This Data Processing Addendum, including its Appendices, ("DPA") applies 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 the associated Agreement (as defined below). The parties agree that this DPA is an addendum to and forms part of the Agreement and that each party shall be subject to the provisions therein, including limitations of liability.

Signing this DPA with Stack will enable Stack to comply with applicable data protection and processing laws and regulations while performing and providing the requested services.

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; and
    b. Complete the information as the data exporter in Appendix 2.

3. 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 legal@stackoverflow.com. This DPA will become legally binding upon Stack's receipt of the validly completed DPA at this email address.

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is entered into by and between Stack Exchange, Inc. ("**Stack**") and the signatory below at the address below ("**Customer**"). The parties agree that notwithstanding anything to the contrary in the Agreement (as defined below), this DPA is hereby incorporated into and made an essential part of the Agreement. Capitalised terms not otherwise defined herein shall have the meanings given to them in the Agreement.

1. **Definitions**

1.1. In this DPA, the following terms will have the meanings set out below and cognate terms will be construed accordingly:

"**Adequate Country**" means a country or territory recognised as providing an adequate level of protection for Personal Data under an adequacy decision made, from time to time, by (as applicable): (i) the Information Commissioner's Office and/or under applicable United Kingdom ("UK") law (including the UK GDPR), or (ii) the European Commission under the EU GDPR.

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

"**Agreement**" means collectively the written agreement(s) under which Stack licences or provides access to the Services.

"**Customer Group Company**" means the Customer and/or any entity that, directly or indirectly, controls, is controlled by, or is under common control with the Customer and is party

to this DPA, where "control" means the power (directly or indirectly) to appoint or remove a majority of the directors of that entity and includes Affiliates.

"**Data Protection Laws**" means all applicable laws, regulations, or other legal requirements relating to privacy, data security, and protection of Personal Data, and the processing of any Personal Data, including but not limited to:

a) in the European Union ("EU"), the General Data Protection Regulation 2016/679 (the "**EU GDPR**");
b) in the UK, the UK General Data Protection Regulation 2016/679, as implemented by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 and the Data Protection Act 2018 (the "**UK GDPR**");
c) in Switzerland, the Swiss Data Protection Act ("**Swiss DPA**"); and
d) State Privacy Laws.

"**Data Subject Request**" means a request from or on behalf of a data subject to exercise any rights in relation to their Personal Data under the Data Protection Laws (may also be referred to as a "Customer Request").

"**EU Clauses**" means the standard contractual clauses for international transfers of personal data to third countries set out in the European Commission's Decision 2021/914 of 4 June 2021 (at http://data.europa.eu/eli/dec_impl/2021/914/oj) incorporating Module Two for Controller to Processor transfers and which form part of this DPA in accordance with Schedule 1 of Appendix 1.

"**Personal Data**" means any personal information relating to, directly or indirectly, an identified or identifiable natural person of Customer that is collected, accessed, used, disclosed, or otherwise processed by Stack on behalf of Customer under this DPA. In accordance with Section 2.2 of this DPA, this may include the Personal Data of a Customer Group Company.

"**Personal Data Breach**" means any breach of security or other action or inaction leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data by any of Stack's staff or sub-processors, or any other identified or unidentified third party. A Personal Data Breach does not include any unsuccessful attempt or activity that does not compromise the security of Personal Data, including routine, unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

"**Restricted Transfer**" means: (i) a transfer of Personal Data from any Customer Group Company to Stack; or (ii) an onward transfer of Personal Data from Stack to a sub-processor of Stack, in each case, where and to the extent the transferred Personal Data is subject to European Data Protection Laws (which includes EU GDPR or UK GDPR, as applicable) and the party receiving the Personal Data does not provide an adequate level of protection for Personal Data within the meaning of European Data Protection Laws.

"**Sensitive Data**" means Personal Data that is protected under a special legislation and requires unique treatment, such as "special categories of data", "sensitive data" or other materially similar terms under the Data Protection Laws, which may include any of the following: (a) social security number, tax file number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) financial or credit information, credit or

debit card number; (c) information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning a person's health, sex life or sexual orientation, or data relating to criminal convictions and offences; (d) Personal Data relating to children; and/or (e) account passwords in unhashed form.

