DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

MASTER SUBSCRIPTION AGREEMENT

This Agreement is effective as of the date last signed by a party hereto ("**Effective Date**") and entered into between Payscale, Inc. and its Affiliates ("**Payscale**") and City of Chandler ("**Customer**"), entered into _____, 2022 (Effective Date). This Agreement governs Customer's use and purchase of Payscale Services.

1. DEFINITIONS

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. For purposes of this definition, "**control**" means direct or indirect ownership or control of more than 50% of the outstanding voting interests of the subject entity.

"**Agreement**" means this Master Subscription Agreement, any amendments, the Documentation (defined in Section 2.5 below), applicable Order Forms, and the Data Processing Agreement (defined in Section 9.3 below).

"**Annual Subscription Fee**" means the annual fee applicable to Customer's subscription to a Payscale Service for a Service Year, excluding any one-time fees (e.g., implementation fees), Professional Service fees, and any Taxes (defined in Section 7.3 below).

"**Beta Service**" means a product, service, data, integration, or other feature that Payscale makes available to Customer to try at Customer's option, and is designated as beta, limited release, preview, non-production, or other similar description.

"**Customer Data**" means employee information Customer or its Users loads or otherwise inputs into the Payscale Services (or provides to Payscale for loading or inputting into the Payscale Services on Customer's behalf) or provided by Customer to Payscale to provide Professional Services.

"**Data Sharing Services**" means the Payscale Services that permit sharing of data between Payscale customers. The Data Sharing Services purchased by Customer are identified on the applicable Order Form and are described in the Documentation.

"**Documentation**" means technical specifications and requirements and other information located at https://www.payscale.com/about/documentation pertaining to specific Payscale Services. Documentation does not include white papers, community forums, training videos or similar resources.

May or Should means something that is not mandatory but is permissible.

"**Order Form**" means Payscale's standard ordering document that identifies the Payscale Services purchased by Customer, attached hereto, made a part hereof, and incorporated by this reference as Exhibit A.

"**Payscale Data**" means data owned by Payscale, including Usage Data, Aggregated Data (defined in Section 4.2 below), and any other data that is provided by Payscale (or its licensors) to Customer. Payscale Data is Payscale's Confidential Information.

"**Payscale Integration**" means Customer's use of any application programming interface ("**API**") or other integration feature between a Payscale Service and a Third Party Service provided by Payscale to Customer.

"**Payscale Services**" means the proprietary products and services of Payscale (including Data Sharing Services, Payscale Data and Professional Services) or its licensors, identified on an Order Form, and subsequently made available to Customer by Payscale in accordance with this Agreement.

"**Professional Services**" means implementation, onboarding, training, and other services related to the Payscale Services as identified on an Order Form. Descriptions of standard Professional Services are available in the Documentation.

"**Service Year**" means a 12-month period beginning on the start date of the Subscription Term and ending one year later.

Shall, Will, or Must means a mandatory requirement.

"**Subscription Term**" means the duration of Customer's subscription to a Payscale Service as set forth on an Order Form and all Renewal Subscription Terms (defined in Section 6.1 below).

"**Survey Publisher**" means a third-party publisher of Third Party Surveys.

"**Term**" means the duration this Agreement is in effect as described in Section 6.1 below.

"Third Party Service" means applications, services, software, or other products supplied by a third party (excluding Payscale's licensors and contractors) that Customer chooses to use with or integrate with a Payscale Service.

"**Third Party Surveys**" means any compensation surveys or data that are loaded, stored, displayed, or processed by a Payscale Service and accessible through Customer's Account (defined in Section 2.1 below). Third Party Surveys are not Customer Data but are considered Confidential Information.

"**Usage Data**" means data and other information related to Customer's use of a Payscale Service (e.g., the number of reports run, the frequency of log-ins, and User behavioral data, such as the types of searches run, and selections made by Customer).

"**User**" means Customer's employees and vendors that are authorized by Customer to use and access the Payscale Services through Customer's Account (defined in Section 2.1 below).

2. PROVISION AND USE OF PAYSCALE SERVICES

2.1 Provision of Payscale Services. During the Subscription Term, and subject to the terms and conditions of this Agreement, Customer may access and use the Payscale Services, as modified, enhanced, or updated from time to time, through a web browser using an account provided by Payscale to Customer ("**Account**") solely for Customer's internal use. Customer may not use its Account for provision of services to third parties.

2.2 Account Access. Customer will designate individuals authorized by Customer to manage, use, and support the Account, and will control creation and assignment of usernames and passwords to Users. Customer is responsible for maintaining the status of its Users and the confidentiality of all usernames, passwords, and other Account access information under its control. Customer will notify Payscale promptly if: (a) Customer reasonably believes that the Account has been compromised, including any unauthorized access, use, or disclosure of Account information; or (b) any other breach of security in relation to its passwords, usernames, or other Account access information may have occurred or is likely to occur. Customer remains responsible for compliance by its Users with all the terms and conditions of this Agreement, and any use of the Payscale Services by Users shall be solely for the benefit of Customer.

2.3 Use Restrictions. Except as expressly allowed under this Agreement (including Section 2.2 above), Customer will not: (a) permit any third party (other than Users) to access or use the Payscale Services; (b) create derivative works based on the Payscale Services; (c) copy, frame, or mirror any part or content of the Payscale Services, other than copying or framing on Customer's own intranet for Customer's internal business purposes; (d) decompile, disassemble, translate, reverse engineer, or otherwise attempt to derive source code or specific data from the Payscale Services, in whole or in part, nor will Customer use any mechanical, electronic, or other method to trace, decompile, disassemble, or identify the source code of, or specific data available through, the Payscale Services or encourage or permit others to do so (except and only to the extent that applicable law prohibits or restricts reverse engineering restrictions); (e) access or use the Payscale Services to (i) develop or improve a competitive product or service, or (ii) copy any features, functions, content, format, graphics, modules, algorithms, arrangement, method of organization, method of interaction, or other design of the Payscale Services for itself, its Affiliates, or a third party; (f) sell, resell, rent, or lease the Payscale Services; (g) use the Payscale Services to store or transmit infringing, libelous, or other unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights; (h) store or transmit virus, malware, or other malicious or harmful code or files through the Payscale Services; (i) interfere with or disrupt the integrity or performance of the Payscale Services; (j) attempt to

gain unauthorized access to Payscale Services or their related systems or networks; (k) disclose the results of any benchmarking or other performance testing of the Payscale Services to a third party without Payscale's prior written consent or (l) exceed the scope of Customer's subscription as specified on an Order Form.

2.4 Provision of Professional Services. Subject to the terms of this Agreement, Payscale will provide Customer the Professional Services set forth in an Order Form. Payscale's performance of the Professional Services is contingent on Customer providing Payscale all necessary Customer Data and other information for Payscale to provide the Professional Services (including any Customer Data or information described in the applicable Documentation) and Customer's active and timely participation. Standard hours set forth in the Documentation for Professional Services are estimates only. The hours available ("**Service Hour Limit**") to Customer during the Subscription Term are set forth in the applicable Order Form. If Customer exceeds the Service Hour Limit during the Subscription Term, the rates specified in the Order Form for such excess hours will apply. Any Professional Service projects set forth in an Order Form must be performed during the Subscription Term set out in such Order Form. Any Professional Service projects purchased on an a la carte basis pursuant to an Order Form must be performed during the same period of Customer's Subscription Term in effect at the time of purchase. Professional Service projects do not carry over to Renewal Subscription Term(s).

2.5 Documentation. Payscale Services are subject to the operational terms set forth in the Documentation. Documentation may be updated by Payscale from time to time in its sole discretion to include additional Payscale Services, new features, or to reflect updated operational processes, but any such changes will not impose additional material legal obligations or liabilities on Customer or reduce a critical functionality of a Payscale Service.

2.6 Beta Services. Payscale may make Beta Services available to Customer. Customer may choose to participate in Beta Services in its sole discretion. Beta Services are intended for evaluation purposes only and not for production use, are not supported, and may be subject to additional terms. Beta Services are not considered "Payscale Services" under this Agreement, but all restrictions, reservation of rights, Customer's obligations concerning the Payscale Services, and rights granted by Customer to Payscale regarding Customer Data and Aggregated Data will apply equally to Customer's use of Beta Services. Unless otherwise agreed by the parties, use of Beta Services expire on the date a version of the Beta Services becomes generally available without the applicable Beta Service designation. Payscale may discontinue Beta Services at any time in its sole discretion and may never make them generally available. Beta Services are provided "AS IS" and Payscale will have no liability for any harm or damage arising out of a Beta Service, provided that Customer's use of Beta Services shall not excuse Payscale's obligations under this Agreement regarding Customer Data.

3. RESPONSIBILITIES OF EACH PARTY

3.1 Payscale Responsibilities. During the Subscription Term, Payscale will: (a) provide Customer support for the Payscale Services, as set forth in the Service Levels Addendum available at https://www.payscale.com/content/legal/sla.pdf, a current copy of which is attached hereto and incorporated herein as Annex A (b) maintain insurance coverage as set forth in the Insurance Addendum available at https://payscale.com/content/legal/ia.pdf, a current copy of which is attached hereto and incorporated herein as Annex D (c) use reasonable efforts to give at least 24 hours' notice of planned downtime via Customer's Account and schedule such planned downtime to the extent practicable during weekend hours from 6:00 p.m. Pacific time Friday to 3:00 a.m. Pacific time Monday); (d) conduct its business in accordance with applicable laws; and (e) be responsible for the performance of its employees and contractors and their compliance with Payscale's obligations under this Agreement.

3.2 Customer Responsibilities. Customer will: (a) be responsible for Users' compliance with this Agreement; (b) be responsible for procuring at its expense the necessary hardware and Internet connection needed to access the Payscale Services; (c) be solely responsible for the accuracy and legality of Customer Data as used under this Agreement (including collecting any required privacy consents from its employees); (d) use reasonable efforts to prevent unauthorized access to, or use of, the Payscale Services through Customer's Account, and notify Payscale; (e) provide assistance, information, data, and other resources reasonably necessary to enable Payscale to perform and provide the Payscale Services; and (f) use the Payscale Services in accordance with applicable Documentation, this Agreement, and applicable laws. Customer's failure to meet these requirements may impact Customer's ability to use the Payscale Services and Payscale shall not be responsible for such impact.

4. DATA RIGHTS AND USAGE

4.1 Customer Data. As between Payscale and Customer, Customer exclusively owns all rights, title, and interest in and to all Customer Data, except where specific rights are expressly granted to Payscale. During the Term and subject to this Agreement, Customer grants to Payscale a license and right to host, access, process, display, copy, transmit, modify, create derivative works of, and otherwise use Customer Data solely to the extent necessary to: (a) fulfill its obligations to Customer under this Agreement; (b) maintain, evaluate, secure, develop, or improve the Payscale Services (e.g., develop enhanced Payscale Services features); and (c) respond to and resolve a User's request for customer support. Customer shall not provide to Payscale or upload to the Payscale Services sensitive data that is not necessary for Payscale to perform its obligations under this Agreement, such as social security numbers or other government identifiers, credit card numbers, bank account numbers, other financial information, or health information.

