Data Processing Addendum

Last updated: May 2026

This Data Processing Addendum ("DPA") supplements any existing and currently valid Terms and Conditions, Subscription Agreement, Services Agreement, Reseller Agreement, Partner Agreement, or other partnership agreement (as applicable, the "Agreement") entered into by and between Customer (as defined in the Agreement) and Findem, Inc. and its affiliates ("Company") This DPA incorporates the terms of the Agreement, and any terms not defined in this DPA shall have the meaning set forth in the Agreement.

PART 1: GENERAL PROVISIONS

1. DEFINITIONS

1.1 "Affiliate" means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

1.2 "Authorized Sub-Processor" means a third-party who has a need to know or otherwise access Customer Personal Data to enable Company to perform its obligations under this DPA or the Agreement, and who is authorized under Section 5 of this DPA.

1.3. "Customer Personal Data" means Personal Data Processed by Company as a Processor on behalf of Customer.

1.4 "Company Account Data" means Personal Data that relates to Company's relationship with Customer, including the names or contact information of individuals authorized by Customer to access Customer's account and billing information of individuals that Customer has associated with its account. Company Account Data also includes any data Company may need to collect for the purpose of managing its relationship with Customer, identity verification, or as otherwise required by applicable laws and regulations.

1.5 "Company Usage Data" means Service usage data collected and Processed by Company in connection with the provision of the Services, including without limitation data used to identify the source and destination of a communication, activity logs, and data used to optimize and maintain performance of the Services, and to investigate and prevent system abuse.

1.6. "Passive Candidate Data" means professional and employment-related Personal Data of potential candidates for employment obtained from various sources that Company makes available to Customers upon request.

1.7 "Data Exporter" means the party identified as the data exporter in Section 9 of this DPA.

1.8 “Data Importer” means the party identified as the data importer in Section 9 of this DPA.

1.9 “Data Protection Laws” means any applicable laws and regulations in any relevant jurisdiction relating to the use or Processing of Personal Data including: (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020 (“CCPA”), (ii) 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”); (iii) the Swiss Federal Act on Data Protection; (iv) the UK Data Protection Act 2018; and (v) the Privacy and Electronic Communications (EC Directive) Regulations 2003 in each case, as updated, amended or replaced from time to time. The terms “Data Subject”, “Personal Data”, “Personal Data Breach”, “Processing”, “Processor,” “Controller,” and “Supervisory Authority” shall have the meanings set forth in the GDPR.

1.10 “Data Subject Request” means a request to exercise individuals’ rights to information, access, rectification, erasure, restriction, portability, objection, the right to withdraw consent, and the right not to be subject to automated individual decision-making in accordance with applicable Data Protection Laws.

1.11 “SCCs” means the 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 adapted to the parties by Section 9 of this DPA.

1.12 “ex-EEA Transfer” means the transfer of Personal Data, which is Processed in accordance with the EU GDPR, from the Data Exporter to the Data Importer (or its premises) outside the European Economic Area (the “EEA”), and such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the EU GDPR.

1.13 “ex-UK Transfer” means the transfer of Personal Data covered by Chapter V of the UK GDPR, which is Processed in accordance with the UK GDPR and the Data Protection Act 2018, from the Data Exporter to the Data Importer (or its premises) outside the United Kingdom (the “UK”), and 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.

1.14 “Services” shall have the meaning set forth in the Agreement.

1.15 “UK Addendum” means the addendum to the SCCs issued by the UK Information Commissioner under Section 119A(1) of the UK Data Protection Act 2018 (version B1.0, in force March 21, 2022).

1.16 “Third-Party Controller” means a Controller for which Customer is a Processor.

1.17 “Sensitive Data” means special category Personal Data as defined in Article 9(1) of the GDPR and any similar concept under applicable Data Protection Laws subjecting a certain category of Personal Data to heightened protection or restrictions.

2. RELATIONSHIP OF THE PARTIES

2.1 **Company's Processor Role**. The parties acknowledge and agree that with regard to the Processing of Customer Personal Data, Company acts as a Processor on behalf of Customer for the purposes specified in Exhibit I.B below. Customer may act either as a Controller or Processor on behalf of a Third-Party Controller, and Company is a Processor. Customer is responsible for compliance with the requirements of Data Protection Laws applicable to Controllers and shall, in its use of the Services, at all times Process Personal Data, and provide instructions for the Processing of Personal Data, in compliance with Data Protection Laws. Customer shall ensure that the Processing of Personal Data in accordance with Customer's instructions will not cause Company to be in breach of the Data Protection Laws. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Company by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data, and (iii) the instructions it provides to Company regarding the Processing of such Personal Data. Customer shall not provide or make available to Company any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Company from all claims and losses in connection therewith. If Customer is a Processor on behalf of a Third-Party Controller, then Customer: is the single point of contact for Company; must obtain all necessary authorizations from such Third-Party Controller; and undertakes to issue all instructions and exercise all rights on behalf of such other Third-Party Controller.

