Data Protection Addendum

This Data Protection Addendum (**"DPA"**) is incorporated into and made part of the Terms of Service (**"Terms"**) or the Agreement signed between Customer and Keploy (" **Agreement**",) as applicable and governs the Processing of Personal Data by Keploy as a Processor on behalf of Customer or Customer Affiliates, as applicable as the Controller. Unless otherwise defined in this DPA, capitalized terms shall have the same meaning as given to them in the Agreement. The term "Agreement" as used in this DPA shall either mean the "Terms" or the "Agreement", as applicable.

The purpose of this DPA is to reflect the parties' agreement with regard to the Processing of Personal Data, in accordance with the requirements of Applicable Data Protection Law. This DPA consists of two parts: (1) the main body of the DPA, and (2) the EU Standard Contractual Clauses. The DPA and the Standard Contractual Clauses have been pre-signed on behalf of Keploy.

In the course of providing the Services to Customer pursuant to the Agreement, the Keploy may Process Personal Data on behalf of Customer and both parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith. To the extent that any terms of the Agreement conflict with the substantive terms of this DPA (as they relate to the protection of Personal Data), the terms of this DPA shall take precedence.

This Data Protection Addendum is entered into by _____(**"Customer")** and Keploy, Inc. (**"Keploy"**), each a **"Party"** and together the **"Parties".**

1. Definition

1.1. **Relationship with Agreement** . This DPA forms part of, and shall be co-terminus with, the Agreement. This DPA shall be applicable to any Personal Data collected during the course of the Services provided under the Agreement.

1.2. **Definitions**. In this DPA, the following terms have the following meanings:

(i) **"Applicable Data Protection Laws"** means all applicable and relevant laws and regulations applicable to Keploy's processing of Personal Data under the Agreement.

(ii) **"Agreement"** means the contract in place between Customer and Keploy in connection with the purchase of Products by Customer.

(iii) **"Customer"** means the first party named above. However, in the event Keploy is required to process Personal Data on the request of an Affiliate of Customer, such Affiliate shall also be deemed as the "Customer". Any reference to the Customer within this DPA, unless otherwise specified, shall include Customer and its Affiliates.

(iv) **"CCPA"** means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

(v) **"Controller"** means the entity which determines the purposes and means of the Processing of Personal Data.

(vi) **"Personal Data"** means any information related to any identified or identifiable natural person.

(vii) **"Processing" or "Process"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(viii) **"Processor"** means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA.

(ix) **"Customer Account Data"** means any Personal Data (other than Test execution data) provided by the Customer during the Services and includes Peronal data or PII to any employee, user, or customer personnel. We refer to this data as **'**Keploy Account data.**'** PII contains names, email addresses, and contact details.

(x) **"Test Execution Data"** means any information, including PII, which is stored (including data stored for back-up) and processed in or transmitted via the Keploy platform by, or on behalf of theCustomer.. **'**Test execution data**'** need not contain any identifiable PII and sensitive PII regarding Customer personnel, customers, end-users, or other third parties.

(xi) "**Data Subjects**" shall have such meaning as provided under the GDPR.

(xii) "**GDPR**" shall mean the Regulation (EU) 2016/679 of the European Parliament and the Council of 27th April 2016 on the protection of natural persons with regard to the processing of Personal data and on the free movement of such data, and repealing Directive 95/46/EC.

(xiii) "**Processing**" means any operation or set of operations performed on data or sets of data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction. "Process," "Processes," and "Processed" shall have the same meaning.

(xiv) **"Restricted Transfer** " means a transfer (directly or via onward transfer) of Personal Data that is subject to Applicable Data Protection Law to a country outside Europe that is not subject to an adequacy decision by the European Commission or the competent UK or Swiss authorities (as applicable).

(xv) **"Security Incident**" means any confirmed breach of security that leads to the accidental, or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data processed by Keploy and/or its Sub-processors in connection with the provision of the Service. For the avoidance of doubt, "Security Incident" does not include unsuccessful attempts or activities that do not compromise the security of personal data, including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

(xvi) "**Services**" means the services provided to the Customer or any other activities performed on behalf of the Customer by Keploy, pursuant to the Agreement.

(xvii) "**Sub-Processor**" means any processor or a third party engaged by or on behalf of Keploy to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA where such entity processes Customer Personal Data.

(xviii) "**Supervisor**"**:** means any data protection supervisory authority as defined in the GDPR with competence over Customer and Keploy's processing of Personal Data.

