DATA PROCESSING AGREEMENT

[DATE]

[INSERT KEYLOOP ENTITY]

AND

[INSERT PROVIDER ENTITY]

THIS AGREEMENT IS DATED: [insert date]

PARTIES

(1) **[INSERT KEYLOOP ENTITY]** a company incorporated in England with registered number 09347879, whose registered office is at The Brickworks, 35-43 Greyfriars Road, Reading, England, RG1 1NP (**Keyloop**); and

(2) **[insert Provider name],** a company incorporated in [country] with registered number [insert], [whose registered office is at [insert address]] **OR** [having its principal place of business at [insert] (**Provider**).

BACKGROUND

(A) Keyloop, or one of the members of its Group, and the Provider entered into an agreement for products and/or services with the Provider on [insert date **OR** or around the date of signature of this Agreement] that may require the Provider to process Personal Data on behalf of Keyloop (**Relevant Contract**).

(B) This Data Processing Agreement (**Agreement**) sets out the additional terms, requirements and conditions on which the Provider will process Personal Data when providing products and/or services under the Relevant Contract, and has priority over any conflicting provisions in the Relevant Contract. This Agreement addresses the mandatory clauses required for contracts between controllers and processors by the UK GDPR and/or the EU GDPR. If mandatory clauses are required in jurisdictions other than the UK and the EU, an addendum to this Agreement may be provided where necessary.

AGREED TERMS

1 DEFINITIONS & INTERPRETATION

1.1. The following definitions apply:

Business Purposes means the services to be provided by the Provider to Keyloop as described in the Relevant Contract and any other purposes specifically identified in the Data Processing Details;

Complaint means a complaint or request relating to either party's obligations under Data Protection Laws relevant to this Agreement or the Relevant Contract, including any compensation claim from a Data Subject or any notice, investigation or other action from a Supervisory Authority;

Controller, Data Subject, Personal Data, Processor, and **Processing** and shall have the meanings given to those terms respectively in the Data Protection Laws;

Data Protection Laws means:

(a) in the UK all applicable data protection and privacy legislation in force from time to time in the UK, including (i) the UK GDPR; (ii) the Data Protection Act 2018 and regulations made under it; (iii) the Privacy and Electronic Communications Regulations (SI 2003/2426), as amended;

(b) in member states of the European Union, the EU GDPR and the Privacy and Electronic Communications Directive (2002/58/EC) as updated by Directive 2009/136/EC and all relevant member state laws or regulations giving effect to or corresponding with any of them which relate to the protection of Personal Data, as amended;

(c) in any other jurisdiction, all applicable legislation and regulatory requirements in force from time to time which apply to a Party relating to the use of Personal Data (including but not limited to the privacy of electronic communications and security of Personal Data);

(d) in any jurisdiction, any legally binding judicial or administrative interpretation of any of the above, any guidance, guidelines, codes of practice, approved codes of conduct or approved accreditation mechanisms issued by any relevant Supervisory Authority;

Data Processing Details means the details of data processing, including the list of Sub-processors, which is found in Appendix 1 and which relates to the Services;

Data Subject Request means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws;

Effective Date means the date upon which the Provider commences provision of the Services;

EU GDPR means the General Data Protection Regulation (EU) 2016/679;

EU Standard Contractual Clauses means the Standard Contractual Clauses set out in the European Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679, as updated, amended, replaced or superseded from time to time by the European Commission;

Group means, in relation to a company, that company's subsidiaries and holding companies and subsidiaries of such holding companies;

Losses means losses, damages, liabilities (including any liability to taxation), claims, costs and expenses, including fines, penalties and reasonable legal and other professional fees and expenses. These include but are not limited to any direct, indirect or consequential losses, loss of profit and loss of reputation even if those heads of loss are excluded under the Relevant Contract;

Personal Data Breach means (i) a breach of security leading to the accidental, unauthorised or unlawful processing of the Personal Data; or (ii) the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data; or (iii) has the meaning given to it (if different) under the applicable Data Protection Laws;

Services means the services provided by the Provider in relation to the Processing of Personal Data as set out in the Relevant Contract;

Sub-processor means a party that processes Personal Data on behalf of a Processor;

Supervisory Authority means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws;

Required TOMs has the meaning given in clause 3.1.

