DATA PROCESSING ADDENDUM

This Data Processing Addendum (this “Addendum”) supplements the Master Subscription Agreement (https://www.payscale.com/content/legal/msa.pdf) or other agreement between PayScale and Customer that governs Customer’s use of the PayScale Offerings (“Agreement”). This Addendum addresses the specific requirements of Data Protection Laws and applies solely to the extent Customer uses a PayScale Offering that Processes Customer Personal Data subject to Data Protection Laws. This Addendum is in effect for the period that PayScale Processes such Customer Personal Data. The Addendum may be amended from time to time by PayScale to comply with any changes to applicable Data Protection Laws. This Addendum was last updated on October 30, 2018 to incorporate feedback from our customers and provide clarifications. The previous version of this Addendum can be found here: https://www.payscale.com/content/legal/dpa-june-2018.pdf.

1. Definitions. All capitalized terms used in this Addendum will have the meaning given to them below. All capitalized terms used in this Addendum but not defined will have the meaning given to such term in the Agreement.

1.1 “Customer Data” has the meaning given to it in the Agreement.

1.2 “Customer Personal Data” means any Customer Data that is Personal Data.

1.3 “Data Protection Laws” means all applicable data protection and privacy laws applicable to the respective party in its role in the Processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law.

1.4 “EU Data Protection Law” means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (“GDPR”).

1.5 “PayScale Network” means PayScale’s data center facilities, servers, networking equipment, and host software systems that are within PayScale’s control and are used to provide the PayScale Offering.

1.6 “Personal Data” means any information relating to an identified or identifiable natural person and includes the meaning given to it under EU Data Protection Law.

1.7 “Privacy Shield” means the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks designated by the U.S. Department of Commerce, the European Commission, and Swiss Administration, respectively, as described at https://www.privacyshield.gov/Program-Overview.

1.8 “Processing” has the meaning given to it under the GDPR and “Process,” “Processes,” and “Processed” will be interpreted accordingly.

1.9 “Security Incident” means an incident that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data stored or otherwise Processed by PayScale and in PayScale’s possession or control.

1.10 “Unsuccessful Security Incident” means an unsuccessful attempt or activity that does not compromise the security of Customer Personal Data, including, but not limited to, pings and other broadcast attacks of firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers), or similar incidents.

2. General Data Processing Requirements

2.1 Roles and Scope

(a) Each party will comply with all Data Protection Laws that apply to it and its obligations under the Agreement and this Addendum, including, EU Data Protection Laws.

(b) In connection with Customer’s use of the PayScale Offering, Customer Personal Data may be loaded, stored, provided, or otherwise Processed through a PayScale Offering. Customer determines what Customer Personal Data is provided to PayScale or loaded into the Cloud Offering, and Customer will not provide PayScale or load Customer Personal Data into the Cloud Offering that is not necessary for PayScale to provide Customer the applicable PayScale Offering.
(c) This Addendum applies when Customer Personal Data is Processed by PayScale in the course of providing the PayScale Offering to Customer pursuant to the Agreement. When Customer Personal Data is Processed by PayScale, PayScale will act as a “processor” to the Customer who may act as either the “controller” or “processor” of Customer Personal Data, as those terms are defined under EU Data Protection Law, except when Customer is acting as the “processor,” in which case PayScale is the “subprocessor.”

(d) This Addendum does not apply to the extent PayScale is deemed a “controller” and does not reduce any data protection commitments PayScale has made to Customer in the Agreement.

2.2 Data Processing Details

(a) Subject Matter: The Customer Personal Data elected to be loaded or provided by Customer to PayScale to use the PayScale Offering. PayScale does not desire to receive any Customer Data or other Confidential Information from Customer that is not necessary for PayScale to perform its obligations under the Agreement, including, sensitive personal information such as social security numbers or other government identifiers, credit card numbers, bank account numbers, and protected health information.

(b) Duration: Subject to the terms of this Addendum and the Agreement and as determined by Customer, but generally the period Customer subscribes to the PayScale Offering.

(c) Nature/Purpose of Processing: To deliver the PayScale Offering for Customer as detailed in the Agreement.

(d) Type of Customer Data: The Customer Personal Data elected to be loaded or provided by Customer to PayScale to use the PayScale Offering, which may include, without limitation, employee names and job titles.

(e) Categories of Data Subjects: The Customer Personal Data elected to be loaded or provided by Customer to PayScale, which may include, without limitation, Personal Data concerning Customer’s employees.

2.3 Data Controller’s Controls. The PayScale Offering includes features that allow Customer to access, correct, retrieve, export/port, or delete Customer Data, as described in applicable Documentation. Customer may use such features to assist with its obligations under Data Protection Laws, including its obligations regarding responding to data subject requests.

