Upwork Global Data Processing Agreement

Last modified: **October 7, 2021**

The Client agreeing to these terms ("**Customer**"), and Upwork Global Inc. or any other entity that directly or indirectly controls, is controlled by, or is under common control with Upwork Global Inc. (as applicable, "**Upwork**") (each, a "party" and collectively, the "parties"), have entered into an agreement under which Upwork has agreed to provide a marketplace where Clients and Freelancers can identify each other and advertise, buy, and sell Freelancer Services online, with such other services, if any, described in the agreement (the "**Service**") to Customer (as amended from time to time, the "**Agreement**").

Unless otherwise agreed to in writing by you and Upwork, to the extent Upwork processes any EU personal data for you as a controller (as defined by the General Data Protection Regulation (EU) 2016/679) in your role as a Customer as defined in this Global Data Processing Agreement (the "**DPA**"), this DPA applies. This DPA, including its appendices, supplements the Agreement. To the extent of any conflict or inconsistency between this DPA and the remaining terms of the Agreement, this DPA will govern.

1. Introduction

This DPA reflects the parties' agreement with respect to the processing and security of Customer Data under the Agreement.

2. Definitions

2.1 The terms "**personal data**", "**data subject**", "**processing**", "**controller**", "**processor**" and "**supervisory authority**" have the meanings given in the GDPR, and the terms "**data importer**" and "**data exporter**" have the meanings given in the Standard Contractual Clauses, in each case irrespective of whether the European Data Protection Legislation or Non-European Data Protection Legislation applies.

2.2 Unless stated otherwise:

- "**Affiliate**" means any entity that controls or is under common control with a specified entity.
- "**Agreed Liability Cap**" means the maximum monetary or payment-based amount at which a party's liability is capped under the Agreement.

- "**Confidential Information**" means any information or materials (regardless of form or manner of disclosure) that are disclosed by or on behalf of one party to the other party that (i) are marked or communicated as being confidential at or within a reasonable time following such disclosure; or (ii) should be reasonably known to be confidential due to their nature or the circumstances of their disclosure. The term "Confidential Information" does not include any information or materials that: (a) are or become generally known or available to the public through no breach of this Agreement or other wrongful act or omission by the receiving party; (b) were already known by the receiving party without any restriction; (c) are acquired by the receiving party without restriction from a third party who has the right to make such disclosure; or (d) are independently developed by or on behalf of the receiving party without reference to any Confidential Information.
- "**Customer Account Data**" means personal data that relates to Customer's relationship with Upwork, including the names and/or contact information of individuals authorized by Customer to access Customer's Upwork account and billing information of individuals that Customer has associated with its Upwork account.
- "**Customer Data**" means the data entered into the Service by or on behalf of any End User, but excludes Customer Account Data.
- "**End User**" means an authorized user of the Service under Customer's account.
- "**Customer Personal Data**" means the personal data contained within the Customer Data.
- "**Data Incident**" means a breach of Upwork's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Upwork. "Data Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
- "**EEA**" means the European Economic Area, Switzerland, and/or the United Kingdom.
- "**European Data Protection Legislation**" means, as applicable: (a) the GDPR and its respective national implementing legislations; (b) the Federal Data Protection Act of 19 June 1992 (Switzerland); and/or the United Kingdom Data Protection Act 2018.
- "**GDPR**" means 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, and repealing Directive 95/46/EC.
- "**New EU SCCs**" means the Standard Contractual Clauses issued pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 *on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, completed as set forth in Appendix 3 to this DPA.