Restricted Transfer means processing of Personal Data collected from the United Kingdom or European Economic Area (**EEA**) in a country outside the United Kingdom or EEA where the country in which the Personal Data is Processed or from which the Personal Data is accessed does not have an adequacy decision in its favour from the United Kingdom (for Personal Data collected from the United Kingdom) or from the European Commission (for Personal Data collected from the EEA).

Term means the Agreement's term as defined in clause 8.1;

UK Addendum means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018 VERSION B1.0, which came into force on 21 March 2022;

UK GDPR means the retained UK law version of the EU GDPR as defined in section 3(10) of the Data Protection Act 2018 and as supplemented by section 205(4).

1.2. This Agreement is subject to the terms of the Relevant Contract and is incorporated into the Relevant Contract. Interpretations and defined terms set out in the Relevant Contract apply to the interpretation of this Agreement.

1.3. The Appendices form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Appendices.

1.4. In case of conflict or ambiguity between:

(a) any provision contained in the body of this Agreement and any provision contained in the Appendices, the provision in the body of this Agreement will prevail;

(b) any of the provisions of this Agreement and the provision of the Relevant Contract, the provisions of this Agreement will prevail.

2 DETAILS OF PROCESSING

2.1. The Parties agree and acknowledge that for the purposes of the Data Protection Laws:

(a) where Keyloop is a Controller, the Provider is a Processor;

(b) where Keyloop is Processing the Personal Data of its own customers (each customer being an **End Customer**), Keyloop is a Processor and the Provider is a Sub-processor. The Parties agree that in this scenario, the clauses of this Agreement will remain applicable to the Provider as a Sub-Processor where Keyloop has an obligation in its contract with End Customers to include clauses with its Sub-processors that are the equivalent of those imposed upon Keyloop by the End Customer as Controller.

2.2. Notwithstanding that Keyloop Holdings (UK) Limited is the lead contracting party, the provisions of this Agreement shall apply to any member of Keyloop's Group and any Personal Data shared by any Keyloop Group member with the Provider. Keyloop Holdings (UK) Limited shall be entitled to enforce any provision of this Agreement on behalf of any members of the Keyloop Group and any Losses suffered by a member of the Keyloop Group shall be deemed to be suffered by Keyloop Holdings (UK) Limited.

2.3. In relation to any Personal Data processed in connection with the performance of the Services, the Provider shall:

(a) comply with its obligations as a Data Processor under and in accordance with the Data Protection Laws and comply with Keyloop's written instructions in relation to the Processing of the Personal Data;

(b) only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes and in accordance with Keyloop's written instructions. The Provider will not process the Personal Data for any other purposes or in a way that does not comply with this Agreement or the Data Protection Laws;

(c) promptly notify Keyloop if any other applicable law requires the Provider to process the Personal Data in breach of clause 2.3(b) before carrying out such processing (unless prohibited from doing so by applicable law);

(d) promptly notify Keyloop if, in the Provider's opinion, Keyloop's instructions do not comply with the Data Protection Laws;

(e) maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third parties unless Keyloop or this Agreement specifically authorises the disclosure, or as required by any applicable laws, courts or regulators (including any Supervisory Authority). If any applicable laws, courts or regulators (including any Supervisory Authority) require the Provider to disclose the Personal Data to a third-party, the Provider must first inform Keyloop of such legal or regulatory requirement and give Keyloop an

opportunity to object or challenge the requirement, unless applicable laws prohibit the giving of such notice;

(f) reasonably assist Keyloop, with meeting Keyloop's compliance obligations under the Data Protection Laws, taking into account the nature of the Provider's processing and the information available to the Provider, including in relation to ensuring the security of the Personal Data, Data Subject rights, data protection impact assessments and reporting to and consulting with any Supervisory Authority under the Data Protection Laws.

2.4. The Provider shall ensure that:

(a) it grants access to the Personal Data only to those authorised personnel who need access to comply with the terms of this Agreement; and

(b) shall ensure that all such authorised persons processing the Personal Data are informed of the confidential nature of the Personal Data and are bound by written confidentiality obligations in respect of the Personal Data or under an appropriate statutory obligation of confidentiality.

2.5. The Provider will take reasonable steps to ensure the reliability, integrity and trustworthiness of, and will conduct reasonable and appropriate background checks consistent with applicable domestic law on, all the Provider's personnel who have access to the Personal Data.