(xix) "**Standard Contractual Clauses**" or **"EU SCCs"** means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. SCCs set out in Annexure 3 which do not ensure an adequate level of protection of Personal Data, which have been approved by the European Commission as adducing adequate safeguards for Restricted Transfers, or any successor clauses thereto or recognized by the European Commission pursuant to Article 46 of the GDPR, or by the relevant Secretary of State where the UK GDPR applies. Standard Contractual Clauses are referred to as "Clauses" within Annexure 3.

In short, it means the contractual clauses dealing with the transfer of Personal Data outside the EEA, which have been approved by (i) the European Commission under the Data Protection Legislation, or (ii) by a competent supervisory authority under Data Protection Legislation.

NOTE : Where the Applicable Data Protection Laws are the laws and regulations of the United Kingdom, references to "***Standard Contractual Clauses***" or "**SCCs**" shall be interpreted to include any standard data protection clauses adopted under UK GDPR, Art.46

(xx) "**Appropriate Technical and Organizational Measures**", "Personal Data", "Personal Data Breach", "Process / Processing", "Controller", "Processor", "Subprocessor" and "Data Subject" shall have the same meaning as ascribed to them under the GDPR provided that "Personal Data" as used herein only applies to Personal Data for which Keploy is a Processor.

2. Ownership Of Test Execution Data

As between the Parties, all Test Execution Data processed under the terms of this DPA and the Agreement shall remain the property of Customer. Under no circumstances will Keploy act, or be deemed to act, as a "Controller" (or equivalent concept) of the Test Execution Data under any Applicable Data Protection Law.

3. Data Processing

a. Keploy shall:

- Process Personal Data for the legitimate business purpose only and/or to provide Keploy Services to the Customer or Permitted Users.

- Process Personal Data only in accordance with the specific instructions of the Customer or Permitted Users unless Processing is required by applicable laws. Such instructions can be in writing or by electronic means.
- Comply with all Applicable Data Protection Laws in the Processing of Personal Data

b. Each Customer or Permitted User hereby instructs and authorizes Keploy (and authorizes Keploy to instruct each Sub processor) to Process Personal Data and Account-Related Information for the above purposes including authorizing Keploy to transfer such data to any country or territory as reasonably necessary for the provision of Keploy Services and consistent with the Agreement.

4. Obligations of Keploy

4.1. The Parties agree that the subject matter and duration of Processing performed by Keploy under this DPA, including the nature and purpose of Processing, the type of Personal Data, and categories of Data Subjects, shall be as described in **Annexure 1** of this DPA.

4.2. As part of the Services to Customer, Keploy shall comply with the obligations imposed upon under Article 28-32 of the GDPR and agrees and declares as follows:

(i) to process Personal Data in accordance with Customer's documented instructions as set out in the Agreement and this DPA, also with regard to transfers of Personal Data to a third country or an international organisation in accordance with Article 28 (3)(a) of the GDPR, unless required to do otherwise by Union or Member State Law to which the Keploy is subject. In any such case, Keploy shall inform Customer of that legal requirement upon becoming aware of the same (except where prohibited by applicable laws);

(ii) to ensure that all staff and management of any member of the Processor are fully aware of their responsibilities to protect Personal Data in accordance with this DPA and have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality in accordance with Article 28 (3)(b) of the GDPR;

(iii) to implement and maintain appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access, provided that such measures shall take into account the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved in the processing and will include those measures described in **Annexure 2;**

(iv) to notify Customer in accordance with Article 33(2) of the GDPR, without undue delay, but in any event within forty-eight (48) hours, in the event of a confirmed Personal Data Breach affecting Customer's Personal Data and to take appropriate measures to mitigate its possible adverse effects;

(v) to comply with the requirements of Section 5 (Use of Sub-processors) when engaging a Sub- processor;

(vi) to assist Customer, taking into account the nature of the Processing and insofar as it is commercially reasonable, to fulfil Keploy's obligation to respond to requests from Data Subjects to exercise their rights under Applicable Data Protection Law (a "Data Subject Request"). In the event that Keploy receives a Data Subject Request directly from a Data Subject, it shall, unless prohibited by law, direct the Data Subject to the Customer. In the event

Customer is unable to address the Data Subject Request, taking into account the nature of the Processing and the information available to Keploy, Keploy shall, on Customer's request and at Customer's reasonable expense (scoped prior to Keploy 's response to the Data Subject Request), address the Data Subject Request, as required under the Applicable Data Protection Law;

(vii) upon request, to provide Customer with commercially reasonable information and assistance, taking into account the nature of the processing and the information available to Keploy, to help Customer to conduct any data protection impact assessment, data transfer impact assessment or Supervisor consultation it is required to conduct under Applicable Data Protection Law;

(viii) upon termination of Customer's access to and use of the Service, to comply with the requirements of Section 9 of this DPA (Return and Destruction of Personal Data);

(ix) to comply with the requirements of Section 6 of this DPA (Audit & Certifications) in order to make available to Customer information that demonstrates Keploy's compliance with this DPA; and

(x) to appoint a Data Protection Officer (DPO) who will act as a point of contact for Customer, and coordinate and control privacy & data protection and security compliance with this DPA, including the measures detailed in Annexure 2. The DPO can be reached by email at support@keploy.io

4.3. Keploy shall immediately inform Customer if, in its opinion, Customer's processing instructions infringe any law or regulation. In such event, Keploy is entitled to refuse processing of Personal Data that it believes to be in violation of any law or regulation.

5. Use of Sub-Processors

5.1. Customer hereby confirms its general written authorisation for Keploy's use of the Sub-processors list ("Sub-processor List") in accordance with Article 28 of the GDPR to assist Keploy in providing the Service and processing Personal Data, provided that such Sub-processors:

(i) agree to act only on Keploy instructions when processing the Personal Data, which instructions shall be consistent with Customer's processing instructions to Keploy;

(ii) agree to protect the Personal Data to a standard consistent with the requirements of this DPA, including implementing and maintaining appropriate technical and organisational measures to protect the Personal Data they process consistent with the Security Standards described in **Annexure 3** to this DPA, as applicable.

5.2. Keploy shall remain liable to Customer for the subcontracted Processing services of any of its Sub-processors under this DPA. Keploy shall update the Sub-processor list page on its Website of any Sub-processor to be appointed at least fifteen (15) days prior to such change.

5.3. In the event that Customer objects (subject to reasonable grounds) to the processing of its Personal Data by any newly appointed Sub-processor as described in Section 5.2, it shall inform Keploy with adequate reasons within fifteen (15) days following the update of its Website Sub-processor list. In such event, Keploy will either (a) instruct the Sub-processor to cease

the processing of Customer's Personal Data, in which event this DPA shall continue unaffected, or (b) allow Customer to terminate this DPA and the Agreement with Keploy immediately.

5.4. The Service provides links to integrations with non Keploy Services, including, without limitation, certain non Keploy Services which may be integrated directly into Customer's account or instance in the Service. If Customer elects to enable, access, or use such non-Keploy Services, its access and use of such non-Keploy Services is governed solely by the terms and conditions and privacy policies of such non-Keploy Services, and Keploy does not endorse and is not responsible or liable for, and makes no representations as to any aspect of such non-Keploy Services, including, without limitation, their content or the manner in which they handle Test Execution Data (including Personal Data) or any interaction between Customer and the provider of such non-Keploy Services. The providers of non-Keploy Services shall not be deemed Sub-processors for any purpose under this DPA.

5.5. Keploy shall be liable for the acts and omissions of its Sub-processors to the same extent Keploy would be liable if performing the services of each Sub-processor directly under the terms of this DPA, unless otherwise set forth in the Agreement.

6. Audits and Certifications

6.1. Audit:

(a) Customer acknowledges that Keploy is regularly audited by independent third-party auditors and/or internal auditors including as may be described from time to time at Upon request, and on the condition that Customer has entered into an applicable non-disclosure agreement with Keploy , Keploy must:

i. supply a summary copy of its audit report(s) (" **Report**") to Customer, so Customer can verify Keploy 's compliance with the audit standards against which it has been assessed, and this DPA; and

ii. provide written responses to all reasonable requests for information made by Customer related to its Processing of Customer Personal Data, including responses to information security, privacy, and audit questionnaires, that are necessary to confirm Keploy's compliance with this DPA, provided that Customer cannot exercise this right more than once per calendar year.

