Data Protection Addendum for Partners/ Customers from European Economic Area

This DoSelect Data Processing Addendum (DPA) is incorporated by reference into any and all services agreements, insertion orders and addendums currently in place between Partner (defined below) and Axilly Labs Private Limited ("DoSelect"), collectively ("Agreement"). This DPA is entered into as of the later of the dates beneath the party's signatures below. By entering into this DPA, Partner represents and warrants that Partner has the authority to legally bind both the Partner and all of Partners personnel, representatives and/or affiliates operating pursuant to any such Agreement referenced herein. The parties agree to comply with the following provisions with respect to any Personal Data of one or more Data Subjects located in the European Economic Area Processed in connection with the Agreement. The purposes of the DPA is to ensure such Processing is conducted in accordance with Data Protection Laws, including the GDPR and with due respect for the rights and freedoms of individuals whose Personal Data are Processed. References to the Agreement will be construed as including this DPA. To the extent that the terms of this DPA differ from those in the Agreement, the terms of this DPA shall govern

Definitions

All terms (capitalized and otherwise) not defined in this DPA including, without limitation, "personal data," "controller" "processing," "data protection officer" "data subject" and "processor," shall have the meanings set forth in the privacy and data protection laws, regulations, and decisions applicable to a party to this DPA ("Applicable Data Protection Law(s)"). For the sake of clarity, Applicable Data Protection Laws include the EU Directive 95/46/EC and the General Data Protection Regulation (2016/679) and any implementing legislation.

"Partners"- are those companies, organizations, body corporate s or individuals, who use our Services to: 1) evaluate the hiring potential of a prospective employee or interns; 2) evaluate the skill proficiency of their students or employees; 3) Host contests; 3) Upskill their students or employees; 4) Any other legitimate activities that can be executed using our Services.

1. Role of the Parties

1.1. Parties agree that the Partner(s) is and will at all times remain the Controller of the Data processed by DoSelect hereunder and that DoSelect may process the Data as a processor and at times, may as a separate and independent controller as strictly required for the Services. In no event will the parties process the Data jointly as joint controllers. Neither party is required to obtain authorization from the other party in relation with its processing of the Data it controls.

1.2. Partner agrees and acknowledges that it is responsible for compliance with all its obligations as a Controller under Applicable Data Protection Law, specifically with reference to transmission of Data to DoSelect (including providing any required notices and obtaining any required consents and/or authorizations, or otherwise securing an appropriate legal basis under Applicable Data Protection Law), and for any decisions and actions taken by the Partner with respect to processing such Data.

1.3. DoSelect is responsible for compliance with its obligations under this DPA and as a processor under Applicable Data Protection Law. DoSelect, including any DoSelect affiliate and/ or Sub-processors, shall process Data solely for the purpose of (i) providing the Services in accordance with the General Terms and Conditions, where applicable, and this DPA (ii) complying with any documented written instructions provided by the Partner(s), or (iii) complying with DoSelect's regulatory obligations. DoSelect will comply with the aforesaid instructions provided by Partner(s), to the extent necessary for DoSelect to (i) comply with its obligations under Applicable Data Protection Law; or (ii) assist the Partner to comply with its respective

obligations under Applicable Data Protection Law relevant to the use or rendering of the Services.

1.4. Each party is separately responsible for honouring data subject access requests under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable) and responding to correspondence, inquiries and complaints from data subjects. Each party shall provide reasonable and timely assistance to the other party as necessary to help facilitate compliance with this sub-section 1.4.

2. Security Measures

2.1. DoSelect has implemented and will maintain appropriate technical and organizational security measures for the processing of Data. These measures are intended to protect Data against the risks inherent to the processing of such Data in the rendering of the Services, and DoSelect may, at its sole discretion and as required to be compliant with Applicable Data Protection Law, modify and amend it from time to time.

2.2 Both parties shall ensure that their respective personnel engaged in the Processing of Personal Data under this DPA are informed of the confidential nature of the Personal Data as well as any security obligations with respect to such Personal Data. The Parties shall ensure that access to Personal Data covered under this DPA is limited to that person who require such access to perform the Services.

2.3 Both parties will (taking into account the nature of the processing of Personal Data under this DPA) cooperatively and reasonably assist each other in ensuring compliance with any of each other's respective obligations with respect to the security of Personal Data and Personal Data breaches under this DPA.