"**State Privacy Laws**" means United States ("US") state privacy laws, which may include but are not limited to:

a) the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code 1798.100 et seq., as amended, including by the California Privacy Rights Act of 2020 (the "CPRA"), and its implementing regulations;
b) the Virginia Consumer Data Protection Act, Code of Virginia title 59.1, Chapter 52 (the "VCDPA"), and its implementing regulations;
c) the Colorado Privacy Act, Colorado Rev. Stat. 6-1-1301 et seq. (the "CPA"), and its implementing regulations;
d) the Utah Consumer Privacy Act, Utah Code 13-61-101 et seq. (the "UCPA"), and its implementing regulations; and
e) the Connecticut Act Concerning Personal Data Protection and Online Monitoring, Conn. PA 22-15 § 1 et seq. ("PDPOM"), and its implementing regulations, or any regulations or guidance issued pursuant thereto.

"**UK Approved Addendum**" means the template Addendum B.1.0 issued by the UK's Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 of the UK on 2 February 2022, and in force since 21 March 2022.

"**UK Mandatory Clauses**" means the Mandatory Clauses of the UK Approved Addendum, as updated from time to time and/or replaced by any final version published by the Information Commissioner's Office.

1.2. The terms "business", "business purpose", "commercial purpose", "consumer", "controller", "data subject", "personal data", "personal information", "processor", "process/processing", "sell", "service provider", "share", "subcontractor", "sub-processor", and "supervisory authority" have the meanings ascribed to them in the Data Protection Laws.

2. **Roles**

2.1. Customer is a business and considered to be the controller and data exporter of Personal Data and Stack is a service provider and considered to be the data importer or processor of the Personal Data, as such terms may be defined in the Data Protection Laws.

2.2. For the avoidance of doubt, a Customer Group Company other than the Customer is not and does not become a party to the Agreement and, subject to the following, is only a party to this DPA. Where a Customer Group Company wants to become a party to this DPA and the EU GDPR or UK GDPR applies, the process in Clause 7 of the EU Clauses applies accordingly.

2.3. Each party will comply (and will procure its personnel to comply and use commercially reasonable efforts to procure its sub-processors to comply), with Data Protection Laws applicable to such party in the processing of Personal Data. As between the parties, Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Personal Data was acquired.

2.4. Customer, in its use of the Services, and Customer's instructions to the Processor, shall comply with Data Protection Laws, the Agreement, and this DPA. Customer shall establish and have any and all required legal bases in order to collect, process, and transfer to Stack the Personal Data, and to authorise the processing activities conducted by Stack on Customer's behalf in accordance with the Agreement and this DPA, including the pursuit of a business purpose.

2.5. Either party will promptly notify the other upon determining that it can no longer comply with its obligations under (i) the Data Protection Laws, (ii) the Agreement, or (iii) this DPA.

3. **Processing Requirements**

3.1. Stack acknowledges that Customer is disclosing Personal Data in connection with the Agreement only for the limited and specified purposes of receiving the Services. In accordance, Stack shall not sell or share Personal Data, or collect, retain, use, disclose, or otherwise process Personal Data for any purpose other than solely on behalf of Customer for the specific purpose of providing the Services or as otherwise required by law. Stack's Processing of Personal Data will be pursuant to the direct business relationship between Stack and Customer and at all times be done in compliance with the Data Protection Laws, the Agreement, and this DPA.

3.2. As a processor, Stack will only process Personal Data: (i) in order to provide the Services to Customer as agreed in the Agreement; or (ii) per Customer's instructions in writing. Stack will notify Customer (unless prohibited by applicable law) if Stack is required under applicable law to process Personal Data other than pursuant to Customer's instructions. As soon as reasonably practicable upon becoming aware, Stack will inform the Customer if, in Stack's opinion, any instructions provided by the Customer infringe the Data Protection Laws. For the purpose of clarification, Stack has no obligation to assess whether instructions by Customer infringe any Data Protection Laws.

3.3. The parties acknowledge that the Services are not intended for the processing of Sensitive Data. Accordingly, Customer shall not submit any Sensitive Data to the Services.

3.4. Stack will not combine Personal Data received from Customer with personal data that Stack receives from, or on behalf of, another person or persons, or collects from its own interaction with consumers, provided that Stack may so combine Personal Data for a business purpose if directed to do so by Customer or as otherwise expressly permitted by the Data Protection Laws.

3.5. Upon termination of the Agreement and upon written request of the Customer, Stack will return or delete the Personal Data, unless applicable law requires or permits otherwise and except as otherwise permitted by the Agreement.

3.6. Customer may, upon providing reasonable notice to Stack, take all reasonable and appropriate steps to prevent, stop, or remediate any unauthorised processing of Customer's Personal Data.

