer is unable to follow the instructions, it shall inform the Personal Data Exporter in writing without undue delay.

2.4. Processing Restrictions. The Personal Data Importer shall process the transferred Personal Data in accordance with the purposes specified in the Data Protection Particulars, unless otherwise directed in writing by the Personal Data Exporter, provided that the Personal Data shall be processed in accordance with the provisions of the Law and its Implementing Regulations in all cases.

2.5. Compliance with the Requests of the Competent Authority. (a) In order for the Competent Authority to exercise its powers under the Law and the Implementing Regulations, the parties shall provide a copy of these Clauses to the Competent Authority upon request and without undue delay. The Competent Authority may request any additional information in relation to transfers of Personal Data. (b) Each party agrees to comply with any requests made by the Competent Authority in relation to these Clauses or the processing of the Transferred Personal Data. (c)

Upon request, the Personal Data Importer (either directly or through the Personal Data Exporter) shall disclose its identity and contact details and the categories of Personal Data being processed to the Personal Data Subject and provide a copy of these items.

2.6. Accuracy and Quality of Personal Data. If The Personal Data Importer realises that any Personal Data transferred is inaccurate or not up-to-date, it shall inform the Personal Data Exporter in writing without undue delay, in which case the Personal Data Importer shall destroy the Personal Data and notify the Personal Data Exporter accordingly, unless the Personal Data Exporter is instructed not to destroy the data because it wishes to correct the transferred Personal Data.

2.7. Duration of Personal Data Processing and Destruction or Recovery. (a) The processing shall be carried out by the Personal Data Importer only for the period during which relevant Services are provided. After completion of the purpose of the processing, the Personal Data Importer shall destroy all Personal Data processed on behalf of the Personal Data Exporter and notify the Personal Data Exporter accordingly unless otherwise instructed by the Personal Data Exporter in the following cases: (i) Return all processed Personal Data to the Personal Data Exporter and delete the copies held by the Data Importer; (ii) If the applicable regulations in the Kingdom require the retention of the transferred Personal Data for an additional period of time. (b) The Personal Data Importer remains bound by these Clauses until the Personal Data is deleted or recovered.

2.8. Personal Data Security and Personal Data Breach Notifications. (a) The Parties shall ensure that the organisational, administrative, and technical measures specified in the Agreement and the Technical and Organisational Measures Document provide a sufficient level of protection for the transferred Personal Data to comply with the requirements of Article (19) of the Law and Article (23) of the Implementing Regulation. (b) The Personal Data Importer shall implement the security measures specified in the Technical and Organisational Measures Document and apply those measures to all transferred Personal Data to ensure the security and protection of Personal Data against any violation that may result in damage to the Personal Data Subject, unlawful action, loss, alteration, disclosure, or unauthorized access to Personal Data. (c) The Personal Data Importer must periodically review the security measures stipulated in the Technical and Organisational Measures Document to ensure that they are implemented as required and update them as needed to ensure compliance with Article (19) of the Law and Article (23) of the Implementing Regulation. (d) If The Personal Data Importer becomes aware of a Personal Data Breach incident that affects the transferred Personal Data or is likely to cause damage to the rights and interests of Personal Data Subjects, the Personal Data Importer must immediately take appropriate and necessary measures to contain the incident to minimise any risks or negative consequences and ensure that it is prevented from reoccurring. The Personal Data Exporter must be notified within (24) hours from the time of occurrence or knowledge of the breach incident, provided that the notification includes a description of the incident, its causes, the measures taken or planned to be taken to contain the incident and prevent its reoccurrence, in addition to the contact details for follow-up by the Personal Data Exporter. If the

Personal Data Exporter realises that the incident may cause damage to Personal Data or Personal Data Subjects or contradict their rights or interests, it shall notify the Competent Authority within (48) hours and in accordance with the requirements set out in Article (24) of the Law's Implementing Regulation. (e) As soon as the Personal Data Exporter receives the Data Importer's notification of a Personal Data breach incident and the incident would harm the Personal Data or the Personal Data Subject or contradict his/her rights or interests, the Personal Data Exporter must provide immediate notification in simple and clear language in accordance with the provisions of Article (24) of the Implementing Regulation to the Personal Data Subjects affected by the data breach incident, provided that the notification includes the potential risks and their nature, the measures taken or planned to be taken to contain the incident, and the contact information of the Personal Data Exporter, Data Importer, and the respective Personal Data Protection Officer of both entities, along with recommendations or consultations to aid the Data Subject in preventing or minimizing the impact of the outlined risks.

2.9. Sensitive Data. Without prejudice to any restrictions related to sensitive data stipulated in the Law and the Implementing Regulations of the Law, the Personal Data Exporter shall ensure that the Personal Data Importer adopts additional means of protection commensurate with the nature of the sensitive data and guarantees its protection from any risks when processing it, while ensuring that the restrictions and additional guarantees described in Data Protection Particulars are applied.

2.10. Subsequent Transfer (a) The Personal Data Importer shall not transfer or disclose the transferred Personal Data to a third party outside the Kingdom unless that party has acceded to these Clauses and in accordance with the appropriate template and the provisions of Clause (7) above. (b) Without prejudice to the provisions of Articles (8) and (15) of the Law and (17) of the Implementing Regulation of the Law, the provisions of the Law and Regulations shall apply to Personal Data that has been previously transferred or disclosed to an entity outside the Kingdom.

2.11. Compliance with these Clauses. (a) The Personal Data Importer shall respond to all inquiries of the Personal Data Exporter within the specified period and provide all information requested by the Personal Data Exporter, in addition to providing the Personal Data Exporter with all information it may request regarding the processing of the transferred Personal Data, including any information necessary to enable the Personal Data Exporter to prove its compliance with the requirements contained in these Clauses or the provisions stipulated in the Law and its Implementing Regulations. (b) Each party shall be responsible for demonstrating to the Competent Authority, upon request, that all obligations under these Clauses have been fulfilled. (c) The Personal Data Importer allows the Personal Data Exporter or its appointed representatives to audit the Data Importer's processing of Personal Data without undue delay upon Personal Data Exporter's request. (d) The Personal Data Exporter must provide the information revealed by the audit when requested by the Competent Authority. (e) The right of audit does not grant the Personal Data Exporter or its representatives access to any confidential information of the Personal Data

Importer as long as this information is not closely related to the processing of the transferred Personal Data.

2.12. Rights of Personal Data Subjects. (a) The Personal Data Importer shall notify the Personal Data Exporter within (48) hours from the time of receipt of the request of any request received from the Personal Data Subject, and the Personal Data Importer shall not have the right to respond to such requests unless the Personal Data Exporter authorizes it to do so. (b) The Personal Data Importer shall take all necessary measures in cooperation with the Personal Data Exporter to respond to the requests of Personal Data Subjects and enable them to exercise their rights under the provisions of the Law and Regulations. (c) The Personal Data Importer is obligated to follow all instructions issued by the Personal Data Exporter regarding the processing of the transferred Personal Data. (d) All statements made to the Personal Data Subject must be presented in a clear, legible, and accessible format.