4.2 Payscale Data. As between Payscale and Customer, Payscale exclusively owns all rights, title, and interest in and to all Payscale Data, except where specific rights are expressly granted. To the extent Customer licenses Payscale Data on a stand-alone basis apart from the use of a web-based Payscale Service, Customer is subject to the following: During the Term and subject to this Agreement, Payscale grants to Customer a non-exclusive, non-transferable, non-sublicensable, revokable (to the extent outlined in this Agreement) worldwide license to access and use the Payscale Data in accordance with the terms set forth in the Documentation under Payscale® for Consultants.

4.3 Usage Data. Customer agrees that Payscale may collect Usage Data, and Payscale may use Usage Data to develop, improve, support, market and operate its products and services during and after the Term of this Agreement. Payscale will not identify Customer as the source of any Usage Data without written permission from Customer.

4.4 Data Sharing Services. Payscale offers Data Sharing Services (e.g., compensation benchmarking surveys) and Customer may elect to participate in these Data Sharing Services to access peer data provided by other Payscale customers. If participating in Data Sharing Services, Customer agrees that Payscale may collect Customer Data stored in the Payscale Services (e.g., Customer's employee data such as pay, job title, and performance rating) to produce an aggregated data source ("**Aggregated Data**"). Payscale shall not include any personal data or information that could be used to identify or reidentify a specific individual in the Aggregated Data. In connection with providing the Data Sharing Services, Customer agrees that: (a) Payscale may modify, analyze, share, license, assign, sell, and otherwise use Aggregated Data in any manner it chooses and for its own purpose (including to develop and offer various versions and cuts of Payscale Data); and (b) the Aggregated Data is Payscale's property and Confidential Information.

(a) Participation. If Customer participates in Data Sharing Services, Customer agrees that its name will be listed and available to others as a part of the Data Sharing Services, as is customary in the compensation data industry. Customer's Aggregated Data may be grouped with other participants in specific data cuts or be able to be segmented with other participants based on specific attributes (e.g., number of employees, geographic location). Customer will have access only to the specific Data Sharing Services (e.g., Payscale Compensation Survey or specific data cuts) that it selects and are listed on the applicable Order Form. Payscale's Data Sharing Services are listed in the Documentation and subject to the specific requirements outlined therein.

(b) Process and Data Accuracy. Payscale may review Aggregated Data for completeness and errors. Customer agrees to cooperate with Payscale on a timely basis to answer questions and to correct any identified problems, omissions, or errors. Despite Payscale's review, Customer acknowledges that it remains accountable for the accuracy of its data. Problems with information quality or delays in providing information may delay implementation of Data Sharing Services.

(c) Opt-Out. Customer may opt-out of participating in the Data Sharing Services at any time by providing Payscale at least 45 days' prior written notice, at which point Customer's Aggregated Data and name will be removed at the next version release or update of the Data Sharing Services. If choosing to opt-out, Customer shall no longer have access to the Data Sharing Services. Notwithstanding the foregoing, Customer understands that Aggregated Data provided before Customer's opt-out will remain a part of the versions of the Data Sharing Services previously released and Customer's name will remain listed as a participant for such versions.

4.5 Reservation of Rights. Payscale retains all right, title, and interest in and to the Payscale Services (and any modifications or derivative works), including all underlying software, source code, data, design, modules, organization, format, algorithm, and other technology, and all logos and trademarks reproduced through the Payscale Services. This Agreement does not grant Customer any intellectual property rights in the Payscale Services or any of its components (including Payscale Data).

4.6 Feedback. Customer may submit suggestions, enhancements, requests, corrections, or other feedback related to the Payscale Services ("**Feedback**"). Customer agrees that all Feedback is given voluntarily. Absent a separate fully executed agreement, Payscale has not agreed to and does not agree to treat as confidential any Feedback Customer provides to Payscale, and nothing in this Agreement or in the parties' dealings arising out of or related to this Agreement will restrict Payscale's right to use, profit from, disclose, publish, keep secret, or otherwise exploit Feedback, without compensating or crediting Customer. Feedback will not be considered Customer's Confidential Information or its trade secret.

5. Third Party Offerings.

5.1 Third Party Surveys. Payscale supports hosting of Third Party Surveys in certain Payscale Services. Data provided in Third Party Surveys is not owned or controlled by Payscale, and Payscale does not warrant or support these Third Party Surveys.

(a) Customer Licensed Third Party Surveys. Where Customer has directly licensed a Third Party Survey from a Survey Publisher and requests that the Third Party Survey be accessible as a part of the Payscale Services, Customer hereby grants to Payscale the right to use, load, host, copy, access, store, display, or otherwise process the Third Party Survey solely to provide Customer the Payscale Services (including any associated Professional Services). Customer represents and warrants that it has secured all necessary rights to authorize this usage by Payscale and releases Payscale from any liability related to Payscale's usage of the Third Party Surveys in connection with Customer's use of the Payscale Services, so long as Payscale's usage is in accordance with this Agreement. Further, Customer acknowledges that it (i) may be required to enter into a non-disclosure agreement with a given Survey Publisher and Payscale prior to the loading of any Third Party Survey; (ii) consents to Payscale contacting the applicable Survey Publisher to verify Customer's survey purchase; and (iii) agrees to provide other proof of purchase as may be requested by Payscale. In the event a Survey Publisher disputes Customer's right to a given Third Party Survey, Payscale may elect to remove the Third Party Survey from the Customer's Account. Customer hereby releases Payscale from any liability, and assumes full responsibility and all liability, that may arise from the use of, or access to, Third Party Surveys if such Third Party Surveys is used, accessed, stored, displayed, or otherwise processed by Payscale on Customer's behalf in accordance with this Agreement or as instructed by Customer.

(b) Payscale Marketplace. Third Party Surveys may be licensed directly through the Payscale Services. If Customer chooses to license a Third Party Survey through a Payscale Service, its use of that Survey is subject to the terms between Customer and the Third Party Survey Publisher, and Customer shall comply with those terms. The standard terms applicable to these Third Party Surveys licensed via the Payscale Services are available in the Documentation.

5.2 Third Party Services. Third Party Services may be licensed directly through the Payscale Services. If Customer chooses to license a Third Party Service through a Payscale Service, its use of that Third Party Service is subject to the terms available in the Documentation that are applicable to such Third Party Services licensed via the Payscale Services. For all other Third Party Services, Customer agrees that Payscale is not responsible for Third Party Services. Use of a Third Party Service is subject to the terms and conditions of the provider of the Third Party Service.

(a) Payscale Integrations.

(i) Payscale may enable or make available Payscale Integrations on a non-exclusive basis solely to allow Customer to integrate a Payscale Service with a Third Party Service. Customer understands and agrees that the development, maintenance, use, and performance of a Payscale Integration are dependent on: (a) the API, software, application, or other service or support provided by the provider of the Third Party Service; and (b) the compatibility, format, and performance of the relevant Third Party Service.

(ii) Customer understands and agrees that by using a Payscale Integration, Payscale may pull, collect, access, provide or share data with the Third Party Service to enable, maintain, support, and improve the integration between the Payscale Service and the Third Party Service. Customer's use of a Third Party Service is subject to the terms of the relevant Third Party Service. By enabling or using the Payscale Integration, Customer acknowledges that it understands and agrees to the terms of this Section.

6. TERM AND TERMINATION

6.1 Term. This Agreement is effective as of the Effective Date and will continue for a period of five years or until the Agreement is terminated as provided for herein or in the Order Form. Customer and Payscale may mutually elect to renew this Agreement for additional terms (each, a "Renewal Subscription Term") upon Customer's written notice to Payscale of its desire to do so at least ninety (90) days prior to the expiration of the then-current term.

6.2 Termination for Cause. A party may terminate this Agreement (and all Order Forms) or a specific Order Form by written notice to the other party if the other party breaches its material obligation under this Agreement, and, if the breach is capable of cure, fails to cure the breach within 30 days after the notice is sent (notice must include specific detail of the breach). If Customer terminates this Agreement or an Order Form due to Payscale's breach, then Payscale will refund Customer the prepaid Annual Subscription Fee applicable to the remainder of the terminated Payscale Services' Service Year, prorated from the effective date of termination and Customer will not be liable for paying fees due for the unused portion remaining Subscription Term. If Payscale terminates this Agreement or an Order Form due to Customer's breach, Payscale will not refund any amounts paid by Customer and Customer remains liable for payment of all fees due under this Agreement.

6.3 Effects of Termination. Upon expiration or termination of this Agreement for any reason: (a) any amounts owed to Payscale under an Order Form before such termination or expiration will be immediately due and payable except as provided in Section 6.1 above; (b) Customer must discontinue all access and use of the Payscale Services and promptly delete all copies of Documentation and Payscale Data in Customer's possession; and (c) Payscale will discontinue providing Customer the Payscale Services and Customer will lose access to the Account. All provisions that by their nature should survive termination or expiration will do so (including payment obligations, indemnification and defense obligations, limitation of liability, and duties of confidentiality). At any time during the Subscription Term, Customer may export its Customer Data then-stored in the Payscale Services in accordance with the Documentation. For up to 30 days after the end of a Subscription Term, following Customer's written request, Payscale will grant Customer access to its Account for the sole purpose of exporting the Customer Data then-stored in the Payscale Service; provided, that, (i) if any assistance is required by Customer from Payscale, Customer will pay Payscale its then-current rates for such assistance, and (ii) following such 30-day period, Payscale will delete Customer Data then stored in the Payscale Services in accordance with its deletion policies and procedures, and Customer consents to this deletion.

7. FEES AND PAYMENT FOR PAYSCALE SERVICES

7.1 Fees. Customer will pay all fees specified in Order Forms. Except as otherwise provided in this Agreement or in an Order Form: (a) fees are based on Payscale Services purchased and not actual usage; (b) fees are quoted in United States dollars; and (c) payment obligations are non-cancelable, and fees paid are non-refundable.

7.2 Invoicing and Payment. Unless otherwise agreed upon in an Order Form: (a) Annual Subscription Fees, and applicable Taxes, if any, will be invoiced in full and in advance annually; and (b) for other amounts due to Payscale under this Agreement, Payscale will invoice Customer in advance and in accordance with the relevant Order Form. Unless otherwise stated in the Order Form, invoiced charges are due 30 days after the date Payscale provides the invoice to the email provided by Customer to Payscale. Customer will provide Payscale complete and accurate billing and contact information and will notify Payscale of any changes to this information. Unless otherwise specified in an Order Form, Payscale will automatically charge Customer's payment information on file for any renewals, upgrades, or overage fees. If any invoiced amount is not received by Payscale by the due date, then without limiting Payscale's rights or remedies, (i) those charges may accrue late interest at the rate of 1.5% of the outstanding balance per month, or the maximum rate permitted by applicable law, whichever is lower, (ii) Payscale may suspend Customer's access to the Payscale Services and stop providing any Professional Services. If an invoiced amount exceeds 30 days past due Payscale may refer collection of the unpaid amount to an attorney or collections agency and Customer shall pay reasonable attorney's fees or collections agency fees. Payscale is not obligated to reinstate the Payscale Services if Customer pays past due amounts after being referred to collections. Payscale will not apply

late interest or suspend Customer's access to the Payscale Services if Customer is disputing applicable fees reasonably and in good faith and is cooperating with PayScale to diligently resolve the dispute.

7.3 Price Protection. Payscale may not increase Fees for Services on an annual basis during the Initial Term hereof unless there is a change in Customer's scope as set forth in the Order Form.

7.4 Taxes. Payscale is responsible for collecting from the Customer any applicable taxes, including sales, use, levies, duties, or any value added or similar taxes (collectively, "**Taxes**") payable with respect to Customer's order of Payscale Services. Payscale is solely responsible for taxes based upon Payscale's net income, assets, payroll, property, and employees. Notwithstanding the foregoing, if Customer is exempt from Taxes, concurrently with execution of this Agreement Customer shall provide Payscale with a certificate evidencing such exemption. If Customer's status as an entity exempt from Taxes changes during the Term, Customer shall promptly notify Payscale.

8. CONFIDENTIALITY

8.1 Meaning of Confidential Information. As used in this Agreement, "**Confidential Information**" means all confidential information disclosed by a party ("**Disclosing Party**") to the other party ("**Receiving Party**"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Customer's Confidential Information includes Customer Data, except for Aggregated Data that includes de-identified and anonymized Customer Data as permitted under this Agreement. Payscale's Confidential Information includes the Payscale Services and Documentation. Confidential Information of each party will include Order Forms, as well as business plans, technical information, product plans and designs, and business processes disclosed by such party. Confidential Information will not include any information that (a) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party, (b) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (c) is received from a third party without breach of any obligation owed to the Disclosing Party, or (d) was independently developed by the Receiving Party without use of, or reference to, the Disclosing Party's Confidential Information. The parties will have the right to disclose the existence but not the terms and conditions of this Agreement unless such disclosure is approved in writing by both parties prior to such disclosure or is made on a confidential basis as reasonably necessary to potential investors, acquirors, or regulators.

8.2 Standard of Care. Except as otherwise permitted in writing by Disclosing Party, Receiving Party will (a) use the same degree of care that it uses to protect the confidentiality of its own Confidential Information of like kind (but in no event less than reasonable care), (b) not disclose or use any Confidential Information of Disclosing Party for any purpose outside the scope of this Agreement, and (c) limit access to Confidential Information of Disclosing Party to those of its employees, contractors, advisors, and agents with a need to know or who need access for purposes consistent with this Agreement and who are bound by confidentiality obligations at least as stringent to those in this Agreement.

8.3 Compelled Disclosure. A party may disclose the other party's Confidential Information if required by applicable law or to comply with a court order or other governmental demand that has the force of law if, to the extent permitted by applicable law, the receiving party promptly notifies the disclosing party of that obligation prior to production so the disclosing party may seek a protective order or other remedy.

9. DATA PROCESSING AND PROTECTION

9.1 General Requirements. Payscale will maintain appropriate administrative, physical, and technical safeguards for the protection of the security and integrity of Customer Data as set forth in Security Addendum located at https://www.payscale.com/content/legal/sa.pdf, a current version of which is attached hereto and incorporated herein as Annex B.

9.2 Data Storage. Customer understands and agrees that the Payscale Services host, process, and otherwise store Customer Data on its servers or using the cloud infrastructure of third party providers. Third party providers shall meet or exceed the safeguards for the protection and security of Customer Data agreed upon by Payscale under this Agreement. Except for Aggregated Data submitted by Customer to the Data Sharing Services,

Customer Data will be separated logically or through other technical means from the data of Payscale's other customers.

9.3 Data Processing Terms. Both parties agree to comply with applicable data privacy laws and regulations. In addition, the Data Processing Addendum available at https://www.payscale.com/content/legal/dpa.pdf, a current version of which is attached hereto and incorporated herein as Annex C ("**DPA**") applies to the extent Customer elects to load Customer Data into a Payscale Service subject to Data Protection Laws (as defined in the DPA).

9.4 Privacy Policy. Customer's use of Payscale Services is subject to Payscale's privacy policy, a current copy of which is located at https://www.payscale.com/about/privacy-policy/.

10. WARRANTIES AND DISCLAIMERS

10.1 Mutual Warranties. Each party warrants to the other party that: (a) it has the authority to enter into this Agreement and perform its obligations under this Agreement; (b) this Agreement does not conflict with any other agreement it is subject to and bound by; and (c) it does not conduct business for any unlawful purpose.

10.2 Payscale Warranties. Payscale warrants to Customer for Customer's benefit only that: (a) the Payscale Services will operate in substantial conformity with then-current and applicable Documentation so long as Customer uses the Payscale Services in accordance with this Agreement and the Documentation and for the limited purpose allowed under this Agreement; and (b) Professional Services will be performed in a professional manner in accordance with this Agreement. For any breach of the foregoing subsection (a), Customer's sole and exclusive remedy will be for Payscale to use commercially reasonable efforts to correct the nonconformity in the Payscale Services. If Payscale determines this remedy to be impracticable, or otherwise is unable to provide a workaround within 30 days of Customer notifying Payscale of the defect, then Customer may terminate the applicable Order Form for material breach in accordance with Section 6.1 above. Customer acknowledges that Payscale Services are subscription-based and that to deliver an improved customer experience, Payscale may make changes to Payscale Services. In such event, Payscale will update applicable Documentation accordingly. Payscale does not warrant that the Payscale Services (including, Payscale Data) are accurate and free from all defects or errors.

10.3 Customer Warranties. Customer warrants to Payscale that: (a) it possesses all necessary licenses, permissions, and other rights in and to Customer Data to grant to Payscale the license and rights to Customer Data as expressly granted in this Agreement; (b) the billing information Customer provides to Payscale is accurate, current, and complete, (c) to the best of its knowledge, Customer Data provided to Payscale is accurate and complete, (d) Customer has the right to use all Third Party Surveys it directs Payscale to make available in the Payscale Services, and € Customer will not use the Payscale Services to violate antitrust or competition laws and regulations.

10.4 Disclaimers. Customer acknowledges that: (a) Payscale Data is for general information only; and (b) Customer's use of the Payscale Services does not constitute any form of advice, recommendation, representation, or arrangement (legal or otherwise) by Payscale or its licensors. Customer acknowledges that it is responsible for all of its decisions regarding compensation, salaries, and benefits regardless of its use of Payscale Services and Customer is encouraged to conduct independent due diligence and seek the assistance of a qualified legal professional in connection with such decisions. Payscale and its licensors do not warrant the access or use of Payscale Services in any specific situation or for any specific application, nor do they warrant that Payscale Data accessible through a Payscale Service will be always accessible or that it will be error free. Customer acknowledges that Payscale provides the Payscale Services to its customers to permit them to make independent decisions regarding benefits and compensation. Because the exchange of salary and benefit information among competitors may be construed in certain circumstances to facilitate an anti-trust violation or violation of relevant competition laws, Payscale has taken measures in the collection and distribution of this information to avoid such perceptions but does not warrant that the Payscale Data could not be used to violate antitrust law. Except as expressly provided in this Agreement, to the maximum extent allowed under applicable law, the Payscale Services are provided "AS IS" and "AS AVAILABLE," and neither party makes any warranties of any kind, whether express, implied, statutory, or otherwise, and each party specifically disclaims all implied warranties, including, any implied warranties of merchantability, fitness for a particular purpose, non-infringement, or any warranties arising during course of performance.

11. [INTENTIONALLY OMITTED]

12. LIMITATION OF LIABILITY

12.1 Indirect and Consequential Damages; Aggregate Liability. TO THE MAXIMUM EXTENT ALLOWED UNDER APPLICABLE LAW AND SUBJECT TO SECTION 12.2 BELOW, A PARTY WILL NOT BE LIABLE TO THE OTHER FOR ANY INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING, LOST PROFITS), REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING, NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, EVEN IF INFORMED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE. TO THE MAXIMUM EXTENT ALLOWED UNDER APPLICABLE LAW AND SUBJECT TO SECTION 12.2 BELOW, A PARTY'S AGGREGATE LIABILITY TO THE OTHER ARISING OUT OF, OR RELATED TO, THIS AGREEMENT (WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY) WILL BE LIMITED TO ACTUAL AND PROVEN DAMAGES IN AN AMOUNT NOT TO EXCEED THE AMOUNT PAID BY CUSTOMER TO PAYSCALE UNDER THIS AGREEMENT DURING THE 36-MONTH PERIOD IMMEDIATELY PRECEDING THE INCIDENT GIVING RISE TO THE CLAIM.

12.2 Exclusions to Limitation of Liability; Limitation of Claims. The limitations set out in Section 12.1 above do not apply to: (a) amounts incurred by a party acting as an Indemnitor under Section 11 above; (b) Customer's obligation to pay amounts due under this Agreement; (c) Customer's use of a Payscale Services in violation of Sections 2.2 (Account Access) or 2.3 (Use Restrictions) above; or (d) actual and proven damages arising from the other party's willful misconduct, fraud, or gross negligence.

13. GENERAL PROVISIONS

13.1 Notices. Payscale may send announcements of general interest by email or by posting on its website or through Customer's Account, such as notices of new features, scheduled downtime, or upcoming events. Payscale will provide Customer with legal notices by email to the address provided by Customer. Customer will promptly notify Payscale if its contact information changes. Customer will provide Payscale with legal notices by email to legal@payscale.com.

13.2 INTENTIONALLY OMITTED

13.3 Assignment. Neither party may transfer or assign this Agreement, or any of its rights or obligations under this Agreement, whether by operation of law or otherwise, without the prior written consent of the other party (not to be unreasonably withheld); except that a party may assign this Agreement in its entirety without the other party's consent in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all its assets. Subject to the foregoing, this Agreement will bind and inure to the benefit of the parties' respective successors and permitted assigns.

13.4 Publicity. Except with Customer's prior written consent, Payscale shall not identify Customer as a Payscale customer in or on Payscale's demonstrations, website, or other promotional materials. Payscale's use of Customer's name and logo will be in accordance with any guidelines provided by Customer. Upon Customer's written request, Payscale will promptly remove Customer's name or any Customer marks from Payscale's website, and to the extent feasible, Payscale's marketing materials. Notwithstanding the foregoing, where Customer is participating in Data Sharing Services, its name will be included in the Data Sharing Service according to Section 4.4(a) and the Documentation.

13.5 Remedies; Severability. Each party acknowledges that damages may be an inadequate remedy if the other party violates its obligations under this Agreement, and each party has the right, in addition to any other rights it may have, to seek injunctive relief without any obligation to post any bond or similar security. No failure or delay by either party in exercising any right under this Agreement will constitute a waiver of that right. Other than as expressly stated in this Agreement, the remedies provided in this Agreement are in addition to, and not exclusive of, any other remedies of a party at law or in equity. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision will be modified by the court and interpreted to best accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of this Agreement will remain in effect.

13.6 Force Majeure. A party's performance of any part of this Agreement (except Customer's payment obligations) will be excused to the extent that it is unable to perform due to natural disasters, terrorism, riots, insurrection, war, extraordinary governmental action, ISP Provider failures or delays, or any other cause which is beyond the reasonable control of such party ("**Affected Party**"), not avoidable by reasonable due diligence, and not caused by the Affected Party (each a "**Force Majeure Event**"). Upon the occurrence of a Force Majeure Event, the Affected Party will (a) exercise commercially reasonable efforts to mitigate damages to the other party and to overcome the Force Majeure Event, and (b) continue to perform its obligations under this Agreement to the extent it is able.

13.7 Export Compliance. Each party will comply with the export laws and regulations of the United States and other applicable jurisdictions in providing and using the Payscale Services. Without limiting the foregoing, (a) each party represents that it is not named on any U.S. government list of persons or entities prohibited from receiving exports, and (b) Customer will not permit Users to access or use the Payscale Services in violation of any U.S. export embargo, prohibition, or restriction. Customer agrees not to export, re-export or transfer any part of the Payscale Services in violation of export laws and regulations.

13.8 Government End Use Provisions; Limited Waiver of Sovereign Immunity. Payscale provides the Payscale Services, including related software and technology, for ultimate federal government end use solely in accordance with the following: Government technical data and software rights related to the Payscale Services include only those rights customarily provided to the public as defined in this Agreement. This customary commercial license is provided in accordance with FAR 12.211 (Technical Data) and FAR 12.212 (Software) and, for Department of Defense transactions, DFAR 252.227-7015 (Technical Data – Commercial Items) and DFAR 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation). If a government agency has a need for rights not conveyed under these terms, the parties must agree to mutually acceptable written addendum specifically conveying such rights. If Customer has sovereign immunity, Customer hereby irrevocably and unequivocally waives Customer's sovereign immunity for the limited purpose of enforcing the terms of this Agreement, and Customer represents and warrants to Payscale that it has procured all necessary consents to grant this waiver. This limited waiver of sovereign immunity includes any action for money damages, injunctive relief, or declaratory relief. Customer agrees that it will not raise sovereign immunity as a defense in any action brought by Payscale to enforce this provision.

13.9 Conflict of Interest. A.R.S. §38-511 applies to this agreement.

13.10 No Israel Boycott. By entering into this Agreement, Payscale certifies that Payscale is not currently engaged in, and agrees for the duration of the Agreement, not to engage in a boycott of Israel as defined by state statute.

13.10 Miscellaneous. Except as otherwise provided in this Agreement, there are no third party beneficiaries under this Agreement. Any claims against Payscale or its Affiliates under this Agreement may only be brought by the Customer entity that is a party to this Agreement. The parties to this Agreement are independent contractors. There is no relationship of partnership, joint venture, employment, franchise, or agency created hereby between the parties. Neither party will have the power to bind the other or incur obligations on the other party's behalf without the other party's prior written consent. Customer agrees that its purchases of all Payscale Services under this Agreement are neither contingent on the delivery of any future functionality or features nor dependent on any oral or written public comments made by Payscale regarding future functionality or features.

13.11 Entire Agreement. This Agreement constitutes the entire agreement between the parties and supersedes all prior and contemporaneous agreements, proposals, or representations, written or oral, concerning its subject matter. No modification, amendment, or waiver of any provision of this Agreement will be effective unless in writing and either signed or accepted electronically by the party against whom the modification, amendment, or waiver is to be asserted. If there's a direct conflict between provisions in this Agreement, the conflict will be resolved by giving precedence to the provision as it appears in the highest-ranked document in the following order: (a) the relevant Order Form; (b) product-specific Documentation; (c) DPA, if applicable; and (d) the body of this Agreement. No terms or conditions included in any purchase order or order documentation (excluding Order Forms) provided by Customer, or as a part of Customer's vendor set-up process, will be incorporated into, or form any part of, this Agreement, and all such terms or conditions are null and void even if such terms or conditions are accepted by Payscale or Payscale accepts payment from Customer.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

13.12 Counterparts. This Agreement may be executed electronically (e.g., via DocuSign or similar service) in counterparts, and all counterparts executed constitutes one agreement, binding upon all the parties. The parties represent and warrant to the other that the individual signing below has the right and authority to execute this Agreement on behalf of the undersigned.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their duly authorized representatives. This Agreement shall be in full force and effect only when it has been approved and executed by the duly authorized City officials.

FOR THE CITY	**FOR PAYSCALE, INC.**
By: _____	By: Mck Madison
Its: Mayor	Its: VP, Sales

APPROVED AS TO FORM:

By: _____

City Attorney

ATTEST:

By: _____

City Clerk

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

EXHIBIT A
ORDER FORM

payscale

Mailing Address: 113 Cherry St, Suite 96140 Seattle, WA 98104 Valid Until 2/28/2022

CUSTOMER NAME: City of Chandler, AZ

CONTACT INFORMATION

Sold To:	**Bill To:**
City of Chandler, AZ	City of Chandler, AZ
175 S Arizona Avenue	175 S Arizona Avenue
Chandler, Arizona 85225	Chandler, Arizona 85225
United States	United States
Kerstin Nold	Traci Tenkely
kerstin.nold@chandleraz.gov	traci.tenkely@chandleraz.gov
(480) 782-2490	+1 480-782-2635

PRODUCT DETAILS

of Employees: 1,240 # of Surveys: 2 # of JDs: N/A Format: N/A

PRODUCT NAME(S)	QUANTITY	TERM (MONTHS)	ANNUALIZED PRICE	TOTAL PRICE
Survey Management - Basic + Peer Global Network	1	60	$30,000.00	$150,000.00
Implementation (1X)	1			$0.00
			TOTAL PRICE:	$150,000.00

BILLING INFORMATION

Billing Cycle: Annual
Payment Terms: Net 30
Currency: USD
Taxes: Prices shown above do not include any state and local taxes that may apply. These taxes are the responsibility of the Customer and will appear on the final Invoice.

TERMS & CONDITIONS

- **Subscription Start Date**: Customer's Subscription Term starts on the date Customer signs this Order Form.
- **Master Subscription Agreement**: This Order Form and Customer's purchase and use of the PayScale products and services described herein are governed by the Master Subscription Agreement ("MSA") entered into between Customer and PayScale concurrently with this Order Form.
- **Documentation**: Payscale Services are subject to product and service specific terms and requirements available at https://www.payscale.com/about/documentation ("Documentation"). The Documentation includes descriptions of standard Professional Services projects.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

Special Terms:

- This Order Form and Customer's purchase and use of the PayScale products and services described herein are governed by our MSA amended as follows:

- **No Auto-Renewal:** The parties agree that Customer's subscription to the products and services purchased under this Order Form will not automatically renew upon expiration of the Subscription Term set out in this Order Form above.

- **Customer List:** PayScale agrees that it will not include Customer's name or logo in its customer lists or other marketing materials unless Customer provides advanced written permission.

- Enter language for Other Alternate Governing State here.

- **Customer Government Entity (Non-Appropriation of Funds):** In accordance with [insert law that applies to customer government entity] law, Customer is a local governmental entity that relies on legislative budget approval to fund the PayScale Offering provided under this Order Form. Customer intends to continue this Order Form for its entire Subscription Term and to satisfy its obligations hereunder, and for each fiscal period: (a) Customer agrees to include in its budget request appropriations sufficient to cover Customer's obligations under this Order Form; (b) Customer agrees to use all reasonable and lawful means to secure these appropriations; and (c) Customer agrees it will not use non-appropriations as a means of terminating this Order Form to acquire functionally equivalent products or services from a third party. Customer reasonably believes that sufficient funds will lawfully be appropriated to satisfy its obligations under this Order Form. If Customer is appropriated insufficient funds (by appropriation, appropriation limitation, or grant) to continue payments under this Order Form and has no other funding source lawfully available to it for such purpose, Customer may terminate this Order Form by providing PayScale at least 30 days prior written notice. Upon termination, Customer will remit all amounts due and all costs reasonably incurred by through the date of termination, and, to the extent of lawfully available funds, through the end of the then-current fiscal period. Upon request by PayScale, Customer will provide a summary of the status of funding for this Order Form.

- **Early Termination Right:** For the initial Subscription Term only, Customer may terminate this Order Form before the end of such initial Subscription Term if: (a) Customer provides PayScale at least 30 days' advanced written notice of termination, where such termination will be effective at the end of the then-current Service Year; (b) Customer completes the onboarding and implementation process for the Cloud Offering at issue; and (c) Customer pays PayScale a termination fee of $19,800.00 if Customer elects to terminate the second and third Service Years or $9,900.00 if Customer elects to terminate the third Service Year. If Customer exercises its option to terminate under this provision, Customer is not entitled to a refund of fees pre-paid prior to such termination for the then-current Service Year and Customer remains obligated to pay PayScale any fees that remain unpaid for the then-current Service Year.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

By signing this Order Form, you represent that you are authorized to sign on behalf of your organization and agree to all referenced terms and conditions.

City of Chandler, AZ		**PayScale, Inc.**	
Signature:		Signature:	Nick Madison
Name:		Name:	Nick Madison
Title:		Title:	VP, Sales
Date:		Date:	March 3, 2022

Annex A

SERVICE LEVELS ADDENDUM

This Service Levels 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 Services ("**Agreement**"). Capitalized terms used in this Addendum and not defined shall have the meanings given to such terms in the Agreement.

1.1 Payscale Service Uptime Availability. During the Subscription Term, Payscale will maintain at least 99.5% monthly uptime percentage ("**Monthly Uptime Percentage**") for the specific Payscale Service subscribed to by Customer as calculated per the below formula using Payscale's systems. "**Downtime**," as used in the below formula, means the total minutes in a calendar month during which the Payscale Service is unavailable, excluding: (a) any planned or scheduled downtime, as described in the Agreement; and (b) any unavailability due to any of the events described in Section 2 below regarding Downtime exclusions (each event referred to as an "**Exclusion Event**").

$$\frac{\text{Total number of minutes in a month} - \text{Downtime}}{\text{Total number of minutes in a month}} \times 100$$

1.2 Downtime Exclusions. The availability of the Payscale Service and calculation of the Monthly Uptime Percentage shall not include the amount of time the Payscale Service is unavailable or not functioning properly as a result of any of the following: (a) software, hardware, or other product or service not provided by Payscale, including, any Third Party Services; (b) Customer's internet service provider (ISP) or web browser; (c) a Force Majeure Event; (d) Technical Requirements are not met by Customer (e.g., incompatible web browser); or € Customer's or any of its Users' error or negligence (e.g., a User has entered the incorrect credentials to access Customer's Account).

1.3 Support Information. Customer will notify Payscale if the Payscale Service is unavailable or experiencing an error ("**Error**") utilizing the technical support link within the Payscale Service (if available) or calling 888-219-0327. Payscale's support hours are 9:00 AM – 8:00 PM (Eastern Time) ("**Business Hours**"), Monday through Friday, excluding any Payscale recognized holidays ("**Business Day**"). Payscale recognized holidays include: New Year's Day, Martin Luther King Day, President's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, the day after Thanksgiving, Christmas Eve, and Christmas Day.

1.4 Support Priority Levels and Response Times. Payscale will use reasonable efforts to respond to Customer's request for support that do not relate to an Error within 7 Business Days (or sooner) of Payscale's confirmed receipt of Customer's request. For Customer's requests related to an Error, Customer's reported Error will be classified under one of the three below described Priority Levels. For such requests, Payscale will classify the Priority Level. If there's a dispute over the Priority Level classification, Customer will promptly notify Payscale and the parties will, in good faith, cooperate with one another to resolve any such disagreement. Payscale will use reasonable efforts to respond to, and resolve (or provide a workaround to), Customer's support requests regarding an Error in accordance with the applicable time frame set out in the table below.