3.7. As applicable, Stack's processing of Personal Data will also be subject to the EU Clauses if Stack processes Personal Data of EU data subjects with a Restricted Transfer. In this case the relevant Customer Group Company being the "data exporter" and Stack being the "data importer" and the term "transfer" in the EU Clauses also includes any "processing". The UK Approved Addendum shall, however, only apply where there is a Restricted Transfer for the purposes of UK GDPR.

4. **Technical and Organisational Security Measures**

4.1. Stack will implement appropriate technical and organisational security measures appropriate to the risks that are presented by the processing of Personal Data, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data as set out in Appendix 4.

4.2. Stack will take reasonable steps to ensure that only authorised personnel have access to Personal Data and that any persons whom it authorises to access the Personal Data are under obligations of confidentiality.

4.3. Stack may arrange for a qualified and independent assessor to conduct an assessment of Stack's policies and technical and organisational measures using an appropriate and accepted control standard or framework and assessment procedure for such assessments. Stack shall provide a report of such assessment to Customer upon written request.

5. **Sub-processors**

5.1. Customer grants a general authorisation to Stack to appoint third parties as sub-processors to support the performance of the Services, including data centre operators, cloud-based software providers, and other outsourced support and service providers. Stack will maintain a list of sub-processors (available at https://stackoverflow.com/legal/gdpr/subprocessors, as may be updated from time to time, and as set out in Appendix 3).

5.2. Stack shall notify Customer of its appointment of new sub-processors via its website thirty (30) days prior to their commencement of sub-processing of Personal Data. Customer may object to Stack's appointment of a sub-processor on reasonable grounds by notifying Stack in writing within fifteen (15) days of the posting. If Customer does not object during such time period, the new sub-processor shall be deemed accepted. In the event Customer objects, the parties shall discuss Customer's concerns in good faith with a view towards achieving a commercially reasonable resolution. If the parties are unable to reach an accord, the Customer may terminate the DPA with no further liability to Stack. Stack may use a new or replacement sub-processor whilst this objection procedure is in process.

5.3. Stack will not subcontract any processing of Customer's Personal Data to any sub-processor without first ensuring the engagement is pursuant to a written contract binding the sub-processor to terms no less protective of Personal Data than those imposed on Stack in this DPA (the "**Relevant Terms**"). Stack shall be liable to Customer for any breach by such sub-processor of any of the Relevant Terms to the extent required under the Data Protection Laws.

6. **Personal Data Breaches, Data Subject Requests & Further Assistance**

6.1. Stack will notify Customer of any Personal Data Breach without undue delay and in any event no later than forty-eight (48) hours after becoming aware of the Personal Data Breach.

6.2. To the extent legally permitted, Stack will notify Customer if it receives a Data Subject Request without undue delay and in any case within seventy-two (72) hours. Stack will not respond to a Data Subject Request, provided that Customer agrees Stack may at its discretion respond to confirm that such request relates to Customer. Customer acknowledges and agrees that the Services may include features that will allow Customer to manage Data Subject Requests directly through the Services without additional assistance from Stack. If Customer does not have the ability to address a Data Subject Request, Stack will, upon Customer's written

request, provide reasonable assistance to facilitate Customer's response to the Data Subject Request to the extent such assistance is consistent with applicable law.

6.3. Taking into account the nature of processing and the information available to Stack, Stack will provide such assistance as Customer reasonably requests in relation to Customer's obligations under Data Protection Laws with respect to: (i) data protection impact assessments; (ii) notifications to the Supervisory Authority under Data Protection Laws and/or communications to data subjects by the Customer in response to a Personal Data Breach; or (iii) Customer's compliance with its obligations under the Data Protection Laws with respect to the security of processing.

6.4. Stack shall conduct, at least annually and at Stack's expense, an audit of Stack's policies and technical and organisational measures in support of the obligations under the Data Protection Laws.

6.5. Stack agrees to cooperate with any reasonable and appropriate audits or reviews, limited to once per year, or other steps that Customer deems reasonably necessary to confirm that Stack processes Personal Data in a manner consistent with Customer's obligations under the Data Protection Laws, including security and privacy questionnaires. Customer shall only use such information, including documents reflecting the outcome of an audit and/or certification, to assess compliance with this DPA, and not for any other purpose. Customer shall maintain the confidentiality of such information and not disclose such information to any third party without Stack's prior written approval.

