

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

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 in the Territory, such as (where relevant):

- (a) the EU GDPR;
- (b) the UK Data Protection Law; and
- (c) 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 (the "UK GDPR"); (b) the UK Data Protection Act 2018 (the "DPA 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 ("PECR").

- 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 all necessary rights and consents to process and disclose Customer Personal Data to Keyloop 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 on the documented written instructions of Customer as set out in the Agreement, unless required to do otherwise 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 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 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 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 or destroy 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 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 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. Upon termination of the Agreement Customer and Keyloop shall remove and delete data as set out at clause 21.2.4 and clause 21.2.5 of the Standard Terms and Conditions;
- 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 Data Protection Legislation (or aspects of it). 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 5.1.4 and 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 prior to the Sub-Processor's processing of Customer Personal Data and shall update the Privacy Hub to reflect any change in identity of a Sub-Processor from time to time. Customer may object to such change 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:
 - 6.5.1 at least equivalent to the obligations imposed on Keyloop pursuant to this Data Processing Addendum; and
 - 6.5.2 compliant with Data Protection Legislation.
- 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, Customer generally authorises Keyloop (and its Sub-Processors) to Transfer Customer Personal Data to recipients based inside or outside of the European Economic Area (EEA), United Kingdom (UK) or any country deemed to be adequate by the European Commission or the UK Government.
- 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 the application of model clauses between Keyloop and the relevant Sub-Processor.