Offerday AI Inc.
Unified Data Processing Addendum (GDPR + CCPA)

Part I: GDPR and General Data Protection Provisions (Data Processing Agreement)

This section of the Unified Data Processing Addendum (the “DPA”) forms part of the Master Service Agreement (the “MSA”) between Offerday AI, Inc. (“Provider”) and its customer (“Client”). This DPA is effective as of the effective date of the MSA.

1. DEFINITIONS

1.1. For the purposes of this DPA, the terms "Personal Data," "Processing," "Controller," "Processor," "Data Subject," "Personal Data Breach," and "Supervisory Authority" shall have the meanings ascribed to them in Article 4 of the General Data Protection Regulation (EU) 2016/679 ("GDPR"), regardless of whether the GDPR applies.

1.2. "Applicable Data Protection Laws" means all laws and regulations applicable to the Processing of Personal Data under the MSA, including, where applicable, the GDPR and national implementing laws.

1.3. "Services" means the services provided by Provider to Client under the MSA, which involve the Processing of Personal Data.

1.4. "Employment Data" means Personal Data relating to job applicants, candidates, employees, or contractors processed in connection with recruitment, hiring, or employment-related activities.

1.5. "Employment Laws" means applicable labor, employment, anti-discrimination, and accessibility laws and regulations, including the California Fair Employment and Housing Act ("FEHA"), where applicable.

2. ROLES OF THE PARTIES

2.1. The Parties acknowledge and agree that for the purposes of Applicable Data Protection Laws: a. Client is the Controller of the Personal Data. b. Provider is the Processor of the Personal Data, acting on behalf of the Client. c. Client retains sole responsibility for compliance with Employment Laws arising from its use of the Services, including decisions made using automated or AI-assisted outputs.

3. DETAILS OF THE PROCESSING

3.1. Subject-matter and Duration of the Processing: The subject-matter of the Processing is the Personal Data provided by Client to Provider for the purpose of utilizing the Services under the MSA. The duration of the Processing shall be for the term of the MSA, unless otherwise agreed in writing or expressed in the Order Form.

3.2. Nature and Purpose of the Processing: The nature and purpose of the Processing is to provide the SaaS hiring platform and related services to Client, assisting Client to manage its recruitment and hiring processes, including storing candidate information, tracking applications, facilitating communication, and providing configurable, AI-assisted or automated features that support recruitment, hiring, and employment-related workflows, where and as enabled by Client.

3.3. Types of Personal Data Processed: The types of Personal Data processed may include, but are not limited to: * Candidate Data: Name, contact information (email, phone, address), resume/CV details, employment history, education, skills, qualifications, application status, interview notes, assessment results, and any other information provided by or about candidates during the recruitment process. * Client User Data: Name, email address, job title, and other contact details for Client's employees or authorized users of the Platform.

3.4. Categories of Data Subjects: The categories of Data Subjects whose Personal Data is processed may include, but are not limited to: * Job applicants/candidates of the Client. * Client's employees, contractors, or agents who are Users of the Platform.

4. OBLIGATIONS OF THE PROVIDER (PROCESSOR)

4.1. Lawful and Documented Instructions: Provider shall process Personal Data only on documented instructions from Client, unless required to do so by Applicable Data Protection Laws to which Provider is subject. In such a case, Provider shall inform Client of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. Provider shall immediately inform Client if, in its opinion, an instruction infringes Applicable Data Protection Laws.

4.2. Confidentiality: Provider shall ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.3. Security of Processing: Provider shall implement and maintain appropriate technical and organizational measures to protect Personal Data, including a security program that aligns with the SOC 2 Type II framework. Such measures are designed to ensure a level of security appropriate to the risk, including protection against unauthorized access, use, disclosure, alteration, or destruction of Personal Data. Provider shall regularly review and update its security practices to maintain compliance with applicable data protection requirements.

4.4. Sub-processing: Provider shall not engage another processor ("Sub-processor") without prior specific or general written authorization of Client. In the case of general written authorization, Provider shall inform Client of any intended changes concerning the addition or replacement of other processors, thereby giving Client the opportunity to object to such changes. Where Provider engages a Sub-processor, Provider shall impose on that Sub-processor data protection obligations that are materially the same as those set out in this DPA. Provider shall remain fully liable to Client for the performance of that Sub-processor's obligations. The sub-processing does not apply to the use of a unified application programming interface (API) such as, but not limited too, Kombo or that of large language models (LLM).

4.5. Data Subject Rights: Taking into account the nature of the Processing, Provider shall assist Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Client's obligation to respond to requests for exercising Data Subject rights under Applicable Data Protection Laws. Provider shall promptly notify Client if it receives a request from a Data Subject concerning their Personal Data. Provider shall not respond to such requests directly without Client's prior written consent, unless required by law. Provider does not independently assess or respond to requests relating to employment decisions or alternative assessments, which remain the responsibility of Client.

