andela

Data Processing Addendum

This Data Processing Addendum ("DPA") supplements and is incorporated by reference into the Master Services Agreement (the "Agreement") entered into by and between the client entity that is party to the Agreement ("Client") and Andela, Inc. ("Andela" and, together with Client, the "Parties"). This DPA incorporates the terms of the Agreement. Andela may update this DPA from time to time, and will provide reasonable notice of any such updates. Any terms not defined in this DPA shall have the meaning set forth in the Agreement.

1. Definitions

1.1 "Authorized Subprocessor" means a third-party entity engaged by Andela to "Process" (as defined herein) "Personal Data" (as defined herein) in order to provide the Services and that has been approved by Client in accordance with Section 6.

1.2 "Andela Account Data" means Personal Data that relates to Andela's relationship with Client, including the names or contact information of individuals authorized by Client to access Client's account and billing information of individuals that Client has associated with its account.

1.3 "Andela Usage Data" means Services usage Personal Data collected and processed by Andela in connection with the provision of the Services, including without limitation Personal Data used to identify the source and destination of a communication, activity logs, and similar Personal Data.

1.4 "Data Privacy Framework" means, as applicable, EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and/or the Swiss-U.S. Data Privacy Framework.

1.5 "Data Subject" means a natural person whose Personal Data is protected by Privacy Laws. For the avoidance of doubt, "Data Subject" includes the term "Consumer" under Privacy Laws.

1.6 "Data Subject Request" means a request from a Data Subject to exercise their rights over Personal Data afforded pursuant to Privacy Laws.

1.7 "EU SCCs" means standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time), as modified by Section 9 of this DPA.

1.8 "ex-EEA Transfer" means the transfer of Personal Data subject to the GDPR from the European Economic Area (the "EEA") to a country where the transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.

1.9 "ex-UK Transfer" means the transfer of Personal Data subject to Chapter V of the UK GDPR from outside the United Kingdom (the "UK") where such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the Data Protection Act 2018.

1.10 "Personal Data" means any information provided to Andela by or on behalf of Client in connection with the Services that relates to an identified or identifiable Data Subject and constitutes "personal data," "personal information," or equivalent term under Privacy Laws.

1.11 "Privacy Laws" means any applicable laws and regulations in any relevant jurisdiction relating to the Processing of Personal Data including, each to the extent applicable (i) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR") and the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR") (together, collectively, the "GDPR"), (ii) the Swiss Federal Act on Data Protection, (iii) the UK Data Protection Act 2018, (iv) the Privacy and Electronic Communications (EC Directive) Regulations 2003, and (v) the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020 (the "CCPA"); in each case, as updated, amended or replaced from time to time. The terms "affiliates," "business purpose," "Controller," "Processor," "sell," "share," or "supervisory authority," shall have the meanings set forth for those or equivalent terms under Privacy Laws. For the avoidance of doubt, the

terms “Controller” and “Processor” include “Business” and “Service Provider,” respectively, as defined in the CCPA.

1.12 “Process” (and its derivatives) means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, securing, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination, sale, transfer, or otherwise making available, alignment or combination, blocking, erasure, or destruction.

1.13 “Standard Contractual Clauses” means, as applicable, the EU SCCs and the UK SCCs.

1.14 “UK Addendum” means the template International Data Transfer Addendum issued by the Information Commissioner and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022 (as may be amended from time to time), as completed by Exhibit D.

1.15 “UK SCCs” means the EU SCCs, as amended by the UK Addendum.

2. Role of the Parties; Description of Processing.

2.1 Except as expressly set forth in this DPA or the Agreement, with respect to Personal Data, Client is the Controller and Andela is a Processor of Client Personal Data, or to the extent Client is a Processor to a third-party Controller, Andela is a subprocessor.

2.2 Andela shall Process Personal Data only (i) for purposes set forth in the Agreement, (ii) in a manner consistent with the documented instructions provided by Client, which shall include the Agreement and this DPA, and (iii) as required by Privacy Laws or a supervisory authority; in such case, Andela shall inform Client of that legal requirement before Processing to the extent legally permitted. The subject matter, nature, purpose, and duration of this Processing, as well as the types of Personal Data collected and categories of Data Subjects involved, are described in Exhibit A to this DPA.

