DATA PROCESSING AGREEMENT (“DPA”)

PRIVACY NOTICE

THIS DPA is dated from the point of both parties completed signatures

PARTIES:

(1) Keepnet Labs Ltd (Keepnet)

(2)

AGREED TERMS:

1. DEFINITIONS AND INTERPRETATION

1.1 In this DPA the following words and expressions have the following meanings unless the context otherwise requires:

Applicable Law: applicable law of the United Kingdom (or a part of the United Kingdom).

Controller, **Data Subject**, **Personal Data**, **Personal Data Breach**, **Processor** and **Processing** will have the respective meanings given to them in applicable Data Protection Laws from time to time (and related expressions, including ***Process***, ***Processed***, and ***Processes*** will be construed accordingly).

Data Protection Laws: all applicable law relating to the Processing, privacy and/or use of Personal Data, as applicable to either party or the Purposes, including: (a) the EU GDPR; (b) the UK GDPR; (c) the Data Protection Act 2018; (d) any laws which implement any such laws; (e) any laws that replace, extend, re-enact, consolidate or amend any of the foregoing; and (f) all mandatory legally binding guidance, guidelines and codes of practice issued by any relevant Data Protection Supervisory Authority relating to such Data Protection Laws.

Data Protection Supervisory Authority: any regulator, authority or body responsible for administering Data Protection Laws.

Purposes: to provide services as part of and in-line with the EULA & Keepnet Labs T&Cs

EU GDPR: the General Data Protection Regulation, Regulation (EU) 2016/679.

Agreement: this refers to the Keepnet Labs EULA and Keepnet Labs T&Cs (end user licence agreement, terms and conditions)

UK GDPR: has the meaning given to it in section 3(10) (as supplemented by section 205(4) of the Data Protection Act 2018.

2. PERSONAL DATA TYPES AND PROCESSING PURPOSES

2.1 For the purpose of Data Protection Laws regarding any Personal Data Processed by Keepnet on behalf of CUSTOMER pursuant to the Purposes, CUSTOMER trading as Company is the Controller and Keepnet is a Processor. Keepnet will process the Data within our platform and CUSTOMER trading as Company as the data controller has the right to determine what data is being used in the platform. Schedule 1 to this DPA describes the subject matter, duration, nature and purpose of the Processing, the Personal Data categories and Data Subject types in respect of which Keepnet may Process to fulfil the Purposes.

2.2 Both parties will comply with all applicable requirements of the Data Protection Laws. This DPA is in addition to, and does not relieve, remove or replace, a party's obligations under the Data Protection Laws.

2.3 Keepnet will not by any act or omission cause CUSTOMER to be in breach of any Data Protection Laws.

3. COMPANY OBLIGATIONS

3.1 If Keepnet Processes any Personal Data on behalf of CUSTOMER pursuant to the Purposes, Keepnet will:

3.1.1 only Process (and will ensure that its personnel only Process) such Personal Data in accordance with this DPA and CUSTOMER's documented instructions from time to time, except where otherwise required by Applicable Law (and in such a case, will inform CUSTOMER of that legal requirement before Processing, unless Applicable Law prevents it doing so on important grounds of public interest). Keepnet will immediately inform CUSTOMER if any instruction relating to the Personal Data infringes or may infringe any Data Protection Laws;

3.1.2 ensure that all employees who are authorised to Process the Personal Data are informed of the confidential nature of such Personal Data and are bound by confidentiality obligations in respect of the Personal Data which are enforceable by Keepnet;

3.1.3 take all reasonable steps to ensure the reliability and integrity of all its employees with access to the Personal Data;

3.1.4 on request, assist CUSTOMER in ensuring compliance with its legal obligations under Data Protection Laws in relation to Data Subject rights, security, breach notifications, data protection impact assessments and reporting to and consulting with supervisory authorities or regulators under the Data Protection Laws;

3.1.5 take all appropriate technical and organisational measures as required by UK GDPR to protect Personal Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access and against all other unlawful forms of processing based on state of the art of

technology, the nature, scope, context and purposes of the Processing, as well as the associated risk of Processing to the rights and freedoms of Data Subjects that may arise from a Personal Data Breach. Such measures will include the security measures noted in Schedule 2.