2.2. **Company's Controller Role**. Company Processes the following categories of Personal Data as a Controller under Data Protection Laws:

- Passive Candidate Data for the purposes of building and maintaining a structured and searchable database that enables employers to identify potential candidates for employment opportunities. Where Customer receives Passive Candidate Data, both parties act as separate and independent Controllers for the sharing of such Passive Candidate Data, as further described in Exhibit I.A.
- Company Account Data and Company Usage Data for the purposes of (i) managing the relationship with Customer; (ii) carrying out Company's core business operations, such as accounting, audits, tax preparation and filing and compliance purposes; (iii) monitoring, investigating, preventing and detecting fraud, security incidents and other misuse of the Services, and to prevent harm to Customer; (iv) for identity verification purposes; (v) complying with legal or regulatory obligations applicable to the Processing and retention of Personal Data to which Company is subject; and (vi) as otherwise permitted under Data Protection Laws and in accordance with this DPA and the Agreement. Company may also Process Company Usage Data as a controller to provide, optimize, and maintain the Services, to the extent permitted by Data Protection Laws.

In these cases, both parties are separately responsible for compliance with their own obligations under Data Protection Laws. Any Processing by the Company as a Controller shall be in accordance with the Company's privacy policy set forth at https://www.findem.ai/privacy-policy.

PART 2: PROVISIONS APPLICABLE WHEN COMPANY ACTS AS A PROCESSOR

3. PROCESSING OF DATA

3.1 To the extent that Company acts as a Processor, Company shall not Process Personal Data (i) for purposes other than those set forth in the Agreement and Exhibit I.B, (ii) in a manner inconsistent with the terms and conditions set forth in this DPA or any other documented instructions provided by Customer, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Supervisory Authority to which the Company is subject; in such a case, the Company shall inform the Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest, or (iii) in violation of Data Protection Laws. Customer hereby instructs Company to Process Personal Data in accordance with the foregoing and as part of any Processing initiated by Customer in its use of the Services.

3.2 The subject matter, nature, purpose, and duration of this Processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit I.B to this DPA.

3.3 Following completion of the Services, at Customer's choice, Company shall return or delete Customer's 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, Company 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 Customer and Company have entered into SCCs 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 SCCs (as applicable) shall be provided by Company to Customer only upon Customer's request.

3.4 US Privacy Law. The Parties acknowledge and agree that the Processing of Personal Data that is subject to the CCPA and/or any other applicable Data Protection Law in the United States shall be carried out in accordance with the terms set forth in Exhibit III.

4. CONFIDENTIALITY

Company shall ensure that any person it authorizes to Process Personal Data has agreed to protect Personal Data in accordance with Company's confidentiality obligations in the Agreement. Customer agrees that Company 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 Customer.

5. AUTHORIZED SUB-PROCESSORS

5.1 Customer acknowledges and agrees that Company may engage its Affiliates and Authorized Sub-Processors to access and Process Customer Personal Data in connection with the Services. By way of this DPA, Customer provides general written authorization to Company to engage Sub-Processors as necessary to perform the Services.

5.2 A list of Company's current Authorized Sub-Processors (the "List") is set forth in Exhibit IV and as may be published on Company's website. Such List may be updated by Company from time to time. Company may provide a mechanism to subscribe to notifications of new Authorized Sub-Processors and Customer agrees to subscribe to such notifications where

available. At least ten (10) days before enabling any third party other than existing Authorized Sub-Processors to access or participate in the Processing of Personal Data, Company will add such third party to the List and notify Customer via email. Customer may object to such an engagement by informing Company within ten (10) days of receipt of the aforementioned notice by Customer, provided such objection is in writing and based on reasonable grounds relating to data protection. Customer acknowledges that certain Sub-Processors are essential to providing the Services and that objecting to the use of a Sub-Processor may prevent Company from offering the Services to Customer.

5.3 If Customer reasonably objects to an engagement in accordance with Section 5.2, and Company cannot provide a commercially reasonable alternative within a reasonable period of time, Customer may discontinue the use of the affected Service by providing written notice to Company. Discontinuation shall not relieve Customer of any fees owed to Company under the Agreement.

5.4 If Customer does not object to the engagement of a third party in accordance with Section 5.2 within ten (10) days of notice by Company, that third party will be deemed an Authorized Sub-Processor for the purposes of this DPA.

5.5 Company will enter into a written agreement with the Authorized Sub-Processor imposing on the Authorized Sub-Processor data protection obligations comparable to those imposed on Company under this DPA with respect to the protection of Personal Data. In case an Authorized Sub-Processor fails to fulfill its data protection obligations under such written agreement with Company, Company will remain liable to Customer for the performance of the Authorized Sub-Processor's obligations under such agreement.

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

6. DATA SUBJECT REQUESTS

6.1 Company shall, to the extent permitted by law, notify Customer upon receipt of a Data Subject Request. If Company receives a Data Subject Request in relation to Customer Personal Data, Company will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. Customer is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of Processing, or withdrawal of consent to Processing of any Personal Data are communicated to Company, and, if applicable, for ensuring that a record of consent to Processing is maintained with respect to each Data Subject.

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

7. ACTIONS AND ACCESS REQUESTS; AUDITS

7.1 Company shall, taking into account the nature of the Processing and the information available to Company, provide Customer with reasonable cooperation and assistance where necessary for Customer to comply with its obligations under the GDPR to conduct a data protection impact assessment and/or to demonstrate such compliance, *provided that* Customer does not otherwise have access to the relevant information. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

7.2 Company shall, taking into account the nature of the Processing and the information available to Company, provide Customer with reasonable cooperation and assistance with respect to Customer's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the GDPR. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

7.3 Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Company shall, either (i) make available for Customer's review copies of certifications or reports demonstrating Company's compliance with prevailing data security standards applicable to the processing of Customer's Personal Data, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Data Protection Laws, allow Customer's independent third party representative to conduct an audit or inspection of Company's data security infrastructure and procedures that is sufficient to demonstrate Company's compliance with its obligations under Data Protection Laws, provided that (a) Customer provides reasonable prior written notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Company'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 data relevant to Customer. Customer shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Company for any time expended for on-site audits. If Customer and Company have entered into SCCs as described in Section 9 (Transfers of Personal Data), the parties agree that the audits described in Clause 8.9 of the SCCs shall be carried out in accordance with this Section 7.3.

7.4 Company shall immediately notify Customer if an instruction, in the Company's opinion, infringes Data Protection Laws.

7.5 In the event of a Personal Data Breach affecting Customer Personal Data, Company shall, without undue delay, inform Customer of the Personal Data Breach and take such steps as

Company in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within Company's reasonable control).

7.6 In the event of a Personal Data Breach affecting Customer Personal Data, Company shall, taking into account the nature of the Processing and the information available to Company, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under the GDPR with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

7.7 The obligations described in Sections 7.5 and 7.6 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer. Company's obligation to report or respond to a Personal Data Breach under Sections 7.5 and 7.6 will not be construed as an acknowledgement by Company of any fault or liability with respect to the Personal Data Breach.

8. DIVERSITY AND INCLUSION OFFERINGS

At the request of Customer, Company may provide functionality that permits Customer to search, sort, and filter candidates by gender, ethnicity, and other characteristics, and any related or similar features now or hereafter developed ("DEI Functionality"). Customer acknowledges that Customer's enablement and use of the DEI Functionality is at its specific election and that Company may suspend Customer's use of DEI Functionality at any time, without prior notice and in its sole discretion, if it believes Customer's use of DEI Functionality violates this Section 8 or Data Protection Laws. Customer warrants that it will use DEI Functionality only to aid in its legitimate efforts to diversify its candidate pool and acknowledges that it is solely responsible for its use of the DEI Functionality and for its recruiting and hiring decisions. Customer further represents and warrants that its use of the DEI Functionality will comply with the terms of the Agreement, this DPA, and Data Protection Laws. In particular, for the avoidance of doubt, where the DEI Functionality involves the Processing of Sensitive Data, Customer is the Controller and is solely responsible for identifying and documenting a valid legal basis for such Processing under Data Protection Laws. Company Processes such data solely on Customer's documented instructions, as a Processor of Customer. Notwithstanding anything to the contrary in this DPA or the Agreement, in connection with any claim or action that arises from the DEI Functionality or that is in any way related to Customer's use of the DEI Functionality (i) Company will have no obligation to defend, indemnify, or otherwise hold Customer harmless, (ii) Company will have no liability to Customer under the Agreement or this DPA, and (iii) Customer agrees to indemnify and hold Company harmless from and against any and all such claims, liabilities, damages (actual and consequential), losses and expenses (including attorneys' fees).

PART 3: PROVISIONS APPLICABLE WHEN THE COMPANY ACTS AS A CONTROLLER OR AS A PROCESSOR

9. TRANSFERS OF PERSONAL DATA

9.1 The parties agree that Company may transfer Personal Data Processed under this DPA outside the EEA, the UK, or Switzerland as necessary to provide the Services. Customer acknowledges that Company's primary Processing operations take place in the United States, and

that the transfer of Customer's Personal Data to the United States is necessary for the provision of the Services to Customer. If Company transfers Personal Data protected under this DPA to a jurisdiction for which the European Commission has not issued an adequacy decision, Company will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Laws.