3. Compliance with Privacy Laws. Client shall, in its use of the Services, at all times Process Personal Data, and provide written instructions for the Processing of Personal Data, in compliance with Privacy Laws. Client represents and warrants that it has obtained and documented all necessary consents, permissions, and rights to disclose the Personal Data and that the Personal Data and Andela’s use thereof as permitted by this Agreement will not infringe or misappropriate any intellectual property; violate any moral, literary, privacy, publicity, or other right of any consumer or entity; Privacy Laws, or violate Client’s own policies, or applicable law. Client shall ensure that the Processing of Personal Data in accordance with Client’s instructions will not cause Andela to be in breach of the Privacy Laws. Client is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Andela by or on behalf of Client, (ii) the means by which Client acquired any such Personal Data, and (iii) the instructions it provides to Andela regarding the Processing of such Personal Data. Client shall not provide or make available to Andela any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services and shall indemnify Andela from all claims and losses in connection therewith. Andela shall promptly notify Client if an instruction, in Andela’s opinion, infringes Privacy Laws or instruction of a supervisory authority.

4. Use of Personal Data. Andela shall not: (i) sell or share Personal Data; (ii) retain, use, or disclose Personal Data outside of Andela’s direct business relationship with Client or for any purpose other than for a business purpose under the CCPA on behalf of Client or as necessary to perform the Services for Client pursuant to the Agreement, except as otherwise permitted in the Agreement or by Privacy Laws; and (iii) combine Personal Data received from, or on behalf of, Client with personal data that it receives from, or on behalf of, another party or person, except as necessary to provide the Services or as otherwise instructed by Client.

5. Audit.

Andela shall maintain records sufficient to demonstrate its compliance with its obligations under this DPA. Upon Client’s written request at reasonable intervals, and subject to reasonable confidentiality

controls, Andela shall, either (i) make available for Client's review copies of certifications or reports demonstrating Andela's compliance with prevailing data security standards applicable to the Processing of Client Personal Data, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Privacy Laws, allow Client's independent third-party representative to conduct an audit or inspection of Andela's data security infrastructure and procedures that is sufficient to demonstrate Andela's compliance with its obligations under Privacy Laws, *provided that* (a) Client provides reasonable prior written notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Andela's business; (b) such audit shall only be performed during business hours and occur no more than once per calendar year; and (c) such audit shall be restricted to Personal Data relevant to Client. Client shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Andela for any time expended for on-site audits. If Client and Andela have entered into Standard Contractual Clauses as described in Section 9 (Transfers of Personal Data), the Parties agree that the audits described in Clause 8.9 of the EU SCCs shall be carried out in accordance with this Section 5.

6. Authorized Subprocessors.

6.1 Client acknowledges and agrees that Andela may (1) engage its affiliates as well as the Authorized Subprocessors listed in Exhibit B to this DPA to Process Personal Data in connection with the Services and (2) from time to time engage additional subprocessors for the purpose of providing the Services, including without limitation the Processing of Personal Data pursuant to Section 6.2. By way of this DPA, Client provides general written authorization to Andela to engage subprocessors as necessary to perform the Services.

6.2 A list of Andela's current Authorized Subprocessors (the "List") will be made available to Client upon written request and such List may be updated by Andela from time to time. Client acknowledges that certain subprocessors are essential to providing the Services and that objecting to the use of a subprocessor may prevent Andela from offering the Services to Client.

6.3 If Client reasonably objects to an engagement of a new subprocessor in accordance with Privacy Laws, and Andela cannot provide a commercially reasonable alternative within a reasonable period of time, Client may discontinue the use of the affected Services by providing written notice to Andela. Discontinuation shall not relieve Client of any fees owed to Andela under the Agreement.

6.4 Andela will enter into a written agreement with Authorized Subprocessors imposing on the Authorized Subprocessors data protection obligations comparable to those imposed on Andela under this DPA with respect to the protection of Personal Data. In case an Authorized Subprocessor fails to fulfill its data protection obligations under such written agreement with Andela, Andela will remain liable to Client for the performance of the Authorized Subprocessor's obligations under such agreement.