- “**Non-European Data Protection Legislation”** means, as applicable, the data protection or privacy laws, regulations, and other legal requirements other than the European Data Protection Legislation.
- “**Notification Email Address**” means the contact email address that you provided to Upwork for the purpose of receiving notices from Upwork.
- “**Old EU SCCs**” means the Standard Contractual Clauses issued pursuant to EU Commission Decision of 5 February 2010 *on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council* (available as of the Effective Date at http://data.europa.eu/eli/dec/2010/87/2016-12-17).
- “**Security Measures**” has the meaning given in Section 7.1.1 (Upwork’s Security Measures).
- **“Standard Contractual Clauses"** means the New EU SCCs or the Old EU SCCs, as applicable.
- “**Subprocessors**” means third parties authorized under this DPA to have logical access to and process Customer Data in order to provide parts of the Service. For clarity, freelancers that clients engage via Upwork are not Subprocessors under this DPA.
- “**Term**” means the period from the DPA’s effective date until the end of Upwork’s provision of the Service, including, if applicable, any period during which provision of the Service may be suspended and any post-termination period during which Upwork may continue providing the Service for transitional purposes.

3. Duration of this DPA

This DPA will remain in effect until, and automatically expire upon, deletion of all Customer Data by Upwork as described in this DPA.

4. Data Protection Legislation

4.1 Application of European Legislation. The parties acknowledge that the European Data Protection Legislation will apply to the processing of Customer Personal Data to the extent provided under the European Data Protection Legislation.

4.2 Application of Non-European Legislation. The parties acknowledge that Non-European Data Protection Legislation may also apply to the processing of Customer Personal Data.

5. Processing of Data

5.1 Roles and Regulatory Compliance; Authorization.

5.1.1 Processor and Controller Responsibilities. If the European Data Protection Legislation applies to the processing of Customer Personal Data, the parties acknowledge and agree that:

a. Customer is a controller (or processor, as applicable), of the Customer Personal Data under European Data Protection Legislation;
b. Upwork is a processor (or subprocessor, as applicable) of the Customer Personal Data under the European Data Protection Legislation; and
c. each party will comply with the obligations applicable to it under the European Data Protection Legislation with respect to the processing of that Customer Personal Data.

5.1.2 Responsibilities under Non-European Legislation. If Non-European Data Protection Legislation applies to either party's processing of Customer Personal Data, the parties acknowledge and agree that the relevant party will comply with any obligations applicable to it under that legislation with respect to the processing of that Customer Personal Data.

5.1.3 Authorization by Third Party Controller. If Customer is a processor, Customer warrants to Upwork that Customer's instructions (defined below) and actions with respect to that Customer Personal Data, including its appointment of Upwork as another processor, have been authorized by the relevant controller to the extent required by applicable law.

5.2 Scope of Processing.

5.2.1 The subject matter and details of the processing are described in Appendix 1.

5.2.2 Customer's Instructions. By entering into this DPA, Customer instructs Upwork to process Customer Personal Data only in accordance with applicable law: (a) to provide the Service; (b) as further specified through Customer's use of the Service; (c) as documented in the Agreement, including this DPA; and (d) as further documented in any other written instructions given by Customer and acknowledged by Upwork as constituting instructions for purposes of this DPA (each and collectively, "**Customer's Instructions**") and only for the foregoing purposes and not for the benefit of any other third party. Upwork may condition the acknowledgement described in (d) on the payment of additional fees or the acceptance of additional terms.

5.2.3 Upwork's Compliance with Instructions. With respect to Customer Personal Data subject to European Data Protection Legislation, Upwork will comply with the instructions described in Section 5.2.2 (Customer's Instructions) (including with regard to data transfers) unless EU or EU Member State law to which Upwork is subject requires other processing of Customer Personal Data by Upwork, in which case Upwork will inform Customer (unless that law prohibits Upwork from doing so on important grounds of public interest) via the Notification Email Address.

6. Data Deletion

6.1 duringthe Term in a manner consistent with the functionality of the Service. If Customer uses the Service to delete any Customer Data during the Term and that Customer Data cannot be recovered by Customer, this use will constitute an instruction to Upwork to delete the relevant Customer Data from Upwork's systems in accordance with applicable law. Upwork will comply with this instruction as soon as reasonably practicable, unless applicable law requires storage. Nothing herein requires Upwork to delete Customer Data from files created for security, backup, and business continuity purposes sooner than required by Upwork's existing data retention processes.

6.2 Deletion on Termination. On expiry of the Term, Customer instructs Upwork to delete all Customer Data (including existing copies) from Upwork's systems in accordance with applicable law. Upwork will comply with this instruction as soon as reasonably practicable, unless applicable law requires storage. Without prejudice to Section 9.1 (Access; Rectification; Restricted Processing; Portability), Customer acknowledges and agrees that Customer will be responsible for exporting, before the Term expires, any Customer Data it wishes to retain afterwards. If the Standard Contractual Clauses as described in Section 10.2 (Transfers of Data Out of the EEA) are applicable to Upwork's processing of Customer Personal Data, the parties agree that the certification of deletion referenced in Clause 12(1) of the Old EU SCCs and in Clauses 8.5 and 16(d) of the New EU SCCs shall be provided only upon Customer's written request. Nothing herein requires Upwork to delete Customer Data from files created for security, backup, and business continuity purposes sooner than required by Upwork's existing data retention processes.

7. Data Security

7.1 Upwork's Security Measures, Controls and Assistance.

7.1.1 Upwork's Security Measures. Upwork will implement and maintain technical and organizational measures designed to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (the "Security Measures"). As described in Appendix 2, the Security Measures include measures to encrypt personal data; to help ensure ongoing confidentiality, integrity, availability and resilience of Upwork's systems and services; to help restore timely access to personal data following an incident; and for regular testing of effectiveness. Upwork may update or modify the Security Measures from time to time provided that such updates and modifications do not degrade the overall security of the Service.

7.1.2 Security Compliance by Upwork Staff. Upwork will take appropriate steps to ensure compliance with the Security Measures by its staff to the extent applicable to their scope of performance, including ensuring that all such persons it authorizes to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.1.3 Upwork's Security Assistance. Customer agrees that Upwork will (taking into account the nature of the processing of Customer Personal Data and the information available to Upwork) assist Customer in ensuring compliance with any of Customer's obligations in respect of security of personal data and personal data breaches, including if applicable Customer's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by:

a. implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Upwork's Security Measures);

b. complying with the terms of Section 7.2 (Data Incidents); and

c. providing Customer with the information contained in the Agreement including this DPA.

7.2 Data Incidents

7.2.1 Incident Notification. If Upwork becomes aware of a Data Incident, Upwork will: (a) notify Customer of the Data Incident promptly and without undue delay after becoming aware of the Data Incident; and (b) promptly take reasonable steps to minimize harm and secure Customer Data.

7.2.2 Details of Data Incident. Notifications made pursuant to this section will describe, to the extent practicable, details of the Data Incident, including steps taken to mitigate the potential risks and any steps Upwork recommends Customer take to address the Data Incident.

7.2.3 Delivery of Notification. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address or, at Upwork's discretion, by direct communication (for example, by phone call or an in-person meeting). Customer is solely responsible for ensuring that the Notification Email Address is current and valid.

7.2.4 No Assessment of Customer Data by Upwork. Upwork will not assess the contents of Customer Data in order to identify information subject to any specific legal requirements. Customer is solely responsible for complying with legal requirements for incident notification applicable to Customer and fulfilling any third party notification obligations related to any Data Incident(s).

7.2.5 No Acknowledgement of Fault by Upwork. Upwork's notification of or response to a Data Incident under this Section 7.2 (Data Incidents) is not an acknowledgement by Upwork of any fault or liability with respect to the Data Incident.

7.3 Customer's Security Responsibilities and Assessment.

7.3.1 Customer's Security Responsibilities. Customer agrees that, without prejudice to Upwork's obligations under Section 7.1 (Upwork's Security Measures, Controls and Assistance) and Section 7.2 (Data Incidents):

a. Customer is solely responsible for its use of the Service, including:
   i. making appropriate use of the Service to ensure a level of security appropriate to the risk in respect of the Customer Data;
   ii. securing the account authentication credentials, systems and devices Customer uses to access the Service;
   iii. backing up its Customer Data; and
b. Upwork has no obligation to protect Customer Data that Customer elects to store or transfer outside of the Service.

7.3.2 Customer's Security Assessment.

a. Customer is solely responsible for reviewing Upwork's security processes and evaluating for itself whether the Service, the Security Measures, and Upwork's commitments under this Section 7 (Data Security) will meet Customer's needs, including with respect to any security obligations of Customer under the European Data Protection Legislation or Non-European Data Protection Legislation, as applicable.
b. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Personal Data as well as the risks to individuals) the Security Measures implemented and maintained by Upwork as set out in Section 7.1.1 (Upwork's Security Measures) provide a level of security appropriate to the risk in respect of the Customer Data.

7.4 Reviews and Audits of Compliance

7.4.1 Customer's Audit Rights.

a. If the European Data Protection Legislation applies to the processing of Customer Personal Data, Upwork will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Upwork's compliance with its obligations under this DPA in accordance with Section 7.4.2 (Additional Business Terms for Reviews and Audits). Upwork will contribute to such audits as described in this Section 7.4 (Reviews and Audits of Compliance).
b. If the Standard Contractual Clauses as described in Section 10.2 (Transfers of Data Out of the EEA) are applicable to Upwork's processing of Customer Personal Data, without prejudice to any audit rights of a supervisory authority under such Standard Contract Clauses, the parties agree that Customer or an independent auditor appointed by Customer

may conductaudits as described in Clause 5(f) and Clause 12(2) of the Old EU SCCs and in Clauses 8.9(c) and (d) of the New EU SCCs in accordance with Section 7.4.2 (Additional Business Terms for Reviews and Audits).

7.4.2 Additional Business Terms for Reviews and Audits.

a. If the European Data Protection Legislation applies to the processing of Customer Personal Data, Customer may exercise its right to audit Upwork under Sections 7.4.1(a) or 7.4.1(b): (1) where there has been a Data Incident within the previous six (6) months or there is reasonable suspicion of a Data Incident within the previous six (6) months or (2) where Customer will pay all reasonable costs and expenses incurred by Upwork in making itself available for an audit. Any third party who will be involved with or have access to the audit information must be mutually agreed to by Customer and Upwork and must execute a written confidentiality agreement acceptable to Upwork before conducting the audit.

b. To request an audit under Section 7.4.1(a) or 7.4.1(b), Customer must submit a detailed audit plan to Upwork's Privacy Contact as described in Section 12 (Privacy Contact; Processing Records) at least thirty (30) days in advance of the proposed audit date, describing the proposed scope, duration, and start time of the audit. The scope may not exceed a review of Upwork's compliance with the Standard Contractual Clauses or its compliance with the European Data Protection Legislation, in each case with respect to the Customer Data. The audit must be conducted during regular business hours at the applicable facility, subject to Upwork policies, and may not interfere with Upwork business activities.

c. Following receipt by Upwork of a request for an audit under Section 7.4.1(a) or 7.4.1(b), Upwork and Customer will discuss and agree in advance on: (i) the reasonable date(s) of and security and confidentiality controls applicable to any review of documentation; and (ii) the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit under Section 7.4.1(a) or 7.4.1(b).

d. Customer will be responsible for any fees it incurs, including any fees charged by any auditor appointed by Customer to execute any such audit.

e. Customer will provide Upwork any audit reports generated in connection with any audit under this section, unless prohibited by law. Customer may use the audit reports only to meet its regulatory audit requirements and to confirm compliance with the requirements of the Standard Contractual Clauses or European Data Protection Legislation. The audit reports, and all information and records observed or otherwise collected in the course of the audit, are Confidential Information of Upwork under the terms of theAgreement.

f. Upwork may object in writing to an auditor appointed by Customer if the auditor is, in Upwork's reasonable opinion, not suitably qualified or independent, a competitor of Upwork, or otherwise unsuitable. Any such

objection by Upwork will require Customer to appoint another auditor or conduct the audit itself.

g. Nothing in this DPA will require Upwork either to disclose to Customer or its auditor, or to allow Customer or its auditor to access:

i. any data of any other customer of Upwork;

ii. Upwork's internal accounting or financial information;

iii. any trade secret of Upwork;

iv. any information that, in Upwork's reasonable opinion, could: (A) compromise the security of Upwork systems or premises; or (B) cause Upwork to breach its obligations under applicable law or its security and/or privacy obligations to Customer or any third party; or

v. any information that Customer or its third party auditor seeks to access for any reason other than the good faith fulfilment of Customer's obligations under the Standard Contractual Clauses or European Data Protection Legislation.

7.4.3 No Modification of Standard Contractual Clauses. Nothing in this Section 7.4 (Reviews and Audits of Compliance) varies or modifies any rights or obligations of Customer or Upworkunder any Standard Contractual Clauses entered into as described in Section 10.2 (Transfers of Data Out of the EEA).

8. Impact Assessments and Consultations

Customer agrees that Upwork will (taking into account the nature of the processing and the information available to Upwork) assist Customer in ensuring compliance with any obligations of Customer in respect of data protection impact assessments and prior consultation, including if applicable Customer's obligations pursuant to Articles 35 and 36 of the GDPR, by providing the information contained in the Agreement including this DPA.

9. Data Subject Rights; Data Export

9.1 Access; Rectification; Restricted Processing; Portability. During the Term, Upwork will, in a manner consistent with the functionality of the Service, enable Customer to access, rectify and restrict processing of Customer Data, including via the deletion functionality provided by Upwork as described in Section 6.1 (Deletion by Customer), and to export Customer Data.

9.2 Data Subject Requests

9.2.1 Customer's Responsibility for Requests. During the Term, if Upwork receives any request from a data subject under European Data Protection Legislation in relation to Customer Personal Data, Upwork will advise the data subject to submit their request to Customer, and Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Service.

9.2.2 Upwork's Data Subject Request Assistance. Customer agrees that Upwork will (taking into account the nature of the processing of Customer Personal Data) reasonably assist Customer in fulfilling an obligation to respond to requests by data subjects described in Section 9.2.1 (Customer's Responsibility for Requests), including, if applicable, Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by complying with the commitments set out in Section 9.1 (Access; Rectification; Restricted Processing; Portability) and Section 9.2.1 (Customer's Responsibility for Requests).

10. Data Transfers

10.1 Data Storage and Processing Facilities. Upwork may, subject to Section 10.2 (Transfers of Data Out of the EEA), store and process the relevant Customer Data anywhere Upwork or its Subprocessors maintain facilities.

10.2 Transfers of Data Out of the EEA, UK, and Switzerland. Customer authorizes Upwork and its Subprocessors to make international transfers of Customer Personal Data in accordance with applicable law and this DPA.

10.2.1 With respect to Customer Personal Data transferred from the European Economic Area, the New EU SCCs incorporated herein shall apply, form part of this DPA, and take precedence over the rest of this DPA as set forth in the New EU SCCs.

10.2.2 With respect to Customer Personal Data transferred from the United Kingdom for which United Kingdom law (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, and such law permits use of the Old EU SCCs but not use of the New EU SCCs, the Old EU SCCs form part of this DPA and take precedence over the rest of this DPA as set forth in the Old EU SCCs, until such time that the United Kingdom adopts new standard contractual clauses, in which case those new standard contractual clauses will control. For purposes of the Old EU SCCs, they shall be deemed completed as follows:

a. The "exporters" and "importers" are the parties and their affiliates to the extent any of them is involved in such transfer, including those set forth in Annex I.A of the New EU SCCs.
b. Clause 9 of the Old EU SCCs specifies that United Kingdom law will govern the Old EU SCCs.
c. The content of Appendix 1 of the Old EU SCCs is set forth in Annex I.B of the New EU SCCs herein.
d. The content of Appendix 2 of the Old EU SCCs is set forth in Annex II of the New EU SCCs herein.

10.2.3 With respect to Personal Data transferred from Switzerland for which Swiss law (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, references to the GDPR in Clause 4 of the New EU SCCs are, to the extent legally required, amended to refer to the Swiss Federal Data Protection Act or its successor instead, and the concept of supervisory authority shall include the Swiss Federal Data Protection and

Information Commissioner.

10.2.4 Customer's acceptance of Upwork's Privacy Policy, which incorporates this DPA, shall be considered a signature to the Standard Contractual Clauses to the extent the Standard Contractual Clauses apply hereunder.

10.3 Disclosure of Confidential Information Containing Personal Data. If the Standard Contractual Clauses as described in Section 10.2 (Transfers of Data Out of the EEA) areapplicable to Upwork's processing of Customer Personal Data, Upwork will, notwithstanding any term to the contrary in the Agreement, ensure that any disclosure of Customer's Confidential Information containing personal data, and any notifications relating to any such disclosures, will be made in accordance with such Standard Contractual Clauses.

10.4 Termination of Standard Contractual Clauses. Notwithstanding the foregoing, the Standard Contractual Clauses shall automatically terminate once the Customer Personal Data transfer governed thereby becomes lawful under Chapter V of the GDPR in the absenceof such Standard Contractual Clauses on any other basis, and Upwork has implemented any measures necessary to comply with such basis.

10.5 Additional Safeguards for the Transfer and Processing of Personal Data from the EEA, Switzerland, and the United Kingdom. To the extent that Upwork processes Customer Personal Data of data subjects located in or subject to the applicable law of the European Economic Area, Switzerland, or the United Kingdom, Upwork agrees to the following safeguards to protect such data to an equivalent level as applicable law.

10.5.1 Upwork and Customer shall encrypt all transfers of Customer Personal Data between them, and Upwork shall encrypt any onward transfers it makes of such personal data, to prevent the acquisition of such data by third parties, such as governmental authorities who may gain physical access to the transmission mechanisms (e.g., wires and cables) while the data is in transmission.

10.5.2 Upwork represents and warrants that:

a. as of the date of this contract, it has not received any directive under Section 702 of the U.S. Foreign Intelligence Surveillance Act, codified at 50 U.S.C. § 1881a ("FISA Section 702").

b. it is not eligible to be required to provide information, facilities, or assistance under FISA Section 702; or that no court has found Upwork to be the type of entity eligible to receive process issued under FISA Section 702: (i) an "electronic communication service provider" within the meaning of 50 U.S.C § 1881(b)(4) or (ii) a member of any of the categories of entities described within that definition.

c. it is not the type of provider that is eligible to be subject to upstream collection ("bulk" collection) pursuant to FISA Section 702, as described in paragraphs 62 & 179 of the judgment in the EU Court of Justice Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ("Schrems II"), and that therefore the only FISA Section 702 process it could be eligible to receive, if it is an "electronic communication service provider" within the meaning of 50 U.S.C § 1881(b)(4), would be based on a specific "targeted selector" i.e., an

identifier that is unique to the targeted endpoint of communications subject to the surveillance.

d. Upwork will never comply with any request under FISA Section 702 for bulk surveillance, i.e., a surveillance demand whereby a targeted account identifier is not identified via a specific "targeted selector" (an identifier that is unique to the targeted endpoint of communications subject to the surveillance).

e. Upwork will use all reasonably available legal mechanisms to challenge any demands for data access through national security process it receives as well as any non-disclosure provisions attached thereto.

f. Upwork will take no action pursuant to U.S. Executive Order 12333.

g. Upwork will promptly notify Customer if Upwork can no longer comply with the applicable Standard Contractual Clauses or the clauses in this Section. Upwork shall not be required to provide Customer with specific information about why it can no longer comply, if providing such information is prohibited by applicable law. Such notice shall entitle Customer to terminate the Agreement (or, at Customer's option, affected statements of work, order forms, and like documents thereunder) and receive a prompt pro-rata refund of any prepaid amounts thereunder. This is without prejudice to Customer's other rights and remedies with respect to a breach of the Agreement.

11. Subprocessors

11.1 Consent to Subprocessor Engagement. Customer specifically authorizes the engagement of Upwork's Affiliates as Subprocessors. In addition, Customer generally authorizes the engagement of any other third parties as Subprocessors ("**Third Party Subprocessors**"). If the Standard Contractual Clauses as described in Section 10.2 (Transfers of Data Out of the EEA) are applicable to Upwork's processing of Customer Personal Data, the above authorizations will constitute Customer's prior written consent to the subcontracting by Upwork of the processing of Customer Personal Data if such consent is required under the Standard Contractual Clauses.

11.2 Information about Subprocessors.

11.2.1 Information about Subprocessors is available upon request by emailing privacyrequests@upwork.com (as may be updated by Upwork from time to time in accordance with this DPA). Subprocessor information will be provided only upon request and is the Confidential Information of Upwork under this Agreement and must be treated with the level of confidentiality afforded to Confidential Information hereunder.

11.2.2 Copies of sub-processor agreements that must be made available to Customer pursuant to Clause 5(j) of the Old EU SCCs may have all commercial information (such as pricing terms) removed by Upwork. Such agreements will beprovided only upon request and are Confidential Information of Upwork under the Agreement.

11.3 Requirements for Subprocessor Engagement. When engaging any Subprocessor, Upwork will:

a. ensure via a written contract that:
    i. the Subprocessor only accesses and uses Customer Data to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including this DPA) and any Standard Contractual Clauses entered into or Alternative Transfer Solution adopted by Upwork as described in Section 10.2 (Transfers of Data Out of the EEA); and
    ii. if the GDPR applies to the processing of Customer Personal Data, the data protection obligations set out in Article 28(3) of the GDPR, as described in this DPA, are imposed on the Subprocessor; and
b. remain liable for all obligations subcontracted to, and all related acts and omissions of, the Subprocessor.

11.4 Opportunity to Object to Subprocessor Changes.

a. Upwork may add or remove Subprocessors from time to time. Upwork will inform Customer of new Subprocessors via a subscription mechanism described in the list of Subprocessors as described above. If Customer objects to a change, it will provide Upwork with notice of its objection to gdpr-dsar@upwork.com including reasonable detail supporting Customer's concerns within sixty days of receiving notice of a change from Upwork or, if Customer has not subscribed to receive such notice, within sixty days of Upwork publishing the change. Upwork will then use commercially reasonable efforts to review and respond to Customer's objection within thirty days of receipt of Customer's objection. If Upwork does not respond to a Customer objection as described above, or cannot reasonably accommodate Customer's objection, Customer may terminate the Agreement by providing written notice to Upwork. This termination right is Customer's sole and exclusive remedy if Customer objects to any new Subprocessor.

12. Privacy Contact; Processing Records

12.1 Upwork's Privacy Contact. Privacy inquiries related to this DPA can be submitted to **privacyrequests@upwork.com** (and/or via such other means as Upwork may provide from time to time).

12.2 Upwork's Processing Records. Customer acknowledges that Upwork is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which Upwork is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly, if the GDPR applies to the processing of Customer Personal Data, Customer will, where requested, provide such information to Upwork via the Service or other means provided by Upwork, and will use the Service or such other means to ensure that all information provided is kept accurate and up-to-date.

13. Liability

13.1 Liability Cap. For clarity, the total combined liability of either party and its Affiliates towards the other party and its Affiliates under or in connection with the Agreement (such as under the DPA or the Standard Contractual Clauses) will be limited to the Agreed Liability Cap for the relevant party, subject to Section 13.2 (Liability Cap Exclusions).

13.2 Liability Cap Exclusions. Nothing in Section 13.1 (Liability Cap) will affect the remaining terms of the Agreement relating to liability (including any specific exclusions from any limitation of liability).

14. Miscellaneous

Notwithstanding anything to the contrary in the Agreement, where Upwork Global, Inc. is not a party to the Agreement, Upwork Global, Inc. will be a third-party beneficiary of Section 7.4 (Reviews and Audits of Compliance), Section 11.1 (Consent to Subprocessor Engagement) and Section 13 (Liability) of this DPA.

Appendix 1: Subject Matter and Details of the Data Processing

Subject Matter

Upwork's provision of the Service to Customer.