(b) Only to the extent Customer cannot reasonably satisfy Keploy's compliance with this DPA through the exercise of its rights under Section 6(a) above, where required by Applicable Data Protection Law or the Standard Contractual Clauses, Customer and its authorized representatives may conduct audits (including inspections) during the term of the Agreement to establish Keploy's compliance with the terms of this DPA, on the condition that Customer and its authorized representatives have entered into an applicable non-disclosure agreement with Keploy. Notwithstanding the foregoing, any audit (or inspection) must be conducted during Keploy's regular business hours, with reasonable advance notice (which may not be less than 30 calendar days) and subject to reasonable confidentiality procedures. Such audit (or inspection) may not require Keploy to disclose to Customer or its authorized representatives, or to allow Customer or its authorized representatives to access:

i. any data or information of any other Keploy customer (or such customer's Users);

ii. any Keploy internal accounting or financial information;

iii. any Keploy trade secret or restricted information.

iv. any information that, in Keploy's reasonable opinion, could: (1) compromise the security of Keploy systems or premises; or (2) cause Keploy to breach its obligations under Applicable Data Protection Law or its security, confidentiality and or privacy obligations to any other Keploy customer or any third party; or

v. any information that Customer or its authorized representatives seek to access for any reason other than the good faith fulfillment of Customer's obligations under the Applicable Data Protection Law and Keploy's compliance with the terms of this DPA.

(c) An audit or inspection permitted in compliance with Section 6 (b) will be limited to once per calendar year, unless (1) Keploy has experienced a Security Incident within the prior twelve
(12) months which has impacted Customer Personal Data; or (2) Customer is able to evidence an incidence of Keploy's material noncompliance with this DPA.

6.2. Additional Independent Audit . To extent the audit reports, certification, documentation and/or third-party audit reports mentioned above are not sufficient to demonstrate compliance with the obligation in this DPA, the Customer may execute or appoint a third-party independent auditor in such an event, the parties agree that:

(i) Customer is responsible for all costs and fees relating to such audit;

(ii) A third-party auditor must be mutually agreed upon between the parties and such auditor shall follow industry standard and appropriate audit procedures;

(iii) The Controller's right to audit shall be subject to giving the Processor at least 4 weeks prior written notice of any such audit at support@keploy.io. The notice period for the right to audit may be reduced as per mutual discussion if such audit is required as part of an investigation by a regulator;

(iv) Such audit must not unreasonably interfere with Keploy's business activities and must be reasonable in time and scope of services;

(v) The parties must agree to a specific audit plan prior to any such audit, which must be negotiated in good faith between the parties; and

(vi) These rights of the Controller shall not extend to facilities that are operated by Sub- processors which the Processor may use to attain its Purpose and provide its Services.

Cloud Security Alliance. The parties acknowledge and agree that to the extent Keploy Processes any Test Execution Data outside the EEA in a country that has not been designated as providing an adequate protection for any Test Execution Data (including personal data any), Keploy shall deemed to provide adequate protection under Applicable Data Protection Laws for any such Test Execution Data due to Keploy's self-assessment under Cloud Security Alliance (CSA) code of conduct.

7. International Data Exports

7.1. Customer acknowledges that Keploy and its Sub-processors may process Personal Data in countries that are outside of the EEA, United Kingdom, and Switzerland ("European Countries"). This will apply even where Customer has agreed with Keploy to host Personal Data in the EEA in accordance with Keploy's regional data hosting policy if such non- European Countries processing is necessary to provide support-related or other services requested by Customer. If Personal Data is transferred to a country or territory outside of EEA, then such transfer will only take place if:

(a) the country ensures an adequate level of data protection.

(b) one of the conditions listed in Article 46 GDPR (or its equivalent under any successor legislation) is satisfied; or

7.2. **EU Standard Contractual Clauses:** Where Keploy processes Personal Data in non-EEA countries, Keploy shall comply with the EU Commission's Standard Contractual Clauses (annexed to EU Commission Decision 2021/914/EU of 4 June 2021) (the "EU SCCs") shall be entered into and incorporated into this DPA by this reference and completed as follows:

To the extent Keploy transfers or Processes any Test Execution Data relating to Data Subjects in the European Union outside the European Union, all actions in relation to such Test Execution Data shall be governed by the Standard Contractual Clauses. A copy of the Standard Contractual Clauses, as applicable currently, is attached hereto as **Annexure 3.**

For the purposes of such Standard Contractual Clauses:

(i) the Customer shall be the "Controller" and the "data exporter" and Keploy shall be the "Processor" and the "data importer";

(ii) the parties agree that Module Two (Controller to Processor) of the Standard Contractual Clauses shall be applicable;

(iii) All references to "Annex I.A" shall instead refer to the parties' details (data exporter: Customer; data importer: Keploy; and contact details) as identified in the Agreement.