9.2 Ex-EEA Transfers. The parties agree that ex-EEA Transfers are made pursuant to the SCCs, which are deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

- 9.2.1 Module One (Controller to Controller) of the SCCs apply when Company is Processing Personal Data as a Controller pursuant to Section 2.2 of this DPA. Module One of the SCCs is hereby incorporated and completed as follows: the "data exporter" is Company; the "data importer" is Customer; the optional docking clause in Clause 7 is implemented; the optional paragraph in Clause 11(a) is struck; Option 1 in Clause 17 is implemented and the governing law is the law of Ireland; the courts in Clause 18(b) are the Courts of Ireland; Annex I and II to Module 1 of the SCCs, are Exhibits I.A and II to this DPA, respectively.

- 9.2.2 Module Two (Controller to Processor) of the SCCs apply when Customer is a controller and Company is Processing Customer Personal Data as a Processor pursuant to Section 2.1 of this DPA. Module Two of the SCCs is hereby incorporated and completed as follows: the "data exporter" is Customer; the "data importer" is Company; the optional docking clause in Clause 7 is implemented; Option 2 of Clause 9(a) is implemented and the time period therein is specified in Section 5.2 above; the optional redress clause in Clause 11(a) is struck; Option 1 in Clause 17 is implemented and the governing law is the law of Ireland; the courts in Clause 18(b) are the Courts of Ireland; Annex I and II to Module 2 of the SCCs are Exhibits I.B and II to this DPA respectively.

- 9.2.3 Module Three (Processor to Sub-Processor) of the SCCs apply when Customer is a Processor on behalf of Third-Party Controller and Company is Processing Customer Personal Data on behalf of Customer as a Sub-Processor pursuant to Section 2.1 of this DPA. Module Three of the SCCs is hereby incorporated and completed as follows: the "data exporter" is Customer; the "data importer" is Company; the optional docking clause in Clause 7 is implemented; Option 2 of Clause 9(a) is implemented and the time period therein is specified in Section 5.2 above; the optional redress clause in Clause 11(a) is struck; Option 1 in Clause 17 is implemented and the governing law is the law of Ireland; the courts in Clause 18(b) are the Courts of Ireland; Annex I and II to Module 2 of the SCCs are Exhibits I.B and II to this DPA respectively.

9.3 Ex-UK Transfers. The parties agree that ex-UK Transfers are made pursuant to the UK Addendum, which is hereby incorporated by reference, and Part 1 is completed as follows:

- 9.3.1: For Module One of the SCCs: (i) in Table 1, the "Exporter" is Company and the "Importer" is Customer, their details are set forth in this DPA, and the Agreement; (ii) in Table 2, the first option is selected and the "Approved EU SCCs" are the SCCs referred to in Section 9.2.1 of this DPA; (iii) in Table 3, Annex 1 (A and B) and 2 to the

"Approved EU SCCs" are Exhibits I.A and II of this DPA; and (iv) in Table 4, both the "Importer" and the "Exporter" can terminate the UK Addendum

- 9.3.2: For Module Two of the SCCs: (i) in Table 1, the "Exporter" is Customer and the "Importer" is Company , their details are set forth in this DPA, and the Agreement; (ii) in Table 2, the first option is selected and the "Approved EU SCCs" are the SCCs referred to in Section 9.2.2 of this DPA; (iii) in Table 3, Annexes 1 (A and B) and II to the "Approved EU SCCs" are Exhibit I.B and Exhibit II respectively; and (iv) in Table 4, both the "Importer" and the "Exporter" can terminate the UK Addendum.
- 9.3.3: For Module Three of the SCCs: (i) in Table 1, the "Exporter" is Customer and the "Importer" is Company , their details are set forth in this DPA, and the Agreement; (ii) in Table 2, the first option is selected and the "Approved EU SCCs" are the SCCs referred to in Section 9.2.3 of this DPA; (iii) in Table 3, Annexes 1 (A and B) and II to the "Approved EU SCCs" are Exhibit I.B and Exhibit II respectively; and (iv) in Table 4, both the "Importer" and the "Exporter" can terminate the UK Addendum.

9.4 Transfers from Switzerland. The parties agree that transfers from Switzerland are made pursuant to the SCCs with the following modifications:

- 9.4.1 The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the 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.

- 9.4.2 The terms of the SCCs shall be interpreted to protect the data of legal entities until the effective date of the Revised FADP.

- 9.4.3 Clause 13 of the 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.

- 9.4.4 The term "EU Member State" as utilized in the 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 SCCs.

- 9.4.5 If Data Protection Laws require the Data Exporter to execute the Standard Contractual Clauses applicable to a particular transfer of Personal Data to a Data Importer as a separate agreement, the Data Importer shall, on request of the Data Exporter, promptly execute such Standard Contractual Clauses incorporating such amendments as may reasonably be required by the Data Exporter to reflect the applicable appendices and annexes, the details of the transfer and the requirements of the relevant Data Protection Laws.

- 9.4.6 If either (i) any of the means of legitimizing transfers of Personal Data outside of the EEA, UK, or Switzerland set forth in this DPA cease to be valid or (ii) any Supervisory Authority requires transfers of Personal Data pursuant to those means to be

suspended, then Company may by notice to Customer, with effect from the date set out in such notice, amend or put in place alternative arrangements in respect of such transfers, as required by Data Protection Laws.

10. SECURITY OF PERSONAL DATA

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, each party shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of Processing Personal Data.

Exhibit II sets forth additional information regarding the technical and organizational security measures implemented by each party in its role as Data Importer under the SCCs.

11. CONFLICT

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

EXHIBIT I.A

Controller to Controller

A. List of Parties

Data exporter(s):

- **Name**: Findem, Inc (the "Company")
- **Address**: 702 Marshall Street, Redwood City, CA 94063
- **Contact person's name, position and contact details**: Lech Kaiel, Head of Data Operations
- **Activities relevant to the data transferred under these Clauses**: The Company makes Passive Candidate Data available to Customer as part of the Services provided to Customer.
- **Signature and date**: By entering into the Agreement, the Company is deemed to have signed the SCCs incorporated herein, as of the Effective Date of the Agreement.
- **Role (Controller/Processor)**: Controller.

Data importer(s):

- **Name**: Customer
- **Address**: As indicated in the Agreement
- **Contact person's name, position and contact details**: As indicated in the Agreement
- **Activities relevant to the data transferred under these Clauses**: The Customer receives Passive Candidate Data from Company as part of the Services it receives from Company.
- **Signature and date**: By entering into the Agreement, the Customer is deemed to have signed the SCCs incorporated herein, as of the Effective Date of the Agreement.
- **Role (Controller/Processor)**: Controller.

B. Description of Transfer

- **Categories of Data Subjects whose Personal Data is transferred**: Individuals whose Personal Data is included in the Passive Candidate Data.
- **Categories of Personal Data transferred**: Professional and employment-related personal data about job candidates to create structured candidate profiles. This may include a candidate's name, professional title, location, and public profile references, as well as career information including employment history, job titles, employers, dates of engagement, role descriptions, education history, professional skills, and publicly available endorsements or recommendations.
- **Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures**: N/A

- **The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis)**: On a continuous basis.
- **Nature of the processing**: The Personal Data will be processed and transferred as described in the Agreement.
- **Purpose(s) of the data transfer and further processing**: The Personal Data will be transferred and further processed for the provision of the Services as described in the Agreement.
- **The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period**: Personal Data will be retained for as long as necessary taking into account the purpose of the Processing, and in compliance with applicable laws, including laws on the statute of limitations and Applicable European Data Protection Law.
- **For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing**: N/A

C. Competent Supervisory Authority

- The competent authority for the Processing of Personal Data relating to Data Subjects located in the EEA is the Irish Data Protection Commission.
- The competent authority for the Processing of Personal Data relating to Data Subjects located in the UK is the UK Information Commissioner.
- The competent authority for the Processing of Personal Data relating to Data Subjects located in Switzerland is the Swiss Federal Data Protection and Information Commissioner.

EXHIBIT I.B

Controller to Processor

A. List of Parties

Data exporter(s):

- **Name**: Customer
- **Address**: As indicated in the Agreement.
- **Contact person's name, position and contact details**: As indicated in the Agreement.
- **Activities relevant to the data transferred under these Clauses**: Customer provides Customer Personal Data to Company in order to receive the Services from Company.
- **Signature and date**: By entering into the Agreement, Data Exporter is deemed to have signed these SCCs incorporated herein, as of the Effective Date of the Agreement.
- **Role (Controller/Processor)**: Controller, or Processor on behalf of Third-Party Controller.

Data importer(s):

- **Name**: Findem, Inc.
- **Address**: 702 Marshall Street, Redwood City, CA 94063
- **Contact person's name, position and contact details**: Lech Kaiel, Head of Data Operations
- **Activities relevant to the data transferred under these Clauses**: The Company Processes Customer Personal Data as part of its Services provided to the Customer
- **Signature and date**: By entering into the Agreement, the Company is deemed to have signed the SCCs incorporated herein, as of the Effective Date of the Agreement.
- **Role (Controller/Processor)**: Processor.

2. Description of Transfer

- **Categories of Data Subjects whose Personal Data is transferred**: Individuals included in Customer Personal Data, such as Applicants for Jobs, Candidates in CRM and Prospective Employees that Company's recruiters or AI agents reach out to. With respect to Getro services, this may also include visitors to the job board, current and prospective professional connections of the Customer, and logged-in users of the Getro admin portal, including members of Customer's organization invited by Customer to administer the Services provided by the Company, and members of an organization within Customer's network invited by Customer to administer the profile of said organization on the Getro platform.
- **Categories of Personal Data transferred**: Categories of Personal Data include name, job title, location, email, phone number, resume/cv if available, work history, skill assessment results, interview transcripts, and IP address.

Additional Personal Data collected is dependent on the product used and the optional proctoring features enabled. Customer has full control over which products and which proctoring features are used.

With respect to Glider services:

	Skill Assessments	Live Interview	Agentic AI Interview	ID Verify	L&D Roleplay
Facial Image	Optional	Optional	Optional	Required	Optional
Face detection	Optional	Optional	Optional	Required	Optional
Facial Movement	Optional	N/A	N/A	N/A	N/A
Candidate Voice	Optional	Required	Required	Required	Required
Video Recording	Optional	Optional	Optional	Optional	Optional
Browser Activity	Optional	Optional	Optional	N/A	Optional
ID Card	Optional	Optional	Optional	Required	N/A

When a candidate captures an image of their ID card, the text on the ID is immediately redacted.

While Company captures facial image and candidate voice, Company is not using this data to identify who the individual is. It therefore falls outside most legal definitions of biometric data and is not classified as sensitive data.

With respect to Getro services:
Contact details (including name, email address, contacts numbers etc.); region where resident/active; professional details (including educational and professional history, achievements and qualifications, and information contained within a subject's resume/cv); job preferences (including location, salary, seniority level and function, etc.); account details (including username, password and communication preferences); device fingerprints (including IP address, browser and operating system etc.); correspondence and communications data (including details contained in emails, messages and other communications between data subject and Company); technical data (including IP address, browser type, internet service provider, device identifier, login information, time zone setting, browser plug-in types and versions, preferred language, operating system and platform, and geographical location); and usage data (including URL, clickstream to,

through and from the website(s) comprising Company's services, pages viewed and searched for, page response times, length of visits to certain pages, referral source/exit pages, page interaction information (such as scrolling, clicks and mouse-overs), date and time pages are accessed, website navigation and search terms used)

- **Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:** To the extent permitted by applicable Data Protection Laws and as instructed by Customer, Company may Process information relating to individuals' racial or ethnic origin if this information is available in employee records per EEOC compliance (i.e., self-declared by the employee). Company only uses this to identify the diversity of the teams or candidate pipeline for reports requested by Customer, subject to strict access controls as set out in Exhibit II. Candidates may request reasonable accommodations based on specific disabilities through an embedded workflow, to allow Candidates to complete screening activities via an alternative method. Although the Company may Process facial images and candidate voices, Company does not use this to identify individuals, which is generally not considered biometric and therefore sensitive data.
- **The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis)**: On a continuous basis.
- **Nature of the processing**: The Personal Data will be processed and transferred as described in the Agreement.
- **Purpose(s) of the data transfer and further processing**: The Personal Data will be transferred and further processed for the provision of the Services as described in the Agreement.
- **The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period**: Company will Process Customer Personal Data as long as required (i) to provide the Services to Customer under the Agreement (including subject to any Customer-configured retention periods) or (ii) by applicable law or regulation. With respect to Customer Personal Data processed for the Getro services, this may be until six (6) months from the date when: (a) the Agreement is terminated or expires; (b) the job board is no longer active; (c) the talent network tool is no longer active; (d) where the data subject is a job seeker who has subscribed to job alerts, when the subject unsubscribes from job alerts; (e) where the data subject is a job seeker who has submitted an application to an open role, when the data subject withdraws their application; (f) where the data subject is a job seeker who has registered to the talent network, when the subject deregisters from the talent network; or (g) where the data subject is an administrator, when the data subject deletes their account or their account is deleted by another administrator.
- **For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing**: For the subject matter and nature of the Processing, reference is made to the Agreement and this DPA. The Processing will take place for the duration of the Agreement.

3. Competent Supervisory Authority

- The competent authority for the Processing of Personal Data relating to Data Subjects located in the EEA is the Irish Data Protection Commission.
- The competent authority for the Processing of Personal Data relating to Data Subjects located in the UK is the UK Information Commissioner.
- The competent authority for the Processing of Personal Data relating to Data Subjects located in Switzerland is the Swiss Federal Data Protection and Information Commissioner.

EXHIBIT II

Description of the Technical and Organizational Security Measures implemented by the Data Importer

The following includes the information required by Annex II of the SCCs and Annex II of the UK Addendum. Section A below describes the technical and organizational measures implemented by Company where it acts as Data Importer (Modules 2 and 3 SCCs), and Section B describes the technical and organizational measures implemented by Customer where it acts as Data Importer (Module 1 SCCs).

