DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") shall apply if and only to the extent Stack Exchange, Inc. ("Stack") collects or otherwise processes personal data on behalf of Customer in connection with performance of its obligations under any online or electronic terms for its business services that reference this policy ("Principal Agreement"). The parties agree that this DPA shall be incorporated into and form part of the Principal Agreement and shall be subject to the provisions therein, including limitations of liability.

This DPA reflects the parties' agreement with regard to the processing of personal data of individuals in the European Union ("EU") both when the data is collected or processed in the EU and when such data is transferred outside the EU. The transfer shall be governed by the Standard Contractual Clauses ("SCC"), also referred to as Model Clauses, that provide a mechanism approved by the European Commission as offering adequate protection for data subjects when such transfers of personal data occur. Signing this DPA with Stack will enable Stack to comply with the laws to collect and process data in the EU and transfer data outside of the EU/EEA as necessary for Stack to perform the services you have requested.

Personal data is defined as any information relating to an identified or identifiable natural person who can be identified directly or indirectly by reference to an identifier such as a name, an identification number, location data, an online identifier or to one of more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.

HOW TO EXECUTE THIS DPA

1. This DPA has been pre-signed on behalf of Stack Exchange, Inc., as the data importer.

2. To complete this DPA, Customer must:

   (a) Complete the information in the signature box and sign on Page 6;
   (b) Complete the information as the data exporter on Page 14 ; and
   (c) Complete the information in the signature box; and
   (d) Sign on Pages 14, 16, and 17.

3. Customer must send the completed and signed DPA to Stack by email, indicating the Customer's full entity name and the Product in the subject heading of the email to privacy@stackoverflow.com. Upon Stack's receipt of the validly-completed DPA at this email address, this DPA shall come into effect and legally bind the parties.

Data Processing Addendum

THIS ADDENDUM IS MADE BETWEEN: Stack Exchange, Inc., a corporation organized under the laws of Delaware, USA with a registered office at 110 William Street, 28th Floor, New York, NY 10038 (**"Stack"** or "**Processor**"); and the signatory below at the address below ("Customer" or "Controller") effective as of the last date of signature date. This DPA is incorporated into and forms part of the Principal Agreement.

Each a "**party**" and together the "**parties**".

BACKGROUND

(A) The Processor will be providing certain Services to the Controller.

(B) The parties have agreed that in order for the Processor to provide the Services, it will be necessary for the Processor to process certain Controller Data.

(C) In light of this processing, the parties have agreed to enter into this Addendum to address the compliance obligations imposed upon the Controller pursuant to the Data Protection Legislation.

NOW IT IS HEREBY AGREED as follows:

1. DEFINITIONS

1.1. In this Addendum, unless otherwise stated or unless the context otherwise requires, each capitalised term will have the meaning set out below. Terms used but not otherwise defined in this clause have the meanings given in the Data Protection Legislation.

"Appropriate Safeguards"	means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under the Data Protection Laws from time to time.
"CCPA"	means the California Consumer Privacy Act, California Civil Code sections 1798.100 et seq., as amended, and its implementing regulations**.**
"Commencement Date"	means the date of execution of this Addendum.
"Controller Data"	means the Personal Data processed under this Addendum together with any additional Personal Data to which the Processor may have access from time to time in performing the Services. In accordance with clause 2.2, this may include the Personal Data of a Controller Group Company.
"Controller Group Company"	means the Controller and any entity that, directly or indirectly, controls, is controlled by, or is under common control with the Controller, where "**control**" means the power (directly or indirectly) to appoint or remove a majority of the directors of that entity and includes Affiliates and may include Authorized Users as defined in the Principal Agreement.
"Data Protection Legislation"	means all applicable laws relating to data protection and privacy including (without limitation) the UK Data Protection Act 2018, the EU General Data Protection Regulation (2016/679) , the EU Privacy and Electronic Communications Directive 2002/58/EC as implemented in each jurisdiction, and any amending or replacement or equivalent legislation from time to time; and the CCPA.
"Personal Data"	means information about an identifiable individual including, but not limited to, any information that qualifies as "Personal Data" or Personal Information under the Data Protection Legislation that Controller authorizes Processor to collect in connection with Processor's provision of the Services under the Principal Agreement**.**
"Principal Agreement"	shall mean the agreement between the parties formed on the date Controller accepted such electronic terms through an online mechanism for the provision of the Services.
"Intellectual Property Rights"	shall mean all copyright and rights in the nature of copyright, design rights, patents, trademarks, database rights, applications for any of the above, moral rights, rights in confidential information, know-how, domain names and any other intellectual or

