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

1.2 “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 Privacy 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.

1.3 “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.

1.4 “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.

1.5 “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.

1.6 “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.

1.7 “Subprocessor” means any person or entity engaged by Payscale to help provide the Payscale Offering, and that Processes Customer Personal Data.

1.8 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.
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.

The parties acknowledge and agree that between Payscale and Customer, Payscale is a Data Processor and Service Provider 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.

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 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 [http://www.payscale.com/about/data-protection/payscales-sub-processors](http://www.payscale.com/about/data-protection/payscales-sub-processors). To receive automated notifications of any change to this list, Customer may subscribe using the form at the bottom of the page linked in this Section 2.6(b).

(c) **New or Replacement Subprocessors.** Payscale will send an electronic prior notice to the email address(es) of Customer’s choosing 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, Israel, India, and Singapore as required to provide the Services. Payscale will not Process such Customer Personal Data on Payscale Networks outside of these locations without prior notice to Customer. 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 into 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**

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.

---

**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, Israel, India, and Singapore as required to provide the Services. Payscale will not otherwise Process such Customer Personal Data outside of these locations without prior notice to Customer.

**The obligations and rights of Customer.**
The obligations and rights of Customer are set out in the Agreement and this DPA.
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 http://www.payscale.com/content/legal/sa.pdf and referenced at Section 9 of the Agreement.
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 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.

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

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.
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.

(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 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.

\(^2\) 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.
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.

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.

---

\(^3\) 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.
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 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 Union4 (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;

(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.

---

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.
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

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

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.
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.

(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.

---

\(^6\) 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.
(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 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.

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.
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. 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-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. 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.

---

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

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

(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:

---

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.
(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.

(c) 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 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 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

(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

---

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-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.
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:

(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.
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).

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).
ANNEX I

DATA PROCESSING DETAILS

A. LIST OF PARTIES

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

Categories of data subjects whose personal data is transferred.
See Exhibit 1.

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

Identify the competent supervisory authority/ies in accordance with Clause 13.
The Republic of Ireland.
ANNEX II

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

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.
ANNEX III

LIST OF SUB-PROCESSORS

See Section 2.6 of the DPA.
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.

BACKGROUND

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

PART 1: TABLES

Table 1: Parties

<table>
<thead>
<tr>
<th>Start date</th>
<th>Date of the Agreement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The Parties</strong></td>
<td>Exporter (who sends the Restricted Transfer)</td>
</tr>
<tr>
<td><strong>Parties’ details</strong></td>
<td>Full legal name: See Annex I to Exhibit 3. Trading name (if different): Main address (if a company registered address): See Annex I to Exhibit 3.</td>
</tr>
<tr>
<td><strong>Signature (if required for the purposes of Section 2)</strong></td>
<td>See signature page of DPA.</td>
</tr>
</tbody>
</table>

Table 2: Selected SCCs, Modules and Selected Clauses

<table>
<thead>
<tr>
<th>Addendum EU SCCs</th>
<th>□ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date: Reference (if any): Other identifier (if any): Or</td>
<td></td>
</tr>
</tbody>
</table>
the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

<table>
<thead>
<tr>
<th>Module</th>
<th>Module in operation</th>
<th>Clause 7 (Docking Clause)</th>
<th>Clause 11 (Option)</th>
<th>Clause 9a (Prior Authorization or General Authorization)</th>
<th>Clause 9a (Time period)</th>
<th>Is personal data received from the Importer combined with personal data collected by the Exporter?</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Module Two (Controller to Processor)</td>
<td>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 1.A</td>
<td>Optional language in Clause 11 shall not apply.</td>
<td>General Authorization</td>
<td>30 days</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Table 3: Appendix Information

“Appendix Information” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As described in Annex I to the Exhibit 3 of this Addendum.
Annex 1B: Description of Transfer: As described in Annex I to the Exhibit 3 of this Addendum.
Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: As described in Annex II to the Exhibit 3 of this Addendum.
Annex III: List of Subprocessors (Modules 2 and 3 only): As described in Annex III to the Exhibit 3 of this Addendum.

Table 4: Ending this Addendum when the Approved Addendum Changes

<table>
<thead>
<tr>
<th>Ending this Addendum when the Approved Addendum changes</th>
<th>Which Parties may end this Addendum as set out in Section 19:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>☑ Importer</td>
</tr>
<tr>
<td></td>
<td>☑ Exporter</td>
</tr>
<tr>
<td></td>
<td>☐ neither Party</td>
</tr>
</tbody>
</table>
PART 2: MANDATORY CLAUSES

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

<table>
<thead>
<tr>
<th>Addendum</th>
<th>This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addendum EU SCCs</td>
<td>The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.</td>
</tr>
<tr>
<td>Appendix Information</td>
<td>As set out in Table 3.</td>
</tr>
<tr>
<td>Appropriate Safeguards</td>
<td>The standard of protection over the personal data and of data subjects’ rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.</td>
</tr>
<tr>
<td>Approved Addendum</td>
<td>The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.</td>
</tr>
<tr>
<td>ICO</td>
<td>The Information Commissioner.</td>
</tr>
<tr>
<td>Restricted Transfer</td>
<td>A transfer which is covered by Chapter V of the UK GDPR.</td>
</tr>
<tr>
<td>UK</td>
<td>The United Kingdom of Great Britain and Norther Ireland.</td>
</tr>
<tr>
<td>UK Data Protection Laws</td>
<td>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.</td>
</tr>
<tr>
<td>UK GDPR</td>
<td>As defined in section 3 of the Data Protection Act 2018.</td>
</tr>
</tbody>
</table>

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties’ obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. 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 Addendum has been entered into.

Hierarchy
9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
   a. Together they operate for data transfers 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 data transfer, and they provide Appropriate Safeguards for those data transfers;
   b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
   c. This Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
   a. References to the “Clauses” means this Addendum, incorporating the Addendum EU SCCs;
   b. In clause 2, delete the words:
      “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”;
   c. 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.”;
   d. Clause 8.7(i) of Module 1 is replaced with:
      “it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;
   e. Clause 8.8(i) of Modules 2 and 3 is replaced with:
      “the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that cover the onward transfer;”
   f. References to “Regulation (EU) 2016/679”, “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)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;
   g. References to Regulation (EU) 2018/1725 are removed;
   h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;
   i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;
   j. Clause 13(a) and Part C of Annex I are not used;
   k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
l. In Clause 16(e), subsection (i) is replaced with:
   “the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018
   that cover the transfer of personal data to which these clauses apply;”;

m. Clause 17 is replaced with:
   “These Clauses are governed by the laws of England and Wales.”;

n. Clause 18 is replaced with:
   “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.”; and

o. The footnotes to the Approve EU SCCs do not form part of the Addendum, except for footnotes 8,
9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or
courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved
Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce
the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:
   a. Makes reasonable and proportionate changes to the Approved Addendum, including correcting errors
      in the Approved Addendum; and/or
   b. Reflects change to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved
Addendum are effective and whether the Parties need to review this Addendum including the Appendix
Information. This Addendum is automatically amended as set out in the revised Approved Addendum from
the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending
the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the
Approved Addendum have a substantial, disproportionate and demonstrable increase in:
   a. Its direct costs of performing its obligations under the Addendum; and/or
   b. Its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial
and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by
providing written notice for that period to the other Party before the start date of the revised Approved
Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes
must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses

<table>
<thead>
<tr>
<th>Mandatory clauses</th>
<th>Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.</th>
</tr>
</thead>
</table>
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.

BACKGROUND

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

INTERPRETATION

1. 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.
2. The Clauses are to be understood to also protect the data of legal entities until the entry into force of the revised FADP.
3. 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.

HIERARCHY

4. 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.

AMENDMENTS

5. 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.
6. 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.

EXECUTION

7. 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.