3 SECURITY

3.1 Taking account of those factors which it must to take account of pursuant to the Data Protection Laws including but not limited to the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the Data Subjects, the Provider shall at all times implement and maintain, at the Provider's cost, appropriate technical and organisational measures, which as a minimum shall be as specified at https://keyloop.com/legal-documentation as may be updated from time to time (**Required TOMs**), to protect against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of the Personal Data.

4 PERSONAL DATA BREACH

4.1 In respect of any Personal Data Breach or any suspected Personal Data Breach which is related to the terms of this Agreement, the Provider shall:

(a) use reasonable endeavours to notify Keyloop within 24 hours, and in any event without undue delay, after becoming aware of a Personal Data Breach and provide Keyloop with such details as it reasonably requires, including:

i. a description of the nature of the Personal Data Breach or suspected Personal Data Breach, including the categories and approximate numbers of Data Subjects and Personal Data records concerned;

ii. the likely consequences of the Personal Data Breach or suspected Personal Data Breach;

iii. a description of the measures taken or proposed to be taken to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(b) restore any lost, destroyed, damaged, corrupted or unusable Personal Data at its own expense as soon as possible.

4.2 Immediately following any Personal Data Breach, the Parties shall co-ordinate with each other to investigate the matter. The Provider shall reasonably co-operate with Keyloop (including the End Customer where applicable), in Keyloop's handling of the matter, including but not limited to, where necessary:

(a) assisting with the investigation and obtaining information required by Supervisory Authorities;

(b) providing Keyloop with physical access to any facilities and operations affected;

(c) facilitating interviews with the Provider's employees, former employees and others involved in the matter, including its officers and directors;

(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Laws or as otherwise reasonably required by Keyloop; and

(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach.

4.3 The Provider will not inform any third-party (including any Data Subject) of any Personal Data Breach without first obtaining Keyloop's written consent except where required to do so under any applicable Data Protection Laws or where required to inform its advisors engaged with respect to the investigation or remediation of the Personal Data Breach or to inform its insurers. The Provider agrees that Keyloop (or the End Customer where applicable) has the sole responsibility for determining whether and how notice of the Personal Data Breach is provided to any Data Subjects or any Supervisory Authority, including the contents and delivery of such notice.

5 CROSS-BORDER TRANSFERS OF PERSONAL DATA

5.1 If and to the extent that the Provider's Processing of Personal Data involves any Restricted Transfer, the Parties hereby agree to enter into, as appropriate, Module Two (Controller to Processor) or Module Three (Processor to Processor) of the EU Standard Contractual Clauses to facilitate the Restricted Transfers of Personal Data collected from the EEA and the UK Addendum to facilitate the Restricted Transfers of Personal Data collected from the United Kingdom, and the EU Standard Contractual Clauses and the UK Addendum shall be considered to be completed and populated in accordance with the terms set out in Appendix 2.

5.2 Any Restricted Transfer by the Provider shall be done only on the basis of documented instructions from Keyloop and in accordance with the Data Protection Laws.

5.3 Keyloop agrees that where the Processor engages a Sub-processor in accordance with clause 6 for carrying out specific processing activities under the terms of this Agreement and those processing activities involve a Restricted Transfer, the Provider and the Sub-processor can ensure compliance with the Data Protection Laws by using the EU Standard Contractual Clauses and/or the UK Addendum as applicable. By signing this Agreement, Keyloop consents to the transfer of Personal Data to the International Recipients (if any) which are listed as Sub-processors in the Data Processing Details at the Effective Date.

6 USING OTHER PROCESSORS

6.1 The Provider has Keyloop's general authorisation for the engagement of Sub-processors from an agreed list. The Provider shall specifically inform in writing Keyloop of any intended changes of that list through the addition or replacement of Sub-processors at least 30 days in advance, thereby giving Keyloop sufficient time to be able to object to such changes prior to the

engagement of the concerned Sub-processor(s). The Provider shall provide Keyloop with the information necessary to enable Keyloop to exercise the right to object.

6.2 In the event that Keyloop does object to the proposed use and the Provider is unable to process Personal Data without using such third-party subcontractor, then Keyloop shall be entitled to terminate this Agreement, and the Relevant Contract, without further liability or obligation of Keyloop.

6.3 Where the Provider engages a Sub-processor for carrying out specific processing activities (on behalf of Keyloop), it shall do so by way of a contract which imposes on the Sub-processor, in substance, the same data protection obligations as the ones imposed on the Provider in accordance with this Agreement. The Provider shall ensure that the Sub-processor complies with the obligations to which the Provider is subject pursuant to this Agreement and to Data Protections Laws.