	industrial property rights (and any licences in connection with any of the same) whether or not registered or capable of registration and whether subsisting in the United Kingdom or any other part of the world.
"Services"	shall mean the Services as defined in the Principal Agreement.
"**Standard Contractual Clauses**"	means the agreement executed by and between Customer and Stack Exchange, Inc. and attached hereto as Exhibit C pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.
"Supervisory Authority"	shall mean the relevant supervisory authority with responsibility for privacy or data protection matters in the jurisdiction of the Controller.

2. APPOINTMENT

2.1. The Processor is appointed by the Controller to process such Controller Data on behalf of the Controller as is necessary to provide the Services and as may subsequently be agreed by the parties in writing. Any such subsequent agreement shall be subject to the provisions of this Addendum.

3. DURATION

3.1. This Addendum shall commence on the Commencement Date and shall continue in full force and effect until the last of the Services are performed. Following the Commencement Date, the provisions of this Addendum shall apply to any processing of Controller Data received prior to execution during any transitional or migration phase.

3.2. Notwithstanding clause 3.1, the Processor's obligations under clauses 4, 5, 6 and 7 shall survive the expiry of this Addendum if and to the extent that the Processor continues to process (including by way of storage) any Controller Data.

4. DATA PROTECTION

4.1. Each party shall comply with its obligations under the Data Protection Legislation in respect of any personal data it processes under or in relation to this Addendum.

4.2. Controller shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Controller acquired Personal Data. Controller specifically acknowledges that its use of the Service will not violate the rights of any Data Subject to the extent applicable under the CCPA, including, but no limited to, those who have opted-out from sales or other disclosures of Personal Data,

4.3. The categories of Controller Data to be processed by the Processor and the processing activities to be performed under this Addendum are set out in Schedule 2 (Personal Data).

4.4. In respect of all Controller Data that it processes on behalf of the Controller, Processor at all times shall:

4.4.1. only process the Controller Data in accordance with the documented instructions given from time to time by the Controller, including with regard to transfers, unless required to do otherwise by applicable law, in which event, the Processor shall inform the Controller of the legal requirement before processing Controller Data other than in accordance with the Controller's instructions, unless that same law prohibits the Processor from doing so;

4.4.2. implement the security requirements set out in Schedule 1 (Information Security) as appropriate technical and organizational measures to protect any Controller Data processed by it against unauthorized and unlawful processing and against accidental loss, destruction, disclosure, damage or alteration;

4.4.3. not publish, disclose or divulge (and ensure that its personnel do not publish, disclose or divulge) any Controller Data to any third party unless the Controller has given its prior written consent or as otherwise required by law;

4.4.4. ensure that only such of its personnel who may be required by the Processor to assist it in meeting its obligations under this Addendum will have access to the Controller Data, and that such personnel are bound by appropriate obligations of confidentiality and take reasonable steps in accordance with standard industry practice to ensure they comply with such obligations;

4.4.5. inform the Controller promptly, and in any event within five (5) business days, to the extent legally permissible, of any enquiry or complaint received from a data subject or Supervisory Authority relating to the Controller Data;

4.4.6. permit the Controller to review any of the Processor's records as may be reasonably required to enable the Controller to assess whether or not the Processor is complying with the provisions of this Addendum in relation to the Controller Data;

4.4.7. provide cooperation and assistance to the Controller as the Controller may reasonably require to allow the Controller to comply with its obligations as a data controller, including in relation to data security; data breach notification; data protection impact assessments; prior consultation with Supervisory Authorities; the fulfilment of data subjects' rights; and any enquiry, notice or investigation by a Supervisory Authority; and

4.4.8. at the request and option of the Controller (whether during or following termination of this Addendum), promptly and as specified by the Controller return or destroy all Controller Data in the possession or control of the Processor, except as otherwise permitted by the Principal Agreement.

4.4.9. refrain from selling (as such term is defined in the CCPA) any Personal Date processed hereunder, without Controller's prior written consent, nor taking any action that would cause any transfer of Personal Information to or from Processor under the Agreement or this DPA to qualify as "selling" such Personal Information under the CCPA.