(iv) all references to "Annex I.B", shall instead refer to Annexure 1 of this DPA; and

(v) all references to "Annex II.B", shall instead refer to Annexure 2 of this DPA.

8. Obligations of Customer

8.1. As part of Customer receiving the Service under the Agreement, Customer agrees to abide by its obligations under Applicable Data Protection Laws.

9. Return and Destruction of Personal Data

9.1. Upon termination of Customer's access to and use of the Service, Keploy will within thirty (30) days following such termination, at the choice of the Customer either:

(a) permit Customer to export its Test Execution Data, at its expense; or

(b) delete all Test Execution Data in accordance with the capabilities of the Service and Article 28 (3)(g) of the GDPR. Following such period, Keploy shall delete all Test Execution Data stored or processed by Keploy on behalf of Customer in accordance with Keploy's deletion policies and procedures. Customer expressly consents to such deletion.

10. Duration

10.1. This DPA will remain in force as long as Keploy processes Personal Data on behalf of Customer under the Agreement.

11. Incident Responses and Data Breach

11.1. Notice of Non-Compliance. If Keploy cannot provide compliance or foresees that it cannot comply with its obligations as set out in this DPA, it agrees to promptly inform the Customer of the same. Upon such notice, the Customer is entitled to suspend the transfer and Processing of any Test Execution Data or Customer Data.

11.2. Notice of Security Breach. Keploy will notify Customer promptly and without undue delay of an actual or potential Security Breach or any security exposure of Customer system or data relating to the Security Breach as it becomes known or as is reasonably requested by Customer. Keploy's notification of a Security Breach will describe, to the extent possible, the nature of the Security Breach, the measures taken to mitigate the potential risks and the measures that Keploy recommends Customer take to address the Security Breach.

11.3. Consequences of a Security Breach Notification . Keploy shall promptly take reasonable steps to minimize harm and secure Test Executionr Data in the event of a Security Breach. Keploy's notification of or response to a Security Breach will not be construed as an acknowledgment by Keploy of any fault or liability with respect to the Security Breach.

11.4. Data Subject Requests. Any request from a Data Subject directly to Keploy shall be directed to the Customer. Upon instruction by the Customer, Keploy shall correct, rectify, or block any Customer Data to the extent they can be done by Keploy. Keploy shall cooperate to the necessary extent and provide the Customer with appropriate support wherever possible in the fulfilment by the Customer of the rights of the Data Subjects pursuant to Articles 12 to 22 GDPR, in the preparation of records of Processing activities, and in the case of necessary data protection impact assessments by the Customer. Except as specified above, Keploy has no obligation to assess any Personal Data in order to identify information subject to any specific legal requirements.

11.5. Confidentiality. Information that may be disclosed in any form between Parties with respect to, or as a result of this DPA, shall be deemed to be Confidential Information (as defined under the Agreement). Information relating to Keploy's database, procedures, and processes shall be considered Confidential Information.

12. Limitation of Liability

11.1. This DPA shall be subject to the limitations of liability agreed between the Parties set forth in the Agreementand any reference to the liability of a Party means that Party and its Affiliates in the aggregate. For the avoidance of doubt, Customer acknowledges and agrees that

Keploy's total liability for all claims from Customer or its Affiliates arising out of or related to the Agreement and this DPA shall apply in aggregate for all claims under both the Agreement and this DPA. For the avoidance of doubt, this section shall not be construed as limiting the liability of either Party with respect to claims brought by Data Subjects.

12. Miscellaneous

12.1. This DPA may not be amended or modified except in writing and signed by both Parties. This DPA may be executed in counterparts. Each Party's rights and obligations concerning assignment and delegation under this DPA shall be as described in the Agreement. Subject to the foregoing restrictions, this DPA will be fully binding upon, inure to the benefit of and be enforceable by the Parties and their respective successors and assigns.

IN WITNESS WHEREOF, the Parties hereto have executed this DPA by their duly authorised officers or representatives as of the last date of execution below ("Effective Date").

Customer:		**Keploy, Inc.:**	
BY:		BY:	
NAME:		NAME:	
TITLE:		TITLE:	
DATE:		DATE:	
EMAIL:		EMAIL:	Attn: Keploy Privacy Team and DPO support@keploy.io

[END OF DPA]

Annexure 1 - Details of Processing

Data Exporter: Customer
Contact Details: Provided in the DPA signature block.
Data Exporter Role: Customer is _____.