3.1.6 taking into account the nature of the Processing, assist CUSTOMER by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of CUSTOMER's obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws;

3.1.7 notify CUSTOMER immediately 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 Data Protection Laws;

3.1.8 notify CUSTOMER promptly if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under Data Protection Laws;

3.1.9 except for any permitted sub-processors listed in Schedule 1, not otherwise authorise or appoint any third party or subcontractor to Process the Personal Data without PARTNER's prior written consent of that further sub-Processor. Keepnet will: a) remain fully liable for any sub-Processors; and b) have a contract in place with such permitted sub-processors that includes the same terms to this DPA and provides an equivalent level of protection for the Personal Data. In particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of UK GDPR;

3.1.10 except for any permitted data transfers to any permitted sub-Processors listed in Schedule 1, not otherwise Process and/or transfer, or otherwise directly or indirectly disclose, any Personal Data outside the area comprising the United Kingdom and European Economic Area unless the prior written consent of CUSTOMER has been obtained (and where consent is given such consent will be set out in a written variation to this DPA) and the following conditions are fulfilled: (a) Keepnet or PARTNER has provided appropriate safeguards in relation to the transfer (e.g. binding corporate rules, the then current version of the UK international data transfer agreement issued by the UK ICO or the then current version of the UK international data transfer addendum issued by the UK ICO plus the then current version of the EU standard contractual clauses); (b) the Data Subject has enforceable rights and effective legal remedies; and (c) Keepnet complies with its obligations under the Data Protection Laws by providing an adequate level of protection to any Personal Data that is transferred;

3.1.11 maintain the confidentiality of all Personal Data and will not disclose such Personal Data to third parties unless CUSTOMER or this DPA specifically authorises the disclosure, or as required by Applicable Law. If a law, court, regulator or supervisory authority requires Keepnet to process or disclose the Personal Data, it will first inform the CUSTOMER of the legal or regulatory requirement and give an opportunity to object or challenge the requirement, unless the law prohibits such notice; and

3.1.12 promptly comply with any CUSTOMER request or instruction requiring it to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised Processing.

4. PERSONAL DATA BREACH

4.1 Keepnet will promptly and without undue delay notify CUSTOMER if it becomes aware that any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable. Keepnet will restore such Personal Data at its own expense.

4.2 Keepnet will within twenty-four (24) hours and without undue delay notify CUSTOMER if it becomes aware of: (a) any accidental, unauthorised or unlawful processing of the Personal Data; or (b) any suspected, actual or threatened occurrence of any Personal Data Breach. Where Keepnet becomes aware of (a) and/or (b), it will, without undue delay, also provide CUSTOMER with the following information:

4.2.1 description of the nature of (a) and/or (b), including the categories and approximate number of both Data Subjects and Personal Data records concerned;

4.2.2 the likely consequences; and

4.2.3 description of the measures taken or proposed to be taken to address (a) and/or (b), including measures to mitigate its possible adverse effects.

4.3 Immediately following any unauthorised or unlawful Personal Data Processing or Personal Data Breach, the parties will coordinate with each other to investigate the matter. Keepnet will reasonably cooperate with CUSTOMER in its handling of the matter.

4.4 Keepnet will not inform any third party of any Personal Data Breach without first obtaining CUSTOMER's prior written consent, except when required to do so by Applicable Law.

4.5 Keepnet agrees that CUSTOMER has the sole right to determine:

4.5.1 whether to provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation or CUSTOMER's discretion, including the contents and delivery method of the notice; and

4.5.2 whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

5. TERM AND TERMINATION

5.1 This DPA will remain in full force and effect so long as: a) the Purposes remain in effect; or b) Keepnet retains any Personal Data related to the Purposes in its possession or control (the "**Term**").

5.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Purposes to protect the Personal Data will remain in full force and effect.