4.5. Controller acknowledges and agrees that (a) Processor Affiliates may be retained as Sub-Processors; (b) Processor may engage third-party Sub-processors in connection with the provision of the Services ("Sub-Processor") in accordance with this Addendum; and (c) Controller agrees to the use of the Sub-processors at https://stackoverflow.com/legal/gdpr/subprocessors ("Sub-processor List"). Processor will enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Personal Data as those in this Addendum, to the extent applicable to the nature of the Services provided by such Sub-processor. In the event Controller enters into the Standard Contractual Clauses set forth in Exhibit C, then Controller agrees that Processor may appoint Sub-processors in accordance with Clause 5(8) of Exhibit C by complying with this Section 4.4 and Section 4.5 below.

4.6. The Controller can object in writing to the processing of its Controller Data by a new Sub-processor within thirty (30) days following the updating of the Sub-processor List and shall describe its legitimate reasons to object. If Controller does not object during such time period, the new Sub processor(s) shall be deemed accepted. If Controller objects to the use of a new Sub-processor pursuant to the process provided hereunder, Processor shall have the right to cure the objection and proceed to use the subcontractor to process Controller Data. If Processor is unable to cure the objection, the Controller may terminate the Agreement with no further liability to Processor.

4.7. The Processor acknowledges and agrees that it shall remain liable to the Controller for any breach of the terms of this Addendum by any Sub-Processor and other subsequent third party processors appointed by it.

4.8. The parties agree that the Controller shall own the Controller Data and the Processor hereby assigns to the Controller any Intellectual Property Rights arising now or in the future from the collection and compilation of the Controller Data, except as otherwise provided in the Principal Agreement.

5. SECURITY BREACHES

5.1. The Processor shall notify the Controller within forty-eight (48) hours of becoming aware of any accidental, unauthorised, or unlawful destruction, loss, alteration, or disclosure of, or access to, Controller Data ("**Security Breach**") or a security incident with the reasonable potential to result in access to Controller Data. The Processor shall also provide the Controller with a detailed description of the Security Breach, the type of data that was the subject of the Security Breach and the identity of each affected person as soon as such information can be collected or otherwise becomes available.

5.2. The Processor agrees to take action immediately, at its own expense, to investigate the Security Breach and to identify, prevent and mitigate the effects of any such Security Breach.

5.3. The Processor may not make public any filing, communication, notice, press release, or report concerning any Security Breach that identifies the Controller ("**Notices**") without the Controller's prior approval, except as may be required by law.

5.4. The Processor shall make available to the Controller for audit purposes written records and other information necessary to demonstrate compliance with this Addendum. Controller must give Processor thirty (30) days written notice of such audit. Any third party involved in an audit must be approved by Processor and agree in writing to confidentiality provisions no less restrictive than those in the Principal Agreement.

6. DATA TRANSFERS

6.1 The Processor shall process Controller Data outside: (i) both the UK and the European Economic Area ("**EEA**"); or (ii) any other territory in which restrictions are imposed on the transfer of Controller Data across borders under the Data Protection Legislation, only in compliance with the Standard Contractual Clauses attached hereto in order to put in place Appropriate Safeguards to protect Controller Data.

6.2 Notwithstanding the foregoing, Processor shall only process Personal Data for the following purposes: (i) processing in accordance with the Principal Agreement and applicable Order Form(s); (ii) processing initiated by Authorized Users in their use of the Services; (iii) processing to comply with other reasonable instructions provided by Controller (e.g., via email or support tickets) and (iv) processing to provide support of and billing for the Product or Services that are consistent with the terms of the Principal Agreement.

6.3 If, for whatever reason, the transfer of Controller Data under Clause 6.1 ceases to be lawful:

(a) the Processor shall, with Controller's consent, implement an alternative lawful transfer mechanism; or

(b) the Controller may terminate the Principal Agreement and this Addendum at no additional charge to Controller.

7. CONTROLLER GROUP COMPANY

7.1. Each Controller Group Company agrees to be bound by the obligations under this DPA and, to the extent applicable, the Principal Agreement. For the avoidance of doubt, a Controller Group Company is not and does not become a party to the Principal Agreement and is only a party to this Addendum. If Controller Group Company is an Authorized User, its access to and use of the Products must comply with the terms and conditions of the Principal Agreement, and any violation of the terms and conditions of the Principal Agreement by a Controller Group Company shall be deemed a violation by Controller.