Data Importer: Keploy, Inc.
Contact Details: Provided in the DPA signature block.
Data Importer Role: Keploy is a processor.

1. **Nature and Purpose of the Processing:** Keploy will process Personal Data in the course of providing Service(s) under the Agreement, which may include operation of a cloud-based Testing services platform. Additional information about Keploy Services is available at Keploy.io. Keploy will process Personal Data as a processor in accordance with Customer's instructions.
2. **Processing Activities:** Personal Data contained in Test Execution Data will be subject to the hosting and processing activities of providing the Services.
3. **Duration of Processing:** The processing of Personal Data shall endure for the duration of the Subscription Term in the MSA and this DPA on a continuous basis
4. **Data Subjects:** Customer may, at its sole discretion, submit Personal Data to the Service(s), which may include, but is not limited to, the following categories of data subjects: employees (including contractors and temporary employees), relatives of employees, customers, prospective customers, service providers, business partners, vendors, End-Users, advisors (all of whom are natural persons) of Customer and any natural person(s) authorized by Customer to use the Service(s).
5. **Categories of Personal Data** : Customer may, at its sole discretion, transfer Personal Data to the Keploy Service(s) which may include, but is not limited to, the following categories of Personal Data: first and last name, email address, title, position, employer, contact information (company, email, phone numbers), communications (telephone recordings, voicemail), and customer service information.
6. **Retention:** Keploy will process and retain Personal Data in accordance with the Section 9 (Return and Destruction of Personal Data) of this DPA and Keploy Data Deletion Policy

[END OF ANNEXURE 1]

Annexure 2

Keploy Technical and Organisational Security Measures

Keploy reserves the right to update its security & privacy program from time to time; provided, however, any update will not materially reduce the overall protections set forth in this DPA .

Keploy will implement and maintain appropriate technical and organisational measures designed to protect Personal Data, including, at a minimum:

(a) Access controls: role-based access control, least privilege, and MFA for administrative access.

(b) Encryption: encryption in transit using TLS (industry-standard) and encryption at rest for production systems storing Personal Data.

(c) Logging & monitoring: audit logging for administrative access and security monitoring for unauthorized access attempts.

(d) Vulnerability management: regular vulnerability scanning and timely remediation based on severity.

(e) Secure development: change management and code review practices for production releases.

(f) Incident response: documented incident response process and breach notification consistent with this DPA.

(g) Backups & resilience: backup procedures and measures designed to maintain availability and recoverability.

(h) Personnel confidentiality: confidentiality obligations for personnel with access to Personal Data.

Keploy may update these measures from time to time, provided such updates do not materially decrease the overall level of protection.

[END OF ANNEXURE 2]

ANNEXURE 3: STANDARD CONTRACTUAL CLAUSES

Select which module(s) applies:

□ MODULE ONE: Transfer Controller to Controller

☒ MODULE TWO: Transfer Controller to Processor

□ MODULE THREE: Transfer Processor to Processor

□ MODULE FOUR: Transfer Processor to Controller

SECTION I

Clause 1: Purpose and Scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex
I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Clause 2: Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these

Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3: Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clauses 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clauses 9(a), (c), (d) and (e);

(iv) Clauses 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clauses Clause 18(a).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4: Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5: Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6: Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7: Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8: Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the

data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all 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.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to

notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the

same country as the data importer or in another third country, hereinafter 'onward transfer') if

the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9: Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 15 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub- processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub- processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10: Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11: Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12: Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non- material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to

claim back from

the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13: Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14: Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its

obligations

under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination

only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15: Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules.

These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16: Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations

applying to the processing in question under Regulation (EU) 2016/679.

Clause 17: Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the laws of Ireland.

Clause 18: Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved before the courts of Ireland.

(b) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(c) The Parties agree to submit themselves to the jurisdiction of such courts.

EXHIBIT A

A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller

☒ **MODULE TWO: Transfer controller to processor**

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name:

Address:

Contact details:

Activities relevant to the data transferred under these Clauses: Use of service provided by data importer.

Signature and date: …

Role (controller/processor): Controller

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: Keploy Inc.

Address: New Burton Road Central Dover, DE United States

Contact details: support@keploy.io

Activities relevant to the data transferred under these Clauses: Service Provision

Signature and date: …

[END OF ANNEXURE 3]