6. PERSONAL DATA RETURN AND DESTRUCTION

6.1 At CUSTOMER's request, Keepnet will give CUSTOMER a copy of or access to all or part of its Personal Data related to the Purposes which is in Keepnet's possession or control in the format and on the media reasonably specified by CUSTOMER.

6.2 On termination of the Purposes for any reason or expiry of its Term, Keepnet will securely delete or destroy or, if directed in writing by CUSTOMER, return and not retain, all or any Personal Data related to this DPA and the Purposes in its possession or control, except to the extent that storage of any such Personal Data is required by Applicable Law (and, if so, Keepnet will inform CUSTOMER of any such requirement and will securely delete such data as soon as it is permitted to do so under Applicable Law).

7. RECORDS AND AUDITS

7.1 Keepnet will keep detailed, accurate and up-to-date written records regarding any Processing of Personal Data that it carries out for CUSTOMER (including but not limited to, the access, control and security of the Personal Data, approved subcontractors and affiliates, the processing purposes, categories of processing, any transfers of personal data to a third country and related safeguards, and a general description of its technical and organisational security measures) (the "**Records**").

7.2 Keepnet will ensure that the Records are sufficient to enable CUSTOMER to verify Keepnet's compliance with its obligations under this DPA and will provide CUSTOMER with copies of such Records upon request.

7.3 Keepnet will make available to CUSTOMER, on request, all information necessary to demonstrate its compliance with the obligations laid down in this DPA and allow for and contribute to audits, including inspections, conducted by CUSTOMER or another auditor mandated by THIRD PARTY to the Processing of CUSTOMER's Personal Data by it under the Purposes. Keepnet will give CUSTOMER and its third-party representatives all necessary assistance to conduct such audits.

8. GENERAL TERMS

8.1 The parties acknowledge and agree that where any amendments to this DPA are necessary to ensure that either party is compliant with the Data Protection Laws then the parties will promptly work together to make such amendments as are reasonably necessary and neither party will unreasonably withhold or delay such amendments.

8.2 Any notice or other communication given to a party under or in connection with this DPA must be in writing and delivered to its registered office. This clause 8.3 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

8.3 No variation of this DPA will be valid unless recorded in writing and signed by or on behalf of each of the parties (or their authorised representatives).

8.4 Neither party will assign or otherwise transfer or subcontract any of its rights or obligations under this DPA (whether in whole or in part) without the prior written consent of the other party.

8.5 If any provision or part-provision of this DPA is or becomes invalid, illegal or unenforceable, it will be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision or part-provision will be deemed deleted. Any modification to or deletion of a provision or part-provision under this clause will not affect the validity and enforceability of the rest of this DPA.

8.6 No one other than a party to this DPA will have any right to enforce any of its terms.

8.7 No failure or delay by a party to exercise any right, power or remedy will operate as a waiver of it nor will any partial exercise preclude any further exercise of the same, or of some other right, power or remedy.

8.8 This DPA constitutes the entire agreement between the parties regarding personal data processing. Each party agrees that it will have no remedies in respect of any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this DPA. Each party agrees that it will have no claim for innocent or negligent misrepresentation or negligent misstatement based on any statement in this DPA.

8.9 This DPA will be governed by, and constructed in accordance with, with the law of England and Wales and the parties submit to the exclusive jurisdiction of the courts of England and Wales.