6.4 The Sub-processors approved as at the Effective Date are as set out in the Data Processing Details in Appendix 1.

6.5 The Provider shall carry out appropriate due diligence of the Sub-processors and shall remain fully liable to Keyloop for the Sub-processors' performance of their obligations in accordance with their contract with the Provider and for the Sub-processors' failure to fulfil their obligations in relation to the Personal Data.

7 COMPLAINTS AND DATA SUBJECT REQUESTS

7.1 The Provider shall:

(a) take such technical and organisational measures as may be appropriate and promptly provide such information and assistance to Keyloop as Keyloop reasonably requires to enable Keyloop to comply with Data Subject Requests;

(b) record and refer all Data Subject Requests it receives to Keyloop without undue delay (and in any event within 48 hours of receipt);

(c) not respond to any Data Subject Request without Keyloop's prior written approval.

7.2 The Provider must notify Keyloop promptly in writing if it receives any Complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either Party's compliance with the Data Protection Laws.

8 TERM & TERMINATION

8.1 This Agreement will remain in full force and effect so long as:

(a) the Relevant Contract remains in effect;

(b) the Provider retains any Personal Data related to the Relevant Contract in its possession or control (**Term**).

8.2 Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Relevant Contract in order to protect the Personal Data will remain in full force and effect

8.3 Notwithstanding clause 8.1 the Parties may agree to remove one or more individual entries in the Data Processing Details as and when a relevant part of the Services is terminated, the date of termination then being a date agreed by the Parties in writing.

8.4 The Provider's failure to comply with the terms of this Agreement is a material breach of the Relevant Contract. In such event, Keyloop may terminate the Relevant Contract or (at its sole option) any part of the Relevant Contract involving the processing of the Personal Data effective immediately on written notice to the Provider without further liability or obligation of Keyloop.

9 RETURN OR DELETION OF PERSONAL DATA

9.1 At the end of provision of the Services, or on termination of the Relevant Contract, or at any other time on the instruction of Keyloop, the Provider shall:

(a) securely destroy the Personal Data (including all copies of it); or, at Keyloop's option,

(b) return the Personal Data to Keyloop in the format reasonably specified by Keyloop; and

(c) certify in writing to Keyloop that it has deleted, destroyed or returned the Personal Data.

9.2 If any law, regulation, or government or regulatory body requires the Provider to retain any Personal Data that the Provider would otherwise be required to return or destroy, it will notify Keyloop in writing of that retention requirement, giving details of the Personal Data that it must retain, the legal basis for such retention, and establishing a specific timeline for deletion or destruction once the retention requirement ends. Until the Personal Data is deleted or returned, the Provider shall continue to ensure compliance with this Agreement.

10 RECORD KEEPING & AUDIT

10.1 The Provider shall maintain complete, accurate and up-to-date written records regarding any processing of the Personal Data, including but not limited to, the access, control and security of the Personal Data, approved Sub-processors, the processing purposes, categories of processing, and a general description of the technical and organisational security measures referred to in clause 3.1 (**Records**).

10.2 The Provider shall ensure that the Records are sufficient to enable Keyloop to verify the Provider's compliance with its obligations under this Agreement and the Data Protection Laws. The Provider shall provide Keyloop with copies on request.

10.3 The Provider shall allow for and contribute to audits, including inspections of the Records, conducted by Keyloop or its appointed independent auditors, or the End Customer where applicable, upon reasonable notice and during normal business hours, for the purpose of demonstrating compliance by the Provider of its obligations under this Agreement and the Data Protection Laws at reasonable intervals or if there are indications of non-compliance.

10.4 The Provider shall promptly address any exceptions noted in the audit reports with the development and implementation of a corrective action plan by the Provider.

11 LIABILITY

11.1 For the avoidance of doubt, any limits on the liability of the Parties set out in the Relevant Contract shall not apply to the terms of this Agreement.

12 GOVERNING LAW & JURISDICTION

12.1 This Agreement shall be governed by and construed in accordance with the laws of England and Wales and shall be subject to the exclusive jurisdiction of the Courts of England.

This Agreement has been entered into on the date stated at the beginning of it.

