DATA PROCESSING ADDENDUM FOR STACK OVERFLOW ENTERPRISE

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 23; and
   (c) Complete the information in the signature box; and
   (d) Sign on Pages 19 and 27.

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.

Exhibit B

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 DPA to address the compliance obligations imposed upon the Controller pursuant to the Data Protection Laws.

NOW IT IS HEREBY AGREED as follows:

1. DEFINITIONS

1.1. In this DPA, 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 Laws.

"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 DPA.
"Controller Data"	means the Personal Data processed under this DPA 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 Laws"	means all applicable laws (Applicable Laws) relating to data protection and privacy including (without limitation) the UK Data Protection Laws, 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.
"EU GDPR"	means the General Data Protection Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data.
"EU Standard Contractual Clauses"	means in respect of Transfers under the EU GDPR: the agreement executed by and between Customer and Stack Exchange, Inc. and attached hereto as Exhibit C, pursuant to the European Commission's decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries which do not have an adequate level of data protection, pursuant to Regulation (EU) 2016/679
"the GDPR"	means the EU GDPR and the UK GDPR.

"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.
"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 CCPA 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.
"Services"	shall mean the Services as defined in the Principal Agreement.
"Supervisory Authority"	shall mean the relevant supervisory authority with responsibility for privacy or data protection matters in the jurisdiction of the Controller.
"Transfer"	bears the same meaning as the word 'transfer' in Article 44 of the GDPR (and related terms such as **Transfers**, **Transferred** and **Transferring** have corresponding meanings.
"UK Data Protection Laws	means the United Kingdom General Data Protection Regulation, Regulation (EU) 2016/679, as it forms part of domestic law in the United Kingdom by virtue of S.3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified from time to time; the UK Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 (as amended) and any amendments from time to time.
"**UK GDPR**"	means the United Kingdom General Data Protection Regulation, Regulation (EU) 2016/679, as it forms part of domestic law in the United Kingdom by virtue of S.3 of the European Union (Withdrawal) Act 2018 as amended or modified from time to time.
"**UK Standard Contractual Clauses**"	means in respect of Transfers under the UK GDPR: the agreement executed by and between Customer and Stack Exchange, Inc. and attached hereto as Exhibit D, pursuant to the European Commission's decision (C (2010)593) of 5 February 2010 for the Transfer of personal data from controllers established in the EEA to processors established in third countries which do not ensure an adequate level of data protection.

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 DPA.

3. DURATION

3.1. This DPA 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 DPA 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 DPA 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 Laws in respect of any personal data it processes under or in relation to this DPA.

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 DPA 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 shall at all times:

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 DPA 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 relating to Controller Data as may be reasonably required to enable the Controller to assess whether or not the Processor is complying with the provisions of this DPA 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 DPA), 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 Information 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 DPA; and (c) Controller agrees to the use of the Sub-processors at https://stackoverflow.com/legal/gdpr/subprocessors the list of which is also attached at Schedule 3 of this DPA and Annex III of the EU SCCs ("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 DPA, 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 and D, then Controller agrees that Processor may appoint Sub-processors in accordance the EU Standard Contractual Clauses and the UK Standard Contractual Clauses by complying with this Section 4.5 and Section 4.6 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 DPA 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 DPA 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 DPA. 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. INTERNATIONAL 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 Laws, only in compliance with the Standard Contractual Clauses attached hereto as Exhibit C for transfers outside the EEA and Exhibit D, for Transfers outside the UK, 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 The Controller acknowledges that due to the nature of cloud services, Controller Data may be Transferred to other geographical locations in connection with use of the Services further to access and/or computerised instructions initiated by Authorized Users. The Controller acknowledges that the Processor does not control such processing and the Controller shall ensure that Authorized Users (and all others acting on its behalf) only initiate the Transfer of Controller Data to other geographical locations if Lawful Safeguards are in place and that such Transfer is in compliance with all Applicable Laws.

6.4 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 DPA 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 DPA. 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 DPA 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 DPA, 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 DPA 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 DPA, 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 DPA 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 DPA and to otherwise fulfil the provisions of this DPA in accordance with its terms.

10. COUNTERPARTS

This DPA 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. MISCELLANEOUS

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

11.2. This DPA 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.

11.3. The provisions of this DPA 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 DPA shall remain in full force and effect.

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

11.5. Any notice required under this DPA 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	Matthew Gallatin	**Signature**	
Name	Matthew Gallatin	**Name**	
		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 DPA.

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 DPA.

Schedule 3

Enterprise: List of Sub-Processors

Name of Sub-Processor (correct entity) and address	Web Address	Contact Details (correct entity details)	What information are they Processing?
Amplitude, Inc. 631 Howard St. Floor 5 San Francisco, CA 94105 USA	www.amplitude.com	contact@amplitude.com	Customer Usage Reports
Catalyst Software Corporation 235 23rd Street, Floor 8 New York, NY 10011 USA	www.catalyst.io	support@catalyst.io	Customer account information
Freshworks, Inc. 2950 S. Delaware Street, Suite 201 San Mateo, CA 94403 USA	www.freshworks.com	support@freshworks.com	Customer Admin user login for product documentation
Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA	www.microsoft.com	support@microsoft.com	Cloud Hosting
Twilio, Inc. 375 Beale St #300 San Francisco, CA USA 94105	www.twilio.com	contact@twilio.com	User emails - Email delivery (sendgrid) (optional service for hosted customers)
Zuora, Inc. 101 Redwood Shores Pkwy, Redwood City, CA 94065 USA	www.zuora.com	support@zuora.com	Account billing information

EXHIBIT C

FOR EU GDPR TRANSFERS

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organizational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) **GENERAL WRITTEN AUTHORISATION:** The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

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

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

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

OR

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

OR

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

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([5]);

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

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

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

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

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do

so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

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

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

15.2 Review of legality and data minimization

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

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

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Republic or Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Republic of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. **LIST OF PARTIES**

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1.	Name: [.....] Address: [.....] Contact person's name, position and contact details: [.....] Activities relevant to the data transferred under these Clauses: 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. Signature and date: [.....] Role (controller/processor): Controller
2.	[.....]