Section A. Measures implemented by Company where it is Data Importer (Modules 2 and 3 SCCs)

Technical and Organizational Security Measure	**Details**
Measures of pseudonymisation and encryption of personal data	Findem uses the minimum AES-256 encryption standard for all Personal Data at rest.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Findem being SOC 2 compliant, Findem has operational security policy, access control policy and asset management policy and dedicated teams to monitor and manage all the asset configurations. We can provide them upon request.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Findem has Business Continuity and Incident Response policies in place for any kind of physical/technical/unforeseen issue handling. We also have support escalation policies in place to ensure timely resolution to all customer related issues/incidents. More on this can be made available upon request.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Findem does annual audits from vendors like Vanta and TAC security who audit Findem on SOC2, and perform penetration testing. We can provide the SOC2 reports to support this.

Measures for user identification and authorization	Findem users need a login id and password which is paired with Multi Factor Authentication for accessing the platform. Findem also integrated with most common SSO vendors like Okta, G-Suite etc. for IAM
Measures for the protection of data during transmission	Findem is a https only website and all the data during transmission is encrypted end to end with appropriate ciphers.
Measures for the protection of data during storage	Findem uses the minimum AES-256 encryption standard for data at rest.
Measures for ensuring physical security of locations at which personal data are processed	All Findem services run on AWS locations which are both SOC2 and PCI compliant.
Measures for ensuring events logging	Findem consistently monitors all the resources and records events using agents installed on all the servers.
Measures for ensuring system configuration, including default configuration	Findem being SOC 2 compliant, Findem has operational security policy, access control policy and asset management policy and dedicated teams to monitor and manage all the asset configurations. We can provide them upon request.
Measures for internal IT and IT security governance and management	Findem has a dedicated IT and security teams to handle all security governance. We have InfoSec and asset management policy which can be provided upon request. All Findem employees need to go through security awareness training certification and accept security policies annually.
Measures for certification/assurance of processes and products	All Findem employees need to go through security awareness training certification and accept security policies annually.

Measures for ensuring data minimisation	Findem does not collect any data that is not needed to provide optimal business value. More on our privacy policy here: https://www.findem.ai/privacy-policy
Measures for ensuring data quality	Findem has well defined policies in place to ensure data quality, data management, business continuity, incident responses and operational security to ensure data quality and integrity for all the services Findem offers.
Measures for ensuring limited data retention	Findem has implemented technical and organizational measures as appropriate to ensure it returns or deletes Personal Data as provided in Section 3.3 of the DPA.
Measures for ensuring accountability	All Findem employees need to go through security awareness training certification and accept security policies annually.
Measures for allowing data portability and ensuring erasure	Findem has taken appropriate technical and organizational measures to assist Customer in handling requests for data portability and erasure.
Technical and organizational measures of sub-processors	Findem requires all Sub-Processors/vendors to sign/adhere to a detailed DPA and security audit and review before Findem can use them as Sub-Processors/vendors.

Section B. Measures implemented by Customer where it is Data Importer (Module 1 SCCs)

Customer will implement industry-standard security measures including the following types of measures:

1. Physical access control

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are Processed, include:

- Establishing security areas, restriction of access paths;
- Establishing access authorizations for employees and third parties;
- Access control system (ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Door locking (electric door openers etc.);
- Security staff;
- Surveillance facilities, video/CCTV monitor, alarm system; and
- Securing decentralized data processing equipment and personal computers.

2. Virtual access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

- User identification and authentication procedures;
- Strong ID/password security procedures (special characters, minimum length and complexity requirements, change of password);
- Automatic blocking (e.g. password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- Creation of one master record per user, user-master data procedures per data processing environment; and
- Encryption of archived data media.

3. Data access control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, include:

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access Personal Data without authorization;
- Reports of access;
- Access procedure;
- Change procedure;

- Deletion procedure; and
- Encryption.

4. Disclosure control

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include:

- Encryption/tunneling;
- Logging; and
- Transport security.

5. Entry control

Technical and organizational measures to monitor whether Personal Data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

- Logging and reporting systems; and
- Audit trails and documentation.

6. Control of instructions

Technical and organizational measures to ensure that Personal Data are Processed solely in accordance with the instructions of a Controller include:

- Unambiguous wording of the contract;
- Formal commissioning (request form); and
- Criteria for selecting a Processor.

7. Availability control

Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include:

- Backup procedures;
- Mirroring of hard disks (e.g. RAID technology);
- Uninterruptible power supply (UPS);
- Remote storage;
- Anti-virus/firewall systems; and
- Disaster recovery plan.

8. Separation control

Technical and organizational measures to ensure that Personal Data collected for different purposes can be Processed separately include:

- Separation of databases;
- "Internal client" concept / limitation of use;
- Segregation of functions (production/testing); and
- Procedures for storage, amendment, deletion, transmission of data for different purposes.

9. Testing controls

Technical and organizational measures to test, assess and evaluate the effectiveness of the technical and organizational measures implemented in order to ensure the security of the processing include:

- Periodical review and test of disaster recovery plan;
- Testing and evaluation of software updates before they are installed;
- Authenticated (with elevated rights) vulnerability scanning; and
- Test bed for specific penetration tests and Red Team attacks.