4.6. Personal Data Breach Notification: Provider shall notify Client without undue delay after becoming aware of a Personal Data Breach affecting Personal Data processed under this DPA. Such notification shall include, to the extent available, all information required under Applicable Data Protection Laws to enable Client to meet its obligations to report or inform Data Subjects of the Personal Data Breach. Provider shall cooperate with Client and take reasonable steps to assist in the investigation, mitigation, and remediation of such Personal Data Breach.

4.7. Assistance to Client: Provider may assist Client in ensuring compliance with the obligations pursuant to Articles 35 and 36 of the GDPR (Data Protection Impact Assessments and prior consultation with Supervisory Authority), taking into account the nature of Processing and the information available to Provider.

4.8. Return and Deletion of Data: Upon termination or expiration of the MSA, or upon Client's written request, Provider shall, at Client's option, delete or return all Personal Data to Client and delete existing copies, unless Applicable Data Protection Laws require storage of such Personal Data.

Notwithstanding the foregoing, where Personal Data constitutes Employment Data or includes automated or AI-assisted inputs or outputs used in recruitment, hiring, or employment-related workflows, Provider may retain such data for a minimum of four (4) years following termination or expiration of the MSA, or for such longer period as required by applicable Employment Laws, including FEHA, for recordkeeping, audit, or legal defense purposes.

Deletion requests shall be subject to any applicable legal hold or statutory retention obligations.

4.9. Demonstration of Compliance: Provider shall make available to Client all information necessary to demonstrate compliance with the obligations laid down in this DPA and allow for and contribute to audits, including inspections, conducted by Client or another auditor mandated by Client.

4.10. Automated or AI-Assisted Features: Provider provides automated or AI-assisted features as tools to support Client workflows and does not make employment decisions. Client is solely responsible for evaluating the use of such features for compliance with Employment Laws, including conducting any required bias, disparate impact, or similar analyses, and for determining whether alternative assessments or accommodations are required.

5. OBLIGATIONS OF THE CLIENT (CONTROLLER)

5.1. Client warrants that it has all necessary rights to provide the Personal Data to Provider for Processing in accordance with this DPA and the MSA.

5.2. Client shall ensure that its instructions to Provider comply with all Applicable Data Protection Laws.

5.3. Client is responsible for establishing and maintaining appropriate legal bases for the Processing of Personal Data, including obtaining any necessary consents or providing required notices to Data Subjects.

6. INTERNATIONAL DATA TRANSFERS

6.1. If the Processing of Personal Data involves transfers of Personal Data outside the European Economic Area (EEA) or to a country not deemed by the European Commission to provide an adequate level of protection, Provider shall ensure that such transfers are made in compliance with Applicable Data Protection Laws, including, where applicable, by implementing Standard Contractual Clauses approved by the European Commission, or other appropriate transfer mechanisms.

7. LIABILITY

7.1. The liability of the Parties under this DPA shall be subject to the limitations of liability set forth in the MSA.

8. GENERAL PROVISIONS

8.1. Order of Precedence: In the event of any conflict or inconsistency between the provisions of this DPA and the MSA, the provisions of this DPA shall prevail with regard to the Processing of Personal Data.

8.2. Governing Law: This DPA shall be governed by and construed in accordance with the governing law clause of the MSA.

Acceptance
This Data Processing Agreement is incorporated into and forms part of the Master Service Agreement ("MSA") between Offerday AI, Inc. and Client. By executing an Order Form or otherwise entering into the MSA, Client agrees to be bound by the terms of this Data Processing Agreement as of the effective date of the MSA.

Part II: U.S. State Privacy Laws – CCPA Addendum

This section of the Unified Data Processing Addendum (the “CCPA Addendum”) forms part of a Master Service Agreement (the “MSA”) between Offerday AI Inc. (“Provider”) and its customer (“Client”). This CCPA Addendum is effective as of the effective date of the MSA.

1. DEFINITIONS

1.1. For the purposes of this CCPA Addendum, the terms "Business," "Service Provider," "Consumer," "Personal Information," "Sale," "Share," "Deidentified," and "Aggregate Consumer Information" shall have the meanings given to them in the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and its implementing regulations ("CCPA").

1.2. "Services" means the services provided by Provider to Client under the MSA, which involve the Processing of Personal Information.

2. ROLES OF THE PARTIES

2.1. The Parties acknowledge and agree that for the purposes of the CCPA: a. Client is the Business. b. Provider is the Service Provider.