Data importer(s):

1.	Name: . **Stack Exchange, Inc:** Address: .110 William Street, 28th Floor, New York, NY 10038 Contact person's name, position and contact details: privacy@stackoverflow.com Activities relevant to the data transferred under these Clauses: 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. Matthew Gallatin 2/24/2022 Signature and date: [.....] Role (controller/processor): Processor

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred

- Employees
- Consultants
- Authorized Third Parties

Categories of personal data transferred

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

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

NONE SHOULD BE PROVIDED

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

Continuous basis in the providing of Services

Nature of the 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.

Purpose(s) of the data transfer and further 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.*

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

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

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

Same as above

C. **COMPETENT SUPERVISORY AUTHORITY**

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

Data Protection Authority (Ireland)

ANNEX II

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

See Schedule 1 **Information Security**

ANNEX III
LIST OF SUB-PROCESSORS

The controller has authorized the use of the following sub-processors:

Name of Sub-Processor (correct entity) and address	Web Address	Contact Details (correct entity details)	What information are they Processing?
Amplitude, Inc. 631 Howard St. Floor 5 San Francisco, CA 94105 USA	www.amplitude.com	contact@amplitude.com	Customer Usage Reports
Catalyst Software Corporation 235 23rd Street, Floor 8 New York, NY 10011 USA	www.catalyst.io	support@catalyst.io	Customer account information
Freshworks, Inc. 2950 S. Delaware Street, Suite 201 San Mateo, CA 94403 USA	www.freshworks.com	support@freshworks.com	Customer Admin user login for product documentation
Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA	www.microsoft.com	support@microsoft.com	Cloud Hosting
Twilio, Inc. 375 Beale St #300 San Francisco, CA USA 94105	www.twilio.com	contact@twilio.com	User emails - Email delivery (sendgrid) (optional service for hosted customers)
Zuora, Inc. 101 Redwood Shores Pkwy, Redwood City, CA 94065 USA	www.zuora.com	support@zuora.com	Account billing information

EXHIBIT D

UK GDPR Transfers

Standard Contractual Clauses

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: _____

Address: _____

Tel: _____

Fax: _____

E-mail: _____

Other information needed to identify the organization: _____

(the **data exporter**)

And

Name of the data importing organization: **Stack Exchange Inc.**

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

Tel: 212-232-8294; fax: 917-979-5453 e-mail: Privacy@stackoverflow.com

Other information needed to identify the organization

(**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 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.

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

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), Clause6, 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 sub-processor 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 sub-processor 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.

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, 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 sub-processor 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 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 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 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

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 sub-processor 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 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.

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 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

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.

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 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.

3. 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 2. 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, namely England and Wales.

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

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 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.

2. 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 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 sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing 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, namely England and Wales.

4. 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

1. 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.

2. 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 1.

The parties intend that these Clauses should only become effective if Art 44 of the General Data Protection Regulation (the "GDPR") applies to a transfer of personal data from the EEA to the UK, because the UK has left the European Union, and the transfer is not permitted under Art 45.

On that basis, the Clauses will become effective on:

(i) the first date Article 44 GDPR applies to a transfer of personal data from the EEA to the UK, and that transfer is not permitted under Article 45 GDPR; or

(ii) the date of the Standard Contractual Clauses, if later.

In this clause, "a transfer of personal data" has the same meaning as in Article 44 of the GDPR.

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

Name (written out in full):

Position

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

Other information necessary in order for the contract to be binding (if any): N/A

2/24/2022	Signature: Matthew Gallatin

On behalf of the data exporter:

Name (written out in full): _____

Position: _____

Address: _____

Other information necessary in order for the contract to be binding (if any): _____

	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 is (please specify briefly your activities relevant to the transfer):

Data Exporter has asked Stack to 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.

The data exporter's business or organisation type is:

IT, digital, technology and telecoms

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

Standard business activities, which apply to most businesses and organisations

IT, digital, technology or telecom services, including use of technology products or services, telecoms and network services, digital services, hosting, cloud and support services or software

Other activities (please provide details):

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

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.

Data subjects

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

- Employees
- Consultants
- Authorized Third Parties

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

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

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

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify): NONE

Processing operations

_ _

The personal data transferred will be subject to the following basic processing activities (please specify):

- Receiving data, including collection, accessing, retrieval, recording, and data entry
- Holding data, including storage, organisation, and structuring
- Protecting data, including restricting, encrypting, and security testing
- Sharing data, including disclosure, dissemination, allowing access or otherwise making available
- Returning data to the data exporter or data subject
- Erasing data, including destruction and deletion

☐ Other (please provide details of other types of processing):

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) (or document/legislation attached):

Schedule 1 of the DPA

Option 1: Please refer to the description of the importer's security measures set forth in Schedule 1 of the DPA