7.2. Where a Controller Group Company becomes a party to this Addendum with Processor, it shall, to the extent required under applicable Data Protection Laws and Regulations, be entitled to exercise the rights and seek remedies under this Addendum, subject to the following: Except where applicable Data Protection Laws and Regulations require the Controller Group Company to exercise a right or seek any remedy under this against Processor directly by itself, the parties agree that (i) solely the Controller as the contracting party to the Principal Agreement shall exercise any such right or seek any such remedy on behalf of the Controller Group Company, and (ii) the Controller that is the contracting party to the Principal Agreement shall exercise any such rights under this Addendum in a combined manner for itself and all of its Controller Group Company and not separately for each Controller Group Company individually.

8. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this Addendum, and all agreements between Controller Group Company and Processor, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Principal Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party under the Principal Agreement and this Addendum together.

9. FURTHER ASSURANCE

The parties shall, and shall ensure that their agents, employees and subcontractors shall, do all things reasonably necessary, including executing any additional documents and instruments, to give full effect to the terms of this Addendum and to otherwise fulfil the provisions of this Addendum in accordance with its terms.

10. COUNTERPARTS

This Agreement may be executed in counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

11. LAW

The parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity. This Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by laws of the country or territory stipulated for this purpose in the Principal Agreement.

12. MISCELLANEOUS

12.1. Clauses and other headings in this Agreement are for convenience of reference only and shall not constitute a part of or otherwise affect the meaning or interpretation of this Agreement. Schedules to this Agreement shall be deemed to be an integral part of this Agreement to the same extent as if they had been set forth verbatim herein.

12.2. This Agreement constitutes the entire agreement between the parties pertaining to the subject matter hereof and supersedes all prior agreements, understandings, negotiations and discussions of the parties in relation to the subject matter.

12.3. The provisions of this Agreement are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this Agreement shall remain in full force and effect.

12.4. The provisions of this Agreement shall inure to the benefit of and shall be binding upon the parties and their respective successors and assigns.

12.5. Any notice required under this Agreement shall be given in writing and sent by nationally recognized courier to the address set forth herein and shall be deemed given upon the date such courier's records indicate delivery was complete.

IN WITNESS the hands of the duly authorised representatives of the parties the day month and year first above written:

Signed on behalf of **STACK EXCHANGE, INC.**		**Signed on behalf of** **Customer/Controller**	
Signature	David Farber	Signature	
Name	David Farber	Name	
Date		Date	

Schedule 1: Information Security

Scope

1. This Schedule applies to all Controller Data collected, generated or otherwise processed by the Processor in the course of providing its Services.

People and Operations

2. All Processor staff including sub-contractors that have access to its data processing systems or the Controller's data processing systems authenticate with a unique username and strong password.

3. The Processor shall have appropriate data protection and data security training in place for all of its staff involved in the processing of Controller Data and carry out such training at reasonable intervals.

4. The Processor shall require its staff to commit themselves contractually to obligations of confidentiality or be under an appropriate statutory obligation of confidentiality.

5. The Processor shall monitor its staff's access to Controller Data. Monitoring shall at a minimum include and capture, successful and unsuccessful log-in attempts, time, date and username. These logs shall be retained for at least 3 months.

Policy and Procedures

6. The Processor shall have in place a company-wide security policy, endorsed and supported by an executive officer in the Processor's senior management team, based upon or aligned with the international standard for Information Security Management (ISO27001).

Accreditations

7. Where the Processor processes Controller Data that falls within the scope of the Payment Card Industry Data Security Standard (PCI DSS), the Processor shall ensure that all processing meets the PCI DSS requirements to the latest version of the standard. This is applicable only to Services purchased through Processor's self-service avenues.

Physical security

8. The Processor shall have the appropriate systems in place to restrict access to its secure premises and sites. Access to secure areas shall be monitored and logged by the Processor.

Application Development

9. Processor provides software as a solution to Controller. In developing the software provided as the Service, the Processor shall adopt secure coding practices that address at a minimum the Open Web Application Security Project (OWASP) top ten vulnerabilities.