3. SCOPE AND PURPOSE OF PROCESSING PERSONAL INFORMATION

3.1. Client's Instructions: Provider is receiving Personal Information from Client in its capacity as a Service Provider to process such Personal Information solely for the specific business purpose of providing the Services to Client as set forth in the MSA and this CCPA Addendum, and for no other purpose.

3.2. Description of Personal Information and Consumers: a. Categories of Personal Information: The categories of Personal Information processed by Provider on behalf of Client may include, but are not limited to, identifiers (e.g., name, email, phone number, address), professional or employment-related information (e.g., resume/CV details, employment history, education, job title), internet or other electronic network activity information (e.g., usage data on the Platform), and inferences drawn from other Personal Information to create a profile about a consumer reflecting their preferences or characteristics (e.g., candidate suitability). b. Categories of Consumers: The categories of Consumers whose Personal Information is processed by Provider may include, but are not limited to, job applicants/candidates of the Client and Client's employees, contractors, or agents who are Users of the Platform.

4. OBLIGATIONS OF THE SERVICE PROVIDER

4.1. Provider certifies that it understands the restrictions set forth in this CCPA Addendum and will comply with them. Provider shall:

a. Process Personal Information only on behalf of Client and for the specific business purpose of providing the Services as set forth in the MSA and this CCPA Addendum, or as otherwise permitted by the CCPA.

b. Not "Sell" or "Share" Personal Information.

c. Not retain, use, or disclose Personal Information for any purpose other than for the business purposes specified in the MSA and this CCPA Addendum, including retaining, using, or disclosing Personal Information for a commercial purpose other than providing the Services, or outside of the direct business relationship between Provider and Client, except as required to comply with applicable employment or recordkeeping laws.

d. Not combine the Personal Information received from Client with Personal Information that Provider receives from or on behalf of another person or from its own interaction with the Consumer, except as permitted by the CCPA. However**,** Provider may enrich Client Personal Information with lawfully obtained third-party or publicly available data solely to improve the accuracy, functionality, or effectiveness of the Services provided to Client, and not for any purpose unrelated to those Services.

e. Comply with all applicable sections of the CCPA, including providing the same level of privacy protection as required by the CCPA.

4.2. Security: Provider shall implement and maintain reasonable security procedures and practices appropriate to the nature of the Personal Information to protect Personal Information from unauthorized access, destruction, use, modification, or disclosure.

4.3. Cooperation with Consumer Rights Requests: Provider shall cooperate with Client in responding to verifiable Consumer requests made pursuant to the CCPA, including requests to access, correct, or delete Personal Information, or to opt-out of the Sale or Sharing of Personal Information. Provider shall: a. Promptly notify Client if it receives a request from a Consumer to exercise any rights under the CCPA with respect to Personal Information processed on behalf of Client. b. Not respond to such Consumer requests directly without Client's prior written authorization, unless otherwise required by the CCPA. c. Provide Client with all necessary information and assistance to enable Client to fulfill its obligations to respond to Consumer requests.

4.4. Sub-processors: Provider may engage sub-processors to process Personal Information on behalf of Client, provided that Provider shall ensure that such sub-processors are subject to written contracts that require them to observe the same obligations as Provider under this CCPA Addendum with regard to Personal Information.

4.5. Audits and Compliance: Provider shall, upon Client's reasonable request, make available to Client all information necessary to demonstrate compliance with the obligations set forth in this CCPA Addendum. Client shall have the right, upon reasonable notice and no more than once per year (unless a Personal Information Breach or other reasonable cause exists), to take reasonable and appropriate steps to ensure that Provider uses the Personal Information in a manner consistent with Client's obligations under the CCPA, including by conducting audits or inspections.

4.6. Notification of Inability to Comply: If Provider determines that it can no longer meet its obligations under this CCPA Addendum, Provider shall promptly notify Client. Upon such notification, Client shall have the right to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Information, or to terminate the portion of the MSA relevant to the processing of Personal Information.

5. CLIENT'S OBLIGATIONS

5.1. Client represents and warrants that it has all necessary rights and permissions to provide the Personal Information to Provider for processing in accordance with the MSA and this CCPA Addendum.

5.2. Client shall ensure that its instructions to Provider comply with the CCPA and all other applicable privacy and data protection laws.

6. RELATIONSHIP TO MSA AND DPA

6.1. This CCPA Addendum supplements the MSA and the DPA (Exhibit A to the MSA). In the event of any conflict or inconsistency between the provisions of this CCPA Addendum and the MSA or DPA concerning the processing of Personal Information subject to the CCPA, the provisions of this CCPA Addendum shall prevail.

6.2. Any capitalized terms not defined herein shall have the meaning ascribed to them in the MSA or the DPA.

This CCPA Addendum is incorporated as **Part II of the Unified Data Processing Addendum** and forms part of the Master Service Agreement as of its Effective Date.