7. **International Transfers**

7.1. Customer agrees that its use of the Services can involve the transfer of Personal Data to, and processing of Personal Data in, the country in which Stack is based. Stack will not process or permit the processing of Personal Data in another country outside the European Economic Area ("EEA"), UK, or Switzerland, except as specified in Sections 7.2-7.4, without in each case the prior written consent of Customer.

7.2. *UK transfers*

a) To the extent Personal Data is transferred to Stack and processed by or on behalf of Stack outside the UK (except if in an Adequate Country) in circumstances where such transfer would be prohibited by the UK GDPR in the absence of a transfer mechanism, the parties agree that the EU Clauses subject to the UK Approved Addendum will apply. The UK Approved Addendum is incorporated into this DPA.
b) Schedule 2 of Appendix 1 references the information required by Tables 1 to 4 inclusive of the UK Approved Addendum.

7.3. *EEA transfers*

a) To the extent Personal Data is transferred to Stack and processed by or on behalf of Stack outside the EEA (except if in an Adequate Country) in circumstances where such transfer would be prohibited by EU GDPR in the absence of a transfer mechanism, the parties agree that the EU Clauses will apply in respect of that processing and are incorporated into this DPA in accordance with Schedule 1 of Appendix 1.
b) Schedule 1 of Appendix 1 contains the information required by the EU Clauses.

7.4. *Swiss transfers*

a) To the extent Personal Data is transferred to Stack and processed by or on behalf of Stack outside of Switzerland (except if in an Adequate Country) in circumstances where such transfer would be prohibited in the absence of a transfer mechanism, the parties agree that the Standard Contractual Clauses also apply mutatis mutandis to the parties' processing of personal data that is subject to the Swiss DPA. Where applicable, references to EU Member State law or EU supervisory authorities shall be modified to include the appropriate reference under Swiss law as it relates to transfers of personal data that are subject to the Swiss DPA.

7.5. Stack may (i) replace the EU Clauses and/or the UK Approved Addendum generally or in respect of the EEA, and/or the UK (as appropriate) with any alternative or replacement transfer mechanism in compliance with the Data Protection Laws, including any further or alternative standard contractual clauses approved from time to time and (ii) make reasonably necessary changes to this DPA by notifying Customer of the new transfer mechanism or content of the new standard contractual clauses (provided their content is in compliance with the relevant decision or approval), as applicable.

8. **Customer Received Data Subject Requests**

8.1. Customer agrees to notify Stack of requests from consumers to exercise rights under the Data Protection Laws, including to delete Personal Data, and Stack agrees to comply with such requests, so long as no exception has been determined to apply, in accordance with the Data Protection Laws and, taking into account the nature of processing and the information available to Stack, by appropriate technical and organisational measures, to provide reasonable assistance to Customer to enable Customer to comply with such valid requests. When Customer notifies Stack of such requests in accordance with this subsection, Customer shall: (a) verify the identity of the consumer to the extent required by the Data Protection Laws, (b) assist in locating the Personal Data shared with Stack, and (c) cooperate in good faith with Stack to determine whether a request should be complied with or whether any exceptions for compliance with the request apply.

9. **De-identified Data**

9.1. Stack shall not process Customer's Personal Data to create de-identified data without first obtaining authorization from Customer. In the event Stack is properly authorised, Stack shall:

a) adopt reasonable measures to prevent deidentified data from being used to infer information about, or otherwise being linked to, a particular natural person or household;
b) maintain and use de-identified data in a de-identified form and not attempt to re-identify the deidentified data, except that Stack may attempt to re-identify the information solely for the purpose of determining whether its de-identification processes satisfy the requirements of the Data Protection Laws; and
c) contractually obligate any recipients of the Deidentified data, including sub-processors, contractors, and other third parties, to comply with the Data Protection Laws.

10. **General**

10.1. This DPA is without prejudice to the rights and obligations of the parties under the Agreement, which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Agreement, the terms (including definitions) of this DPA shall prevail so far as the subject matter concerns the processing of

Personal Data. This DPA sets out all of the terms that have been agreed between the parties in relation to the subjects covered by it. Other than in respect of statements made fraudulently, no other representations or terms shall apply to or form part of this DPA.

10.2. Stack's maximum aggregate liability to Customer under or in connection with this DPA shall not under any circumstances exceed the maximum aggregate liability of Stack to the Customer as set out in the Agreement.