Priority Level	Initial Response Time	Resolution Response Time
Priority Level 1 – The Payscale Service is unavailable (e.g., login page is unavailable and no access to the Payscale Service is achieved) due to a failure of Payscale's software, hardware, or ISP connections, but not to include any problems or outages caused by an Exclusion Event.	1 Business Hour	1 Business Day
Priority Level 2 – A Payscale Service defect that affects a primary feature or function or causes critical service disruption or degradation, and that requires correction to achieve full Payscale Service functionality (e.g., the Payscale Service is available but a single module is not working), but only to include problems with Payscale's software, hardware, or ISP connections but not to include any problems arising from an Exclusion Event. The defect under this priority level does not make the Payscale Service unavailable, but may disable a major feature or function.	1 Business Day	3 Business Days
Priority Level 3 – A Payscale Service defect that affects a secondary or minor feature or function, but does not require correction to achieve full Payscale Service functionality, or general service issues such as slow response time (e.g., a feature is responding but very slowly), but only to include problems caused by Payscale's software, hardware, or ISP connections but not to include any problems arising from an Exclusion Event.	2 Business Days	10 Business Days

1.5 Miscellaneous. This Addendum is effective as of the date this Addendum is signed by both parties and will terminate automatically upon the expiration of the applicable Payscale Service Subscription Term or the termination of the relevant Order Form, whichever is earlier. 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.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

Annex B

SECURITY ADDENDUM

This Security 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 Services ("**Agreement**"). Capitalized terms used in this Addendum and not defined shall have the meanings given to such terms in the Agreement. This Addendum is in effect for the period that Payscale processes any information Customer or its Users loads or otherwise inputs into the Payscale Services (or provides to Payscale for loading or inputting into the Payscale Services on Customer's behalf), and any information provided by Customer relating to its use of Professional Services ("**Customer Data**"). The Addendum may be amended from time to time by Payscale provided that such updates do not result in the degradation of the overall security of the Payscale Services.

1. SCOPE

1.1 Payscale maintains a security program ("**Security Program**") to protect Customer Data following guidance derived from industry standard frameworks such as, but not limited to, AICPA Trust Services Criteria (SOC2), NIST Cybersecurity Framework (CSF), International Organization for Standardization (ISO), and Center for Internet Security (CIS).

1.2 The Security Program is applicable to all Payscale Services (the "**Covered Payscale Services**") except for Benchmark.

2. OPERATING PLANS

2.1 Incident Response Plan. Payscale maintains an incident response plan, including a breach notification process, to assess, escalate, and respond to identified cyber security incidents that impact the organization, the services provided to Customers, or result in data loss. Discovered intrusions are resolved in accordance with established procedures. The incident response plan is reviewed and updated at least annually.

2.2 Business Continuity & Disaster Recovery Plan. Payscale has a business continuity and disaster recovery plan in place to manage significant disruptions to operations and infrastructure. This plan is reviewed and tested annually by information technology, operations, and information security teams. Business continuity and resilience is supported using resilient cloud architectures, services, and providers.

3. CUSTOMER DATA.

3.1 Delineation and Identification. Payscale has implemented processes to delineate and identify Customer Data for special handling within Payscale's organization.

3.2 Data Segregation. Payscale maintains the capability to segregate and isolate Customer Data, disable functionality of applications using Customer Data, and deploy suitable application controls and firewalls so that Customer Data will not be commingled or corrupted by data from other sources.

3.3 Encryption.

(a) Data in Transit. When Processing Customer Data, public connections to Customer computing environments and any other transmission via data transmission services or using the Internet will be protected using, as applicable, the following cryptographic technologies: IPSec, SSL/TLS, SSH/SCP, SFTP, or other technologies that provide similar or greater levels of security. Encryption algorithms will be of sufficient strength to protect data to commercially reasonable security levels and will utilize industry recognized hashing functions. Transmission may not use any cryptography algorithms developed internally by or for Payscale.

(b) Data at Rest. Customer Data at rest shall be protected using one or more industry standard and commercially reasonable encryption technologies as supported and applicable to the underlying storage.

(c) Removable Media. Payscale has policies and procedures in place designed to ensure that its employees and contractors are not permitted to copy Customer Data to a removable media device such as a USB

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

flash, external hard drive, or CD/DVD for storage except where such action is authorized for backup purposes or at Customer request. All such media shall have encryption and other reasonable security measures restricting access and use as required by this Addendum.

4. SECURITY. Payscale's systems have been designed to ensure that all physical and virtual hosts, networks, services, or platforms in which Customer Data is stored or processed are: (a) maintained solely on Payscale's or its third-party service providers property or premises and (b) maintained in a secure manner that satisfies the requirements of this Addendum.

4.1 Perimeter Defense. Payscale utilizes private networks and firewalls to secure internal systems, services, and networks from unauthorized access. Networks are protected by Intrusion Detection and Intrusion Prevention systems or designated to allow only authorized traffic.

4.2 Monitoring. Payscale utilizes a security information event monitoring (SIEM) system to pull security log and event information from servers, firewalls, routers, system users, and administrator activity. The SIEM is configured for alerts and is monitored on an ongoing basis. Logs contain details on the date, time, source, and type of events. Security operations personnel monitor items detected and take appropriate action.

4.3 Vulnerability Management. Payscale monitors and scans for vulnerabilities on a regular basis. Vulnerability scans are run on a scheduled basis using industry-recognized scanning tools. Payscale follows a mitigation and remediation process where identified vulnerabilities are assessed and remediated by vendor supplied patches or where not applicable or available, through mitigating controls. On an annual basis, Payscale conducts third-party penetration tests on the Covered Payscale Services to identify security vulnerabilities.

4.4 Vendor Security. Payscale maintains a vendor management program that assesses all vendors that access, store, process, or transmit Customer Data for appropriate security controls. Payscale communicates security and confidentiality requirements and operational responsibilities to third parties through contractual agreements, as necessary. The impact of any issues identified is assessed and remediated, if necessary.

4.5 Physical Security.

(a) Payscale Offices. Physical access to Payscale offices is granted based on job responsibilities and work location. Access to offices can only be approved by appropriate personnel. Physical access is removed when access is no longer required and as a component of the employee termination process. Visitor logs are maintained. Badge readers control access to restricted areas within Payscale offices and data center locations. Unauthorized badge access attempts are denied and logged.

(b) Data Centers. Physical security controls and assurance reports are evaluated on an annual basis for data centers.

(i) Data center facilities include (1) physical access restrictions and monitoring that shall include a combination of any of the following: multi-zone security, person-traps, appropriate perimeter deterrents (e.g., fencing, berms, guarded gates), on-site guards, biometric controls, CCTV, and secure cages; and (2) fire detection and fire suppression systems both localized and throughout the data center floor.

(ii) Payscale hosts Covered Payscale Services in data centers that have attained SOC 2 Type II attestations (or equivalent or successor attestations or certifications). Each data center includes full redundancy and fault tolerant infrastructure for electrical, cooling and network systems. The deployed servers are enterprise scale servers with redundant power to ensure maximum uptime and service availability. Payscale Service data centers are serviced by multiple network connections, carriers, and/or ISPs for fault tolerance, redundancy, and availability.

(iii) Payscale uses industry standard (or substantially equivalent) processes for secure destruction of sensitive materials, including Customer Data, before such media leaves Payscale's data centers.

4.6 Covered Payscale Service Authentication. Payscale has policies and procedures in place that require that, regarding any users of Covered Payscale Services:

(a) Each user must have a unique user ID and must be assigned a password.

(b) The Covered Payscale Services must log the date and time for all failed and successful user attempts to access the Covered Payscale Service.

(c) The Covered Payscale Services must log the date and time for all password changes to the Covered Payscale Service

(d) The Covered Payscale Services must limit the number of failed log-on attempts to a maximum of 10 before disabling the user ID.

(e) The Covered Payscale Offer must authenticate a valid user ID and password or token prior to granting access to network or system resources containing or permitting access to Customer Data.

(f) Authentication data transmitted over a public or shared network must be encrypted.

4.7 Endpoints. Endpoint protection is installed and activated on all endpoint devices to monitor and protect in real-time for virus and malware infections. Virus definition updates are pushed out to endpoint devices automatically on a regularly scheduled basis. Endpoints are provisioned with encrypted disks and remote lock capability. Payscale restricts personnel from disabling endpoint protection measures.

5. MALICIOUS CODE.

5.1 Payscale utilizes commercially reasonable controls and processes to prevent the operation and transmission of malicious code for all computer systems containing or permitting access to Customer Data and in the delivery of its Covered Payscale Service.

5.2 Covered Payscale Services shall not contain viruses or malware that may result in either (a) inoperability of the Covered Payscale Service or (b) interruption, interference with the operation of the Covered Payscale Service (collectively, "**Illicit Code**"). If the Covered Payscale Service is found to contain any Illicit Code that adversely affects its performance or causes a material security risk to Customer Data, Payscale shall, as Customer's exclusive remedy, use commercially reasonable efforts to remove the Illicit Code.

6. UPDATES TO COVERED CLOUD OFFERINGS.

6.1 Payscale follows a software development life cycle for Covered Payscale Services. All software development and releases are tracked and follow industry standard processes for code development, review, and testing. Releases are tracked and approved following best practices supporting separation of duties and least privileged where applicable and feasible. Software changes are tested prior to release with issues being identified and logged.

6.2 Payscale deploys updates to the Covered Payscale Services during scheduled maintenance windows, details of which are posted within the Covered Payscale Services prior to the scheduled period. In the event of a service interruption, Payscale posts a notification to the website describing the affected services.

7. PAYSCALE PERSONNEL

7.1 Background. Payscale performs background screening on all employees and contractors who have access to Customer Data in accordance with Payscale's then-current information technology security policy, subject to applicable laws.

7.2 Compliance. Payscale takes appropriate steps to ensure compliance with the Security Program by its employees, contractors, and subprocessors, to the extent applicable to their scope of performance, and all persons authorized to access Customer Data are under an obligation of confidentiality.

(a) Employee Policies. Payscale policies and operating procedures related to security are made available to personnel via the corporate intranet. Security policies and procedures are reviewed annually and updated as needed. Personnel are required to review and acknowledge these policies and procedures during on-boarding and annually thereafter. Payscale maintains a disciplinary process for personnel that do not comply with its security and confidentiality policies.

(b) Security and Privacy Awareness. Payscale maintains a security and privacy awareness program that includes appropriate training and education of Payscale personnel. Such training is conducted at time of hire and at least annually throughout employment at Payscale. Payscale conducts periodic security awareness education and communications regarding creating and maintaining a secure workplace.

7.3 Data Access. Payscale classifies informational assets in accordance with its data classification policy. Payscale assigns application and data rights based on authorized user roles and responsibilities, which align with the principle of least privilege and separation of duties where applicable and feasible.

(a) Restricted Access. Payscale's policies require that Customer Data will be accessible only by authorized Payscale employees, officers, directors, agents, contract workers and others who have a legitimate business need to access such information, with suitable user authentication, sign-on procedures, and access controls that satisfy the requirements of this Addendum.