10. The Processor will have documented policies and/or processes identifying where security checks, and the associated methods, are applied throughout the development lifecycle.

11. The Processor will ensure that logs of activities on customer interfaces (for example but not limited to web server and database logs) and IT admin activity logs, both at server and GUI level, are logged remotely from the servers themselves. The logs should be retained as per the Processor's own retention policies, which should be notified to the Controller.

12. At least annually, the Processor shall, at its own cost, undertake an independent application and/or infrastructure penetration testing of Services provided to the Controller using an internationally recognised methodology such as OWASP. Evidence of independent testing can be provided to the Controller if requested in writing.

13. Vulnerability scans shall be performed at least quarterly. Processor shall install have (b) critical security patches within thirty (30) days of the vendor's release date; and (c) non-critical security patches within ninety (90) days of the vendor's release date.

Infrastructure

14. The Processor shall manage changes to Services provided in accordance with the Principal Agreement and shall not decrease the overall effectiveness of security controls.

15. All infrastructure used in provision of the Services and/or hosting of Controller Data will be subject to frequent vulnerability assessment and remediation cycles.

Data handling

16. The Processor shall segregate Controller Data from any of the Processor's other customers' data. Where dedicated physical segregation is not possible, separate logical databases or storage instances are acceptable. Where separate logical instances are not possible and segregation relies on access control permissions, or views, the Processor must have real time monitoring and alerting to the system administrator for changes to these parameters.

17. The Processor will use widely recognised encryption protocols and techniques to protect Controller Data, during: (i) transit (data input); (ii) exchange with contracted third parties (data output); and (iii) for storage (only if Controller has purchased a service hosted on Stack's third party provider system). Where appropriate, the Processor will pseudonymise Controller Personal Data as soon as possible, which means processing the Controller Personal Data in a way that it can no longer be attributed to a specific data subject without the use of additional information.

18. The Processor shall undertake appropriate measures to prohibit Controller Data from being transferred or copied onto unencrypted portable devices, such as USB sticks or flash drives.

Data Deletion

19. Where Controller requests in writing that the Processor delete Controller Data, deletion means physical or logical deletion, so that the data cannot be restored. Logical deletion methods will be considered appropriate if they are multi-pass overwrite methods. Upon Controller's written request, the Processor will provide written confirmation that deletion has been completed, including the physical deletion and method used.

Schedule 2: Personal Data

DETAILS OF THE PROCESSING

Subject Matter of Processing Stack processes the personal data of Customer's administrative users to provide access to the Product and Service and support and maintenance and the personal data of other Customer designated personnel to conduct billing and collection activities.

Duration of Processing

The subject matter and duration of the Processing of the Customer Personal Data are set out in the Principal Agreement and this Addendum.

Nature and Purpose of Processing

Stack will Process Personal Data as necessary to perform the Services as detailed on the applicable ordering document pursuant to the Principal Agreement between the Parties and as further instructed by Customer in its use of the Services.

Types of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which depending on the product may include, but is not limited to:

- Full Name
- Business Email
- Business Username
- Business IP Address
- Business Password Hash
- Business Browser ID

Types of Sensitive Data

- None

Categories of Data Subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer as Controller, and which includes, but is not limited to Personal Data relating to the following categories of data subjects:

- Employees
- Consultants
- Authorized Third Parties

Customer may not submit for processing and Stack will not collect, store, or process any payment collection information other than described herein.

Obligations and Rights of Stack and Stack's Affiliates

The obligations and rights of Stack and Stack's Affiliates are set out in the Principal Agreement and this Addendum.

EXHIBIT C

Standard contractual clauses—set II—controller to processor (Model Clauses)

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 organization: [insert]
Address: [insert]
E-mail: [*insert*]

]

(the data **exporter**)

And

Name of the data importing organization:	**Stack Exchange, Inc.**
Address:	110 William Street, 28th Floor, New York, NY 10038
E-mail:	e-mail:privacy@stackoverflow.com

(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.

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 sub-processor**' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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 organizational security measures**' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

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.

3 Third-party beneficiary clause

(a) 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(a) and (b), Clause 7, Clause 8(b), and Clauses 9 to 12 as third-party beneficiary.

(b) The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(b), 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.