6.5 If Client and Andela have entered into Standard Contractual Clauses as described in Section 9 (Transfers of Personal Data), (i) the above authorizations will constitute Client's prior written consent to the subcontracting by Andela of the Processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the Parties agree that the copies of the agreements with Authorized Subprocessors that must be provided by Andela to Client pursuant to Clause 9(c) of the EU SCCs may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by Andela beforehand, and that such copies will be provided by Andela only upon written request by Client.

7. Confidentiality; Security of Personal Data.

7.1 Andela shall ensure that any person it authorizes to Process Personal Data has agreed to protect Personal Data in accordance with Andela's confidentiality obligations in the Agreement. Client agrees that Andela may disclose Personal Data to its advisers, auditors or other third parties as reasonably required in connection with the performance of its obligations under this DPA, the Agreement, or the provision of Services to Client.

7.2 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Andela shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of Processing Personal Data, as described in Exhibit C.

8. Personal Data Security Incident.

8.1 In the event of a confirmed breach of security leading to the unauthorized disclosure of, or access to Client Personal Data Processed by Andela or its Authorized Subprocessors under the Agreement ("Personal Data Security Incident"), Andela shall, without undue delay, inform Client of the Personal Data Security Incident and take such steps as Andela in its sole discretion deems necessary and reasonable to remediate such Personal Data Security Incident, to the extent that remediation is within Andela's reasonable control.

8.2 In the event of a Personal Data Security Incident, Andela shall, taking into account the nature of the Processing and the information available to Andela, provide Client with reasonable cooperation and assistance necessary for Client to comply with its obligations under Privacy Laws with respect to notifying (i) the relevant supervisory authority or regulatory agency and (ii) Data Subjects affected by such Personal Data Security Incident without undue delay.

8.3 The obligations described in Sections 8.1 and 8.2 shall not apply in the event that a Personal Data Security Incident results from the actions or omissions of Client. Andela's obligation to report or respond to a Personal Data Security Incident under Sections 8.1 and 8.2 will not be construed as an acknowledgement by Andela of any fault or liability with respect to the Personal Data Security Incident

9. Transfers of Personal Data.

9.1 The Parties agree that Andela may transfer Personal Data processed under this DPA outside the EEA, the UK, or Switzerland as necessary to provide the Services. Client acknowledges that the transfer of Personal Data to the United States is necessary for the provision of the Services to Client. If Andela transfers Personal Data processed under this DPA to a jurisdiction for which the European Commission has not issued an adequacy decision, Andela will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Privacy Laws.

9.2 Ex-EEA Transfers. The Parties agree that ex-EEA Transfers shall either be made pursuant to (i) the Data Privacy Framework to the extent the recipient of the ex-EEA Transfer is certified accordingly, or (ii) the EU SCCs, which are deemed entered into (and incorporated into this herein by reference) and completed as follows:

9.2.1 Module One (Controller to Controller) of the EU SCCs applies when Andela is processing Personal Data as a controller pursuant to Section 9 of this DPA.

9.2.2 Module Two (Controller to Processor) of the EU SCCs applies when Client is a controller and Andela is a processor of Personal Data in accordance with Section 2 of this DPA.

9.2.3 Module Three (Processor to Subprocessor) of the EU SCCs applies when Client is a processor and Andela is a subprocessor of Personal Data in accordance with Section 2 of this DPA.

9.3 For each module, where applicable the following applies:

9.3.1 The optional docking clause in Clause 7 does not apply.

9.3.2 In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of subprocessor changes shall be 30 days.

9.3.3 In Clause 11, the optional language does not apply.

9.3.4 All square brackets in Clause 13 are hereby removed.

9.3.5 In Clause 17 (Option 1), the EU SCCs will be governed by the laws of the Republic of Ireland.

9.3.6 In Clause 18(b), disputes will be resolved before the courts of the Republic of Ireland.

9.3.7 Exhibit B to this DPA contains the information required in Annex I of the EU SCCs.

9.3.8 Exhibit C to this DPA contains the information required in Annex II of the EU SCCs,

9.3.9 By entering into this DPA, the Parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.

9.4 Ex-UK Transfers. The Parties agree that ex-UK Transfers shall either be made pursuant to (i) the Data Privacy Framework to the extent that recipient of the ex-UK Transfer is certified accordingly, or (ii) the UK SCCs, which are deemed entered into and incorporated herein by reference. The UK Addendum (including the EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales.