(b) Authentication. Payscale has policies and procedures in place, regarding its employees and contractors, that require that: (i) users have a unique account identifier or user ID, (ii) authentication credentials such as passwords and tokens must not be used by anyone other than the users to whom they are assigned; and (iii) authentication credentials such as passwords may not be written down or stored in an unencrypted fashion. Payscale promptly disables authentication access for terminated users.

(i) Passwords. Payscale has established password policies and procedures based on industry standards and best practices including, but not limited to NIST Special Publication 800-63(b). Password policies focus on complexity and length and are promptly changed if suspected of being disclosed to unauthorized parties.

(ii) Multifactor Authentication. Direct access to production networks and systems is protected by multifactor authentication protocol. Such protocol may include certificate, device, PIN, or unique identifier.

(c) Access Review. Payscale periodically reviews its access to production systems of the Covered Payscale Service for administrative account access, appropriateness, and personnel changes. Where supported and feasible, separate administrator accounts are provisioned and used by authorized personnel to perform privileged functions.

8. OVERSIGHT AND REVIEW.

8.1 Periodic Adjustment. Payscale will regularly monitor, evaluate, and adjust, as appropriate, the Security Program considering any relevant changes to applicable laws.

8.2 Internal Audits. Internal audits are aligned to the Security Program and compliance requirements. Payscale conducts internal control assessments to validate that its controls are operating effectively. Issues identified from assessments are documented, tracked, and remediated as appropriate. Internal controls related to security are audited by an external independent auditor at least annually and in accordance with applicable industry standards.

8.3 External Audit Reports. Payscale will maintain commercially reasonable audit reports such as the AICPA SOC2 (or equivalent or successor attestations or certifications) produced by third parties and updated annually based on an audit performed at least once every 12 months (the "**External Audit Reports**") to evaluate the continued effectiveness of the Security Program for Covered Payscale Services. Payscale may add or remove standards at any time where such standard changes: (i) do not materially impact the integrity of the Security Program or (ii) are no longer applicable to the Covered Payscale Service. Payscale may replace an External Audit Report with an equivalent or enhanced alternative. Upon request by a Customer, Payscale will make the External Audit Reports available for review by Customer to demonstrate compliance by Payscale with its obligations under this Addendum. Payscale regularly reviews controls as described in the External Audit Reports.

8.4 Review Personnel. Payscale has a designated information security function responsible for the development, maintenance, review, and approval of Payscale's security standards and policies. The function is responsible for the oversight and governance of the Security Program.

9. CUSTOMER RESPONSIBILITIES

9.1 Transfer. Covered Payscale Services provide secure methods for Customers to transfer Customer Data directly to Covered Payscale Services and role-based access controls. Customer is responsible for configuring such access controls within the Covered Payscale Service.

9.2 Access. Covered Payscale Services allow Customers to: (a) integrate with SAML solutions, (b) manage passwords; and (c) prevent access by users with an inactive account. Customer manages each user's access to and use of the Covered Payscale Services by assigning to each user a credential and user role that controls the level of access to the Covered Payscale Service. Customer is solely responsible for reviewing the Security Program and making an independent determination as to whether it meets Customer's requirements, considering the type and sensitivity of Customer Data that Customer processes within the Covered Payscale Services. Customer is responsible for protecting the confidentiality of each user's login and password and managing each user's access to the Covered Payscale Services.

9.3 Storage. Customer is responsible for its use of the Covered Payscale Service and its storage of any copies of Customer Data outside Payscale's or Payscale's subprocessors' systems.

9.4 Customer's Security Assessment. Customer agrees, based on its current and intended use of the Covered Payscale Service, that the Covered Payscale Service, Security Program, and Payscale's commitments under this Addendum (a) meet Customer's needs and (b) provide a level of security appropriate to the risk in respect of the Customer Data.

9.5 Contact. Customer agrees to identify and maintain appropriate contact(s) for all information security incident and information security-related communication.

9.6 No Assessment of Customer Data. Payscale has no obligation to assess Customer Data to identify information subject to any specific legal requirements.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

Annex C

DATA PROCESSING AGREEMENT

This Data Processing Agreement (this "**DPA**") amends the Master Subscription Agreement (https://www.payscale.com/content/legal/msa.pdf) or other agreement entered into between Payscale Inc., and Customer, including any duly-executed Order Forms (collectively, the "**Agreement**"). This DPA 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 applicable Data Protection Laws.

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

1.1 "**Customer Data**" means all information Customer or its Users loads or otherwise inputs into the Payscale Offering (or provides to Payscale for loading or inputting into the Payscale Offering on Customer's behalf), and any information provided by Customer relating to its use of Professional Services.

1.2 "**Customer Personal Data**" means any Customer Data that is Personal Data.

1.3 "**Data Protection Laws**" means all laws – to the extent applicable to the Agreement – relating to privacy, security, or protection of Personal Data, as may be defined in such laws, including without limitation the EU General Data Protection Regulation (Regulation 2016/679) ("**GDPR**") and the California Consumer Protection Act ("**CCPA**"), the United Kingdom Data Protection Act 2018 ("**UK DPA 2018**"), the Swiss Federal Data Protection Act of 19 June 1992 ("**FADP**") and any subsequent supplements, amendments, or replacements to the same. The parties acknowledge that pursuant to Cal. Civ. Code § 1798.145(h)(1), employee information that would otherwise be considered Personal Data is exempted from the CCPA until the California Privacy Rights Act ("**CPRA**") comes into effect.

1.4 "**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 Process Customer Personal Data.

1.5 "**Personal Data**" means any information processed by Payscale, in connection with the performance of a Payscale Offering that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household or with a particular individual's or household's device; or any inferences drawn therefrom. For the avoidance of doubt, the parties acknowledge that data that has been stripped of identifiers and aggregated will not be deemed Personal Data.

1.6 "**Processing**" means the collection, receipt, recording, organization, structuring, alteration, use, transmission, access, sharing, provision, disclosure, distribution, copying, transfer, storage, management, retention, deletion, combination, restriction, summarizing, aggregation, correlation, inferring, derivation, analysis, adaptation, retrieval, consultation, destruction, disposal or other handling of Personal Data. "**Process**," "**Processes**," "**Processed**" or "**Processing**" will be interpreted accordingly.

1.7 "**Security Incident**" means any unauthorized interference with the availability of, or any unauthorized, accidental or unlawful destruction, misuse, loss, alteration, acquisition of, disclosure of, damage or access to, or any other unauthorized Processing of Customer Personal Data stored or otherwise Processed by Payscale and in Payscale's possession or control.

1.8 "**Subprocessor**" means any person or entity engaged by Payscale to help provide the Payscale Offering, and that Processes Customer Personal Data.

1.9 The terms "**Sale**" and "**Service Provider**" shall have the same meaning as in the CCPA and their cognate terms shall be construed accordingly. The terms "**Controller**," "**Processor**," and "**Data Subjects**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. General Data Processing Requirements

2.1 Roles and Responsibilities

(a) Each party will comply with its obligations under applicable Data Protection Laws in connection with the Processing of Customer Personal Data.

(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 in its sole discretion determines what Customer Personal Data is provided to Payscale or loaded into the Payscale Offering, and Customer will not provide Payscale or load Customer Personal Data into the Payscale Offering that is not necessary for Payscale to provide Customer the applicable Payscale Offering identified in the Agreement. Customer shall have sole responsibility for the accuracy, quality, and legal basis for collection of Customer Personal Data and the means by which Customer obtained the Personal Data.

(c) The parties acknowledge and agree that between Payscale and Customer, Payscale is a Data Processor in connection with the Processing of Company Personal Data pursuant to the Agreement, and Customer is a Controller of Customer Personal Data. If the Customer is a Data Processor, Customer represents and warrants that Customer's instructions and Processing of Customer Personal Data, including its appointment of Payscale as a subprocessor, have been authorized by the respective Controller.

(d) To the extent Payscale uses or otherwise processes Customer Personal Data subject to Data Protection Laws for business operations incident to providing the Payscale Offering to Customer, Payscale will comply with the obligations of an independent data controller under Data Protection Laws for such use ("**Payscale Business Purposes**"). Examples of such uses include but are not limited to marketing and communications regarding Customer accounts, billing, collections, security, fraud detection and prevention, operating and improving the Payscale offering, and other business purposes authorized by Data Protection Laws.

2.2 Data Processing Details: Payscale will process Customer Personal Data for the purpose of, and as necessary to, provide the Payscale Offering described in the Agreement, including information as set forth in **Exhibit 1**.

2.3 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. Payscale will promptly notify Customer in writing, and in any case within ten (10) business days, if Payscale receives (i) any requests from a data subject, with respect to Customer Personal Data Processed by Payscale, including individual opt-out requests, requests for access and/or deletion and all similar individual rights requests; or (ii) any complaint or inquiry relating to the Processing of Customer Personal Data, including allegations that the Processing infringes any individual's or third party's rights. Payscale will not respond to any such request or complaint unless expressly authorized to do so by Customer or required to respond under applicable Data Protection Laws.

2.4 Customer Instructions. Payscale shall use, retain, and disclose Customer Personal Data only as necessary for the specific business purpose of providing the Payscale Offering and in accordance with Customer's instructions including as described in the Agreement. Payscale shall not sell Customer Personal Data, nor use, retain, or disclose Customer Personal Data outside of its business relationship with the Customer or for any other purpose except as required by law. If Payscale is compelled to do so by applicable law, it shall inform the Customer of that legal requirement before complying, unless providing such notice is prohibited by law. The terms of the Agreement 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 DPA 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 any additional mutually agreed upon fees. Payscale will inform Customer if, in Payscale's reasonable opinion, any of Customer's instructions infringes applicable Data Protection Laws.

2.5 Data Protection Compliance Assistance

(a) Payscale certifies that it shall comply at all times with and, at Customer's expense, reasonably assist Customer in complying with its obligations under the applicable Data Protection Laws, including without

limitation, conducting data protection impact assessments, and any consultations with the supervisory or regulatory authority.

(b) Payscale shall not perform its obligations under this Agreement in such a way as to cause Customer to breach any of its obligations under applicable Data Protection Laws.

2.6 Sub-processing

(a) **General Authorization**. Customer hereby authorizes and agrees that Payscale may use Subprocessors engaged by Payscale to perform its obligations under this DPA and the Agreement or to provide certain services on Payscale's behalf, such as database storage. Payscale will impose by way of contract on its Subprocessors the same (or substantially similar) data protection obligations as set out in this DPA and the Agreement, and Payscale remains responsible for the Processing activities of its Subprocessors.

(b) **Subprocessor List**. The Subprocessors that are currently authorized to access and Process Customer Personal Data are listed at https://www.Payscale.com/content/legal/Payscale-GDPR-Subprocessor-List.pdf. Customer may request the then-current Subprocessor list by submitting a request to privacy@payscale.com.

(c) **New or Replacement Subprocessors**. Payscale will send an electronic prior notice to Customer's then-current Account administrator of any intended addition or replacement of Subprocessors and allow Customer to reasonably object to such changes by notifying Payscale in writing within thirty (30) days of receipt of Payscale's notice of an addition or replacement of a Subprocessor. 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 Subprocessor with regard to Customer Personal Data or will offer an alternative to provide the Payscale Offering without such Subprocessor;

(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 Subprocessor 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 Subprocessor 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.

(iv) 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 thirty (30) days of 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 sixty (60) days after it was raised by Customer, and Payscale has not received any notice of termination from Customer, Customer will be deemed to have accepted the new or replacement Subprocessor.

(d) **Emergency Subprocessor Replacement.** Notwithstanding Section 2.6(c) above, Payscale may change a Subprocessor where the reason for the change is outside of Payscale's reasonable control. In this case, Payscale will inform Customer of the replacement Subprocessor as soon as possible. Customer retains its right to object to a replacement Subprocessor under Section 2.6(c) above.

3. Security Standards

3.1 Payscale Responsibilities. Payscale has developed and implemented, and will maintain, monitor, and use appropriate administrative, technical, physical, and organizational security measures, safeguards, procedures, and practices designed to protect the Customer Data against Security Incidents, enumerated at **Exhibit 2**.

(a) Payscale also performs appropriate training for its personnel regarding security and confidentiality of Customer Data.

(b) Payscale also ensures that persons authorized to process Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.2 Customer Responsibilities. Customer understands and agrees that Customer is solely responsible for its own actions in the relevant Payscale Offering, and Customer will keep its Account passwords and login information confidential, and it will be responsible for all activity and payments owed under its Account.

4. Data Processing Location and Data Transfers.

(a) As of the date this DPA was last updated, Customer Personal Data in the Payscale Offering is Processed in Payscale Networks in the following locations: the United States, the United Kingdom, and Canada. Processing operations may also occur in the Philippines, Australia, Ireland, and Singapore as required to provide the Services. Payscale will not Process such Customer Personal Data on Payscale Networks outside of these locations without Customer's knowledge and written authorization (where Customer authorization received by email or other electronic means is acceptable). In the event a Payscale Network becomes available outside the United States ("**New Payscale Network Location**"), Payscale will provide Customer with the ability to select the New Payscale Network Location for Payscale to Process Customer Personal Data in.

(b) Subject to its obligations under this DPA, Payscale may Process Customer Personal Data in various jurisdictions in which it operates, provided Payscale cooperates with Customer to comply with applicable data transfer restrictions and obligations required by applicable Data Protection Laws.

(c) With regard to Customer Personal Data subject to any Data Protection Laws of any country, region, or territory requiring a mechanism for valid transfer of Personal Data to a third country (such countries, regions, or territories, "**Limited Data Countries**" or "**Limited Data Country**" and such data "**Limited Transfer Data**"), Payscale may not receive and Process such Limited Transfer Data (and shall not authorize any third party to receive or transfer Limited Transfer Data on its behalf) from such Limited Transfer Countries unless it takes such measures to provide adequate protection for the Limited Transfer Data consistent with the requirements of the applicable Data Protection Laws of such Limited Transfer Countries. Such measures may include:

- **(i)** Processing in a country, a territory or one or more specified sectors that are considered by the European Commission or such other relevant data authority or applicable Data Protection Laws of such Limited Transfer Countries as providing an adequate level of data protection;
- **(ii)** The parties' agreement to enter in to and comply with the Standard Contractual Clauses in **Exhibit 3** (for transfers out of the European Economic Area) and/or **Exhibit 4** (for transfers out of the UK) and/or **Exhibit 5** (for transfers out of Switzerland) and any successors or amendments to such clauses or such other applicable contractual terms adopted and approved under Data Protection Laws of Limited Transfer Countries with respect to that Processing;
- **(iii)** Receiving or transferring European Economic Area ("**EEA**") data in accordance with applicable Data Protection Laws in the EEA; or
- **(iv)** Implementing any other data transfer mechanisms approved under applicable Data Protection Laws.

(d) To the extent that any substitute or additional appropriate safeguards under any applicable Data Protection Laws of Limited Transfer Countries are required to transfer data from a Limited Transfer Country, as applicable, to any third country, the parties agree to implement the same as soon as practicable and document such requirements for implementation in an attachment to this DPA governing the parties' Processing of Limited Transfer Data.

5. Incident Response Plan

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

5.1 Security Incidents. In the event of a material Security Incident, Payscale will: (a) without undue delay, and in no event more than seventy-two (72) hours, notify Customer of such Security Incident promptly upon discovery thereof, and (b) promptly take appropriate steps to investigate, mitigate, and remedy the Security Incident. For the purposes of clarity, a Security Incident will *not* be considered material if such Security Incident does not actually impact or compromise the security of Customer Personal Data. Examples of non-material Security Incidents include without limitation 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. Customer agrees that only material Security Incidents are subject to the requirements of this Section 5. In addition, Payscale's cooperation or obligation to report or respond to Security Incidents under this DPA 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.

5.2 Payscale Cooperation. In connection with any material Security Incident, Payscale will reasonably cooperate with Customer in connection with: (a) making available to Customer full details as may be available to Payscale relating to the Security Incident; (b) Customer's investigation of the Security Incident; (c) actions reasonably necessary or required for Customer to mitigate resulting harm; and (d) fulfilling Customer's obligations to notify the relevant supervisory authority and individuals affected by the Security Incident in accordance with applicable Data Protection Laws.

5.3 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. If Payscale is compelled to do so by applicable law, it shall inform the Customer of that legal requirement before complying, unless providing such notice is prohibited by law. Further, subject to Payscale's legal obligations, 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 individuals, and the nature and extent of any such remediation. Upon confirmation of a material 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 as required by Data Protection Laws.

6. Audit Rights

6.1 Audits.

(a) Upon written request from the Customer, Payscale shall make available to the Customer once a year such information as is reasonably required by the Customer to demonstrate Payscale's compliance with its obligations under this DPA (including its annual SOC 2 Type II certification, or equivalent or successor attestations or certifications) (together, "**Payscale Security Documentation**"). If the Payscale Security Documentation is not considered sufficient in Customer's reasonable opinion to demonstrate Payscale's compliance with its obligations under this Agreement, then to the extent required under applicable Data Protection Laws, Payscale will comply with Customer's request for additional information (for example through completing a reasonable questionnaire provided by Customer or a third party acting on Customer's behalf, each a "**Questionnaire**,"), regarding Payscale's compliance with this DPA. The work required by Payscale to complete any such request for additional information beyond addressing gaps or specifically identified deficiencies in the Payscale Security Documentation 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 request, it will notify Customer and the parties will mutually agree upon any additional fees to be paid by Customer.

(b) If the Customer in its reasonable opinion determines that the information provided under subsection (a) is (i) not sufficient and (ii) required under applicable Data Protection laws, Payscale will allow the Customer or a third party acting on behalf of the Customer to conduct Audits solely as necessary to fulfill Customer's obligations under Data Protection Laws no more than once annually.

(c) Any such Audit under subsection (b) will occur only after Customer has provided Payscale with at least sixty (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. Individuals responsible for conducting such Audit shall be subject to a contract of confidentiality with Payscale. The work required by Payscale to participate in any Audit beyond addressing gaps or specifically identified deficiencies in the Payscale Security Documentation 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. If the Audit reveals any vulnerability or inadequacy, Payscale shall correct any such vulnerability or inadequacy at its sole cost and expense.

(d) Without limiting the foregoing, Customer may request completion of a Questionnaire or an Audit more than once in any 12-consecutive month period following a material Security Incident.

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 DPA. Any information disclosed in connection with a Questionnaire or Audit will be deemed Payscale's Confidential Information.

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 applicable law and the terms of the Agreement, for up to thirty (30) days following the end of the Subscription Term and following Customer's written request to Payscale, 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 Payscale Offering if: (a) Customer is in compliance with its obligations under the Agreement; 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. For the avoidance of doubt, if any assistance is required by Customer from Payscale beyond this Section 7.1, Customer will pay Payscale its then-current rates for such assistance.

7.2 Deletion by Payscale. Following Customer's written request, Payscale will delete Customer Personal Data then-stored in the Payscale Offering 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 compliance with any legal obligations; 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 will remain subject to the terms of 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 such party. Each party's liability under this DPA 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) the limitation of liability provision in Section 12.1 of the Agreement will apply to indemnity obligations by either party for any claims relating to this DPA or Data Protection Laws, notwithstanding Section 12.2(a) of the Agreement.

9. Miscellaneous. The parties agree that this DPA will replace any existing data processing agreement the parties may have previously entered into in connection with the Payscale Offering. Any claims against Payscale or its Affiliates under this DPA may only be brought by the Customer entity that is a party to the Agreement. In no event shall this DPA or any party restrict or limit the rights of any data subject or of any competent supervisory authority. This DPA 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 DPA, the Agreement remains in full force and effect. In the event of a direct conflict between the Agreement and this DPA, the terms of this DPA will control.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

EXHIBIT 1

DATA PROCESSING DETAILS

Subject matter of the Processing of Customer Personal Data.

The subject matter of the Processing of Customer Personal Data is as described in the Agreement and in connection with Customer's provision of Personal Data to Payscale in connection with the Payscale Offering.

Duration of the Processing of Customer Personal Data.

Subject to the terms of this DPA and the Agreement and as determined by Customer, but generally the period Customer subscribes to the Payscale Offering.

The nature and purpose of the Processing of Customer Personal Data.

To deliver the Payscale Offering for Customer as detailed in the Agreement.

The types of Customer Personal Data to be Processed.

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.

The Types of Sensitive Customer Personal Data to be Processed.

None. 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.

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

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.

The frequency of the transfer of Customer Personal Data from Customer to Service Provider.

Continuous.

Location of Processing of Personal Data by Service Provider.

As of the date this DPA 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, Canada, and the United Kingdom. Processing operations may also occur in the Philippines, Australia, Ireland, and Singapore as required to provide the Services. Payscale will not otherwise Process such Customer Personal Data outside of these locations

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

without Customer's knowledge and authorization (where Customer authorization received by email or other electronic means is acceptable).

The obligations and rights of Customer.

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

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

EXHIBIT 2

SECURITY MEASURES

Payscale will maintain appropriate administrative, physical, and technical safeguards for the protection of the security and integrity of Customer Data as set forth in the Security Addendum located at https://www.payscale.com/content/legal/sa.pdf and referenced at Section 9 of the Agreement.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

EXHIBIT 3

EU STANDARD CONTRACTUAL CLAUSES

The parties agree that Limited Transfer Data transferred between and among the parties shall be subject to the Standard Contractual Clauses to the extent applicable.

(A) The parties acknowledge the importance of the protection of Personal Data and the legal restrictions on international transfers of Personal Data.

(B) Accordingly, the parties agree to abide by the GDPR, UK DPA 2018, and Swiss Addendum, and other applicable Data Protection Laws of Limited Transfer Regions recognizing the Standard Contractual Clauses or similar principles, as applicable, and enter into these standard contractual clauses to ensure that Customer Personal Data transfers outside any Limited Transfer Regions to any third country other than a country, region, or territory that the relevant data authority has determined to offer an adequate level of data protection are lawful and subject to adequate data protections. To the extent Customer Personal Data is not subject to Article 3(2) of the GDPR, or similar provisions of Data Protection Laws of Limited Transfer Regions, this Exhibit 3 shall not apply.

1. CLARIFICATION OF DEFINITIONS & TERMS

(A) The terms “data controller” or “controller,” “data exporter,” “data importer,” “data processor” and “Personal Data” shall have the meaning under the GDPR, UK Addendum 2018, Swiss Addendum, or applicable Data Protection Laws of Limited Transfer Regions as applicable.

(B) For Limited Transfer Regions outside the EU, references to the General Data Protection Regulation will be replaced by applicable Data Protection Laws of the respective Limited Transfer Regions and for Clauses 13, 17 and 18, references to EU Member State shall be replaced with the applicable Limited Transfer Region.

(C) Section 1 Clause 1 (a) of the Standard Contractual Clauses (Definition of Data Importer): The “data importer” means Service Provider.

(D) Section 1 Clause 1 (a) of the Standard Contractual Clauses (Definition of Data Exporter): The “data exporter” means Customer.

(E) With respect to objections to Sub-processors under Section 1 Clause 9, the parties will work together to find a mutually acceptable resolution to such objection, and if unsuccessful, Customer’s sole remedy is termination of the relevant Services under the terms of the Agreement

2. APPLICABLE MODULES

With respect to Processing of Customer Personal Data,

A. When Customer is a Data Exporter and Controller, and Service Provider is a Data Importer and Processor - Module 2 shall apply.
B. When Customer is a Data Exporter and Processor, and Service Provider is a Data Importer and Processor, Module 3 shall apply.
C. References to Modules 1 and 4 in the Standard Contractual Clauses shall not apply and language referencing these modules shall not be treated as part of this Agreement.

3. AMENDMENTS OR UPDATES

The parties agree that to the extent that any additional appropriate safeguards under Data Protection Laws of Limited Transfer Regions recognizing the Standard Contractual Clauses or similar principles are required to export data to any third country, or to the extent that the Standard Contractual Clauses are substituted or replaced or not recognised under any such law, the parties agree to either promptly implement the same or

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

agree to use another acceptable method for transfer of such data and promptly amend this Exhibit 3 as necessary to comply with such requirements.

4. CONFLICTS

If the terms of the Agreement conflict with the Standard Contractual Clauses, the terms of the Standard Contractual Clauses will prevail.

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1 - Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 - Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 - Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – *Module One*: Clause 8.5 (e) and Clause 8.9(b); *Module Two*: Clause 8.1(b), 8.9(a), (c), (d) and (e); *Module Three*: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); *Module Four*: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – *Module Two*: Clause 9(a), (c), (d) and (e); *Module Three*: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – *Module One*: Clause 12(a) and (d); *Modules Two and Three*: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – *Modules One, Two and Three*: Clause 18(a) and (b); *Module Four*: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 - Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 - Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 - Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 - Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE ONE: Transfer controller to controller

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation[2] of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union[3] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

---

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.[5]

8.2 Purpose limitation

[5] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach

(including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[6] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

[6] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE FOUR: Transfer processor to controller

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data,7 the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter

[7] This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9 - Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION: The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[8] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) ***OPTION 2: GENERAL WRITTEN AUTHORISATION*** The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-

[8] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.9 The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 - Data subject rights

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[10] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

---

[9] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[10] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation

(EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11 - Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 - Liability

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 - Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) [***Where the data exporter is established in an EU Member State***:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[***Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a***

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[***Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679***:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 - Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;11

[11] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [***For Module Three***: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [***for Module Three***:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [***for Module Three***: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 - Obligations of the data importer in case of access by public authorities

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

---

frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[***For Module Three***: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [***For Module Three***: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [***For Module Three***: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 - Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [***for Module Three***: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [***For Modules One, Two and Three***: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [***For Module Four***: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 - Governing law

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

[***OPTION 2 (for Modules Two and Three)***: These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of __Ireland__ (***specify Member State***).]

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (***specify country***).

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

Clause 18 - Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of __Ireland__ (***specify Member State***).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts of _____ (***specify country***).

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

APPENDIX

*EXPLANATORY NOTE: It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be use*d.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

ANNEX I

DATA PROCESSING DETAILS

A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Data exporter(s):

Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: See Exhibit 1.

Signature and date: See signature and date of the DPA.

Role (controller/processor): Controller

Data importer(s):

Name: Payscale

Address: 113 Cherry St., Suite 96140, Seattle, WA 98104 USA

Contact person's name, position and contact details: Kristin Boraas, General Counsel, legal@payscale.com

Activities relevant to the data transferred under these Clauses: See Exhibit 1.

Signature and date: See signature and date of the DPA.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred.

See Exhibit 1.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

Categories of personal data transferred.

See Exhibit 1.

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

See Exhibit 1.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

See Exhibit 1.

Nature of the processing.

See Exhibit 1.

Purpose(s) of the data transfer and further processing.

See Exhibit 1.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.

See Exhibit 1.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing.

See Section 2.6 of the DPA and Exhibit 1.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13.

The Republic of Ireland.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

ANNEX II

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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE: The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

The description of technical and organization measures designed to ensure the security of Customer Personal Data is described more fully in Exhibit 2 of this DPA.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

The description of technical and organization measures designed to ensure the security of Personal Data is described more fully in Exhibit 2 of this DPA.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

ANNEX III

LIST OF SUB-PROCESSORS

See Section 2.6 of the DPA.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

EXHIBIT 4

UK ADDENDUM TO THE EU STANDARD CONTRACTUAL CLAUSES

The parties agree that Limited Transfer Data transferred between and among the parties shall be subject to this Exhibit to the extent applicable.

1. BACKGROUND

   The Information Commissioner has published a form of this Exhibit for public consultation as providing appropriate safeguards for the purposes of transfer of personal data to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and, with respect to data transfer from controllers to processors and/or processors to processors.

2. CLARIFICATION OF DEFINITIONS & TERMS

   Where this Exhibit uses terms that are defined in the Clauses – attached hereto as Exhibit 3 – those terms shall have the same meaning as in the Clauses. In addition, the following terms have the following meanings:

   A. "**UK Data Protection Laws**" means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
   B. "**UK GDPR**" means the United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.
   C. "**UK**" means the United Kingdom of Great Britain and Northern Ireland.

3. INTERPRETATION

   A. This Exhibit shall be read and interpreted in light of the provisions of UK Data Protection Laws, and so that it fulfils the intention for it to provide the appropriate safeguards as required by Article 46 of the GDPR.
   B. This Exhibit shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.
   C. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Exhibit has been entered into.

4. HIERARCHY

   In the event of a conflict or inconsistency between this Exhibit and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Exhibit is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

5. INCORPORATION OF THE CLAUSES
    A. This Exhibit incorporates the Clauses which are deemed to be amended to the extent necessary so that they operate:
        a. For transfer made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that transfer; and
        b. To provide appropriate safeguards for transfers in accordance with Article 46 of the UK GDPR.
    B. The amendments required by this Section 5 include, without limitation:
        a. References to the "Clauses" means this Exhibit as it incorporates the Clauses.
        b. Clause 6 Description of the transfer(s) is replaced with:

            "The details of the transfer(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer."

        c. References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws.
        d. References to Regulation (EU) 2018/1725 are removed.
        e. References to the "Union", "EU" and "EU Member State" are all replaced with the "UK."
        f. Clause 13(a) and Part C of Annex II are not used; the "competent supervisory authority" is the Information Commissioner;
        g. Clause 17 is replaced to state "These Clauses are governed by the laws of England and Wales".
        h. Clause 18 is replaced to state:
        "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."
        i. The footnotes to the Clauses do not form part of this Exhibit.

6. AMENDMENTS
    A. The Parties may agree to change Clause 17 and/or 18 to refer to the laws and/or courts of Scotland or Northern Ireland.
    B. The Parties may amend this Addendum provided it maintains the appropriate safeguards required by Art 46 UK GDPR for the relevant transfer by incorporating the Clauses and making changes to them in accordance with Section 4 above.

7. EXECUTION
    The Parties may enter into this Exhibit incorporating the Clauses in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in the Clauses. This includes without limitation amendment of the Clauses in accordance with this Exhibit, and executing those amended Clauses.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

EXHIBIT 5

SWISS ADDENDUM TO THE EU STANDARD CONTRACTUAL CLAUSES

The parties agree that Limited Transfer Data transferred between and among the parties shall be subject to this Exhibit to the extent applicable. Certain adaptations to the Clauses are necessary in order to comply with Swiss legislation and thus provide an adequate level of protection for data transfers from Switzerland to a third country in accordance with Article 6 paragraph 2 letter a FADP.

1. BACKGROUND

   The Swiss Federal Data Protection and Information Commissioner ("**FDPIC**") has recognized the EU Standard Contractual Clauses as standard clauses under FADP.

2. INTERPRETATION

   A. Neither the Clauses nor this Exhibit shall be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18c.
   B. The Clauses are to be understood to also protect the data of legal entities until the entry into force of the revised FADP.
   C. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Exhibit has been entered into.

3. HIERARCHY

   In the event of a conflict or inconsistency between this Exhibit and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Exhibit is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

4. AMENDMENTS
   A. The Parties may agree, as required, to change Clause 17 and/or 18 to refer to the laws and/or courts of Switzerland (where FDPIC will be the competent supervisory authority) or another country that allows and grants rights as a third party beneficiary for contractual claims regarding data transfers pursuant to the FADP.
   B. The Parties may amend this Addendum provided it maintains the appropriate safeguards required by applicable Data Protection Laws for the relevant transfer by incorporating the Clauses and making changes to them in accordance with Section 4 above.

5. EXECUTION
   The Parties may enter into this Exhibit incorporating the Clauses in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in the Clauses. This includes without limitation amendment of the Clauses in accordance with this Exhibit, and executing those amended Clauses.

DocuSign Envelope ID: CAD8B452-5EC3-4D84-9554-4A43F20E656D

Annex D

INSURANCE ADDENDUM

This Insurance 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 Services ("**Agreement**"). Capitalized terms used in this Addendum and not defined shall have the meanings given to such terms in the Agreement.

1. Insurance Coverage. Payscale maintains, at its own expense and the following insurance coverage minimums, which shall apply throughout the Subscription Term:

1.1 Commercial General Liability. Commercial General Liability coverage, with the following limits:
- (i) $1,000,000 - Each Occurrence
- (ii) $1,000,000 - Personal and Advertising Injury
- (iii) $2,000,000 - General Aggregate
- (iv) $2,000,000 - Products and Completed Operations Aggregate

1.2 Statutory Workers' Compensation and Employers' Liability. Workers' Compensation Liability coverage with statutory limits, as required by the states having jurisdiction over Payscale's employees, and Employer's Liability coverage with the following limits:
- (i) $1,000,000 - Each Accident
- (ii) $1,000,000 - Each Employee (disease)
- (iii) $1,000,000 - Policy Limit (disease)

1.3 Errors & Omissions and Cyber Liability. Errors & Omissions (Professional Liability) and Cyber Liability coverage, written together, with a $10,000,000 - per claim-aggregate limit.

1.4 First and Third-Party Crime Liability. First and Third-Party Crime Liability coverage with a $500,000 - per claim-aggregate limit.

1.5 Umbrella Liability. Umbrella Liability coverage, written on an occurrence basis, with a $5,000,000 - per claim-aggregate limit.

2. ADDITIONAL INSURANCE PROVISIONS AND ENDORSEMENTS.

2.1 Additional Insured. Upon Customer's email request to finance@payscale.com, Customer shall be named as an additional insured on Payscale's Commercial General Liability and Umbrella Liability coverage.

2.2 Primary and Non-Contributory. Payscale's Commercial General Liability and Worker's Compensation coverages are primary and non-contributory.