Signed by a duly authorised signatory for and on behalf of **Keyloop** ..... Name: Position:	Signed by a duly authorised signatory for and on behalf of **Provider** ..... Name: Position:

APPENDIX 1 - DATA PROCESSING DETAILS

TABLE 1: DATA PROCESSING

Details of Data Protection Officer or equivalent contact	*[Include the name and contact details of the person responsible for data protection within the Provider's business]*
Subject matter of Processing	*[Include details of the subject matter of processing]*
Purpose of Processing	*[Include details of the purpose of processing]*
Nature of Processing	*[Include details of the nature of processing]*
Duration of Processing	The later of (i) the termination or expiry of the Relevant Contract or (ii) the termination of the last of the Services to be performed by the Provider.
Categories of Data Subjects	*[list all categories of data subject whose Personal Data would be processed]*
Categories of Personal Data	*[list all categories of Personal Data processed and include details of special categories of personal data here also – if relevant]*

TABLE 2: INTERNATIONAL TRANSFERS

Territory to which the data will be transferred	*[include all countries]*
Cross-border Transfer Mechanism	*[include the mechanism used by the Provider to transfer data – e.g. Adequacy, Binding Corporate Rules, Standard Contractual Clauses Insert a copy of the SCCs, the IDTA or other mechanism into Appendix 2 below if it is available when the DPA is prepared]*

TABLE 3: SUB-PROCESSORS

Name of Sub-processor & DPO Details	Data Subject Type	Categories of Personal Data	Purpose of Processing	Countries where Processed	Valid Mechanism for Transfer
[insert details]	*[e.g. employees, customers]*	*[e.g. name, address, ID etc.]*	*[e.g. data centre storage]*	*[e.g. India, USA, Japan etc.]*	*[e.g. SCCs with its Sub-processors]*

APPENDIX 2 - APPLICABLE INTERNATIONAL TRANSFER DOCUMENT(S)

Restricted Transfers under the EU Standard Contractual Clauses

Restricted Transfers made under the terms of the EU Standard Contractual Clauses (with Keyloop as data exporter and the Provider as data importer), which clauses are hereby incorporated by reference into this Agreement and which shall come into effect upon the commencement of a Restricted Transfer. The parties make the following selections for the purposes of the EU Standard Contractual Clauses:

a) Clause 7 – Docking clause shall apply;
b) Clause 9 – Use of subprocessors Option (2), "general written authorisation" shall apply and the "time period" shall be 30 days;
c) Clause 11(a) – Redress the optional language shall not apply;
d) Clause 13(a) – Supervision: The Supervisory Authority of the Republic of Ireland shall act as competent supervisory authority.
e) Clause 17 – Governing law "Option 1" shall apply and the Member State shall be the Republic of Ireland;
f) Clause 18 – Choice of forum and jurisdiction shall be the Republic of Ireland;
g) Annex I – the Data Exporter is Keyloop and the Data Importer is the Provider (in each case as identified, including in relation to their places of establishment, in this Agreement) and the processing operations are deemed to be those described in Appendix 1 of this Agreement;
h) Annex II – see the Required TOMs at https://keyloop.com/legal-documentation;
i) Annex III – see Appendix 1 to this Agreement.

Restricted Transfer subject to the UK GDPR

The Parties hereby enter into the UK Addendum which is incorporated by reference into this Agreement and which shall come into effect upon the commencement of any Restricted Transfer of Personal Data collected from Data Subjects in the United Kingdom. For Table 1 of the UK Addendum, the Data Exporter is Keyloop and the Data Importer is the Provider (in each case as identified, including in relation to their places of establishment, in this Agreement). Table 2 shall be deemed to be prepopulated in accordance with the provisions selected for "Restricted Transfer subject to the EU GDPR" above. The Appendix Information of the UK IDTA shall be deemed to be prepopulated with the relevant sections of Appendix 1 of this Agreement and the Required TOMs at https://keyloop.com/legal-documentation.

Each party's agreement and consent to this Agreement shall be considered a signature to the Standard Contractual Clauses and/or the UK Addendum. If required by the laws or regulatory procedures of any jurisdiction, the Parties shall execute or re-execute the EU Standard Contractual Clauses and/or the UK Addendum as separate documents. In case of conflict between the EU Standard Contractual Clauses and/or the UK Addendum (as applicable), and this Agreement, the Standard Contractual Clauses and/or the UK Addendum (as applicable) will prevail.