9.5 Transfers from Switzerland. The Parties agree that transfers from Switzerland shall either be made pursuant to (i) the Data Privacy Framework to the extent that recipient of the transfer from Switzerland is certified accordingly, or (ii) the EU SCCs with the following modifications:

9.5.1 The terms “General Data Protection Regulation” or “Regulation (EU) 2016/679” as utilized in the EU SCCs shall be interpreted to include the Federal Act on Data Protection of 19 June 1992 (the “FADP,” and as revised as of 25 September 2020, the “Revised FADP”) with respect to data transfers subject to the FADP.

9.5.2 Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information Commissioner (“FDPIC”) of Switzerland shall have authority over data transfers governed by the FADP and the appropriate EU supervisory authority shall have authority over data transfers governed by the GDPR. Subject to the foregoing, all other requirements of Clause 13 shall be observed.

9.5.3 The term “EU Member State” as utilized in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

9.6 Supplementary Measures. In respect of any transfer of Personal data made pursuant to the Standard Contractual Clauses, the following supplementary measures shall apply:

9.6.1 If Andela receives a formal legal request from any government intelligence or security service/agencies in the country to which the Client Personal Data is being exported, for access to (or for copies of) such Personal Data (each, a “Government Agency Request"), Andela shall attempt to redirect the Government Agency Request to Client. As part of this effort, Andela may provide Client’s basic contact information to the government agency. If Andela is compelled to disclose Client Personal Data, to the extent legally permitted, Andela shall notify Client of the demand and reasonably cooperate to allow Client to seek a protective order or other appropriate remedy. Andela shall not voluntarily disclose Client Personal Data to any law enforcement or government agency. The Parties shall determine whether all or any transfers of Client Personal Data pursuant to this DPA should be suspended in light of such a Government Agency Request.

9.6.2 The Parties will confer as appropriate to consider whether: (i) the protection afforded by the laws of the country of Andela to Data Subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in the EEA or the UK, as applicable; (ii) additional measures are reasonably necessary for the transfer to comply with Privacy Laws; and (iii) it is still appropriate for Personal Data to be transferred to the relevant jurisdiction; Andela, taking into account all relevant information available, including guidance by supervisory authorities, to the Parties.

9.6.3 If either (i) any of the means of legitimizing a transfer cease to be valid or (ii) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, the Parties agree to amend the means of legitimizing transfers in accordance with Privacy Laws. To the extent necessary to ensure the enforceability of the Standard Contractual Clauses, the Parties shall execute the Standard Contractual Clauses as a separate agreement.

10. Data Protection Assessments. Taking into account the nature of Andela's Processing and the information available to Andela, Andela shall reasonably cooperate with Client to conduct any data protection or privacy impact assessments as required by Privacy Laws, including by providing Client with information and documents necessary for such assessments that Client cannot otherwise obtain without Andela's assistance. Notwithstanding the foregoing, Client and Andela each remain responsible only for the measures respectively allocated to them under Privacy Laws pertaining to any such assessment.

11. Data Subject Request.

11.1 Andela shall, to the extent permitted by Privacy Laws, notify Client upon receipt of a Data Subject Request. If Andela receives a Data Subject Request in relation to Personal Data, Andela will advise the Data Subject to submit their request to Client and Client will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. Client is solely responsible for ensuring that Data Subject Requests communicated to Andela, and, if applicable, for ensuring that a record of consent to Processing, are maintained with respect to each Data Subject.

11.2 Andela shall, at the written request of Client, and taking into account the nature of the Processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Client in complying with Client's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, *provided that* (i) Client is itself unable to respond without Andela's assistance and (ii) Andela is able to do so in accordance with all applicable laws, rules, and regulations. Client shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Andela.

12. Return or Destruction of Personal Data. Upon the termination or expiration of the Agreement, at Client's choice, Andela shall return or delete Personal Data, unless further storage of such Personal Data is required or authorized by applicable law. If return or destruction is impracticable or prohibited by law, rule or regulation, Andela shall take measures to block such Personal Data from any further processing (except to the extent necessary for its continued hosting or processing required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control. If Client and Andela have entered into Standard Contractual Clauses as described in Section 9 (Transfers of Personal Data), the Parties agree that the certification of deletion of Personal Data that is described in Clause 8.1(d) and Clause 8.5 of the EU SCCs (as applicable) shall be provided by Andela to Client only upon Client's written request. Notwithstanding the foregoing, Andela may retain Personal Data in accordance with Andela's records retention and digital archival back-up policies ("Records Management Policy") provided such retention remains subject to the terms of the Agreement and provided further that such Personal Data is destroyed in due course in accordance with Andela's Records Management Policy.

13. Andela's Role as a Controller. The Parties acknowledge and agree that with respect to Andela Account Data and Andela Usage Data, Andela is an independent controller, not a joint controller with Client. Andela will Process Andela Account Data and Andela Usage Data as a controller (i) to manage the relationship with Client; (ii) to carry out Andela's core business operations, such as accounting, audits, tax preparation and filing and compliance purposes; (iii) to monitor, investigate, prevent and detect fraud, security incidents and other misuse of the Services, and to prevent harm to Client; (iv) for identity verification purposes; (v) to comply with legal or regulatory obligations applicable to the Processing of Personal Data to which Andela is subject; and (vi) as otherwise permitted under Privacy Laws and in accordance with this DPA and the Agreement. Andela may also Process Andela Usage Data as an independent controller to provide, optimize, and maintain the Services, to the extent permitted by Privacy

Laws. Any Processing by Andela as an independent controller shall be in accordance with Andela's Privacy Policy**.**

14. Miscellaneous. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in the Standard Contractual Clauses; (2) the terms of this DPA; (3) the Agreement, and (4) Andela's privacy policy. Any claims brought in connection with this DPA will be subject to the Agreement, including, but not limited to, the exclusions and limitations set forth in the Agreement.

Exhibit A

Details of Andela's Data Processing

I. **Nature and Purpose of Processing:** Andela will Process Personal Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this DPA, and in accordance with Client's written instructions as set forth in the Agreement and this DPA. The nature of Processing includes, without limitation:

A. **Receiving Personal Data**, including collection, accessing, retrieval, recording, and data entry

B. **Holding Personal Data**, including storage, organization and structuring

C. **Using Personal Data**, including analysis, consultation, and testing

D. **Updating Personal Data**, including correcting, adaptation, alteration, alignment and combination

E. **Protecting Personal Data**, including restricting, encrypting, and security testing

F. **Disclosing Personal Data**, including dissemination, allowing access or otherwise making available

G. **Returning Personal Data** to the data exporter or Data Subject

H. **Erasing Personal Data**, including destruction and deletion

II. **Duration of Processing:** Andela will Process Personal Data as long as required (i) to provide the Services to Client under the Agreement; (ii) for Andela's legitimate business needs; or (iii) by applicable law or regulation. Andela Account Data and Andela Usage Data will be Processed and stored as set forth in Andela's privacy policy.

III. **Categories of Data Subjects:** Client employees and/or contractors; Talent on behalf of Client as Agent on Record.

IV. **Categories of Personal Data:** Andela Processes Personal Data contained in Andela Account Data, Andela Usage Data, and any Personal Data provided by Client (including any Personal Data Client collects from its end users and processes through its use of the Services) to provide the Services or as otherwise set forth in the Agreement or this DPA. Categories of Personal Data include name, location, email address, phone or fax number, address.

V. **Sensitive Data or Special Categories of Data:** Solely to the extent provided or instructed by the Client in accordance with Privacy Laws. Talent payment data, demographic data, and resume or other professional or employment related data.

Exhibit B

The following includes the information required by Annex I and Annex III of the EU SCCs, and Table 1, Annex 1A, and Annex 1B of the UK Addendum.

1. The Parties

	Data Exporter	**Data Importer**
Name:	Client	Andela Inc.
Address:	As designated within the Client's account	169 Madison Avenue, Suite 15766 New York, New York 10016 United States of america
Contact:	As designated within the Client's account	Andela Legal legal@andela.com
Signature and Date:	By entering into the Agreement, Client is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the date that Client entered into the Agreement.	By entering into the Agreement, Data Importer is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date of the Agreement.
Role	**Role C:** As provided in Section 2 of this DPA.	**Role Controller/Processor:** As provided in Section 2 and Section 13 of the DPA.