10.3. This DPA will be governed by and construed in accordance with the laws of the jurisdiction governing the Agreement unless otherwise required by Data Protection Laws, in which case this DPA will be governed by the laws of the Republic of Ireland. However, where a dispute arises regarding the processing of UK Personal Data under this DPA, such dispute shall be governed by the laws of England and Wales and shall be brought in London, England.

10.4. This DPA constitutes the complete and exclusive understanding and agreement of the Parties with respect to the subject matter herein. Any waiver, modification or amendment of any provisions of this DPA will be effective only if in writing and signed by the Parties hereto.

10.5. If and to the extent that any provision of this DPA is held to be illegal, void, or unenforceable in any jurisdiction, such provision shall be given no effect in that jurisdiction, but without invalidating any of the remaining provisions of this DPA.

IN WITNESS WHEREOF, each party has caused this DPA to be executed by its duly authorised representatives and made effective as of the signature date below.

Stack Exchange Inc	**[Customer Company Name]**
By: Matthew Gallatin	By:
Name: Matthew Gallatin	Name:
Title: CFO	Title:
Date: 1/10/2023	Date:

APPENDIX 1 – SPECIFIC JURISDICTION PROVISIONS

SCHEDULE 1 - EU CLAUSES

1. As applicable, for the purposes of this Schedule 1, the EU Clauses (Module II), available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN, shall be incorporated by reference to this Schedule and the DPA and shall be considered an integral part thereof, and the Parties' signatures in the DPA shall be construed as the Parties' signature to the EU Clauses. In the event of an inconsistency between the DPA and the EU Clauses, the latter will prevail.

2. For the purposes of the EU Clauses, the following shall apply:

   - Customer shall be the data exporter and Stack shall be the data importer. Each party agrees to be bound by and comply with its obligations in its role as exporter and importer respectively as set out in the EU Clauses.

   - Clause 7 (Docking clause) shall be deemed as included.

   - Clause 9 (Use of sub-processors): OPTION 2 – GENERAL WRITTEN AUTHORISATION shall apply. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance.

   - Clause 11 (Redress): optional clause (optional redress mechanism before an independent dispute resolution body) shall be deemed as not included.

   - Clause 13 (a) (Supervision):

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

     - *Where Customer is not established in an EU Member State but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:* The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

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

   - Clause 17 (Governing law):

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

- Clause 18 (b) (Choice of forum and jurisdiction): The Parties agree that any dispute between them arising from the EU Clauses shall be resolved by the courts of the Republic of Ireland.

3. Any provision in the EU Clauses relating to liability of the parties with respect to each other shall be subject to the limitations and exclusions of the Agreement.
4. Any provision in the EU Clauses relating to the right to audit shall be interpreted in accordance with Clause 6.4 of the DPA and the Agreement.

SCHEDULE 2 - UK DATA TRANSFERS

For the purposes of the UK Approved Addendum,

1. the information required for Table 1 is contained in Appendix 2 of this DPA and the start date shall be deemed dated the same date as the EU Clauses;
2. in relation to Table 2, the version of the EU Clauses to which the UK Approved Addendum applies is Module Two for Controller to Processor;
3. in relation to Table 3, the list of parties and description of the transfer are as set out in Appendix 2 of this DPA, Stack's technical and organisational measures are set in Appendix 4 of this DPA, and the list of Stack's sub-processors shall be provided pursuant to Appendix 3 of this DPA; and
4. in relation to Table 4, neither party will be entitled to terminate the UK Approved Addendum in accordance with clause 19 of the UK Mandatory Clauses, and Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "data exporter".

SCHEDULE 3 - EFFECTIVE DATES OF STATE PRIVACY LAWS

The Parties agree that the provisions of the respective State Privacy Law shall take effect on the below date and shall be of no force or effect prior to that date:

1. CPRA on January 1, 2023
2. VCDPA on January 1, 2023
3. CPA on July 1, 2023
4. PDPOM on July 1, 2023
5. UCPA on December 31, 2023

APPENDIX 2

Data Processing Details

A. LIST OF PARTIES

Data exporter(s):

Name: [_____]

Address: [_____]

Contact person's name, position and contact details: [_____]

Activities relevant to the data transferred under these Clauses:

- The data exporter has asked the data importer to process personal data as necessary to provide data importer's services and products as agreed to under the Agreement between the Parties.

Signature and date: please refer to signature and date in the DPA.

Role (controller/processor): Controller

Data importer(s):

Name: Stack Exchange Inc.