SCHEDULE 1

Description	Details

<table>
<tr><td>Subject matter, nature and purpose of the processing of Personal Data by Keepnet Labs under the EULA and T&Cs</td><td>Subject matter
Keepnet Labs customer services support, training dashboard, including and not limited to data protection, information security training and various security training and threat simulations, and threat intelligence and phishing incident response software and services.
Nature
The Personal Data Processed by Keepnet will be subject to the following basic processing activities:
☐ Receiving data, including collection, accessing, retrieval, recording, and data entry
☐ Holding data, including storage, organisation and structuring
☐ Using data, including analysing, consultation and testing
☐ Updating data, including correcting
☐ Protecting data, encrypting, and security testing
☐ Returning data to CUSTOMER or data subject
☐ Erasing data, including destruction and deletion
Purpose
To provide the Services under the EULA & T&Cs</td></tr>
<tr><td>Duration of the processing of Personal Data by Keepnet Labs under the EULA and T&Cs</td><td>Ongoing, until the Purpose has concluded.</td></tr>
<tr><td>Type of Personal Data being processed by Keepnet Labs under the EULA and T&Cs</td><td>The Personal Data Processed by Keepnet concerns the following categories of data:
Personal Data
• Name, email address, telephone number, department details, and locations.
• Training records.</td></tr>
<tr><td>Categories of data subjects of the Personal Data processed by Keepnet Labs under the EULA and T&Cs</td><td>The Personal Data Processed by Keepnet concerns the following categories of Data Subjects:
Each category includes current, past and prospective data subjects. Where any of the following is itself a business or organisation, it includes its staff.
☐ staff including volunteers, agents, temporary and casual workers</td></tr>
<tr><td>Permitted Sub-Processors (if any)</td><td><table><tr><th>Sub-processor full corporate name</th><th>Country of processing by that Sub-processor</th><th>Appropriate Safeguards for such transfer
(e.g. international data transfer agreement,</th></tr></table></td></tr>
</table>

			binding corporate rules, country is governed by an adequacy decision)
	AWS	UK	N/A
	Microsoft Azure	UK	N/A
	N/A	N/A	N/A

SCHEDULE 2:

Technical and Organisational Security Measures

Below is a general description from Data Processor on how they will ensure data security as part of their contracted services to Data Controller as per the agreed DPA.

Technical Security Measures:

ISO 27001 certification
ISO 27017
ISO 27018
ISO 42001:2023

Organisational Security Measures:

List our relevant data protection and information security policies:

- Information Security and Privacy Policy
- Information Security Roles & Responsibilities
- ISMS Scope
- HR Security Policy
- Acceptable Use Policy
- Access Control and Password Policy
- Web Application Security Policy
- System Documentation Policy
- Supplier Security Policy
- Remote Working Policy
- Media Protection Policy
- Database Credentials Security Policy
- Data Protection Policy
- Cryptography Policy
- Configuration Management Policy
- Clean Desk Policy
- Environmental Policy
- Change Management Policy
- Cloud Asset Management Policy
- Information Classification and Handling Policy
- Document Management Procedure
- Corrective and Remedial Actions Procedure
- Risk Management Procedure
- Internal Audit Procedure
- Management Review Procedure
- Continual Improvement Procedure
- Secure System Engineering Principles
- Security Event Monitoring Procedure
- Incident Response Procedure
- Data Retention and Disposal Procedure
- Business Continuity Planning
- Access Management Procedure
- Incident Management Procedure
- Information Security in Project Management Procedure
- Physical Security Controls Procedure
- Performance Evaluation Procedure
- Organisational Controls Procedure
- Access Control Procedure
- Asset Management Procedure
- Business Continuity Management
- Compliance with Legal and Regulatory Requirements Procedure

- Statement of Applicability
- ISMS Objectives
- Asset and Risk Inventory
- Audit Program
- Audit Plan
- Corrective Action Form
- Internal Audit Report
- Management Review Meeting Report
- Incident Record Form
- ISMS Tasks
- List of The Legislative and Regulatory References
- Change Request Form
- Communication Table
- Performance Indicators
- Corrective Action List
- Internal Audit Checklist
- Access Control List (noted as repeated)
- Approved Supplier Evaluation Table
- Information Security Continuity Plan
- HR Employee Screening Form
- IS Incident Form
- Business Continuity Plan
- Roles and Responsibilities Table
- Information Security Governance Process
- Security Policy Management Process
- Requirements Management Process
- Information Security Risk Assessment Process
- Information Security Risk Treatment Process
- Security Implementation Management Process
- Process to Control Outsourced Services
- Process to Assure Necessary Awareness and Competence
- Information Security Incident Management Process
- Internal Audit Process
- Performance Evaluation Process
- Information Security Improvement Process
- Records Control Process
- Resource Management Process
- Communication Process
- Information Security Customer Relationship Management Process

Keepnet Labs

Name:
Title:
Signature:
Date:

Company

Name:
Title:
Signature:
Date: