Upwork Global Data Processing Agreement

Last modified: **November 5, 2020**

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 Model Contract 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.
- “**Model Contract Clauses**” or ”**MCCs**” means the European Commission Decision C(2010)593 Standard Contractual Clauses for Controllers to Processors.

- “**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.
- “**Security Measures**” has the meaning given in Section 7.1.1 (Upwork’s Security Measures).
- “**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 Deletion by Customer. Upwork will enable Customer to delete Customer Data during the 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 Model Contract 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 Model Contract Clauses 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 Model Contract 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 Model Contract Clauses, the parties agree that Customer or an independent auditor appointed by Customer may conduct audits as described in Clause 5(f) and Clause 12(2) of the Model Contract Clauses 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 Model Contract 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 Model Contract 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 the Agreement.

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 Model Contract Clauses or European Data Protection Legislation.

7.4.3 No Modification of MCCs. Nothing in this Section 7.4 (Reviews and Audits of Compliance) varies or modifies any rights or obligations of Customer or Upwork under any Model Contract 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. If Customer Personal Data originating in the EEA is transferred by Customer to Upwork in a country that has not been found to provide an adequate level of protection under European Data Protection Legislation, the parties agree that the transfer shall be governed by the Model Contract Clauses which are attached hereto as Appendix 3 and incorporated herein by reference. Customer's acceptance of Upwork's Privacy Policy, which incorporates this DPA, shall be considered a signature to the Model Contract Clauses to the extent the Model Contract Clauses apply hereunder.

10.3 Disclosure of Confidential Information Containing Personal Data. If the Model Contract Clauses as described in Section 10.2 (Transfers of Data Out of the EEA) are applicable 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 Model Contract Clauses.

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

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 Model Contract 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 Clause 5(h) and Clause 11 of the Model Contract 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 Model Contract Clauses may have all commercial information (such as pricing terms) removed by Upwork. Such agreements will be provided 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 Model Contract 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 Model Contract 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: Model Contract Clauses

Standard Contractual Clauses (Processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation: Customer (as defined in the DPA).

(the data **exporter**)

And

Name of the data importing organisation: Upwork (as defined in the DPA).

(the data **importer**)
each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses

or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own

processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is: Customer.

Data importer
The data importer is: Upwork.

Data subjects
The personal data transferred concern the following categories of data subjects: As set forth in Appendix 1 of the DPA.

Categories of data
The personal data transferred concern the following categories of data: As set forth in Appendix 1 of the DPA.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data: As set forth in Appendix 1 of the DPA (if and as applicable).

Processing operations
The personal data transferred will be subject to the following basic processing activities: Processing to carry out the Services pursuant to the Agreement.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

Upwork will implement and maintain the technical and organisational security measures set forth in Appendix 2 of the DPA.