2.4 Data Subject Rights. The PayScale Offering will include certain features that Customer may use to allow it to comply with its obligations toward data subjects, as described in applicable Documentation. PayScale will comply with Customer’s reasonable requests for assistance with responding to a data subject request. If PayScale receives a request from Customer’s data subject to exercise one or more of its rights under EU Data Protection Law, PayScale will redirect the data subject to make its request directly to Customer and PayScale will notify Customer that it received such request from a data subject.

2.5 Customer Instructions. The terms of the Agreement and this Addendum coupled with Customer’s use and configuration of the features of the PayScale Offering are Customer’s complete and final instructions to PayScale for the Processing of Customer Personal Data. If Customer has Processing instructions for PayScale that are outside the scope of this Addendum or the Agreement, then prior to performing such Processing instructions, such Processing will require a mutual written agreement between the parties and will be subject to mutually agreed upon fees.

2.6 Data Processing Location. As of the date this Addendum was last updated, all Customer Personal Data loaded (or provided to PayScale to load) in the Cloud Offering is Processed in PayScale Networks located in the United States. PayScale will not Process such Customer Personal Data outside of the United States without Customer’s knowledge and authorization (where Customer authorization received by email or other electronic means is acceptable).

2.7 Sub-processing

(a) General Authorization. Customer hereby authorizes and agrees that PayScale may use sub-processors engaged by PayScale to perform its obligations under this Addendum and the Agreement or to provide certain services on PayScale’s behalf, such as database storage (“Sub-processors”). PayScale will impose on its Sub-processors the same (or substantially similar) data protection obligations as set out in this Addendum and the Agreement (as appropriate taking into consideration the type of Customer Personal Data Processed by a Sub-processor and the nature of the Processing), and PayScale remains responsible for the Processing activities of its Sub-processors.
(b) **Sub-processor List.** Customer may view a list of PayScale’s current Sub-processors at https://www.payscale.com/content/legal/PayScale-GDPR-Subprocessor-List.pdf, and if such list is not available, Customer may request the then-current Sub-processor list by contacting PayScale’s support team at cs@payscale.com.

(c) **New or Replacement Sub-processors.** PayScale will send an electronic notice to Customer’s then-current Account administrator of any intended addition or replacement of Sub-processors and allow Customer to reasonably object to such changes by notifying PayScale in writing within 30 days after receipt of PayScale’s notice of an addition or replacement of a Sub-processor. Customer’s objection notice must include an explanation for the reasonable grounds of Customer’s objection that relates to the protection of Customer Personal Data, in which case PayScale will have the right to cure Customer’s objection through one of the following options (to be selected at PayScale’s sole discretion):

(i) PayScale will cancel its plans to use the Sub-processor with regard to Customer Personal Data or will offer an alternative to provide the PayScale Offering without such Sub-processor;

(ii) PayScale will take the corrective steps requested by Customer in its objection notice (which will eliminate Customer’s objection) and proceed to use the Sub-processor with regard to Customer Personal Data; or

(iii) PayScale may cease to provide or Customer may agree not to use (temporarily or permanently) the particular aspect of the PayScale Offering that would involve the use of such Sub-processor with regard to Customer Personal Data, subject to a mutual agreement of the parties to adjust the fee for the PayScale Offering considering the reduced scope of the PayScale Offering.

If none of the above options are reasonably available and Customer’s objection has not been resolved to the mutual satisfaction of the parties within 30 days after PayScale’s receipt of Customer’s written objection, either party may terminate the Order Form at issue by providing the other party written notice and Customer will be entitled to a refund of any prepaid Annual Subscription Fees applicable to the remainder of the terminated PayScale Offering’s Service Year (excluding any one-time fees such as fees for Professional Services), pro-rated from the effective date of termination. If Customer’s objection remains unresolved 60 days after it was raised by Customer, and PayScale has not received any notice of termination from Customer, Customer will be deemed to accept the new or replacement Sub-processor.

(d) **Emergency Sub-processor Replacement.** Notwithstanding Section 2.7(c) above, PayScale may change a Sub-processor where the reason for the change is outside of PayScale’s reasonable control. In this case, PayScale will inform Customer of the replacement Sub-processor as soon as possible. Customer retains its right to object to a replacement Sub-processor under Section 2.7(c) above.

3. **Security Standards.** PayScale has developed and implemented, and will maintain, monitor, and use appropriate administrative, technical, and physical security measures, safeguards, procedures, and practices designed to: (a) protect the confidentiality, integrity, and availability of Customer Data against Security Incidents; and (b) restrict access to Customer Data to those who need to have access to perform their legitimate job functions. PayScale also performs appropriate training and imposes appropriate contractual obligations upon its personnel regarding security and confidentiality.

4. **Privacy Shield and Data Transfer Mechanism.** PayScale is self-certified under the Privacy Shield and adheres to the requirements of the Privacy Shield Principles in respect of certification under the Privacy Shield. Customer may view PayScale’s Privacy Shield certification status by reviewing the Privacy Shield List available on the Privacy Shield site located at https://www.privacyshield.gov/list. PayScale agrees to maintain a valid certification to the Privacy Shield or any other lawful data transfer mechanism that is recognized under EU Data Protection Law as providing an adequate level of protection for cross-border Personal Data transfers.

5. **Incident Response Plan**

5.1 **Security Incidents.** In the event of a Security Incident, PayScale will: (a) without undue delay (but no later than the time frame required by applicable Data Protection Law), notify Customer of any Security Incident promptly upon discovery of the Security Incident; and (b) promptly take steps to mitigate the Security Incident’s adverse effects or the resulting harm.

5.2 **Customer Notifications.** As part of the notification described in Section 5.1 above, PayScale will, to the extent known or can be reasonably determined: (a) describe the nature of the Security Incident, including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Customer Personal Data records concerned; (b) communicate the name and contact details of the PayScale contact where more information can be obtained; (c) describe the likely consequences of the Security
Incident; and (d) describe the measures taken or proposed to be taken by PayScale to address the Security Incident, including, where appropriate, measures to mitigate its possible adverse effects. PayScale will notify Customer of Security Incidents by contacting Customer’s designated contact in its Account settings.

5.3 PayScale Cooperation. In connection with any Security Incident, PayScale will reasonably cooperate with Customer in connection with: (a) Customer’s investigation of the Security Incident; (b) actions reasonably necessary or required for Customer to mitigate resulting harm; and (c) fulfilling Customer’s obligations to notify the relevant supervisory authority and data subjects of a Security Incident in accordance with applicable Data Protection Laws.

5.4 Security Incident Disclosure. Subject to applicable laws or contractual requirements, PayScale will not inform any third party of any Security Incident without first obtaining Customer’s prior written consent, other than to inform any complainant that the matter has been forwarded to Customer’s legal counsel, except that if such disclosure is required by applicable law, PayScale will use commercially reasonable efforts to obtain Customer’s approval, which will not be unreasonably withheld. Further, subject to applicable laws or contractual requirements, PayScale agrees that Customer will have the sole right to determine: (a) whether notice of the Security Incident is to be provided to any individuals, regulators, law enforcement agencies, or others as required by law or regulation, or otherwise in Customer’s reasonable discretion; and (b) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation. Upon confirmation of a Security Incident, at Customer’s written request, PayScale will use reasonable commercial efforts to cooperate with Customer in connection with Customer’s notification of subjects affected by the Security Incident.

5.5 Unsuccessful Security Incidents. Customer agrees that an Unsuccessful Security Incident is not subject to the requirements of this Section 5. In addition, PayScale’s cooperation or obligation to report or respond to Security Incidents under this Addendum and the Agreement is not and will not be interpreted as an acknowledgment by PayScale of any fault or liability of PayScale with respect to a Security Incident.

6. Security Assessments and Audit Rights

6.1 Customer Questionnaires and Audits. Customer agrees to use PayScale’s information technology security policy and other PayScale-supplied information to reduce redundant assessments and audits. No more than once in any 12-consecutive month period, upon reasonable advanced written request by Customer:

(a) PayScale will complete a reasonable information security questionnaire provided by Customer ("Questionnaire"), or a third party on Customer’s behalf, regarding PayScale’s administrative, physical, and logical safeguards for protecting Customer Personal Data being handled or services being provided by PayScale solely to confirm PayScale’s compliance with this Addendum. The work required by PayScale to complete any such Questionnaire may be considered by PayScale as out-of-scope regarding the PayScale Offering provided by PayScale under the Agreement. If PayScale considers such work to be out-of-scope, then prior to the start of any work in connection with such Questionnaire, it will notify Customer and the parties will mutually agree upon any additional fees to be paid by Customer.

(b) PayScale will cooperate with Customer, or a third-party auditor on Customer’s behalf, in the performance of an assessment, audit, examination, or review of PayScale’s information, security and protection, environment, practices and capabilities, relating to Customer Personal Data solely to confirm PayScale’s compliance with this Addendum (each, an "Audit"). Any such Audit will occur only after Customer has provided PayScale with at least 60 days prior written notice and during a mutually agreed upon date, time, and location. Audits must not unreasonably interfere with PayScale’s business or operations and the scope of such Audit will be subject to PayScale’s reasonable pre-approval. The work required by PayScale to participate in any Audit will be considered out-of-scope regarding the PayScale Offering provided by PayScale under the Agreement and will result in additional fees (at a mutually agreed upon hourly rate) and project expenses to be paid by Customer, unless otherwise agreed in writing prior to the start of any work in connection with such Audit.

(c) Without limiting the foregoing, Customer may request completion of a Questionnaire or an Audit more than once in any 12-consecutive month period, (i) if there has been a Security Incident, or (ii) solely to the extent that an additional Questionnaire or Audit is necessary to confirm PayScale’s ability to comply with a change in applicable Data Protection Laws.

6.2 Scope of Audits. To ensure that PayScale complies with applicable Data Protection Laws and its contractual obligations regarding data privacy and security, Customer agrees that PayScale is not required to provide Customer or its auditor with access to the PayScale Network in a manner that may compromise the security, privacy, or confidentiality of PayScale’s other clients’ confidential or proprietary information, or the security of the PayScale Network, regardless of anything to the contrary in the Agreement or this Addendum. Any
information disclosed in connection with a Questionnaire or Audit will be deemed PayScale’s Confidential Information.

6.3 Audit Rights under Data Protection Laws. To the extent applicable Data Protection Laws include audit rights by Customer, Customer agrees to carry out its audit rights under such Data Protection Laws by instructing PayScale to carry out the audit as described in this Section 6 of this Addendum. Nothing in this Section 6 affects any supervisory authority’s or data subject’s rights under EU Data Protection Law.

6.4 Customer’s Independent Determination and Privacy Impact Assessment. Customer is responsible for reviewing the information provided by PayScale and making an independent determination as to whether the PayScale Offering meets Customer’s requirements and other obligations under applicable Data Protection Laws or contractual obligations. The information made available by PayScale under the Agreement and this Addendum is intended to assist Customer in complying with Customer’s obligations under applicable Data Protection Laws regarding data protection impact assessments and prior consultation. Customer acknowledges that PayScale will not assess the contents of Customer Data to identify information subject to any specific legal requirements.

7. Retrieval or Deletion of Customer Data

7.1 Retrieval and Deletion by Customer. The PayScale Offering provides Customer with features that allow Customer to export, retrieve, or delete Customer Data as described in applicable Documentation. During the Subscription Term, Customer will have the ability to export, retrieve, or delete Customer Data on its own in accordance with this Section 7.1. Subject to the terms of the Agreement, for up to 30 days following the end of the Subscription Term and following Customer’s written request to PayScale, at Customer’s expense, PayScale will grant Customer a limited right to access its Account for the sole purpose of allowing Customer to export, retrieve, or delete any Customer Data then-stored in the Cloud Offering if: (a) Customer is in compliance with its obligations under the Agreement (including, its payment obligations); and (b) such access does not subject PayScale to penalties or other liability and is permitted under applicable laws (including, Data Protection Laws) or the order of a governmental or regulatory body.

7.2 Deletion by PayScale. Following Customer’s written request, PayScale will delete Customer Personal Data then-stored in the Cloud Offering using the controls PayScale has developed for this purpose subject to the following: (a) such deletion is allowed under applicable laws (including, Data Protection Laws) or the order of a governmental or regulatory body; (b) PayScale may retain relevant Customer Personal Data for PayScale’s internal record keeping and other auditing purposes (e.g., a copy of the Agreement which may include the name of the individual that executed the Agreement); and (c) such deletion is subject to PayScale’s then-current data retention or similar back-up policy that automatically archives certain portions of Customer Data where such data will be protected in accordance with the measures described in the Agreement and this Addendum and will remain subject to the terms of this Addendum and the Agreement (including, confidentiality obligations).

8. Costs Allocation and Liability. Each party will bear the costs of the remediation, mitigation, and other related costs to the extent a Security Incident is caused by it. Each party’s liability under this Addendum will be subject to the terms of the Agreement (including, any limitations of liability provisions), and, for clarification, (a) a Security Incident shall not be considered a breach of a party’s confidentiality obligations, (b) any exclusions to the limitation of liability provision regarding indemnification under the Agreement will not apply to any claims relating to this Addendum or Data Protection Laws, and (c) Section 11.2 of the Agreement does not apply to this Addendum.

9. Miscellaneous. The parties agree that this Addendum will replace any existing data processing agreement the parties may have previously entered into in connection with the PayScale Offerings. Any claims against PayScale or its Affiliates under this Addendum may only be brought by the Customer entity that is a party to the Agreement. In no event shall this Addendum or any party restrict or limit the rights of any data subject or of any competent supervisory authority. This Addendum will be governed by and construed in accordance with the governing law, jurisdiction, and venue provisions in the Agreement, unless otherwise required by applicable Data Protection Laws. Except as amended by this Addendum, the Agreement remains in full force and effect. If there’s a direct conflict between the Agreement and this Addendum, the terms of this Addendum will control.