Address: 110 William Street, 28th Floor, New York, NY 10038

Contact person's name, position and contact details:
- Privacy Counsel, privacy@stackoverflow.com

Activities relevant to the data transferred under these Clauses:
- The data importer will process personal data as necessary to provide the services and products as detailed on the applicable ordering document as agreed to under the Agreement between the Parties.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Subject Matter of the processing	Stack's provision of the Services to Customer pursuant to the Agreement.
Nature and purpose of processing	Stack's provision of the Services to Customer pursuant to the Agreement, including security and integrity, repair functionality, and performing Services on behalf of Customer.
Types / Categories of Personal Data	▪ Full Name ▪ Business Email, Business Username; Business IP Address ▪ Business Password Hash, Business Browser ID

Sensitive Personal Data and applied restrictions	None
Categories of Data Subjects or Consumers	Authorised Users at the Discretion of Customer, which may include: ▪ Employees of Customer ▪ Consultants of Customer ▪ Agents or Third Parties
Frequency of Transfer	Continuous basis in the providing of Services
Duration of processing	For the duration of the Agreement, or until the processing is no longer necessary for the purposes.
Transfers to (Sub-) processors	See Appendix 3

C. COMPETENT SUPERVISORY AUTHORITY

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

- Data Protection Authority of Ireland

APPENDIX 3

LIST OF APPROVED SUB-PROCESSORS

In accordance with the applicable section(s) of this DPA, data importer may use the sub-processors currently listed at https://stackoverflow.com/legal/gdpr/subprocessors, and as may be updated from time to time in accordance with the applicable terms of this DPA.

APPENDIX 4

TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

1. **Scope**
   a. This Appendix 4 applies to all Personal Data collected, generated or otherwise processed by Stack in the course of providing its Services.

2. **People and Operations**
   a. All Stack staff, including sub-contractors, that have access to its data processing systems or the Customer Group Company's data processing systems authenticate with a unique username and strong password.
   b. Stack shall have appropriate data protection and data security training in place for all of its staff involved in the processing of Personal Data and carry out such training at reasonable intervals.
   c. Stack shall require its staff to commit themselves contractually to obligations of confidentiality or be under an appropriate statutory obligation of confidentiality.
   d. Stack shall monitor its staff's access to Personal 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.

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

4. **Accreditations**
   a. Where Stack processes Personal Data that falls within the scope of the Payment Card Industry Data Security Standard (PCI DSS), Stack 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 Stack's self-service avenues.

5. **Physical security**
   a. Stack 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 Stack.

6. **Application Development**
   a. Stack provides software as a solution. In developing the software provided as the Service, Stack shall adopt secure coding practices that address at a minimum the Open Web Application Security Project (OWASP) top ten vulnerabilities.
   b. Stack will have documented policies and/or processes identifying where security checks, and the associated methods, are applied throughout the development lifecycle.
   c. Stack 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 (if the Service is hosted on Stack's third-party provider system). The logs will be retained as per Stack's retention policies.
   d. At least annually, Stack shall, at its own cost, undertake an independent application and/or infrastructure penetration testing of Services provided to the Customer Group Company using an internationally recognised methodology such as OWASP. Evidence of independent testing can be provided, if requested in writing.

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

7. **Infrastructure**
   a. Stack shall manage changes to Services provided in accordance with the Agreement and shall not decrease the overall effectiveness of security controls.
   b. All infrastructure used in provision of the Services and/or hosting of Personal Data will be subject to frequent vulnerability assessment and remediation cycles.

8. **Data handling**
   a. Stack shall segregate Personal Data from any of Stack'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, Stack will have real time monitoring and alerting to the system administrator for changes to these parameters.
   b. Stack will use widely recognised encryption protocols and techniques to protect Personal Data, during: (i) transit (data input); (ii) exchange with contracted third parties (data output); and (iii) for storage (if the Service is hosted on Stack's third-party provider system). Where appropriate, Stack will pseudonymise the Personal Data as soon as possible. For the sake of clarity, pseudonymising means processing the Personal Data in a way that it can no longer be attributed to a specific data subject without the use of additional information.
   c. Stack shall undertake appropriate measures to prohibit Personal Data from being transferred or copied onto unencrypted portable devices, such as USB sticks or flash drives.

9. **Data Deletion**
   a. Stack shall undertake standard industry practices when deleting Personal Data. For the sake of clarification, 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 receipt of a written request for the deletion of Personal Data, Stack will provide written confirmation that deletion has been completed, including the physical deletion and method used, as applicable.