(c) The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(b), 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 sub-processor shall be limited to its own processing operations under the Clauses.

(d) 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.

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 organizational 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, unauthorized 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 sub-processor pursuant to Clause 5(b) and Clause 8(c) 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 sub-processing 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 sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor 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 Clauses 4 (a) to (i).

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 organizational 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 unauthorized access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized 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 Principal contract for sub-processing, 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 sub-processing, it has previously informed the data exporter and obtained its prior written consent;

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

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

6 Liability

(a) 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 sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

(b) If a data subject is not able to bring a claim for compensation in accordance with paragraph (a) against the data exporter, arising out of a breach by the data importer or his sub-processor 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 sub-processor of its obligations in order to avoid its own liabilities.

(c) If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs (a) and (b), arising out of a breach by the sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

7 Mediation and jurisdiction

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

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

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

(b) 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.

8 Cooperation with supervisory authorities

(a) 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.

(b) The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, 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.

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

9 Governing law

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

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.

11 Sub-processing

(a) 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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor 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 sub-processor's obligations under such agreement.

(b) The prior written contract between the data importer and the sub-processor 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 (a) 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 sub-processor shall be limited to its own processing operations under the Clauses.

(c) The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph (a) shall be governed by the law of the Member State in which the data exporter is established.

(d) The data exporter shall keep a list of sub-processing 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.

12 Obligation after the termination of personal data-processing services

(a) The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor 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.

(b) The data importer and the sub-processor 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 (a).

On behalf of the data exporter:

Name (written out in full): [*insert*]

Position: [*insert*]

Address: [*insert*]

Other information necessary in order for the contract to be binding (if any): [*insert*]

(stamp)	Signature……..……..……
(stamp of organization)	

On behalf of the data importer: Stack Exchange, Inc.

Name (written out in full): David Farber

Position: Director Financial Planning &Analysis

Address: 110 William Street, 28th Floor, New York, NY 10038 USA.*t*]

Other information necessary in order for the contract to be binding (if any): [*insert*]

David Farber

Signature_____**…**

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed 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's business or organisation type is:

- ☐ Central government
- ☐ Charitable and voluntary
- ☐ Education and childcare
- ☐ Finance, insurance and credit
- ☐ General business
- ☐ Health
- ☐ IT, digital, technology and telecoms
- ☐ Justice and policing
- ☐ Land and property services
- ☐ Legal and professional advisers
- ☐ Local government
- ☐ Marketing and research
- ☐ Media
- ☐ Membership association
- ☐ Political
- ☐ Regulators
- ☐ Religious
- ☐ Research
- ☐ Retail and manufacture
- ☐ Social care
- ☐ Trade, employer associations, and professional bodies
- ☐ Traders in personal data
- ☐ Transport and leisure
- ☐ Utilities and natural resources
- ☐ Other – Please add details:

The data exporter is using the personal data which is being transferred for the following purposes or activities:

As necessary to perform the Services as detailed on the applicable ordering document pursuant to the Principal Agreement between the Parties and as further instructed by data exporter in its use of the Services.

Data importer

The data importer processes the personal data of data importer's administrative users to provide access to the Product and Service and support and maintenance and the personal data of other data importer designated personnel to conduct billing and collection activities.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

- Employees
- Consultants

- Authorized Third Parties

Data exporter may not submit for processing and data importer will not collect, store, or process any payment collection information other than as described in the Data Protection Addendum.

Categories of data

The personal data transferred concern the following categories of data:

- Full Name
- Email
- Username
- IP Address
- Password Hash
- Browser ID

Processing operations

The personal data transferred will be subject to the following basic processing activities:

X Receiving data, including collection, accessing, retrieval, recording, and data entry
X Holding data, including storage, organization and structuring
X Returning data to the data exporter or data subject

DATA EXPORTER

Name: [*insert*]

Authorized Signature:…….

DATA IMPORTER **Stack Exchange, Inc.**

Name: David Farber

David Farber

Authorized Signature:…….

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix 2 forms part of the Clauses and must be completed and signed by the parties.

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

See Schedule 1, Information Security Schedule, attached to the Data Protection Addendum

DATA EXPORTER

Name: [*insert*]

Authorized Signature:…….

DATA IMPORTER **Stack Exchange, Inc.**

Name: David Farber

David Farber

Authorized Signature:…….