2.4 Further, Partner(s) shall maintain administrative, physical and technical safeguards for the protection of the security, confidentiality and integrity of Personal Data under this DPA. Partner(s) will implement and maintain technical and organizational measures to protect such Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to Personal Data. The Security Measures may include measures to encrypt Personal Data; to help ensure ongoing confidentiality, integrity, availability and resilience of Partner(s) systems and services; to help restore timely access to Personal Data following an incident and for regular testing of effectiveness.

3. Sub-Processors and Sub-Processing

3.1. Partner acknowledges and agrees that DoSelect may engage third-party Sub-processors in connection with the provision of the Services. DoSelect agrees that any agreement with a Sub-processor will include substantially the same data protection obligations as set out in this DPA.

3.2. A list of Sub-processors is available in the DoSelect user interface or at a particular web page hosted by DoSelect. DoSelect may change the list of such other Sub-processors by no less than 10 business days' notice via the DoSelect user interface. If Partner objects to DoSelect's change in such Sub-processors, DoSelect may, as its sole and exclusive remedy, terminate the portion of the Agreement relating to the Services that cannot be reasonably provided without the objected-to new Sub-processor by providing 30 days' written notice to Partner.

3.3. Where Partner engage third-party Sub-processors in connection with the provision of the Services, Partner must provide a list of Sub-Processors to DoSelect, at DoSelect's written request. Partner will have a written agreement with each Sub-processor and agrees that any agreement with a Sub-processor will include substantially the same data protection obligations as set out in this DPA and DPA.

3.4. Both parties shall be liable for the acts and omissions of its Sub-processors to the same extent such party would be liable under the terms of this DPA and DPA.

4. Security Breach

4.1. If either party becomes aware of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to any Personal Data transmitted, stored or otherwise processed on the other party's equipment or facilities under this DPA ("Security Breach"), such party will promptly notify the other party of the Security Breach. Notifications made pursuant to this section will take place within a reasonable time and certainly no longer than three business days after discovery and shall describe, to the extent possible, details of the Security Breach, including steps taken to mitigate the potential risks and any recommended steps that either or both parties should take to address the Security Breach. Each party will promptly investigate the Personal Data Breach if it occurred on its infrastructure or in another area it is responsible for and will assist the other party as reasonably necessary for both parties to meet their obligations under Applicable Data Protection Laws.

4.2. Both parties agree that an unsuccessful Security Breach attempt will not be subject to this Section 4. An unsuccessful Security Breach attempt is one that results in no unauthorized access to personal data processed pursuant to this DPA or to any of either party's equipment or facilities storing personal data.

4.3. Any notification of or response to a Security Breach under this Section 4 will not be construed as an acknowledgment by either party of any fault or liability with respect to the Security Breach.

5. Liability

Both parties agree that their respective liability under this DPA shall be apportioned according to each party's respective responsibility for the harm (if any) caused by each respective party.

6. Retention of Data.

On expiry of the Agreement, both parties hereby instruct the other to delete all Personal Data (including existing copies) from their respective systems and discontinue processing of such Personal Data in accordance with Data Protection Law as soon as reasonably practicable and within the time frame, wherein, the processing of such data does not serve any 'legitimate business interest' as defined in the Data Protection Law. This requirement shall not apply to the extent that the Personal Data has been archived on backup systems so long as such Personal Data is isolated and protected from any further processing except to the extent required by applicable law, in the case the data is not subject to any Data Protection Law) and where the applicable law requires further storage.

7. Cross-Border Data Transfers.

7.1 The use of or provision of the Services may require the transfer of Personal Data of Data Subjects located in the EU to countries outside the EEA. Each party will ensure an appropriate mechanism that is recognized by applicable Data Protection Laws is implemented to allow for the data transfer and shall ensure both it and its Data Controllers, Data Processors, and Sub-Processors will comply with the related requirements of the alternative mechanism for data transfer.

8. Miscellaneous

8.1 This DPA will take effect on the date it is executed by Partner and DoSelect at the bottom of this Agreement (the Effective Date) and will remain in effect until, and automatically expire upon, the deletion of all Personal Data by DoSelect or Partner through the Services as described in this DPA.

8.2 Nothing in this DPA shall impact Partners intellectual property rights with respect to Personal Data provided by Partner under the Agreement except to the extent required by applicable law.

8.3 Nothing in this DPA shall confer any benefits or rights on any person or entity other than the parties to this DPA.

8.4 This DPA may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one Agreement.

IN WITNESS of which the parties have executed this Agreement on the date set out above.

Signed by:

Partner

Name:

Designation:

Date:

Axilly Labs Private Limited

Name: Rohit Agrawal

Designation: CEO

Date: