AL Talent, Inc. (d/b/a “Wellfound”)

Data Processing Addendum

This Data Processing Addendum (“**DPA**”) is entered into as of the Addendum Effective Date and forms part of Wellfound’s (defined below) terms of service (available at https://angel.co/terms) or other agreement by and between: (1) AL Talent, Inc., a Delaware corporation (known as “AngelList Talent” but now doing business as “**Wellfound**”) and/or Wellfound Affiliates (defined below); and (2) the undersigned customer of Wellfound and/or any Wellfound Affiliates (“**Customer**”) for Services (defined below) provided by Wellfound and/or any Wellfound Affiliates (the “**Agreement**”) to reflect the parties’ agreement with regard to the Processing of Personal Data (defined below). Each of Customer, Wellfound and any Wellfound Affiliate that is party to the Agreement may be referred to herein as a “party” and together as the “parties.”

Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Customer Affiliates, if and to the extent Wellfound and/or any Wellfound Affiliate Processes Personal Data for which such Customer Affiliates qualify as a Data Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Customer Affiliates and the term “Wellfound” shall include Wellfound and Wellfound Affiliates.

In the course of providing the Services to Customer pursuant to the Agreement, Wellfound may Process Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

HOW TO EXECUTE THIS DPA

Customer will be deemed to have agreed to the Agreement and this DPA if continuing to use the Services on or after May 25, 2018. You may countersign this DPA for your own records by following the steps below:

1. This DPA consists of two parts: the main body of the DPA and Annex 1, 2 and 3.
2. This DPA has been pre-signed on behalf of Wellfound.
3. To complete this DPA, Customer must complete the information and sign on page 9.
4. Send the completed and signed DPA to Wellfound by email, indicating the Customer’s legal name (as set out in the Agreement, if applicable), to talent-legal@angel.co.

HOW THIS DPA APPLIES

If the Customer entity agreeing to this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, Wellfound is party to this DPA.

If the Customer entity agreeing to this DPA is not a party to the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA.

This DPA shall not replace any comparable or additional rights relating to Processing of Wellfound’s data contained in the Agreement (including any existing data processing addendum to the Agreement).

DATA PROCESSING TERMS

1. DEFINITIONS

1.1. In this DPA the following terms shall have the meanings set out in this Paragraph 1.1, unless expressly stated otherwise:

(a) “**Addendum Effective Date**” means (a) 25 May 2018, if Customer clicked to accept or the parties otherwise agreed to this DPA in respect of the applicable Agreement prior to or on such date; or (b) the date on which Customer clicked to accept or the parties otherwise agreed to this DPA in respect of the applicable Agreement, if such date is after 25 May 2018.

(b) "**Adequate Country**" means a country or territory outside the European Economic Area that the European Commission has deemed to provide an adequate level of protection for Personal Data pursuant to a decision made in accordance Article 45(1) of the GDPR.

(c) "**Wellfound Affiliates**" means any companies which are controlled by Wellfound, which control Wellfound or which are under common control with Wellfound and are Data Processors of any Customer Personal Data. For these purposes, "**control**" and its derivatives mean to hold, directly or indirectly, more than 50% of the respective shares with voting rights.

(d) "**Anonymised Data**" means any Personal Data (including Customer Personal Data), which has been anonymised such that the Data Subject to whom it relates cannot be identified, directly or indirectly, by Wellfound, an Wellfound Affiliate or any other party reasonably likely to receive or access that anonymised Personal Data.

(e) "**Business Day**" means any day which is not a Saturday, Sunday or public holiday, and on which the banks are open for business, in San Francisco, California.

(f) "**Cessation Date**" has the meaning given in Paragraph 9.1.

(g) "**Controller Data**" means any Personal Data Wellfound independently collects from a Data Subject or a third party for Processing or other legitimate business purposes in connection with Wellfound providing certain services to the Data Subject.

(h) "**Customer Affiliates**" means any companies which are controlled by Customer, which control Customer or which are under common control with Customer and either: (i) are Data Controllers of any Customer Personal Data; and/or (ii) on whose behalf Wellfound, an Wellfound Affiliate and/or any Subprocessor otherwise processes any Customer Personal Data. For these purposes, "**control**" and its derivatives mean to hold, directly or indirectly, more than 50% of the respective shares with voting rights.

(i) "**Customer Personal Data**" means any Personal Data Processed by or on behalf of Wellfound on behalf of Customer under the Agreement excluding any Controller Data.

(j) "**Data Protection Laws**" means the EU General Data Protection Regulation 2016/679 (the "**GDPR**") and to the extent the GDPR is no longer applicable in the United Kingdom, any implementing legislation or legislation having equivalent effect in the United Kingdom (references to "**Articles**" or "**Chapters**" of the GDPR shall be construed accordingly).

(k) "**Data Subject Request**" means the exercise by Data Subjects of their rights under, and in accordance with, Chapter III of the GDPR.

(l) "**Data Subject**" means the identified or identifiable natural person located in the European Economic Area to whom Customer Personal Data relates.

(m) "**Delete**" means to remove or obliterate Personal Data such that it cannot be recovered or reconstructed, and "**Deletion**" shall be construed accordingly.

(n) "**Personnel**" means a person's employees, agents, consultants or contractors.

(o) "**Post-cessation Storage Period**" has the meaning given in Paragraph 9.2.

(p) "**Restricted Country**" means a country or territory outside the European Economic Area that is not an Adequate Country.

(q) "**Restricted Transfer**" means: (i) a transfer of Customer Personal Data from Customer to Wellfound in a Restricted Country; or (ii) an onward transfer of Customer Personal Data from Wellfound to a Subprocessor in a Restricted Country, (in each case) where such transfer would be prohibited by Data Protection Laws without a legal basis therefor under Chapter V of the GDPR.

(r) "**Services**" means those services and activities to be supplied to or carried out by or on behalf of Wellfound and/or Wellfound Affiliates for Customer pursuant to the Agreement.

(s) "**Standard Contractual Clauses**" means the standard contractual clauses issued by the European Commission (from time-to-time) for the transfer of Personal Data from Data Controllers established inside the European Economic Area to Data Processors established in Restricted Countries.

(t) "**Subprocessor**" means any third party appointed by or on behalf of Wellfound and/or Wellfound Affiliates to Process Customer Personal Data.

1.2. In this DPA:

(a) the terms, "**Data Controller**", "**Data Processor**", "**Personal Data**", "**Personal Data Breach**", "**Process**" (and its derivatives) and "**Supervisory Authority**" shall have the meaning ascribed to the corresponding terms in the Data Protection Laws;

(b) unless otherwise defined in this DPA, all capitalised terms shall have the meaning given to them in the Agreement; and

(c) any reference to any statute, regulation or other legislation in this DPA shall be construed as meaning such statute, regulation or other legislation, together with any applicable judicial or administrative interpretation thereof (including any binding guidance, guidelines, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant Supervisory Authority).

2. PROCESSING OF CUSTOMER PERSONAL DATA

2.1. In respect of Customer Personal Data, the parties acknowledge that:

(a) Wellfound acts as a Data Processor; and

(b) Customer acts as the Data Controller.

2.2. Wellfound shall:

(a) comply with all applicable Data Protection Laws in Processing Customer Personal Data; and

(b) not Process Customer Personal Data other than:

(i) on Customer's instructions (subject always to Paragraph 2.9); and

(ii) as required by applicable laws.

2.3. [Intentionally Omitted]

2.4. Customer instructs Wellfound to Process Customer Personal Data as necessary:

(a) to provide the Services to Customer; and

(b) to perform Wellfound's obligations and exercise Wellfound's rights under the Agreement.

2.5. Annex 1 (*Data Processing Details*) sets out certain information regarding Wellfound's Processing of Customer Personal Data as required by Article 28(3) of the GDPR.

2.6. Customer may amend Annex 1 (*Data Processing Details*) on written notice to Wellfound from time to time as Customer reasonably considers necessary to meet any applicable requirements of Data Protection Laws.

2.7. Nothing in Annex 1 (*Data Processing Details*) (including as amended pursuant to Paragraph 2.6) confers any right or imposes any obligation on any party to this DPA.

2.8. Where Wellfound receives an instruction from Customer that, in its reasonable opinion, infringes the GDPR, Wellfound shall inform Customer.

2.9. Customer acknowledges and agrees that any instructions issued by Customer with regards to the Processing of Customer Personal Data by or on behalf of Wellfound pursuant to or in connection with the Agreement:

(a) shall be strictly required for the sole purpose of ensuring compliance with Data Protection Laws; and

(b) (without limitation to the generality of Paragraph 2.7) shall not relate to the scope of, or otherwise materially change, the Services to be provided by Wellfound under the Agreement.

2.10. Notwithstanding anything to the contrary herein, Wellfound may terminate the Agreement in its entirety upon written notice to Customer with immediate effect if Wellfound considers (in its reasonable discretion) that:

(a) it is unable to adhere to, perform or implement any instructions issued by Customer due to the technical limitations of its systems, equipment and/or facilities; and/or

(b) to adhere to, perform or implement any such instructions would require disproportionate effort (whether in terms of time, cost, available technology, manpower or otherwise).

For the avoidance of doubt, this Paragraph 2.10 does not refer to the instructions set out in Paragraph 2.4.

2.11. Customer represents and warrants on an ongoing basis that, for the purposes of Article 6 of the GDPR, there is, and will be throughout the term of the Agreement, a valid legal basis for the Processing by Wellfound of Customer Personal Data in accordance with this DPA and the Agreement (including, any and all instructions issued by Customer from time to time in respect of such Processing).

3. WELLFOUND PERSONNEL

3.1. Wellfound shall take reasonable steps to ensure the reliability of any Wellfound Personnel who Process Customer Personal Data, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. SECURITY

4.1. 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 (which may be of varying likelihood and severity) for the rights and freedoms of natural persons, Wellfound shall in relation to Customer Personal Data implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2. In assessing the appropriate level of security, Wellfound shall take account in particular of the risks presented by the Processing, in particular from a Personal Data Breach.

5. SUBPROCESSING

5.1. Customer authorises Wellfound to appoint Subprocessors in accordance with this Paragraph 5.

5.2. Wellfound may continue to use those Subprocessors already engaged by Wellfound as at the date of this DPA, subject to Wellfound meeting within a reasonable timeframe (or having already met) the obligations set out in Paragraph 5.4.

5.3. Wellfound shall give Customer prior written notice of the appointment of any new Subprocessor, including reasonable details of the Processing to be undertaken by the Subprocessor. If, within ten business days of receipt of that notice, Customer notifies Wellfound in writing of any objections (on reasonable grounds) to the proposed appointment:

(a) Wellfound shall use reasonable efforts to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor; and

(b) where:

(i) such a change cannot be made within thirty days from Wellfound receipt of Customer's notice;

(ii) no commercially reasonable change is available; and/or

(iii) Customer declines to bear the cost of the proposed change,

either party may by written notice to the other party with immediate effect terminate the Agreement either in whole or to the extent that it relates to the Services which require the use of the proposed Subprocessor.

5.4. With respect to each Subprocessor, Wellfound shall ensure that the arrangement between Wellfound and the Subprocessor is governed by a written contract including terms which offer at least an equivalent level of protection for Customer Personal Data as those set out in this DPA (including those set out in Paragraph 4).

6. DATA SUBJECT RIGHTS

6.1. Taking into account the nature of the Processing, Wellfound shall provide Customer with such assistance as may be reasonably necessary and technically possible in the circumstances, to assist Customer in fulfilling its obligation to respond to Data Subject Requests.

6.2. Wellfound shall:

(a) promptly notify Customer if Wellfound receives a Data Subject Request; and

(b) ensure that Wellfound does not respond to any Data Subject Request except on the written instructions of Customer (and in such circumstances, at Customer's cost) or as required by applicable laws, in which case Wellfound shall to the extent permitted by applicable laws inform Customer of that legal requirement before Wellfound responds to the Data Subject Request.