10. IT governance

Technical and organizational measures to improve the overall management of IT and ensure that the activities associated with information and technology are aligned with the compliance efforts include:

- Certification/assurance of processes and products;
- Processes for data minimization;
- Processes for data quality;
- Processes for limited data retention;
- Processes for ensuring accountability; and
- Data subject rights policies.

Exhibit III: United States Privacy Law Exhibit

This United States Privacy Law Exhibit ("Exhibit III") supplements the DPA and includes additional information required by applicable Data Protection Laws in the United States, including the CCPA and its implementing regulations, in each case, as updated, amended or replaced from time to time. Any terms not defined in this Exhibit III shall have the meanings set forth in the DPA and/or the Agreement.

- 1. Definitions

1.1 For purposes of this Exhibit III, the terms "Business," "Business Purpose," "Commercial Purpose," "Consumer," "Personal Information," "Processing," "Sell," "Service Provider," "Share," and "Verifiable Consumer Request" shall have the meanings set forth in the CCPA.

1.2 All references to "Personal Data," "Controller," "Processor," and "Data Subject" in the DPA shall have the meaning defined in applicable Data Protection Laws in the United States.

1.3 In the event of a conflict in the meanings of defined terms in this Exhibit III, the meaning from the law applicable to the state of residence of the relevant Consumer and/or Data Subject applies.

- 2. Obligations

2.1 Except with respect to Company Account Data and Company Usage Data (as defined in the DPA), the parties acknowledge and agree that Company is a Service Provider / Processor for the purposes of the applicable Data Protection Laws in the United States (to the extent it applies) and Company is receiving Personal Information / Personal Data from Customer in order to provide the Services pursuant to the Agreement, which constitutes a Business Purpose.

2.2 Customer shall disclose Personal Information / Personal Data to Company only for the limited and specified Business Purposes described in Exhibit I.B. to this DPA.

2.3 Company shall not Sell or Share Personal Information / Personal Data provided by Customer under the Agreement.

2.4 Company shall not retain, use, or disclose Personal Information / Personal Data provided by Customer pursuant to the Agreement for any purpose, including a Commercial Purpose, other than as necessary for the specific purpose of performing the Services for Customer pursuant to the Agreement, or as otherwise set forth in the Agreement or as permitted by the applicable Data Protection Laws in the United States.

2.5 Company shall not retain, use, or disclose Personal Information / Personal Data provided by Customer pursuant to the Agreement outside of the direct business relationship between Company and Customer, except where and to the extent permitted by the applicable Data Protection Laws in the United States.

2.6 Company shall notify Customer if it makes a determination that it can no longer meet its obligations under the applicable Data Protection Laws in the United States. Upon receiving

notice from Company in accordance with this subsection, Customer may direct Company to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Information / Personal Data.

2.7 Company will not combine Personal Information / Personal Data received from, or on behalf of, Customer with Personal Information / Personal Data that it receives from, or on behalf of, another party, or that it collects from its own interaction with the Consumer.

2.8 Company shall comply with all obligations applicable to Service Providers under the applicable Data Protection Laws in the United States, including by providing Personal Information / Personal Data provided by Customer under the Agreement the level of privacy protection required by applicable Data Protection Laws in the United States.

2.9 Company shall only engage a new sub-processor to assist Company in providing the Services to Customer under the Agreement in accordance with Section 4.1 of the DPA, including, without limitation, by: (i) notifying Customer of such engagement via the notification mechanism described in Section 4.1 of the DPA at least ten (10) days before enabling a new Sub-Processor; and (ii) entering into a written contract with the sub-processor requiring sub-processor to observe all of the applicable requirements set forth in the applicable Data Protection Laws in the United States.

- 3. Consumer Rights

3.1 Company shall assist Customer in responding to Verifiable Consumer Requests to exercise the Consumer's rights under the applicable Data Protection Laws in the United States as set forth in Section 7 of the DPA.

- 4. Audit Rights

4.1 To the extent required by applicable Data Protection Laws in the United States, Company shall allow Customer to conduct inspections or audits in accordance with Sections 8.3 and 8.4 of the DPA.

Exhibit IV: Sub-Processor List

Infrastructure Providers

Name	Location	Description of processing	Findem Service
Amazon Web Services, Inc	United States, Ireland	Third party hosting and sending provider	All
OpenAI OpCo, LLC	United States	Candidate resume/data + user inputs for enhancement/Q&A service	All
SendGrid (Twilio, Inc)	United States	Sending emails through the Findem platform	Findem and Getro branded products
The Rocket Science Group LLC d/b/a Mailchimp	United States	Email provider	Glider branded products
Vonage Business Inc	United States	Storage and processing of Video	Glider branded products