2. **Description of the Transfer**

Data Subjects	As described in Exhibit A of the DPA
Categories of Personal Data	As described in Exhibit A of the DPA
Special Category Personal Data (if applicable)	As described in Exhibit A of the DPA
Nature of the Processing	As described in Exhibit A of the DPA
Purposes of Processing	As described in Exhibit A of the DPA
Duration of Processing and Retention (or the criteria to determine such period)	As described in Exhibit A of the DPA
Frequency of the transfer	As necessary to provide perform all obligations and rights with respect to Personal Data as provided in the Agreement or DPA

Recipients of Personal Data Transferred to the Data Importer	Andela will maintain and provide the List upon written request.

3. Competent Supervisory Authority

The supervisory authority shall be the supervisory authority of the Data Exporter, as determined in accordance with Clause 13 of the EU SCCs. The supervisory authority for the purposes of the UK Addendum shall be the UK Information Commissioner's Officer.

4. List of Authorized Subprocessors

Client can request the List of Andela's current Authorized Subprocessors by emailing legal@andela.com.

Exhibit C

Description of the Technical and Organisational Security Measures Implemented by the Data Importer

The following includes the information required by Annex II of the EU SCCs and Appendix II of the UK Addendum.

1. **Confidentiality**. Andela maintains electronic access control designed to prevent unauthorized access to or use of Andela's Personal Data Processing and Personal Data storage systems, including through the use of secure passwords, automatic blocking/locking mechanisms, two-factor authentication, and encryption of data carriers/storage media. Andela's employees and contractors are bound by written confidentiality agreements, receive training on privacy and security obligations, and are only permitted to Process Personal Data in accordance with the obligations under the Agreement, including this DPA, and Client's documented instructions.

2. **Internal Access Controls**. Andela has implemented permission-based access controls designed to prevent unauthorized access to, modification of, or deletion of Personal Data through a central management system.

3. **Isolation Control**. Andela segregates Personal Data depending on the purpose for collection, including but not limited to logical segregation on a per client basis.

4. **Pseudonymisation**. Where appropriate, and taking into account the state of the art, costs of implementation, and the nature, scope, context, and purposes of the Processing, Andela employs pseudonymization to protect Personal Data.

5. **Data Entry Control**. Andela has policies in place designed to provide a process for verification of modification to or deletion of Personal Data, including but not limited to logging of changes and document management.

6. **Availability Control**. Andela has implemented policies designed to prevent the accidental destruction or loss of Personal Data, such as through the use of regular backups, a "UPS" or uninterruptible power supply, virus protection, firewalls, reporting procedures, and contingency planning.

7. **Vendor Controls**. Andela has implemented procedures for vendor diligence, contracting, onboarding, and order management designed to provide necessary oversight for Andela's vendors to mitigate the risk of unauthorized Processing.

Exhibit D

UK Addendum

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Part 1: Tables

Table 1: Parties

Start Date	This UK Addendum shall have the same effective date as the DPA	
The Parties	Exporter	Importer
Parties' Details	Client	Andela
Key Contact	*See* Exhibit B of this DPA	*See* Exhibit B of this DPA

Table 2: Selected SCCs, Modules and Selected Clauses

EU SCCs	The Version of the Approved EU SCCs which this UK Addendum is appended to as defined in the DPA and completed by Section 6.2 and 6.3 of the DPA.

Table 3: Appendix Information

Annex 1A: List of Parties	As per Table 1 above
Annex 2B: Description of Transfer	*See* Exhibit B of this DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	*See* Exhibit C of this DPA
Annex III: List of Authorized Subprocessors (Modules 2 and 3 only):	*See* Exhibit B of this DPA

Table 4: Ending this UK Addendum when the Approved UK Addendum Changes

Ending this UK Addendum when the Approved UK Addendum changes	☒ Importer ☒ Exporter ☐ Neither Party

Part 2: Mandatory Clauses

The Mandatory Clauses of the UK Addendum are incorporated herein by reference.