7. PERSONAL DATA BREACH

7.1. Wellfound shall notify Customer without undue delay upon Wellfound becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information (insofar as such information is, at such time, within Wellfound's possession) to allow Customer to meet any obligations under Data Protection Laws to report the Personal Data Breach to:

(a) affected Data Subjects; or

(b) the relevant Supervisory Authority(ies) (as may be determined in accordance with the Data Protection Laws).

7.2. Wellfound shall co-operate with Customer and take such reasonable commercial steps as may be directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

8.1. Wellfound shall provide reasonable assistance to Customer, at Customer's cost, with any data protection impact assessments, and prior consultations with Supervisory Authorities (as defined in the GDPR), which Customer reasonably considers to be required of Customer by Article 35 or Article 36 of the GDPR, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing by, and information available to, Wellfound.

9. DELETION OR RETURN OBLIGATIONS

9.1. Subject to Paragraphs 9.2 and 9.5, upon the date of cessation of any Services involving the Processing of Customer Personal Data (the "**Cessation Date**"), Wellfound shall immediately cease all Processing of the Customer Personal Data for any purpose other than for storage.

9.2. Subject to Paragraph 9.5, to the extent technically possible in the circumstances (as determined in Wellfound's sole discretion), on written request to Wellfound (to be made no later than twenty days after the Cessation Date (the "**Post-cessation Storage Period**")), Wellfound shall either (at Wellfound's option):

(a) return a complete copy of all Customer Personal Data within Wellfound's possession to Customer by secure file transfer, promptly following which Wellfound shall Delete all other copies of such Customer Personal Data; or

(b) Delete all Customer Personal Data then within Wellfound's possession.

9.3. Wellfound shall comply with any written request made pursuant to Paragraph 9.2 within thirty days of the Cessation Date.

9.4. In the event that during the Post-cessation Storage Period, Customer does not instruct Wellfound in writing to either Delete or return the Customer Personal Data pursuant to Paragraph 9.2, Wellfound shall promptly after the expiry of the Post-cessation Storage Period either (at its option):

(a) Delete; or

(b) irreversibly render Anonymised Data,

all Customer Personal Data then within Wellfound's possession to the fullest extent technically possible in the circumstances.

9.5. Wellfound and any Subprocessor may retain Customer Personal Data where required by applicable law, for such period as may be required by such applicable law, provided that Wellfound and any such Subprocessor shall ensure:

(a) the confidentiality of all such Customer Personal Data; and

(b) that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the applicable law requiring its storage and for no other purpose.

9.6. If requested by Customer, Wellfound shall provide written certification to Customer that it has fully complied with its obligations under this Paragraph 9 without undue delay.

10. AUDIT RIGHTS

10.1. Wellfound shall make available to Customer on request such information as Wellfound (acting reasonably) considers appropriate in the circumstances to demonstrate its compliance with this DPA.

10.2. Subject to Paragraphs 10.3 and 10.4, in the event that Customer (acting reasonably) is able to provide documentary evidence that the information made available by Wellfound pursuant to Paragraph 10.1 is not sufficient in the circumstances to demonstrate Wellfound's compliance with this DPA, Wellfound shall allow for and contribute to audits, including on-premise inspections, by Customer or an auditor mandated by Customer in relation to the Processing of the Customer Personal Data by Wellfound.

10.3. Customer shall give Wellfound reasonable notice of any audit or inspection to be conducted under Paragraph 10.1 (which shall in no event be less than fifteen business days' notice unless required by a Supervisory Authority pursuant to Paragraph 10.4(f)) and shall use its best efforts (and ensure that each of its mandated auditors uses its best efforts) to avoid causing, and hereby indemnifies Wellfound in respect of, any damage, injury or disruption to Wellfound's premises, equipment, Personnel, data, and business (including any interference with the confidentiality or security of the data of Wellfound's other customers or the availability of Wellfound's services to such other customers) while its Personnel and/or its auditor's Personnel (if applicable) are on those premises in the course of any on-premise inspection.

10.4. Wellfound need not give access to its premises for the purposes of such an audit or inspection:

(a) to any individual unless he or she produces reasonable evidence of their identity and authority;

(b) to any auditor whom Wellfound has not given its prior written approval (not to be unreasonably withheld);

(c) unless the auditor enters into a non-disclosure agreement with Wellfound on terms acceptable to Wellfound;

(d) where, and to the extent that, Wellfound considers, acting reasonably, that to do so would result in interference with the confidentiality or security of the data of Wellfound's other customers or the availability of Wellfound's services to such other customers;

(e) outside normal business hours at those premises; or

(f) on more than one occasion in any calendar year during the term of the Agreement, except for any additional audits or inspections which Customer is required to carry out by Data Protection Law or a Supervisory Authority, where Customer has identified the relevant requirement in its notice to Wellfound of the audit or inspection.

10.5. The parties shall discuss and agree upon the costs, scope, timing, and duration of any inspection or audit to be carried out by or on behalf of Customer pursuant to Paragraph 10.2 in advance of such inspection or audit and, unless otherwise agreed in writing between the parties, Customer shall bear any third party costs in connection with such inspection or audit and reimburse Wellfound for all costs incurred by Wellfound and time spent by Wellfound (at Wellfound's then-current professional services rates) in connection with any such inspection or audit.

11. RESTRICTED TRANSFERS

11.1. Subject to Paragraph 11.3, to the extent that any Processing by either Wellfound or any Subprocessor of Customer Personal Data involves a Restricted Transfer, the parties agree that:

(a) Customer – as "data exporter"; and

(b) Wellfound or Subprocessor (as applicable) – as "data importer", shall enter into the Standard Contractual Clauses in respect of that Restricted Transfer and the associated Processing in accordance with Paragraph 11.3.

11.2. In respect of any Standard Contractual Clauses entered into pursuant to Paragraph 11.1:

(a) Clause 17 of such Standard Contractual Clauses shall be populated as follows:

> *"These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands."*

(b) Annex 1 to such Standard Contractual Clauses shall be populated with the corresponding information set out in Annex 1;

(c) Annex 2 to such Standard Contractual Clauses shall be populated with the corresponding information set out in Annex 2; and

(d) Annex 3 to such Standard Contractual Clauses shall be populated with the corresponding information set out in Annex 3.

11.3. The Standard Contractual Clauses shall be deemed to come into effect under Paragraph 11.1 automatically upon the commencement of the relevant Restricted Transfer **provided that** Paragraph 11.1 shall not apply to a Restricted Transfer unless its effect is to allow the relevant Restricted Transfer and the associated Processing to take place without breach of applicable Data Protection Laws.

12. ANONYMOUS DATA

12.1. Customer acknowledges and agrees that Wellfound shall be freely able to use and disclose Anonymised Data for Wellfound's own business purposes without restriction.

13. CONTROLLER DATA

13.1. Customer acknowledges and agrees that (as between the parties) Wellfound shall be freely able to use and disclose (without restriction) the Controller Data for any such purposes as Wellfound may in its sole discretion determine.

13.2. To the extent that any Controller Data constitutes Personal Data for the purposes of the Data Protection Laws, Wellfound:

(a) shall be an independent Data Controller in respect of such Controller Data;

(b) may independently determine the purposes and means of its Processing of such Controller Data.

14. ORDER OF PRECEDENCE

14.1. This DPA shall be incorporated into and form part of the Agreement.

14.2. In the event of any conflict or inconsistency between:

(a) this DPA and the Agreement, this DPA shall prevail; or

(b) any Standard Contractual Clauses entered into pursuant to Paragraph 11 and this DPA, those Standard Contractual Clauses shall prevail.

[REMAINDER OF PAGE INTENTIONALLY BLANK]

[**SIGNATURE PAGE TO DATA PROCESSING ADDENDUM**]

This DPA has been entered into and become a binding and effective part of the Agreement with effect from the Addendum Effective Date.

Signed by: Amit Matani	Signed by:
______________________________	______________________________
Title: CEO	Title:
WELLFOUND	Customer Entity Name
Date: 12/27/22	Date:

ANNEX I

This Annex 1 to the DPA includes certain details of the Processing of Customer Personal Data: as required by Article 28(3) GDPR; and (where applicable in accordance with Paragraph 12) to populate Appendix 1 to the Standard Contractual Clauses.