Duration of the Processing

The Term plus the period from the expiry of the Term until deletion of all Customer Data by Upwork in accordance with the DPA.

Nature and Purpose of the Processing

Upwork will process Customer Personal Data for the purposes of providing the Service to Customer in accordance with the DPA.

Categories of Data

Data relating to End Users or other individuals provided to Upwork via the Service, by (or at the direction of) Customer or by End Users. The open nature of the Service does not impose a technical restriction on the categories of data Customer may provide. The personal data transferred may include: name, username, password, email address, telephone and fax number, title and other business information, general information about interest in and use of Upwork services; and demographic information.

Data Subjects

Data subjects include End Users and the individuals about whom data is provided to Upwork via the Service by (or at the direction of) Customer or by End Users.

Appendix 2: Security Measures

Upwork will implement and maintain the Security Measures set out in this Appendix 2. Upwork may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Service. Upwork will:

- Conduct information security risk assessments at least annually and whenever there is a material change in the organization's business or technology practices that may impact the privacy, confidentiality, security, integrity or availability of Customer Personal Data.
- Regularly and periodically train personnel who have access to Customer Personal Data or relevant Upwork Systems.
- Maintain secure user authentication protocols, secure access control methods, and firewall protection for Upwork Systems that Process Customer Personal Data.
- Maintain policies and procedures to detect, monitor, document and respond to actual or reasonably suspected Information Security Incidents.
- Implement and maintain tools that detect, prevent, remove and remedy malicious code designed to perform an unauthorized function on or permit unauthorized access to Upwork Systems.
- Implement and maintain up-to-date firewalls.
- Implement and use cryptographic modules to protect Customer Personal Data in transit and, when commercially reasonable, at rest.
- Maintain reasonable restrictions on physical access to Customer Personal Data and relevant Upwork Systems.

Appendix 3: Standard Contractual Clauses

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.

---

[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 of 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 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.

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 transfers)

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.

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 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 Union[2] (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.

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.

---

[2] 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.

(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.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) 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 10 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.[3] 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.

---

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

(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 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.

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 TWO: Transfer controller to processor

(a) 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.

(b) 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.

(c) 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.

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

(e) 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 TWO: Transfer controller 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 TWO: Transfer controller 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.

(a) 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.

(a) 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 TWO: Transfer controller to processor

(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[4];

---

[4] 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.

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

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

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

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

(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 . 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 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 TWO: Transfer controller to processor

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.

(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.).

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

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

15.2 Review of legality and data minimisation

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

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

(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.]

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 TWO: Transfer controller to processor

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.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller 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.

(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.

APPENDIX

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s): Customer

Activities relevant to the data transferred under these Clauses: *Obtaining the Services from Data Importer*

Role: Controller

Data importer(s): Upwork Global Inc.

Activities relevant to the data transferred under these Clauses: *Providing the Services to Data Exporter.*

Role: Processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

Data subjects include End Users and the individuals about whom data is provided to Upwork via the Service by (or at the direction of) Customer or by End Users.

Categories of personal data transferred

Data relating to End Users or other individuals provided to Upwork via the Service, by (or at the direction of) Customer or by End Users. The open nature of the Service does not impose a technical restriction on the categories of data Customer may provide. The personal data transferred may include: name, username, password, email address, telephone and fax number, title and other business information, general information about interest in and use of Upwork services; and demographic information.

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.

None anticipated.

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

Continuously, for the length of the Agreement between the parties.

Nature of the processing

Upwork will process Customer Personal Data to provide the Service to Customer in accordance with the DPA.

Purpose(s) of the data transfer and further processing

Upwork will process Customer Personal Data for the purposes of providing the Service to Customer in accordance with the DPA.

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

The Term plus the period from the expiry of the Term until deletion of all Customer Data by Upwork in accordance with the DPA.

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

Upwork's subprocessors will process personal data to assist Upwork in providing the Services pursuant to the Agreement, for as long as needed for Upwork to provide the Services.

C. COMPETENT SUPERVISORY AUTHORITY

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

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

See Appendix 2 to the DPA.