Annex 1.A.

A. LIST OF PARTIES

Data exporter(s):

1. Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: Controller of the Customer Personal Data, and Data Exporter to Data importers.

Signature and date:

Role (controller/processor): Controller

Data importer(s):

1. Name: Wellfound

Address: 228 PARK AVE S PMB 40533, New York, NY 10003-1502

Contact person's name, position and contact details: Amit Matani, CEO, talent-legal@angel.co

Activities relevant to the data transferred under these Clauses: Processing of Customer's Personal Data as described below in Annex 1.B.

Signature and date: ____________________, Dec. 27, 2022

Role (controller/processor): Processor

Annex 1.B.

B. DESCRIPTION OF TRANSFER AND PROCESSING ACTIVITIES

The nature and purpose of the Processing of Customer Personal Data

Wellfound will Process Customer Personal Data as necessary to perform the Services pursuant to the Agreement and as further instructed by Customer in its use of the Services.

Subject matter and duration of the Processing of Customer Personal Data

The subject matter and duration of the Processing of the Customer Personal Data are set out in the Agreement and the DPA.

The categories of Data Subjects to whom the Customer Personal Data relates

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer’s prospects, customers, business partners and vendors
- Employees, prospective employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer’s users authorized by Customer to use the Services

The types of Customer Personal Data to be Processed

Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

Names, titles, position, employer, contact information (email, phone, fax, physical address etc.), identification data, professional life data, personal life data, connection data, investment data, banking data or localization data (including IP addresses).

Special Categories of Personal Data (if any)

Customer may submit special categories of Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion. Such special categories of Personal Data include, but may not be limited to, Personal Data with information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning an individual’s health or sex life.

The obligations and rights of Customer

The obligations and rights of Customer are set out in the Agreement and the DPA.

Annex 1.C.

C. COMPETENT SUPERVISORY AUTHORITY

Customer’s representative under Article 27 is:

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The following describes Wellfound's technical and organizational measures implemented by Wellfound to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

Wellfound uses industry-standard physical, managerial, and technical safeguards to preserve the integrity and security of data. Wellfound limits access to Personal Data to those employees and other staff who have a business need to have such access. All such people are subject to a contractual duty of confidentiality. Wellfound periodically reviews its policies and procedures to evaluate their effectiveness and ensure that they remain up to date

Wellfound has put in place procedures to respond to any actual or suspected Personal Data breach. In the event that personal information is compromised as a result of such a breach of security, Wellfound may promptly notify those persons whose personal information has been compromised by posting a notice on its website, or by sending an e-mail those persons affected.

A description of the specific technical and organizational measures to be taken by Wellfound sub-processors is described in Annex III.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorized the use of the following sub-processors:

1. **Amazon Web Services**, 410 Terry Avenue North Seattle, WA 98109. AWS is responsible for storage of all of Wellfound Customer Personal Data. AWS security measure are described here: https://aws.amazon.com/compliance/gdpr-center/

2. **Amplitude**, Keizersgracht 277, 1016ED Amsterdam, The Netherlands. Amplitude is a web analytics company that processes Customer Personal Data related to user names, email address, work history and general website data usage. Steps taken by Amplitude to protect Customer Personal Data are described here: https://amplitude.com/privacy

3. **Asana**, 633 Folsom Street, Suite 100, San Francisco, CA 94107, United States. Asana provides Wellfound a project management tool that processes some Customer Personal Data related to user names and email addresses. Steps taken by Asana to protect Customer Personal Data are described here: https://asana.com/terms#privacy-statement

4. **Atlassian**, Level 6, 341 George Street, Sydney, NSW 2000, Australia. Atlassian provides Wellfound a project management tool that processes some Customer Personal Data related to user names and email addresses. Steps taken by Asana to protect Customer Personal Data are described here: https://www.atlassian.com/legal/privacy-policy

5. **Bill.com**, 6220 America Center Drive, Suite 100. San Jose, CA 95002. Bill.com provides Wellfound billing services and processes Customer Personal Data related to user names and email addresses and billing addresses. Steps taken by Bill.com to protect Customer Personal Data are described here: https://www.bill.com/privacy

6. **Canny.io**, 831 N Tatnall St Ste M 140, Wilmington, Delaware, 19801, United States. Canny.io provides Wellfound a customer feedback tool and processes Customer Personal Data related to user names and email addresses. Steps taken by Canny.io to protect Customer Personal Data are described here: https://canny.io/privacy

7. **Datadog**, New York HQ, New York Times Bldg, 620 8th Ave #45th, United States. Datadog provides Wellfound a application monitoring tool and processes Customer Personal Data related to user names, email addresses., work history and website usage data. Steps taken by Datadog to protect Customer Personal Data are described here: https://www.datadoghq.com/legal/privacy/

8. **Datafold**, 340 S Lemon Ave 7573, Walnut, California, 91789, United States, Datafold provides Wellfound data infrastructure software services and processes Customer Personal Data related to data Wellfond stores within the Redshift data warehouse. Steps taken by Datafold to protect Customer Personal Data are described here: https://www.datafold.com/privacy-policy

9. **dbt Labs**, 915 Spring Garden St Suite 500, Philadelphia, Pennsylvania, 19123, United States; dbt Labs provides Wellfound data transformation software services and processes Customer Personal Data related to data Wellfond stores within the Redshift data warehouse. Steps taken by dbt Labs to protect Customer Personal Data are described here: https://www.getdbt.com/cloud/privacy-policy/

10. **Elasticsearch**, 800 W El Camino Real #350, Mountain View, CA, Elastic provides Wellfound search infrastructure software services and processes Customer Personal Data related to user names, email addresses, work history and messaging on Wellfound's platform. Steps taken by Elastic to protect Customer Personal Data are described here: https://www.elastic.co/legal/privacy-statement

11. **Facebook**, 1 Hacker Way, Menlo Park, CA 94025, USA, Facebook provides Wellfound marketing and advertising software services and processes Customer Personal Data related to user email addresses for retargeting. Steps taken by Facebook to protect Customer Personal Data are described here: https://www.facebook.com/privacy/policy/

12. **Front.com**, 1455 Market Street, Floor 19, San Francisco, CA 94103, United States; Front.com provides Wellfound customer support and processes Customer Personal Data related to user names and email addresses. Steps taken by Front.com to protect Customer Personal Data are described here: https://front.com/legal/privacy-notice

13. **Fullstory.com**, 1745 Peachtree Rd NW Suite G, Atlanta, GA 30309; Fullstory provides Wellfound with user research and processes Customer Personal Data related to user names, email addresses and website usage data. Steps taken by Fullstory to protect Customer Personal Data are described here: https://www.fullstory.com/privacy-resources/

14. **Gong.io**, 265 Cambridge Ave, Suite 60717. Palo Alto, CA 94306. Gong.io provides Wellfound with sales software support and processes Customer Personal Data related to user names and email addresses. Steps taken by Gong to protect Customer Personal Data are described here: https://www.gong.io/privacy-policy/

15. **Google** (including Google Ads, Google Analytics and Google Workspace), 1600 Amphitheatre Parkway, Mountain View, California; Google provides Wellfound with marketing, advertising, web analytics and email and calendar solutions for internal usage within Wellfound and external communication, and processes Customer Personal Data related to user names, email addresses, website usage and anonymized website usage and sometimes work history data. Steps taken by Gong to protect Customer Personal Data are described here: https://policies.google.com/privacy?hl=en-US

16. **Help Scout**, 177 Huntington Ave Ste 1703, Boston, Massachusetts, 02115, United States, Helpscout provides Wellfound customer support software and processes Customer Personal Data related to user names, email addresses and conversations with users. Steps taken by Helpscout to protect Customer Personal Data are described here: https://www.helpscout.com/company/legal/privacy/

17. **HireAbility**, 25 Nashua, Londonderry, New Hampshire, 03053, United States, HireAbility provides Wellfound software capable of parsing resume data and processes Customer Personal Data that is included in the resumes submitted by Wellfound users. Steps taken by HireAbility to protect Customer Personal Data are described here: https://www.hireability.com/company/privacy/

18. **Hotjar Ltd**., Dragonara Business Centre 5th Floor, Dragonara Road, Paceville, St Julian's STJ 3141, Malta; Hotjar provides Wellfound software for conducting user surveys and processes Customer Personal Data including email addresses and website usage data. Steps taken by Hotjar to protect Customer Personal Data are described here: https://www.hotjar.com/legal/policies/privacy/

19. **Interable.com**, Interable provides Wellfound with an email tool and processes Customer Personal Data related to email addresses and website usage data. Steps taken by Interable to protect Customer Personal Data are described here: https://iterable.com/trust/privacy-policy/

20. **LinkedIn**, 1000 W Maude Ave, Sunnyvale, CA, LinkedIn provides Wellfound with marketing and advertising and processes Customer Personal Data related to email addresses for retargeting. Steps taken by LinkedIn to protect Customer Personal Data are described here: https://www.linkedin.com/legal/privacy-policy

21. **Outreach.io**, 333 Elliott Ave W #500, Seattle, WA 98119. Outreach.io provides Wellfound with an email tool and processes Customer Personal Data related to email addresses and website usage data. Steps taken by Outreach.io to protect Customer Personal Data are described here: https://www.outreach.io/privacy-policy

22. **Quip**, 415 Mission St floor 5, San Francisco, CA 94103, Quip provides Wellfound with an internal and external collaboration tool, and processes Customer Personal Data related to user names, email addresses and work history data. Steps taken by Quip to protect Customer Personal Data are described here: https://quip.com/about/privacy

23. **Redis Labs**, 700 E El Camino Real #250, Mountain View, CA 94041, Redis Labs provides Wellfound with an internal data infrastructure tool and processes Customer Personal Data related to user names and email addresses. Steps taken by Redis Labs to protect Customer Personal Data are described here: https://redis.com/legal/privacy-policy/

24. **Rollbar**, 510 Federal Street Suite 401 San Francisco, CA 94107, Rollbar provides Wellfound with tool for tracking internal errors and processes Customer Personal Data related to user names and email addresses. Steps taken by Rollbar to protect Customer Personal Data are described here: https://docs.rollbar.com/docs/security

25. **Salesforce**, Salesforce Landmark, 415 Mission St, San Francisco, CA 94105, Salesforce provides Wellfound with customer relationship management software and processes Customer Personal Data related to user names, email addresses, company connection and website usage data. Steps taken by Salesforce to protect Customer Personal Data are described here: https://www.salesforce.com/company/privacy/full_privacy/

26. **Segment** and **Sendgrid (Twilio)**, 101 Spear St 1st Floor, San Francisco, CA 94105; Twilio provides Wellfound with software tools for data infrastructure and to manage sending and receiving emails, and processes Customer Personal Data related to user names, email addresses and website usage data. Steps taken by Twilio to protect Customer Personal Data are described here: https://www.twilio.com/legal/privacy

27. **Slack**, 500 Howard Street San Francisco, CA 94105; Slack provides Wellfound with an internal and external collaboration tool, and processes Customer Personal Data related to user names, email addresses and work history data. Steps taken by Slack to protect Customer Personal Data are described here: https://slack.com/trust/privacy/privacy-policy

28. **Split Software**, The Sequoia Building, 2317 Broadway floor 3, Redwood City, CA 94063; Split Software provides Wellfound with A/B testing tool and processes Customer Personal Data related to user names and IDs. Steps taken by Split Software to protect Customer Personal Data are described here: https://www.split.io/legal/privacy-policy/

29. **Stripe**, 354 Oyster Point Blvd South San Francisco, CA 94080; Stripe provides Wellfound with billing services and processes Customer Personal Data related to user name, email addresses and billing addresses. Steps taken by Stripe to protect Customer Personal Data are described here: https://stripe.com/privacy

30. **Tremendous**, 1592 Union St Ste 502, San Francisco, California, 94123, United States; Tremendous provides Wellfound with incentives processing tool and processes Customer Personal Data related to user names and email addresses. Steps taken by Tremendous to protect Customer Personal Data are described here: https://www.tremendous.com/privacy.